PLN-(I)SN07-004

Succession

(I)SN07 Release Change Reference Manual

(I)SN07 Standard 01.02 December 2004

NORTEL NETWORKS™

Succession

(I)SN07 Release Change Reference Manual

DMS on Succession

Publication number: PLN-SN07-004
Product release: (I)SN07
Document release: Standard 01.02
Date: December 2004

Copyright © 2004 Nortel Networks

All Rights Reserved.

Printed in the United States of America.

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Information subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

NORTEL NETWORKS, DMS, and TOPS are trademarks of Nortel Networks Corporation. Microsoft Windows is a trademark of Microsoft Corporation.

Limitation of liability: Neither Nortel Networks nor any of its agents or suppliers shall be liable for any indirect, consequential, incidental, or exemplary damages, or economic losses (including damages for loss of business profits, business interruption, loss of business information and the like), arising from the use, inability to use, or performance of the software or this license agreement, even if Nortel Networks or such agent or supplier has been advised of the possibility of such damages and/or losses, and whether any such damage and/or loss arises out of contract (including fundamental breach), tort (including negligence), or otherwise. The entire liability of Nortel Networks for any claim or loss, damage or expense from any cause whatsoever, whether arising out of contract (including fundamental breach), tort (including negligence), or otherwise shall in no event exceed the price paid by you under this license agreement. In some jurisdictions you may have additional rights, in which case some of the above may not apply to you.

Publication history

August 2004

Version 01.01 Preliminary release for SN07.

Table of Contents

RelDoc Introduction 13

SN07 Feature Subset Cross Reference Tables: North American Features 15
Functional Descriptions List 33
Functional Description (FN): A00001319 43
Functional Description (FN): A00001649. 49
Functional Description (FN): A00001650 65
Functional Description (FN): A00001742 68
Functional Description (FN): A00001743 72
Functional Description (FN): A00001847 91
Functional Description (FN): A00001888 112
Functional Description (FN): A00001890 187
Functional Description (FN): A00001893 and A00001894 188
Functional Description (FN): A00001895 194
Functional description (FN): A00001898 203
Functional description (FN): A00001935 206
Functional Description (FN): A00001990. 208
Functional description (FN): A00002008 214
Functional Description (FN): A00002009 224
Functional Description (FN): A00002011. 233
Functional Description (FN): A00002012. 236
Functional Description (FN): A00002013. 240
Functional Description (FN): A00002016 243
Functional Description (FN): A00002020 253
Functional Description (FN): A00002047 257
Functional Description (FN): A00002133 266
Functional Description (FN): A00002137. 287
Functional Description (FN): A00002146 289
Functional description (FN): A00002155 293
Functional description (FN): A00002164 297
Functional Description (FN): A00002186 305
Functional Description (FN): A00002196 308
Functional Description (FN): A00002251 323
Functional Description (FN): A00002281 326
Functional Description (FN): A00002340 328
Functional Description (FN): A00002380 333
Functional Description (FN): A00002431 339
Functional Description (FN): A00002432 345

Functional Description (FN): A00002433 351
Functional Description (FN): A00002499 358
Functional Description (FN): A00002505. 365
Functional Description (FN): A00002510 372
Functional Description (FN): A00002538. 375
Functional Description (FN): A00002549 377
Functional Description (FN): A00002555 380
Functional Description (FN): A00002558 383
Functional Description (FN): A00002585 388
Functional Description (FN): A00002607 407
Functional description (FN): A00002739 412
Functional Description (FN): A00002740 420
Design Description Excerpts: A00002741 431
Functional Description (FN): A00002744 435
Functional Description (FN): A00002746 438
Functional Description (FN): A00002756 440
Functional Description (FN): A00002757 507
Functional Description (FN): A00002765 510
Functional Description (FN): A00002760 521
Functional Description (FN): A00002765. 538
Functional Description (FN): A00002766. 549
Functional Description (FN): A00002822. 552
Functional Description (FN): A00002823. 571
Functional Description (FN): A00002858. 574
Functional Description (FN): A00002900. 584
Functional Description (FN): A00002901. 595
Functional Description (FN): A00002960. 611
Functional Description (FN): A00002970. 620
Functional Description (FN): A00002966. 628
Functional Description (FN): A00002979. 631
Functional Description (FN): A00003073. 634
Functional Description (FN): A00003154. 639
Functional Description (FN): A00003154. 641
Functional Description (FN): A00003233. 653
Functional Description (FN): A00003273. 656
Functional Description (FN): A00003277. 657
Functional Description (FN): A00003279. 659
Functional description (FN): A00003280 661

Functional Description (FN): A00003371 669
Functional Description (FN): A00003452 671
Functional Description (FN): A00003454 673
Functional Description (FN): A00003459 682
Functional Description (FN): A00003485 692
Functional Description (FN): A00003486 696
Functional Description (FN): A00003487 701
Functional Description (FN): A00003489 759
Functional Description (FN): A00003490 761
Functional Description (FN): A00003495 768
Functional Description (FN): A00003496 770
Functional Description (FN): A00003506 772
Functional Description (FN): A00003531 797
Functional Description (FN): A00003560 812
Functional Description (FN): A00003562 825
Functional Description (FN): A00003567 838
Functional Description (FN): A00003568 841
Functional Description (FN) A00003571 905
Functional Description (FN) A00003576 908
Functional Description (FN) A00003591 910
Functional Description (FN): A00003604 925
Functional Description (FN): A00003613 935
Functional Description (FN): A00003615 945
Functional Description (FN): A00003617 947
Functional description (FN): A00003618 964
Functional Description (FN): A00003630 973
Functional Description (FN): A00003649 994
Functional Description (FN): A00003650 998
Functional Description (FN): A00003651 1001
Functional Description (FN): A00003662 1005
Functional Description (FN): A00003667 1008
Functional Description (FN): A00003669 1010
Functional Description (FN): A00003672 1013
Functional Description (FN): A00003687 1015
Functional Description (FN): A00003693 1046
Functional Description (FN): A00003698 1051
Functional Description (FN): A00003704 1056
Functional Description (FN): A00003711 1067

Functional Description (FN): A00003717 1257
Functional Description (FN): A00003718-3719 1273
Functional Description (FN): A00003720. 1293
Functional Description (FN): A00003767 1295
Functional Description (FN): A00003767 1299
Functional Description (FN): A00003773. 1303
Functional Description (FN): A00003789. 1308
Functional Description (FN): A00003905 1316
Functional Description (FN): A00003923 1318
Functional Description (FN): A00003933 1329
Functional Description (FN): A00003947. 1453
Functional Description (FN): A00003948. 1469
Functional Description (FN): A00003951. 1528
Functional description (FN): A00003952 1552
Functional Description (FN): A00003971. 1555
Functional Description (FN): A00003995. 1558
Functional Description (FN): A00004005. 1563
Functional Description (FN): A00004020. 1606
Functional Description (FN): A00004036. 1615
Functional Description (FN): A00004037. 1663
Functional Description (FN): A00004045. 1668
Functional description (FN): A00004046 1677
Functional description (FN): A00004096 1692
Functional Description (FN): A00004109. 1710
Functional description (FN): A00004126 1713
Functional description (FN): A00004131 1716
Functional description (FN): A00004137 1721
Functional Description (FN): A00004260. 1735
Functional Description (FN): A00004271. 1740
Functional Description (FN): A00004391. 1744
Functional Description (FN): A00004414. 1753
Functional Description (FN): A00004422. 1756
Functional Description (FN): A00004430. 1768
Functional Description (FN): A00004449. 1779
Functional Description (FN): A00004500. 1781
Functional Description (FN): A00004554. 1796
Functional description (FN): A00004568 1800
Functional description (FN): A00004713 1807

Functional description (FN): A00004772 1809
Functional Description (FN): A00004859. 1813
Functional Description (FN): A00004860. 1824
Design Description excerpts: A00004868 1829
Functional Description (FN): A00004872 1832
Functional Description (FN): A00004873 1838
Functional description (FN): A00004922 1853
Functional Description (FN): A00004923 1862
Functional Description (FN): A00005007. 1864
Functional Description (FN): A00005016. 1870
Functional Description (FN): A00005073. 1873
Functional Description (FN): A00005074. 1877
Functional Description (FN): A00005089 1882
Functional Description (FN): A00005123 1885
Functional Description (FN): A00005124 1888
Functional Description (FN): A00005160 1890
Functional Description (FN): A00005190 1897
Functional Description (FN): A00005192 1899
Functional description (FN): A00005193 1904
Functional description (FN): A00005268 1905
Functional Description (FN): A00005317. 1910
Functional Description (FN): A00005322. 1911
Functional Description (FN): A00005337. 1915
Functional Description (FN): A00005363. 1921
Functional Description (FN): A00005375. 1928
Functional Description (FN): A00005391. 1929
Functional Description (FN): A00005485. 1931
Functional Description (FN): A00005538. 1932
Functional Description (FN): A00005734. 1937
Functional Description (FN): A00005758. 1943
Functional Description (FN): A00005986. 1945
Functional Description (FN): A00006032. 1951
Functional Description (FN): A00006483. 1954
Design Description excerpts: A00006495 1956
Functional Description (FN): A00006496. 1959
Functional Description (FN): A00006639. 1963
Functional Description (FN): A00006693. 1968
Functional Description (FN): A00006741. 1973

Functional Description (FN): A00007063 1995
Functional Description (FN): A00007211 2002
CR: Q00681924 2004

Fault Management List 2005
Fault Management (FM): A00001893 2009
Fault Management (FM): A00002012 2013
Fault Management (FM): A00002013 2023
Fault Management (FM): A00002020 2027
Fault Management (FM): A00002146 2031
Fault Management (FM): A00002380 2035
Fault Management (FM): A00002433 2041
Fault Management (FM): A00002499 2048
Fault Management (FM): A00002510 2053
Fault Management (FM): A00002549 2055
Fault Management (FM): A00002607 2059
Fault Management (FM): A00002757 2060
Fault Management (FM): A00002823 2069
Fault Management (FM): A00002858 2073
Fault Management (FM): A00002970 2079
Fault Management (FM): A00003371 2081
Fault Management (FM): A00003487 2091
Fault Management (FM): A00003567 2101
Fault Management (FM): A00003591 2107
Fault Management (FM): A00003650 2113
Fault Management (FM): A00003667 2121
Fault Management (FM): A00003687 2127
Fault Management (FM): A00003767 2133
Fault Management (FM): A00003933 2137
Fault Management (FM): A00003947 2160
Fault Management (FM): A00003971 2163
Fault Management (FM): A00004045 2191
Fault Management (FM): A00004045 2226
Fault Management (FM): A00004260 2229
Fault Management (FM): A00004271 2235
Fault Management (FM): A00004391 2237
Fault Management (FM): A00004430 2241
Fault Management (FM): A00005016 2248

Fault Management (FM): A00005073 2257
Fault Management (FM): A00005074 2263
Fault Management (FM): A00005160 2265
Fault Management (FM): A00005192 2269
Fault Management (FM): A00005322 2273
Fault Management (FM): A00005363. 2299
Fault Management (FM): A00005375. 2301

Configuration Management List 2323
Configuration (CN): A00001847 2327
Configuration (CN): A00001890 2336
Configuration (CN): A00001893 2365
Configuration (CN): A00001898 2390
Configuration (CN): A00002009 2413
Configuration (CN): A00002012 2420
Configuration (CN): A00002013 2454
Configuration (CN): A00002020 2459
Configuration (CN): A00002146 2471
Configuration (CN): A00002196 2482
Configuration (CN): A00002380 2497
Configuration (CN): A00002431 2524
Configuration (CN): A00002433 2541
Configuration (CN): A00002510 2555
Configuration (CN): A00002555 2558
Configuration (CN): A00002558 2565
Configuration (CN): A00002585 2569
Configuration (CN): A00002607 2579
Configuration (CN): A00002858 2590
Configuration (CN): A00002858 2606
Configuration (CN): A00002858 2613
Configuration (CN): A00002900 2619
Configuration (CN): A00002901. 2623
Configuration (CN): A00002960 2628
Configuration (CN): A00002970 2632
Configuration (CN): A00002979 2641
Configuration (CN): A00003073 2649
Configuration (CN): A00003074 2659
Configuration (CN): A00003454 2665

Configuration (CN): A00003487. 2674
Configuration (CN): A00003486. 2752
Configuration (CN): A00003487. 2768
Configuration (CN): A00003489 2845
Configuration (CN): A00003490 2854
Configuration (CN): A00003506 2907
Configuration (CN): A00003531 2932
Configuration (CN): A00003567. 2954
Configuration (CN): A00003571. 2965
Configuration (CN): A00003591. 2970
Configuration (CN): A00003615 2973
Configuration (CN): A00003630. 2977
Configuration (CN): A00003667. 3002
Configuration (CN): A00003669. 3005
Configuration (CN): A00003672 3016
Configuration (CN): A00003687 3019
Configuration (CN): A00003767 3048
Configuration (CN): A00003773. 3062
Configuration (CN): A00003789 3065
Configuration (CN): A00003905 3072
Configuration (CN): A00003923. 3089
Configuration (CN): A00003933 3097
Configuration (CN): A00003947 3114
Configuration (CN): A00003948. 3127
Configuration (CN): A00003971. 3205
Configuration (CN): A00003995. 3209
Configuration (CN): A00004005. 3238
Configuration (CN): A00004036. 3252
Configuration (CN): A00004045. 3254
Configuration (CN): A00004046. 3258
Configuration (CN): A00004126. 3260
Configuration (CN): A00004131. 3264
Configuration (CN): A00004137. 3267
Configuration (CN): A00004260. 3270
Configuration (CN): A00004271. 3295
Configuration (CN): A00004391. 3297
Configuration (CN): A00004414. 3320
Configuration (CN): A00004500. 3322

Configuration (CN): A00004872 3332
Configuration (CN): A00005007 3336
Configuration (CN): A00005016 3338
Configuration (CN): A00005073 3344
Configuration (CN): A00005074. 3349
Configuration (CN): A00005160. 3351
Configuration (CN): A00005190 3375
Configuration (CN): A00005193 3382
Configuration (CN): A00005363 3384
Configuration (CN): A00005734 3390
Configuration (CN): A00006483 3392
Configuration (CN): A00006693. 3397

Performance Management List. 3419
Performance (PF): A00002012 3421
Performance (PF): A00002340 3429
Performance (PF): A00002538 3438
Performance (PF): A00002766 3441
Performance (PF): A00003487 3444
Performance (PF): A00003531 3529
Performance (PF): A00003687 3535
Performance (PF): A00003767 3561
Performance (PF): A00003773 3565
Performance (PF): A00004036 3569
Performance (PF): A00004271 3591
Performance (PF): A00004430 3596
Performance (PF): A00004500 3607
Performance (PF): A00005160 3610
Performance (PF): A00005160 3625

Accounting List. 3629
Accounting: A00004036 3631
Accounting: A00004137 3638
Accounting: A00005363 3641

RelDoc Introduction

DMS* - FAMILY SOFTWARE

PRODUCT COMPUTING MODULE LOAD RELEASE DOCUMENT

(PCL) Release Document

The DMS-250 Family Software release document is supplied for each Software Stream. This release document provides software feature information pertinent to the new software load.

A status of DRAFT or PRELIMINARY means the final feature content of the software release has not been finalized and features may be added or deleted without notice. A status of STANDARD indicates that the feature content of the software release is firm.

The release document consists of the following sections:

FEATURE CONTENT
This section provides information concerning DMS-250 Family System features associated with software releases. Each office configuration is customized to meet Telco/Carrier requirements. The following subsections include information necessary to determine that system software changes have occurred since the last software release.

> ***Note:*** Only features NEW or CHANGED in the release(s) covered by the document are included

CROSS REFERENCE TABLES
This section contains tables to make it more efficient to find information. A description of the tables precedes them.

The following sections provide information necessary to support changes applicable to the new software release. Only features that impact a section category are included; therefore, some sections may be left out of this NTP because none of the features for this release had an impact to that section.

- Functional Descriptions (FN) -summarizes the functions of the feature

- Fault Management (FM)
  - — Logs (LG) -indicates major additions/changes to the LOGs
- Configuration (CN)
  - — Data Schema (DS) -indicates major additions/changes to the Data Schema table
  - — Service Orders (SO) -indicates major additions/changes to the Service Orders
  - — User Interface (UI) - indicates major additions/changes to the User Interface
- Accounting (ACC)
  - — Automatic Message Accounting (AM) -indicates major additions/ changes to the AMA
- Performance (PF)
  - — Operational Measurements (OM) -indicates major additions/changes to the OM groups

How To Use the Feature Content Section

The feature content software section contains the documentation for the features new or changed in the release. There are tables included to help in the reading of the feature content section.

The items in the tables are feature numbers and feature functional groups. Features are designed by NT against an NT featid.

A functional group is made up of several features.

- Table1: Feature to Functional Group Cross Reference

  These tables list all features new to the release that may be included in the release document. The functional group is indicated along with the Nortel Technologies featid and its title against which the documentation has been written.

- Table 2: Functional Groups to Feature Impacts Cross Reference

  These tables list all documentation listed in the feature content section. As stated above, the documentation is sorted first by feature functional group, and then by featid within the functional group. This table indicates which sections (for example, FM, CN, PF, or ACC) are included in the release document.

SN07 Feature Subset Cross Reference Tables: North American Features

Feature to Functional Group Cross Reference

Table 1 shows feature IDs, feature titles, and the corresponding functional group (under Stream and release).

For details on specific features, refer to the FN sections starting on page 43.

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00001319.AA10	Device activity & RMID-PWID restoration tool & Panther enhancements	Core20
A00001649	SBA Robustness: End-to-end Integrity	SDM20
A00001650.AA09	SBA Patch Size Reduction	SDM20
A00001742.AA05	OMDD Capacity Enhancements	SDM20
A00001743.AA04	Syslog Consolidation for Succession	SDM20
A00001847.AA31	ABI Expansion Datafill	Core20
A00001888.AC02	CS2000 Line Test for MG9000 Lines	Core20
A00001890.AA31	Refer to A00001888	Core20
A00001893	MG9K Imaging (includes A00001894)	PNM07
A00001895.AC09	H323 Base Application	Core20
A00001935	Provisioning Support for Centrex-IP Nodes and Lines	PNM07
A00001990.AA02	CAIN via CICROUTE PEP Sourcing	Core20, Core20
A00002008.AA08	SBA:CBM Introduction	Core20, SDM20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00002009.AA04	Enhance Display on PSET	Core20
A00002011.AA08	DMS-100: Virtual Office Worker	Core20
A00002012.AA13	XA-Core CMIC/RTIF HIOP Maintenance Software	Core20
A00002013.AA06	Intelligent Network T1 Timer Expiry Message Suppression	Core20
A00002016.AA02	AINDENY Enhancements	Core20
A00002020.AB10	ESA Translation Download	Core20
A00002047.AA13	Double Density Spectrum Backplane	Core20
A00002133.AA05	CBM HA Installation, Patching and SW Delivery	SDM20
A00002137.AA01	DS512 Link Mtc Robustness - CM	Core20
A00002146.AA09	MAPCI ABI Link Test & Legacy Comparison	
A00002155.AA11	SSH Core File Transfer (SCFT) for CBM and SDM	SDM20
A00002164.AA10	Application Manager for High Availability (HA)	SDM20
A00002186.AA08	IOM DDU Capacity Enhancement	Core20
A00002196.AA15	Enhanced Do Not Disturb	Core20
A00002251.AA13	192M Shared Memory Extension	Core20
A00002281.AA02	Table AMAPRT Expansion	Core20
A00002340.AA07	Add Extension Registers for Billing OM's	Core20
A00002380.AA21	MG9K ABI ESA	Core20, MG9K07, XPM20
A00002431.AA16	LX82BA Capacity Delivery	SPM20, Core20
A00002432.AA24	Enhanced Spectrum Overload Operational Measurements (OMs) and Logs	SPM20, Core20
A00002433.AA08	XA-Core Baseline Control	XAC21
A00002499.AA05	Store Audit for XA-Core	XAC21
A00002505	Universal Signaling Point Interface Client - GUI	USP09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00002510.AA11	LANCOMM IP over IRM	XAC21
A00002538.AA19	Performance Measurements Tools	Core20, XAC20
A00002549.AA04	CSP20 Callp Robustness	XAC20
A00002555.AA03	SERVORD Manipulation of the GND Option	Core20
A00002558.AA07	LDI display for Class phone	Core20
A00002585	TMM Support For PTS Trunk, POST by Carrier	PNM07
A00002607.AA11	ABI XPM SITE and MG9K Location support	Core20
A00002739.AA15	Virtual Call Admissions Control (VCAC) on Communication Server 2000	GWC10, Core20
A00002740.AA03	International Directory Assistance Call Completion (IDACC)	TOPS20
A00002741	Supernode Billing Application Base Real Time Billing Robustness	SDM20
A00002744.AA05	SBA: Automatic Recovery File Closure	SDM20
A00002746.AB01	ABI XPM Fault Isolation & QueryPM	Core20
A00002756.AA23	Japan Trunk Services	Core20, GWC10
A00002757.AA08	CBM Fault Management (HA)	SDM20
A00002760.AA11	Panther Enhancements For Hybrid Office Support	Core20
A00002765.AA06	XLAGRP Refinements for Coin Station-Paid Routing	TOPS20
A00002766.AA05	Add Extension Registers for Billing OM's	Core20
A00002822.AA07	User Interface Manager for CBM	SDM20
A00002823.AA08	SDM Core HA Maintenance (HA OAMMTCE)	SDM20
A00002858.AA26	Node ISTB for SPM Carrier Outage	SPM20, Core20
A00002900.AA09	China INAP Compliance Enhancement Part 2	GWC10, XPM20
A00002901.AA08	Enhanced Meet-Me Conference (EMMC)	Core20
A00002960.AA12	Originator Identification Screening	Core20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00002966.AA07	Base Re-architecture Phase 2	SDM20
A00002970.AA11	SMG4 Remote Site Provisioning	Core20
A00002979.AA08	Panther Electronic Software Delivery	Core20, SDM21
A00003073.AA30	SimRing Deny Redirection (SRDR)	Core20
A00003074	MG9000 Manager Capacity Increase	PNM07
A00003154.AA09	SN07 Take Back and Transfer Enhancements	Core20
A00003233.AA01	LANComm Tool Enhancements	Core20
A00003273.AA15	Refer to A00003933 (Session Server project)	NGSS07
A00003277.AA14	Refer to A00003933 (Session Server project)	NGSS07
A00003279.AB35	Refer to A00003933 (Session Server project)	Core20, NGSS07, GWC10
A00003280.AA12	SIP on NGSS Tracing/Debug Framework	NGSS07, GWC10
A00003371	Common Inventory and Data Consolidation	PNM07
A00003452.AA05	Intelligent Portal Insertion for Low Portal Density Networks	GWC10
A00003454	Secure_and_Firewall_Compatible_CS2M_and_UE9KEM_ Client_GUI_Communication	PNM07
A00003459.AA18	SSC re-architecture: SYSB Line alarm/log and LGRP alarm/ pm map support	Core20, GWC10
A00003485.AA12	ISUP 200,000 Ports Trunk Support.	Core20
A00003486.AA13	Gateway location information	Core20
A00003487.AA32	SN07 Trimodal Call Server Features	Core20
A00003490.AA22	Support for ABI XPM Tuple Change - XA-Core	Core20
A00003495.AA15	APG integration with MP for NAT traversal.	GWC10
A00003496.AA10	Control of Shasta Media Proxy	GWC10
A00003506.AA17	H.248 Per Trunk Signalling (PTS) Development	Core20, GWC10
A00003531	MG9K EM – Frame location enhancements	PNM07

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00003560	Patching SSPFS, CBM, and IEMS via the NPM	PNM07
A00003562	SAM21 Element Manager (EM) support for CICM	PNM07
A00003567	MG9000 Element Manager support for ABI ESA	PNM07
A00003568.AA02	CICM ECS Location Identification	CICM07, GWC10, PNM07
A00003571	MG9000 Cards Support A00003571 (ITP, ITX, ABI, SCO)	PNM07
A00003576.AA10	Trunk Security	PNM07, GWC10
A00003591	MG9000 OC3 Channelization support from EM	PNM07
A00003604	OC3 Channelized Support	MG9K07
A00003613	SSPFS: CBM Configuration Parameters	PNM07
A00003615	SSPFS packaging/patch enhancements	PNM07
A00003617	AlarmD Integration	PNM07
A00003618	Succession Solaris Platform Foundation Service (SSPFS) - High Availability Enhancement	PNM07
A00003630.AA18	TGCP for the Cable Market	Core20, GWC10, PNM07
A00003649.AA07	SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core	Core20
A00003650.AA08	MG4K-IP Logs Core Component	Core20
A00003651.AA10	MG4K-IP XA-Core Support for IPCCM (IP Control Connection Management) & OAM (Operations Administration & Maintenance)	Core20
A00003662.AA09	Trimodal Call Server Bridge Maintenance	Core20
A00003667	SESM NB Alarm Interface Changes required for OSS	PNM07
A00003669.AA08	Media Gateway 4000 - Internet Protocol (MG4K-IP) Prep Feature	Core20, SPM20
A00003672.AA02	NTLZ20CA Core Definition	Core20
A00003687.AA07	TOPS Wireless Intelligent Network Integration	TOPS20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00003693.AA02	MG9K ESA for SMSI subtending ABI	MG9K07, XPM20
A00003698.AB01	Razor Gateway Requirements For Trunking	GWC10, Core20, NGSS07
A00003704.AA10	OSSAIN Enhancements for SN07	TOPS20
A00003711.AA24	CS2000 SUPPPORT FOR GateWay Inter Machine Trunk (GWIMT) ON Passport Voice Gateway	GWC10, Core20
A00003717	CICM Flow Through Provisioning, CICM Component	CICM07, PNM07
A00003718-3719	Alarms, Logs & Performance for Centrex IP Client Manager	CICM07
A00003720.AA04	Compact Call Server Hybrid Asynchronous Transfer Mode Processor Mezzanine Card Replacement	Core20
A00003737	LCI Remote Access, Enhancements and MG9000 Security	MG9K07
A00003767.AA29	IP ABI PPVM Robustness & Msg Loss Alarms	GWC10, Core20, MG9K07
A00003773.AA08	Trunk Group Based Quality of Service (QOS) Operational Measurement (OM) support for MG4K-IP	Core20, SPM20
A00003789.AA14	INTRA IMT CAUSE Enhancements	Core20
A00003905.AA07	DIRP Enhancements for Billing	Core20
A00003923.AA13	CTX / RES SCAI Redirection	Core20
A00003933.AA14	Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application	Core20
A00003947.AA16	Trimodal LOGs and Operational Measurements (OM)	Core20, TOPS20, Core20
A00003948	Tri-modal provisioning	PNM07
A00003951	i2001 Internet Telephone and a common User Interface for the i2001, i2002 and i2004	CICM07
A00003952.AA09	Centrex IP Client Manager 3069 termination capacity	CICM07
A00003971.AA10	SPM Log Robustness	Core20, SPM20
A00003995	SN07 H.323 Gateway Change Capability	PNM07

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00004005.AA18	Nortel Carrier Grade Linux (NCGL) platform “Session Server”	Core20
A00004020	USP Java GUI Introduction to Succession	USP09
A00004036.AA42	Off-Board Service Control	Core20
A00004037.AA08	USNBD - FSK CDC Over Trunks	Core20
A00004045.AA06	Calling Line Identification Directory Number (CLIDN) for DMS-250	Core20
A00004046.AA10	Echo Cancellation Support for TriModal Call Server 2000	Core20
A00004096.AA11	North America (NA) H.323 Support for Networked Meridian Customer Defined Network (MCDN) Services	GWC10
A00004109	MG9K Hardware Upgrade and Call Processing Changes	MG9K07
A00004126.AA13	SPM ECAN Control Enhancement	Core20
A00004131.AA16	UCS PRI B-Channel Negotiation	Core20
A00004137.AA12	ANI Billing	Core20
A00004260.AA24	XPKT301 Alarm Banner for MG4K/IW/DPT	Core20
A00004271.AA08	SIP App Server SOC	Core20
A00004391	ACD Agent Expansion from 9,999 to 30,000 Agents	Core20
A00004414.AA03	SIP Call Server SOC	Core20
A00004422.AA12	Enhanced 911 Dynamic Packet Trunks Session Initiation Protocol-Telephony Call Trace	GWC10, Core20
A00004430.AA08	SVC Failure OMs	Core20
A00004449.AA08	OP_E911-Trunk Support	Core20
A00004500.AA15	IN TCAP Messaging on IP	Core20
A00004554.AA04	SDM FX System Backup Enhancements	SDM20
A00004568.AA06	H.323 NA Network CAS Tunneling	Core20
A00004713.AA04	1+1 Speedometer Support	Core20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00004772. AA10	Destination ACD DN MIS Reporting	Core20
A00004859	T1400 to N240 migration procedure	PNM07
A00004860	SSPFSHA Cluster & Application Upgrade Procedures	PNM07
A00004872.AA25	Services Support for the UA-IP Solution	GWC10, Core20
A00004873	MS2000 CLUI Enhancements	PNM07
A00004922.AA10	DMS-250 N449 PRI Enhancements - GWC	GWC10
A00004923.AA12	AT&T DMS-250 N449 PRI Enhancements - SPM	SPM20
A00005007.AA11	Cause Indicators parameter support for DTAG AMA Enhancement	GWC10, Core20
A00005016	VMG Out of Service Alarms	PNM07
A00005073.AA19	SBA Outbound Connection Security	SDM20
A00005074.AA07	OMDD: Outbound Connection Security	SDM20
A00005089.AA04	NOA Routing for IC Agency - TRAVER Enhancement	Core20
A00005123	CS2M Configuration Install Script Enhancements	PNM07
A00005124.AA01	Compact Hybrid China Cutover Tools - Production Software	Core20
A00005160.AA12	OSSAIN XA-Core Data Messaging Capacity Enhancements	TOPS20
A00005190.AA09	CBM 800 OC3 Core Node and Link Maintenance	Core20
A00005192.AA28	CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance	SDM20
A00005193.AA04	9+1 Performance Measurements Tools Support	Core20
A00005268.AA05	SBA: Multi-volume Support for Core Backup	SDM20
A00005317	WanBuilder Heartbeat Ping	MG9K07
A00005322.AA08	Spectrum Common Equipment Module (CEM) Overload Enhancement: Asynchronous Transfer Mode Resource Module (ATMRM) Status	SPM20
A00005337.AA04	CBM 800 OC3 BRISC Connectivity	SDM20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00005363.AA16	CAIN FlexCDR Enhancements	Core20
A00005375	New Shelf Discovery Alarms	PNM07
A00005391.AA04	SBA: Support for Verizon GNS personal Toll Free Service	SDM20
A00005485	SAM21 Platform Installation on SSPFS	PNM07
A00005538.AA14	Preset Conference on Succession	Core20, GWC10
A00005734.AA05	Multiple Time Zone (MTZ) support for CICM lines	Core20
A00005758.AA03	ESUP over TELNET Support	SDM20
A00005986	EM integration with PAM+ proxy	CICM07
A00006032.AA07	Loop Reversal On Answer (LROA), Loop Reversal on Seizure (LRS) and Insert Tone on Coin Phone Termination (NO-COLL) SN07 Support for Cable & Wireless Caribbean	GWC10
A00006483.AA02	Audio Server Node Announcement Capacity Increase to 1280	Core20, GWC10
A00006495	H.323 Flexible Carriers	Core20, GWC10, PNM07
A00006496	H.323 Multiple D Channels	GWC10
A00006639.AA02	MG9K Overload OM pegs	Core20
A00006693	XA-Core IO Capacity Monitoring Toolset	Core20
A00006741.AA08	H.323 Gatekeeper to CS2K Gatekeeper Interworking	GWC10
A00007063	H.323 Gateway Profile Changes	PNM07
A00007211	H.323 GWC600 Log Changes	GWC10
Q00681924	AIN Response Simplification	Core20

Functional Group to Feature Impacts Cross Reference

Table 2 is organized alphabetically by functional group. Within each group, the features are listed numerically. The table also indicates which sections are

included for a given feature (for example, FN, FM, CN, PF, or ACC) in the release document.

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core20	A00001319.AA10	Y				
Core20	A00001847.AA31	Y		Y		
Core20	A00001888.AC01	Y				
Core20	A00001890.AA31	Y		Y		
Core20	A00001895.AC08	Y				
Core20	A00001898.AA29	Y		Y		
Core20	A00001990.AA02	Y				
Core20, SDM20	A00002008.AA08	Y				
Core20	A00002009.AA04	Y		Y		
Core20	A00002011.AA08	Y				
Core20	A00002012.AA13	Y	Y	Y		Y
Core20	A00002013.AA06	Y	Y	Y		
Core20	A00002016.AA02	Y				
Core20	A00002020.AB10	Y	Y	Y		
Core20	A00002047.AA11	Y				
Core20	A00002137.AA01	Y				
Core20	A00002146.AA09	Y	Y	Y		
Core20	A00002186.AA08	Y				
Core20	A00002196.AA14	Y		Y		
Core20	A00002251.AA13	Y				
Core20	A00002281.AA02	Y				
SDM20	A00002340.AA07	Y				Y
Core20, MG9K07, XPM20	A00002380.AA21	Y	Y	Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core20, SPM20	A00002431.AA16	Y		Y		
Core20, SPM20	A00002432.AA24	Y				
Core20, XAC21	A00002433.AA07	Y	Y	Y		
Core20, XAC21	A00002499.AA05	Y	Y			
Core20, XAC21	A00002510.AA08	Y	Y	Y		
Core20	A00002538.AA19					Y
Core20	A00002549.AA04	Y	Y			
Core20	A00002555.AA03	Y		Y		
Core20	A00002558.AA07	Y		Y		
Core20	A00002607.AA11	Y	Y	Y		
Core20, GWC10	A00002739.AA15	Y				
Core20	A00002746.AB01	Y		Y		
Core20, GWC10	A00002756.AA17	Y				
Core20	A00002760.AA11	Y		Y		
Core20	A00002766.AA05	Y				Y
Core20	A00002901.AA07	Y		Y		
Core20	A00002960.AA12	Y		Y		
Core20	A00002970.AA11	Y	Y	Y		
Core20	A00003073.AA29	Y		Y		
Core20	A00003154.AA09	Y				
Core20	A00003233.AA01	Y				
Core20, NGSS07, GWC10	A00003279.AB35	Y				
Core20	A00003487.AA27	Y	Y	Y		Y
Core20	A00003490.AA21	Y		Y		
Core20, GWC10	A00003459.AA18	Y		Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core20	A00003485	Y				
Core20	A00003486	Y		Y		
Core20, GWC10	A00003489	Y		Y		
Core20, GWC10	A00003506.AA15	Y		Y		
Core20, GWC10, PNM07	A00003630.AA18	Y		Y		
Core20	A00003649.AA07	Y				
Core20	A00003650.AA08	Y	Y			
Core20	A00003651.AA10	Y				
Core20	A00003662.AA09	Y				
Core20, SPM20	A00003669.AA08	Y		Y		
Core20	A00003672.AA02	Y		Y		
Core20	A00003720.AA04	Y				
Core20, SPM20	A00003773.AA08	Y		Y		Y
Core20	A00003789.AA13	Y		Y		
Core20	A00003905.AA07	Y		Y		
Core20	A00003923.AA13	Y		Y		
Core20	A00003933.AA07	Y	Y	Y		
Core20, TOPS20	A00003947.AA16	Y	Y	Y		
Core20	A00004005.AA12	Y		Y		
Core20	A00004036.AA42	Y		Y	Y	Y
Core20	A00004037.AA08	Y				
Core20	A00004045.AA06	Y	Y	Y		
Core20	A00004046	Y		Y		
Core20	A00004126	Y		Y		
Core20	A00004131.AA16	Y		Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core20	A00004137.AA12	Y		Y	Y	
Core20	A00004260.AA24	Y	Y	Y		
Core20	A00004271	Y	Y	Y		Y
Core20	A00004391	Y	Y	Y		
Core20	A00004414	Y		Y		
Core20	A00004430.AA08	Y	Y			Y
Core20	A00004449	Y				
Core20	A00004500.AA15	Y		Y		Y
Core20	A00004554.AA04	Y				
Core20	A00004568.AA06	Y				
Core20	A00004713	Y				
Core20	A00004772. AA10	Y				
Core20	A00005089.AA04	Y				
Core20	A00005124.AA01	Y				
Core20	A00005190.AA09	Y		Y		
Core20	A00005193	Y		Y		
Core20	A00005363.AA16	Y	Y	Y	Y	
Core20, GWC10	A00005538.AA13	Y				
Core20	A00005734.AA04	Y		Y		
Core20, GWC10	A00006483	Y		Y		
Core20, GWC10, PNM07	A00006495	Y				
Core20	A00006639.AA02	Y				
CICM07, GWC10, PNM07	A00003568.AA02	Y				
CICM07, PNM07	A00003717	Y				
CICM07	A00003951	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
CICM07	A00005986	Y				
CICM07	A00003952.AA09	Y				
GWC10, XPM20	A00002900.AA09	Y		Y		
GWC10	A00003452.AA05	Y				
GWC10	A00003495.AA15	Y				
GWC10	A00003496.AA10	Y				
GWC10, Core20, NGSS07	A00003698.AA16	Y				
GWC10, Core20	A00003711.AA22	Y				
GWC10, Core20, MG9K07	A00003767.AA29	Y	Y	Y		Y
GWC10	A00004096.AA11	Y				
GWC10, Core20	A00004422.AA11	Y				
GWC10, Core20	A00004872	Y		Y		
GWC10	A00004922.AA10	Y				
GWC10, Core20	A00005007	Y		Y		
GWC10	A00006032.AA07	Y				
GWC10	A00006496	Y				
GWC10	A00006741	Y				
GWC10	A00007211	Y				
MG9K07, XPM20	A00003693.AA02	Y				
MG9K07	A00004109	Y				
MG9K07	A00005317	Y				
NGSS07	A00003273.AA15	Y				
NGSS07	A00003277.AA14	Y				
NGSS07, GWC10	A00003280.AA12	Y				
PNM07	A00001893	Y	Y	Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
PNM07	A00001935	Y				
PNM07	A00002585	Y		Y		
PNM07	A00003074	Y		Y		
PNM07	A00003371	Y	Y			
PNM07	A00003454	Y		Y		
PNM07	A00003531	Y		Y		Y
PNM07	A00003560	Y				
PNM07	A00003562	Y				
PNM07	A00003567	Y	Y	Y		
PNM07	A00003571	Y		Y		
PNM07, GWC10	A00003576	Y				
PNM07	A00003591	Y	Y	Y		
PNM07	A00003613	Y				
PNM07	A00003615	Y		Y		
PNM07	A00003617	Y				
PNM07	A00003618	Y				
PNM07	A00003667	Y	Y	Y		
PNM07	A00003948	Y		Y		
PNM07	A00003995	Y		Y		
PNM07	A00004859	Y				
PNM07	A00004860	Y				
PNM07	A00004873	Y				
PNM07	A00005016	Y	Y	Y		
PNM07	A00005123	Y				
PNM07	A00005375	Y	Y			
PNM07	A00005485	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
PNM07	A00007063	Y				
SDM20	A00001649	Y				
SDM20	A00001650.AA09	Y				
SDM20	A00001742.AA05	Y				
SDM20	A00001743.AA04	Y				
SDM20	A00002133.AA05	Y				
SDM20	A00002155.AA10	Y				
SDM20	A00002164.AA10	Y				
SDM20	A00002744.AA05	Y				
SDM20	A00002757.AA08	Y	Y			
SDM20	A00002822.AA07	Y				
SDM20	A00002823.AA08	Y	Y			
SDM20	A00002966.AA07	Y				
SDM21	A00002979.AA07	Y		Y		
SDM20	A00004554.AA04	Y				
SDM20	A00004868	Y				
SDM20	A00005073.AA18	Y	Y	Y		
SDM20	A00005074.AA07	Y	Y	Y		
SDM20	A00005192.AA24	Y	Y			
SDM20	A00005268.AA05	Y				
SDM20	A00005337.AA04	Y				
SDM20	A00005391.AA04	Y				
SDM20	A00005758.AA03	Y				
SPM20, Core20	A00002858.AA26	Y	Y	Y		
SPM20, Core20	A00003971.AA10	Y	Y	Y		
SPM20	A00004923.AA11	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
SPM20	A00005322.AA08	Y	Y			
TOPS20	A00002740.AA03	Y				
TOPS20	A00002765.AA06	Y				
TOPS20	A00003687.AA06	Y	Y	Y		Y
TOPS20	A00003704.AA10	Y				
TOPS20	A00005160.AA10	Y	Y	Y		Y
USP09	A00004020	Y				

Functional Descriptions

Introduction

This chapter describes new and changed features that are planned for this release.

Featid	Title
A00001319.AA10	Device activity & RMID-PWID restoration tool & Panther enhancements
A00001649	SBA Robustness: End-to-end Integrity
A00001650.AA09	SBA Patch Size Reduction
A00001742.AA05	OMDD Capacity Enhancements
A00001743.AA04	Syslog Consolidation for Succession
A00001847.AA31	ABI Expansion Datafill
A00001888.AC02	CS2000 Line Test for MG9000 Lines
A00001890.AA31	Refer to A00001888
A00001893	MG9K Imaging (includes A00001894)
A00001895.AC09	H323 Base Application
A00001898.AA29	ABI RMM Support
A00001935	Provisioning Support for Centrex-IP Nodes and Lines
A00001990.AA02	CAIN via CICROUTE PEP Sourcing
A00002008.AA08	SBA:CBM Introduction
A00002009.AA04	Enhance Display on PSET

A00002011.AA08	DMS-100: Virtual Office Worker
A00002012.AA13	XA-Core CMIC/RTIF HIOP Maintenance Software
A00002013.AA06	Intelligent Network T1 Timer Expiry Message Suppression
A00002016.AA02	AINDENY Enhancements
A00002020.AB10	ESA Translation Download
A00002047.AA13	Double Density Spectrum Backplane
A00002133.AA05	CBM HA Installation, Patching and SW Delivery
A00002137.AA01	DS512 Link Mtc Robustness - CM
A00002146.AA09	MAPCI ABI Link Test & Legacy Comparison
A00002155.AA11	SSH Core File Transfer (SCFT) for CBM and SDM
A00002164.AA10	Application Manager for High Availability (HA)
A00002186.AA08	IOM DDU Capacity Enhancement
A00002196.AA15	Enhanced Do Not Disturb
A00002251.AA13	192M Shared Memory Extension
A00002281.AA02	Table AMAPRT Expansion
A00002340.AA07	Add Extension Registers for Billing OM's
A00002380.AA21	MG9K ABI ESA
A00002431.AA16	LX82BA Capacity Delivery
A00002432.AA24	Enhanced Spectrum Overload Operational Measurements (OMs) and Logs
A00002433.AA08	XA-Core Baseline Control
A00002499.AA05	Store Audit for XA-Core
A00002505	Universal Signaling Point Interface Client - GUI
A00002510.AA11	LANCOMM IP over IRM
A00002538.AA19	Performance Measurements Tools

A00002549.AA04	CSP20 Callp Robustness
A00002555.AA03	SERVORD Manipulation of the GND Option
A00002558.AA07	LDI display for Class phone
A00002585	TMM Support For PTS Trunk, POST by Carrier
A00002607.AA11	ABI XPM SITE and MG9K Location support
A00002739.AA15	Virtual Call Admissions Control (VCAC) on Communication Server 2000
A00002740.AA03	International Directory Assistance Call Completion (IDACC)
A00002741	Supernode Billing Application Base Real Time Billing Robustness
A00002744.AA05	SBA: Automatic Recovery File Closure
A00002746.AB01	ABI XPM Fault Isolation & QueryPM
A00002756.AA23	Japan Trunk Services
A00002757.AA08	CBM Fault Management (HA)
A00002760.AA11	Panther Enhancements For Hybrid Office Support
A00002765.AA06	XLAGRP Refinements for Coin Station-Paid Routing
A00002766.AA05	Add Extension Registers for Billing OM's
A00002822.AA07	User Interface Manager for CBM
A00002823.AA08	SDM Core HA Maintenance (HA OAMMTCE)
A00002858.AA26	Node ISTB for SPM Carrier Outage
A00002900.AA09	China INAP Compliance Enhancement Part 2
A00002901.AA08	Enhanced Meet-Me Conference (EMMC)
A00002960.AA12	Originator Identification Screening
A00002966.AA07	Base Re-architecture Phase 2
A00002970.AA11	SMG4 Remote Site Provisioning
A00002979.AA08	Panther Electronic Software Delivery

A00003073.AA30	SimRing Deny Redirection (SRDR)
A00003074	MG9000 Manager Capacity Increase
A00003154.AA09	SN07 Take Back and Transfer Enhancements
A00003233.AA01	LANComm Tool Enhancements
A00003273.AA15	Refer to A00003933 (Session Server project)
A00003277.AA15	Refer to A00003933 (Session Server project)
A00003279.AB35	Refer to A00003933 (Session Server project)
A00003280.AA12	SIP on NGSS Tracing/Debug Framework
A00003371	Common Inventory and Data Consolidation
A00003452.AA05	Intelligent Portal insertion for low portal density networks.
A00003454	Secure_and_Firewall_Compatible_CS2M_and_UE9KEM_Client_GUI_Communication
A00003459.AA18	SSC re-architecture: SYSB Line alarm/log and LGRP alarm/pm map support
A00003485.AA12	ISUP 200,000 Ports Trunk Support.
A00003486.AA13	Gateway location information
A00003487.AA32	SN07 Trimodal Call Server Features
A00003489.AA09	ABI SMS Support
A00003490.AA22	Support for ABI XPM Tuple Change - XA-Core
A00003495.AA15	APG integration with MP for NAT traversal.
A00003496.AA10	Control of Shasta Media Proxy
A00003506.AA17	H.248 Per Trunk Signalling (PTS) Development
A00003531	MG9K EM – Frame location enhancements
A00003560	Patching SSPFS, CBM, and IEMS via the NPM
A00003562	SAM21 Element Manager (EM) support for CICM

A00003567	MG9000 Element Manager support for ABI ESA
A00003568.AA02	CICM ECS Location Identification
A00003571	MG9000 Cards Support A00003571 (ITP, ITX, ABI, SCO)
A00003576.AA10	Trunk Security
A00003591	MG9000 OC3 Channelization support from EM
A00003604	OC3 Channelized Support
A00003613	SSPFS: CBM Configuration Parameters
A00003615	SSPFS packaging/patch enhancements
A00003617	AlarmD Integration
A00003618	Succession Solaris Platform Foundation Service (SSPFS) - High Availability Enhancement
A00003630.AA18	TGCP for the Cable Market
A00003649.AA07	SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core
A00003650.AA08	MG4K-IP Logs Core Component
A00003651.AA10	MG4K-IP XA-Core Support for IPCCM (IP Control Connection Management) & OAM (Operations Administration & Maintenance)
A00003662.AA09	Trimodal Call Server Bridge Maintenance
A00003667	SESM NB Alarm Interface Changes required for OSS
A00003669.AA08	Media Gateway 4000 - Internet Protocol (MG4K-IP) Prep Feature
A00003672.AA02	NTLZ20CA Core Definition
A00003687.AA07	TOPS Wireless Intelligent Network Integration
A00003693.AA02	MG9K ESA for SMSI subtending ABI
A00003698.AB01	Razor Gateway Requirements For Trunking
A00003704.AA10	OSSAIN Enhancements for SN07

A00003711.AA24	CS2000 SUPPPORT FOR GateWay Inter Machine Trunk (GWIMT) ON Passport Voice Gateway
A00003717	CICM Flow Through Provisioning, CICM Component
A00003718-3719	Alarms, Logs & Performance for Centrex IP Client Manager
A00003720.AA04	Compact Call Server Hybrid Asynchronous Transfer Mode Processor Mezzanine Card Replacement
A00003737	LCI Remote Access, Enhancements and MG9000 Security
A00003767.AA29	IP ABI PPVM Robustness & Msg Loss Alarms
A00003773.AA08	Trunk Group Based Quality of Service (QOS) Operational Measurement (OM) support for MG4K-IP
A00003789.AA14	INTRA IMT CAUSE Enhancements
A00003905.AA07	DIRP Enhancements for Billing
A00003923.AA13	CTX / RES SCAI Redirection
A00003933.AA14	Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application
A00003947.AA16	Trimodal LOGs and Operational Measurements (OM)
A00003948	Tri-modal provisioning
A00003951	Covers the work required to support the i2001 Internet Telephone and a common User Interface for the i2001, i2002and i2004
A00003952.AA09	Centrex IP Client Manager 3069 termination capacity
A00003971.AA10	SPM Log Robustness
A00003995	SN07 H.323 Gateway Change Capability
A00004005.AA18	Nortel Carrier Grade Linux (NCGL) platform “Session Server”
A00004020	USP Java GUI Introduction to Succession
A00004036.AA42	Off-Board Service Control
A00004037.AA08	USNBD - FSK CDC Over Trunks

A00004045.AA06	Calling Line Identification Directory Number (CLIDN) for DMS-250
A00004046.AA10	Echo Cancellation Support for TriModal Call Server 2000
A00004096.AA11	North America (NA) H.323 Support for Networked Meridian Customer Defined Network (MCDN) Services
A00004109	MG9K Hardware Upgrade and Call Processing Changes
A00004126.AA13	SPM ECAN Control Enhancement
A00004131.AA16	UCS PRI B-Channel Negotiation
A00004137.AA12	ANI Billing
A00004260.AA24	XPKT301 Alarm Banner for MG4K/IW/DPT
A00004271.AA08	SIP App Server SOC
A00004391	ACD Agent Expansion from 9,999 to 30,000 Agents
A00004414.AA03	SIP Call Server SOC
A00004422.AA12	Enhanced 911 Dynamic Packet Trunks Session Initiation Protocol-Telephony Call Trace
A00004430.AA08	SVC Failure OMs
A00004449.AA08	OP_E911-Trunk Support
A00004500.AA15	IN TCAP Messaging on IP
A00004554.AA04	SDM FX System Backup Enhancements
A00004568.AA06	H.323 NA Network CAS Tunneling
A00004713.AA04	1+1 Speedometer Support
A00004772. AA10	Destination ACD DN MIS Reporting
A00004859	T1400 to N240 migration procedure
A00004860	SSPFSHA Cluster & Application Upgrade Procedures
A00004872.AA25	Services Support for the UA-IP Solution
A00004873	MS2000 CLUI Enhancements

A00004922.AA10	DMS-250 N449 PRI Enhancements - GWC
A00004923.AA12	Refer to A00004922
A00005007.AA11	Cause Indicators parameter support for DTAG AMA Enhancement
A00005016	VMG Out of Service Alarms
A00005073.AA19	SBA Outbound Connection Security
A00005074.AA07	OMDD: Outbound Connection Security
A00005089.AA04	NOA Routing for IC Agency - TRAVER Enhancement
A00005123	CS2M Configuration Install Script Enhancements
A00005124.AA01	Compact Hybrid China Cutover Tools - Production Software
A00005160.AA12	OSSAIN XA-Core Data Messaging Capacity Enhancements
A00005190.AA09	CBM 800 OC3 Core Node and Link Maintenance
A00005192.AA28	CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance
A00005193.AA04	9+1 Performance Measurements Tools Support
A00005268.AA05	SBA: Multi-volume Support for Core Backup
A00005317	WanBuilder Heartbeat Ping
A00005322.AA08	Spectrum Common Equipment Module (CEM) Overload Enhancement: Asynchronous Transfer Mode Resource Module (ATMRM) Status
A00005337.AA04	CBM 800 OC3 BRISC Connectivity
A00005363.AA16	CAIN FlexCDR Enhancements
A00005375	New Shelf Discovery Alarms
A00005391.AA04	SBA: Support for Verizon GNS personal Toll Free Service
A00005485	SAM21 Platform Installation on SSPFS
A00005538.AA14	Preset Conference on Succession
A00005734.AA05	Multiple Time Zone (MTZ) support for CICM lines

A00005758.AA03	ESUP over TELNET Support
A00005986	EM integration with PAM+ proxy
A00006032.AA07	Loop Reversal On Answer (LROA), Loop Reversal on Seizure (LRS) and Insert Tone on Coin Phone Termination (NOCOLL) SN07 Support for Cable & Wireless Caribbean
A00006483.AA02	Audio Server Node Announcement Capacity Increase to 1280
A00006495	H.323 Flexible Carriers
A00006496	H.323 Multiple D Channels
A00006639.AA02	MG9K Overload OM pegs
A00006693	XA-Core IO Capacity Monitoring Toolset
A00006741.AA08	H.323 Gatekeeper to CS2K Gatekeeper Interworking
A00007063	H.323 Gateway Profile Changes
A00007211	H.323 GWC600 Log Changes
Q00681924	AIN Response Simplification

1: Functional Description (FN): A00001319

1.1 Feature name

ACT.A00001319: Device activity & RMID-PWID restoration tool & Panther enhancements

1.2 Description

This activity provides two new functionalities:

- A new CI tool ‘SPMRESALIGN’ which ensures the following:
  a. The RMID-PWID values of the Resource RMs (DSP & VSP RMs) are aligned.
  b. The activity of DSP & VSP RMs are aligned as per the table MNCKTPAK datafill.
- A new automated task as a part of Panther Upgrade. When this new task is executed, it will align the RMID-PWID values of all the resource RMs of all the SPMs in the office.

1.2.1 New CI tool SPMRESALIGN

A new CI tool ‘SPMRESALIGN’ is introduced as a part of this feature. This tool aligns the RMID-PWID values of the DSP/VSP RMs of the all the SPMs in the office. Once the RMID-PWID values of a particular RM is aligned, the activity of that particular RM is aligned as per the table MNCKTPAK datafill. The tool is implemented as a new CI directory.The tool can be directly accessed from the CI prompt.The tool has the following commands:

- Align the RMID-PWID values of the resource RMs of all the SPMs in the office.

  CI:
  >SPMRESALIGN
  SPMRESALIGN:
  >align all

- Align the RMID-PWID values of the resource RMs based on the variant of SPMs

  CI:
  >SPMRESALIGN
  SPMRESALIGN:
  >align <variant>

  where the variant can be DMSCP, SMG4 or IW-DPT.

- Align the RMID-PWID values of the resource RMs of a single SPM.

  CI:
  >SPMRESALIGN
  SPMRESALIGN:
  >align spm <no>
  This command is applicable for all variants of SPMs.

- Align the RMID-PWID values of the resource RMs for a range of SPMs.

  CI:
  >SPMRESALIGN
  SPMRESALIGN:
  >align spm <from_no> <to_no>
  This command is applicable for all variants of SPMs.

This tool is a single user tool. i.e. only one user can use the tool at a time. Also all the command in this tool are privclassed. For this, the command 'SPMRESALIGN; & 'align' will be added to the table CMDS.

Please refer to section 13.9 of Configuration Document for more details on the CI tool.

1.2.2 Panther Enhancements

This feature enhances the planning phase of PMUPGRADE to create a default task. This new task is to align the RMID-PWID values of all the SPMs present in the entire office. The new task is appended to the upgrade plan and will be passed to the SWUPGRADE tool. The new task will be created only if there is atleast one SPM is available in the upgrade plan.

In SWUPGRADE, the craft person can view this new task by issuing the command 'display steps'. An example is as shown in Figure 1, "SWUPGRADE steps"

Figure 1 SWUPGRADE steps

```
>swupgrade pm
SWUPGRADE:

>display steps

SWUPGRADE steps for target PM:

1_A_SPM                 Needed    Perm  Act    Proc
ALIGN_RMS               Needed    Perm  Act    Proc
UPGRADE_COMPLETE Needed    Perm Act      Proc
```

The default task created is ALIGN_RMS. This task is an automated task. i.e. it is automatically executed as soon as all the upgrade tasks are completed. As this step starts executing, it halts for a user confirmation to proceed or abort this step. The following warning message will be displayed on the Panther screen

****WARNING: This step ALIGN_RMS will align the RMID-PWID values of all the Resource RMs of the SPMs in the office. Do you wish to continue?**
Please confirm ("YES", "Y", "NO", or "N"):

Once the craft person enters “YES”, Panther will start aligning the RMID-PWID values of the all the resource RMs in the office. If the craft person enters “NO”, it aborts this task.

Panther automatically triggers this alignment task only if all the other task in the plan is successfully completed without any failure. Also the user confirmation has to be turned off in the Panther planning phase. Otherwise Panther waits for a manual intervention after each task is completed, to trigger the next task.

On the other hand, the craft person can manually execute this alignment task by overriding all the other upgrade tasks. The craft person has to issue the following command:

>runstep ALIGN_RMS.

All the progress message that are part of the new CI tool will be printed on the Panther screen also. Please refer to section 13.9 in Configuration document to get more information on the progress messages.

1.2.3 Log generation

A new SPM log is introduced to make the craftperson aware that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values. A particular RM group will be excluded from the alignment due to three reasons:

- PWID duplication
- Any RM in invalid state.
- Sparing failure.

Under all these circumstances the new SPM log '**SPM605**' will be generated giving necessary information to the craftperson and what action to be taken. This is only an info log and there is no alarm associated with it. The fields of the SPM605 log is as shown in Figure 2, "SPM605 Log Format"

Figure 2 SPM605 Log Format

a) PWID Duplication

```
SPM605  MAR25 05:06:48 3004 INFO RMID-PWID Alignment
        Prot group  : SPM 3 VSP
        Prot grp id  : 1
        Result       : Not Aligned
        Reason       : PWID duplication.
        Action       : Rectify the duplication and execute SPMRESALIGN
```

b) Any RM in invalid state

```
SPM605  MAR25 05:06:48 3004 INFO RMID-PWID Alignment
        Prot group  : SPM 3 VSP
        Prot grp id  :1
        Result       : Not Aligned
        Reason       : VSP 1 not in ISV/ISTB.
        Action       : Bring this RM to INSV and execute SPMRESALIGN
```

c) Sparing failure

```
SPM605  MAR25 05:06:48 3004 INFO RMID-PWID Alignment
        Prot group  :  SPM 3 VSP
        Prot grp id  :  1
        Result       :  Not Aligned
        Reason       :  Unsuccessfull sparing
        Action       :  Review the logs related to sparing
```

Please refer to the fault management document for more information on this log.

1.3 Hardware Requirements or Dependencies

None.

1.4 Software Requirements or Dependencies

None.

1.5 Limitations and restrictions

Following RM groups are excluded from the alignment process.

- If any RM in the group is having a PWID duplication.
- If there is no inactive RM in the group.
- If any RM in the group is in invalid state (offl, sysb, cbsy, manb).

No action is taken on these RM groups to align the RMID-PWID values. However, proper warning messages will be displayed. Please refer to section 13.9 in Configuration document to get more information on the warning messages.

1.6 Interactions

When the office upgrade using Panther is in progress, the craftperson is restricted from executing the commands in the ‘SPMRESALIGN’ tool. Proper message will be displayed to the craftperson.

a) In a multiple window upgrade shift, after each days shift the craft can run the CI tool on the SPMs which finished the upgrade or.

b) The craftperson can run the automated task from panther . This will be run automatically after all the steps. Proper message will be displayed that it will align the RMID-PWID values of all the Reousrce RMs in the office.

1.7 Applicable customer facing sections

Fault Management	
Logs	X
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A

Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A
Real-time	N/A
Engineering Information	N/A

1.8 Glossary

Term	Description
SPM	Spectrum Peripheral Module
RM	Resource Module
RMID	Resource Module ID
PWID	ProtWhom ID
DSP	Digital Signal Processor
VSP	Voice Signal Processor

2: Functional Description (FN): A00001649

2.1 Feature name

SBA Robustness: End-to-end Integrity[A00001649]
This feature has two parts:
1. SBA Backup Alarms Precedence

2. Add "clli" command to BILLMTC Interface.

2.2 Description

Section 2.2.1 below gives a brief description on SBA Backup Alarms Precedence and section 2.2.2 below gives a brief description of Add “clli” command to BILLMTC interface.

2.2.1 SBA Backup Alarms Precedence

All the SBA alarms on the DMS are reported on the MAP under the SDMBIL sub-level available under the APPL banner and the severity is set to match the highest {Critical, Major, Minor} in case of multiple alarms.

NOCOM alarm appears on the MAP at the SDMBIL level when the communication to SDM cannot be established.

This feature is to provide a change in the priority for the backup alarms: BAK50, BAK70, BAK90, NOBAK, NOSTOR so that these alarms take precedence over NOCOM alarm.

The severity of the alarms BAK50,BAK70 will all be changed from major to critical.

If the stream is in backup for more than 10 minutes, a SDMB320 log will be generated every 2 minutes indicating the same.This is an existing log.

The backup alarms BAK50, BAK70, BAK90, NOBAK and NOSTOR alarm will take precedence over the following critical alarms:

DSKWR, LODSK, NOFL, NOVOL, FTPW, SBAIFT.

This enhancement prevents loss of billing by ensuring that appropriate alarms are generated which will inform the operational personnel well in advance so that preventive maintenance action can be performed.

2.2.2 Add "clli" command to BILLMTC Interface

The SDM/SBA “BILLMTC” refers to Billing Maintenance Interface. This interface is similar to CM MAPCI interface. BILLMTC is available through a telnet session to SDM or from an SDM terminal. Also BILLMTC will be accessible from the ETA and ATA connected to SDM.

CLLI(Common Language Location Identifier) is a string with a maximum of eleven characters which uniquely identifies the switch. The switch name is available in OFCENG table under the field OFFICE_CLLI_NAME and is datafilled when the switch is being provisioned.

This feature is an enhancement for Supernode Billing Application RMI to introduce a new command which retrieves and displays CLLI (Common Language Location Identifier, in the context of this feature the CLLI will refer to the Telco “name” of the switch) at BILLMTC level. This command will display the name of the CLLI connected to SDM.

2.3 Requirements.

2.3.1 Requirements for SBA Backup Alarms Precedence

Modify BAK50, BAK70 alarms to critical.

Modify BAK50,BAK70,BAK90 NOBAK & NOSTOR to take higher precedence than NOCOM at SDMBIL level.

2.3.2 Requirements for Add "clli" command to BILLMTC Interface

1. "clli" command will be available from BILLMTC Interface.

2. "clli" command will be available at all levels of BILLMTC.

3. The command will not appear on BILLMTC menu(non-menu command).

4. The command will not be a numbered command at BILLMTC menu.

5. The help command, without any parameter at BILLMTC will display help for "clli" along with help for other commands.

6. “Help clli” will not display any help.

7. The command returns core CLLI name and "clli" command does not have any parameters.

2.4 Target Audience

This document is intended for:

— SDM Architecture Team

— SDM GPS

— SDM Verification

— SDM Documentation

2.5 Functional overview

Section 2.5.1 below gives a functional overview of “SBA Backup Alarms Precedence” and section 2.5.2 below gives a brief functional overview of “Add “clli” command to BILLMTC interface.”

2.5.1 “SBA Backup Alarms Precedence”

This feature is to change the priority of the backup alarms so that these alarms take precedence over NOCOM alarm.

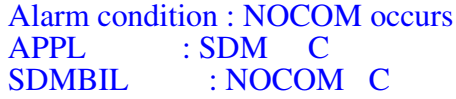
When the NOCOM alarm appears on the MAP at the SDMBIL level, the streams on the CM go to backup mode. The billing records then generated will be written to backup files on backup volumes configured for the stream.

Eventually the backup space on core will start getting used up and backup alarms will start appearing on the SDMBIL banner depending upon the amount of used space. When 50% of backup space has been used up, the BAK50 alarm will appear on the SDMBIL banner on the MAP indicating that only 50% of the configured backup space is available for the stream.

Once 70% of the backup space is used, the BAK50 alarm will be changed to BAK70 alarm. Again when a situation is reached wherein only 10% of the free space is available, BAK70 alarm will be replaced by the BAK90 alarm. Eventually when the system runs out of backup space, NOBAK alarm will appear under the SDMBIL banner replacing the BAK90 alarm.

Once the NOBAK alarm comes up for a stream, any further records generated would still persist in the buffer pool {buffer allocated to the stream}.Eventually if the situation continues the buffers would get depleted and a NOSTOR{Critical} alarm will appear under SDMBIL level.

Figure 1



```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 AMDI     04SBPT  NODLOG     .        1 SPM      .        .         ...      .      SDM
  *C*                                *C*                                          *C*
 POST                 OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL          TOPSIP
  0 Quit                .       .      SysB     .       .   NOCOM .
  2 Post_                              *C*                     *C*
  3
  4                  AMA :       Bkup   Pri:        InSv   Rec:        InSv
  5                                     Bkup:       Bkup   Comm:       InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10            DispAL
 11 DispAL     critical:ALL:NOCOM:Communication to SDM cannot be established.
 12
 13 Status     major: AMA: BAKUP: Backup time exceeds 10 minutes.
 14 Query
 15
 16
 17 Audit
```

Figure 2

```
Alarm condition : Still in NOCOM, but we have just hit BAK50
APPL            : SDM    C
SDMBIL          : BAK50  C
```

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 AMDI     04SBPT  NODLOG     .        1 SPM      .        .         ...      .      SDM
  *C*                                *C*                                          *C*
 POST                 OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL          TOPSIP
  0 Quit                .       .      SysB     .       .    BAK50 .
  2 Post_                             *C*                      *C*
  3
  4                  AMA :       Bkup  Pri:        InSv  Rec:        InSv
  5                                    Bkup:       Bkup  Comm:       InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10           DispAL
 11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
 12          critical: AMA: BAK50: WARNING, less than 50% free space for Backup
 13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
 14 Query
 15
 16
 17 Audit
 18
```

Figure 3

```
Alarm condition : Still in NOCOM, but we have just hit BAK70
APPL            : SDM    C
SDMBIL          : BAK70  C
```

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 AMDI     04SBPT  NODLOG     .        1 SPM      .        .         ...      .      SDM
  *C*                                *C*                                          *C*
 POST                 OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL          TOPSIP
  0 Quit                .       .      SysB     .       .    BAK70  .
  2 Post_                             *C*                      *C*
  3
  4                  AMA :       Bkup  Pri:        InSv  Rec:        InSv
  5                                    Bkup:       Bkup  Comm:       InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10           DispAL
 11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
 12          critical: AMA: BAK70: WARNING, less than 30% free space for Backup
 13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
 14 Query
 15
 16
 17 Audit
 18
```

Figure 4

```
Alarm condition :Still in NOCOM, but we have just hit BAK90
APPL            : SDM    C
SDMBIL          : BAK90  C
```

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 AMDI    04SBPT NODLOG    .      1 SPM     .       .       ...     .     SDM
  *C*                            *C*                                    *C*
 POST                OAMAP  ATMFW   SDM   SPMCP  SWMTC  SDMBIL        TOPSIP
  0 Quit               .      .     SysB    .      .  BAK90 .
  2 Post_                            *C*                  *C*
  3
  4                  AMA :      Bkup  Pri:       InSv  Rec:       InSv
  5                                   Bkup:      Bkup  Comm:      InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10           DispAL
 11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
 12         critical: AMA: BAK90: WARNING, less than 10% free space for Backup
 13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
 14 Query
 15
 16
 17 Audit
 18
```

Figure 5

```
Alarm condition : Still in NOCOM, but we run out of backup space
APPL            : SDM    C
SDMBIL          : NOBAK  C
```

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 AMDI     04SBPT  NODLOG     .        1 SPM      .        .         ...      .      SDM
  *C*                                *C*                                          *C*
 POST                  OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL          TOPSIP
  0 Quit                 .       .      SysB     .       .   NOBAK  .
  2 Post_                               *C*                    *C*
  3
  4                   AMA :       Bkup   Pri:        InSv   Rec:        InSv
  5                                      Bkup:       Bkup   Comm:       InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10            DispAL
 11 DispAL     critical:ALL:NOCOM:Communication to SDM cannot be established.
 12            critical: AMA: NOBAK: ERROR, no space on Backup volumes.
 13 Status     major: AMA: BAKUP: Backup time exceeds 10 minutes.
 14 Query
 15
 16
 17 Audit
 18
```

Figure 6

```
Alarm condition : Still in NOCOM, but we run out of buffers .
APPL            : SDM    C
```

```
SDMBIL            : NOSTOR C

XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 AMDI     04SBPT  NODLOG     .        1 SPM      .        .         ...      .      SDM
  *C*                                *C*                                          *C*
 POST                 OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL          TOPSIP
  0 Quit                .       .      SysB     .       .     NOSTOR.
  2 Post_                              *C*                     *C*
  3
  4                   AMA :       Bkup  Pri:         InSv  Rec:         InSv
  5                                     Bkup:       Bkup  Comm:        InSv
  6 TST
  7 Bsy
  8 RTS
  9 Conf_
 10            DispAL
 11 DispAL     critical:ALL:NOCOM:Communication to SDM cannot be established.
 12            critical:AMA:NOBAK: ERROR, no space on Backup volumes.
 13 Status     critical:AMA:NOSTOR:No memory available to buffer records.
 14 Query      major: AMA: BAKUP: Backup time exceeds 10 minutes.
 15
 16
 17 Audit
 18
```

2.5.2 “Add "clli" command to BILLMTC Interface”

This feature will add a new functionality whereby a new command ("clli") will be introduced under the SBA RMI subsystem to retrieve the CLLI name from BILLMTC Interface.

This command is hidden and does not appear on the BILLMTC level. The command is available from all BILLMTC level as a non menu command. The user can run the "clli" command from any level of BILLMTC interface to get the CLLI name.

"clli" command is not available either as a numbered command or as a menu command, unlike other commands in BILLMTC interface. The user has to directly enter the command “"clli"” at the BILLMTC interface from any level to retrieve the CLLI name.

2.5.2.1 "clli" command

Command name: "clli"

Command description:

"clli" command displays the current information about the CLLI connected with the sdm. The command should be used at BILLMTC level. The command is case in-sensitive.

The "clli" command response will be,

<Core CLLI Name>

Command Format:
clli

Parameters
None

Response :
<Core CLLI Name>

Figure 7 The “clli” command executed from BILLMTC level of BILLMTC interface

```
BILLMTC            MSH4_CALL_SERVER
```

```
 0 Quit
 2 Set
 3
 4 CONFSTRM

 5
 6
 7
 8 APPL
 9 Query
10 Mib
11 DispAl
12 Displogs
13 FILESYS
14 SCHEDULE
15 TOOLS
16 TAPE
17 Help
18 Refresh
root       > clli
Time  09:28
```

Figure 8 The “clli” command executed from BILLMTC; SCHEDULE level of BILLMTC interface.

```
SCHEDULE       MSH4_CALL_SERVER
 0 Quit
```

```
 2 Set
 3
 4
 5
 6
 7 Add
 8 Change
 9 Delete
10 List
11 RTB
12
13
14
15
16
17 Help
18 Refresh
root       >  clli
```

2.5.2.2 Help for clli

Help for “clli” command is available at all levels. To get the help for clli, enter the “help” without parameters at any billmtc level, help for “clli” command will be displayed along with the help for other commands.

Figure 9 The “help”command issued at BILLMTC interface

```
BILLMTC      The commands available at this level....
 0 Quit       0 Quit     -> Quits the current level
 2 Set        2 Set      -> Sets context
 3            3
 4 CONFSTRM   4 CONFSTRM -> Enters CONFSTRM level
 5            5
 6            6
 7            7
 8 APPL       8 APPL     -> Enters APPL level
 9 Query      9 Query    -> Displays current state of streams
10 Mib       10 Mib      -> Sets and gets MIB objects
11 DispAl    11 Dispal   -> Displays all current SDM alarms
12 Displogs  12 Displogs -> Displays logs not yet sent to CM
13 FILESYS   13 FILESYS  -> Enters FILESYS level
14 SCHEDULE  14 SCHEDULE -> Enters SCHEDULE level
15 TOOLS     15 TOOLS    -> Enters TOOLS level
16           16 TAPE     -> Enters TAPE level
17 Help      17 Help     -> Available commands with syntax
18 Refresh   18 Refresh  -> Refreshes the screen
  maint      MORE...
Time  12:16
```

Figure 10 Press enter to continue for the help for “clli”

```
BILLMTC      clli:  Displays core CLLI
 0 Quit
 2 Set
 3
 4 CONFSTRM
 5
 6
```

```
 7
 8 APPL
 9 Query
10 Mib
11 DispAl
12 Displogs
13 FILESYS
14 SCHEDULE
15 TOOLS
16
17 Help
18 Refresh
  maint      >
Time  12:17
```

2.6 Hardware requirements

None

2.7 Limitations and restrictions

2.7.1 “SBA Backup Alarms Precedence“ will put the following limitations.

Any critical alarm raised by SBA under the SDMBIL banner will be masked by the backup alarm if any. To see all the alarms (critical, major, minor) raised by SBA, the user will have to invoke the DispAl command to see the list of all SBA alarms.

2.7.2 “Add "clli" command to BILLMTC Interface“ will put the following limitations

The command is available only at BILLMTC level. The command can not be used at SDMRLOGIN level.

2.8 Interaction.

NA

2.9 Logs (LG)

Not Applicable

2.10 Data schema (DS)

Not Applicable

2.11 Alarms (AL)

Not Applicable

2.12 Command interface (BILLMTC)

2.12.1 New/modified commands

New command has been added through this “Add "clli" command to BILL-MTC interface.

Table 1

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/ BILLMTC level name	MENU/NON-MENU /HIDDEN
clli	NEW	-	BILLMTC	HIDDEN

2.13 Modules changed:

Table 2 “SBA Backup Alarms Precedence”

	Module name	Details
1	BUFMAPI	Details of the changes will be given during the coding.
2	BUFDEVI	Details of the changes will be given during the coding.
3	BUFBAKI	Details of the changes will be given during the coding.

Table 3 Add "clli" command to BILLMTC interface

	Module name	Details
1	RMIcll.H	Details of the changes will be given during the coding.
2	RMIcl.C	Details of the changes will be given during the coding.
3	RMIsm.C	Details of the changes will be given during the coding.
4	datareformat	Details of the changes will be given during the coding.

3: Functional Description (FN): A00001650

3.1 Feature name

SBA Patch Size Reduction

3.2 Description

SDM SBA application is delivered to Nortel's customers as SDM_SBA.DMS500 and SDM_AFT.DMS500 filesets in the previous releases. The total size of the two filesets are greater than 160[1] MB (40MB + 120MB). When there is a change in SBA base code to fix issues, the whole 120 MB fileset must be packaged and delivered. In an extreme case, if a change is in base MIB functional component, the two filesets of 160MB will also be required if AFT is installed. In most of the cases, SBA base fix does not require the AFT fileset to be delivered to the customers.

In the past releases, SBA fix filesets were stored into 4Gg DAT tape and shipped to customer sites. However, Nortel's SDM fix delivery method have been migrating from shipping MNCL tape(s) to downloading the filesets (or packages) into the customer networks via IP protocols (i.e. electronic delivery).

In cases where customer only has 28.8K modem in the networks, the total download time would be more than 9 hours (120MB / 211Kbytes per minute[2]) for SBA SDM_SBA.DMS500 fileset and more than 3 hours for AFT fileset. If the customers has high speed cable connection, then the time for SBA and AFT would be 3 hours and 48 minutes; and 55 minutes respectively. Therefore, the "fix filesets" would not be downloaded completely before maintenance window had expired even though the customer has high speed connection.

This feature reduces SBA/AFT deliverable(s)[3] size by de-coupling ACE and eighteen SBA base libraries code from SBA/AFT executable(s). The SBA base shared libraries will be packaged into the SBA fileset/package. The ACE library code will be packaged separately. The fileset/package for ACE is named as SDM_ACE.dist in AIX platform and SDM_ACE_5.3.0.0.pkg in Solaris platform.

3.3 Hardware Requirements or Dependencies

No new hardware required

[1]The size information are taken from 19.72.0.0 NCL load. The SDM_SBA.DMS500-19.69.0.0.tape file is 120,287,232 bytes and the SDM_AFT.DMS500-19.69.0.0.tape file 40,079,360 bytes.
[2]Data taken from "SDM Wellness Patching 3.1" presentation.
[3]The deliverable(s) could be the whole SBA in a single fileset or a number of filesets of different sizes.

3.4 Software Requirements or Dependencies

SBA and AFT requires ACE fileset and package in AIX and Solaris platforms respectively. The ACE fileset/package contains ACE shared libraries. This is the only copy of ACE library code. The filesets/packages must be installed in the following orders[1]:

1. ACE
2. SDM_SBA.DMS500
3. SDM_AFT.DMS500

Similarly, the packages/filesets must be removed in the following orders.

1. SDM_AFT.DMS500
2. SDM_SBA.DMS500
3. ACE

In case ACE fileset is upgraded/patched, SBA and AFT fileset must be BSY/RTS after the new ACE fileset is installed otherwise SBA and AFT software will be running with the order version of ACE. This might lead to run time problems.

3.5 Limitations and restrictions

- SBA/AFT cannot be installed before ACE is installed.
- ACE cannot be removed before SBA/AFT are un-installed from the system. In CBM, the Solaris “pkgrm” command does not prevent user from removing lower layer package that are needed by other upper layer package. In other words, there is nothing stopping user from removing ACE fileset even if SBA/AFT have not been un-installed. It is important to note that if a user removes ACE package from the system, SBA/AFT will not function.
- SBA/AFT must be BSY/RTS if ACE is upgraded on the system.

3.6 Interactions

None

[1]The installations follows the standard CBM and nSDM procedure

3.7 Applicable customer facing sections

Fault Management

- Logs __N/A____
- Alarms __N/A____

Configuration

- Data Schema ___N/A____
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

3.8 Glossary

Term	Description
ACE	The ADAPTIVE Communication Environment. “It freely available, open-source object-oriented (OO) framework that implements many core patterns for concurrent communication software”

4: Functional Description (FN): A00001742

4.1 Feature name

OMDD Capacity Enhancements

4.2 Description

Currently, the SDM OMMD application can handle, in 2.5 minutes, 6000 tuples for five minute transfer period and 8000 tuples for office transfer period, each tuple containing a maximum of 32 registers.

This activity enhances the capacity of the present OMDD application so that a transfer of 12000 OM tuples (containing a maximum of 32 registers each) from the core to the downstream OSS can be done in less than 2.5 minutes for the office transfer period. This activity also addresses any storage issues on the SDM that may arise while handling the transfer of 12000 OM tuples.

4.2.1 Improving OMDD performance

In real time, the OMDD application performs the following operations :

1. Receives OM data from the CM (through OM access).
2. Converts it into CSV files based on the Report Registration configurations.
3. Sends out the CSV files to the downstream OSS using FTP.

This activity addresses the performance issues of OMDD in the above steps.

The following are achieved by this activity.

1) Improved OMDD performance in terms of the overall latency time from the core to the OSS, which is reduced from the current >3.5 minutes to less than 2.5 minutes for 12000 tuples with 32 registers each.

2) Improved OMDD performance in terms of CPU utilization.

4.2.2 Improving OMDD storage handling

File Transfer schedules are used by the report registrations to schedule the transfer of OM report files downstream. Once a file transfer schedule event occurs, the report files associated with the event, as defined in the report registration, are FTP'd downstream. They are then moved from the */omdata/closedNotSent* directory to the */omdata/closedSent* directory.

The OM files progress through the following states:

- Open — OM files continue to be written to the file.
- ClosedNotSent — No more OM's are being written to the file. The file has not been transferred to any OSS.
- ClosedSent — The ftp event which transfers the file to the downstream OSS is completed.

The OM files in closedSent and closedNotSent are currently audited every midnight. At that time, a check is made for the File Retention period.Those files in */omdata/closedSent* which have reached the the File Retention Period for */omdata/closedSent* are deleted. Also, those files in */omdata/closedNotSen*t which have reached the File Retention Period for */omdata/closedNotSent* are deleted. If */omdata* is 100% full before the midnight,then OMDD cannot open any new files.

This activity increases the frequency of auditing */omdata* from once in 24 hours to once in 12 hours. During that time, in addition to checking for files with expired retention period, a check is made to see if */omdata* usage exceeds the threshold value of 60 %. If the usage is above 60 % a custlog is generated to make the customer aware of the low storage available. In the next audit, if */omdata* usage is above 70%, files in */omdata/closedSent* will get deleted. If even after deleting all files in */omdta/closedSent*, the usage is above 50%, the files */omdata/closedNotSent* are deleted one by one (the oldest file first), until the usage falls below 50%. A custlog is generated for each closedNotSent file that gets deleted.

The following is the custlog that is generated when audit finds that /omdata usage exceeds 60 %:

SDM330 MAJOR TBL SDM OM FILE RETENTION
ODM:Audit finds /omdata usage exceeds 60 percent. OM files will be deleted in the next audit if the usage exceeds 70 percent.

The following is the custlog that is generated when a file in */omdata/closedNotsent* is deleted by audit to make more than 50 % available space in */omdata.*

SDM331 MAJOR INFO SDM OM FILE RETENTION
ODM: The file <filename> from closeNotSent direcory deleted by audit to free up space in /omdata.

- Where <filename> is the name of the file deleted from */omdata/closedNotSent.*

4.3 Hardware Requirements or Dependencies

- SDM with SDM20 load.
- CM with SDM connectivity.

4.4 Software Requirements or Dependencies

- Table Access Service and OM Access Service application on the SDM should be present and should be in INSV state.
- CM - SDM connectivity should be up.

4.5 Limitations and restrictions

This activity does not introduce any new limitation or restriction on the OMDD application. The performance of the application can degrade if either the SDM or the core is heavily loaded.

4.6 Interactions

None

4.7 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	___N/A___
Configuration	
Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

4.8 Glossary

Term	Description
CM	Computing Module
ODM	OMD Manager
OM	Operational Measurements
OMDD	OM Data Delivery
OMUI	OM User Interface
SDM	SuperNode Data Manager

5: Functional Description (FN): A00001743

5.1 Feature name

Syslog Consolidation for Succession.

5.2 Feature Synopsis

This activity uses the Log Delivery application to

- Provide a single consolidated northbound log feed for all the components in a succession node.
- Implement the initial phase of Lost Log detection for Non-CM logs.
- Enhance the Lost Log indication mechanism for CM logs.
- Enhance the Log Delivery application's capacity to handle bursty traffic of logs.
- Enhance Logroute tool to make it more user friendly and to remove redundant processing.

5.3 Functional Overview

5.3.1 Introduction

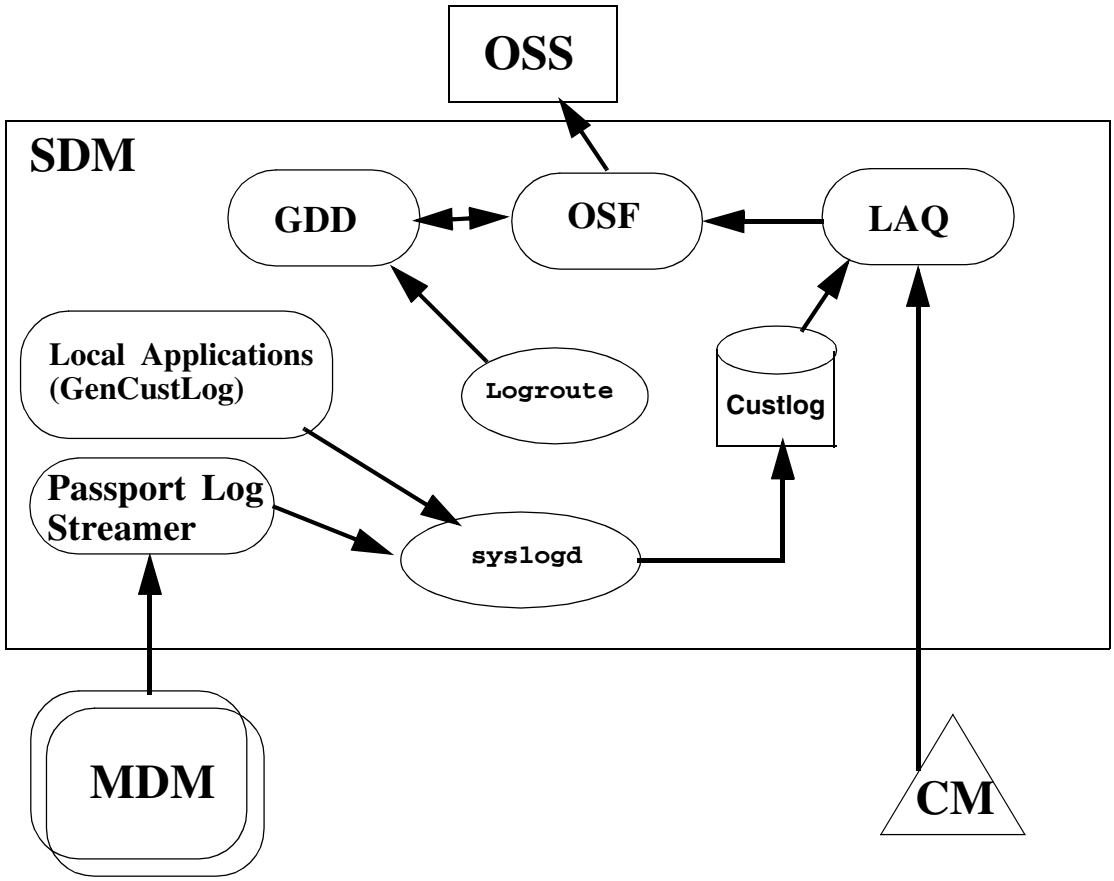
The Log Delivery Application is used to collect CM logs and Customer logs, format them in either STD or SCC2 format and route them to remote (Telco) hosts, printers and/or UNIX files.

Log Delivery application has two components - **LAQ** and **OSF**. LAQ is the component which is used to receive the logs from the CM and custlog file, parse the logs and send them to OSF.

OSF receives these logs, formats the logs (into STD or SCC2 depending on the format configured for that device in Logroute) and sends the logs to the configured destination (that is, whether these logs need to be written to an UNIX file or sent to some remote destination).

Figure 1 shows the current design of the Log Delivery Application.

Figure 1 Interaction Between Component



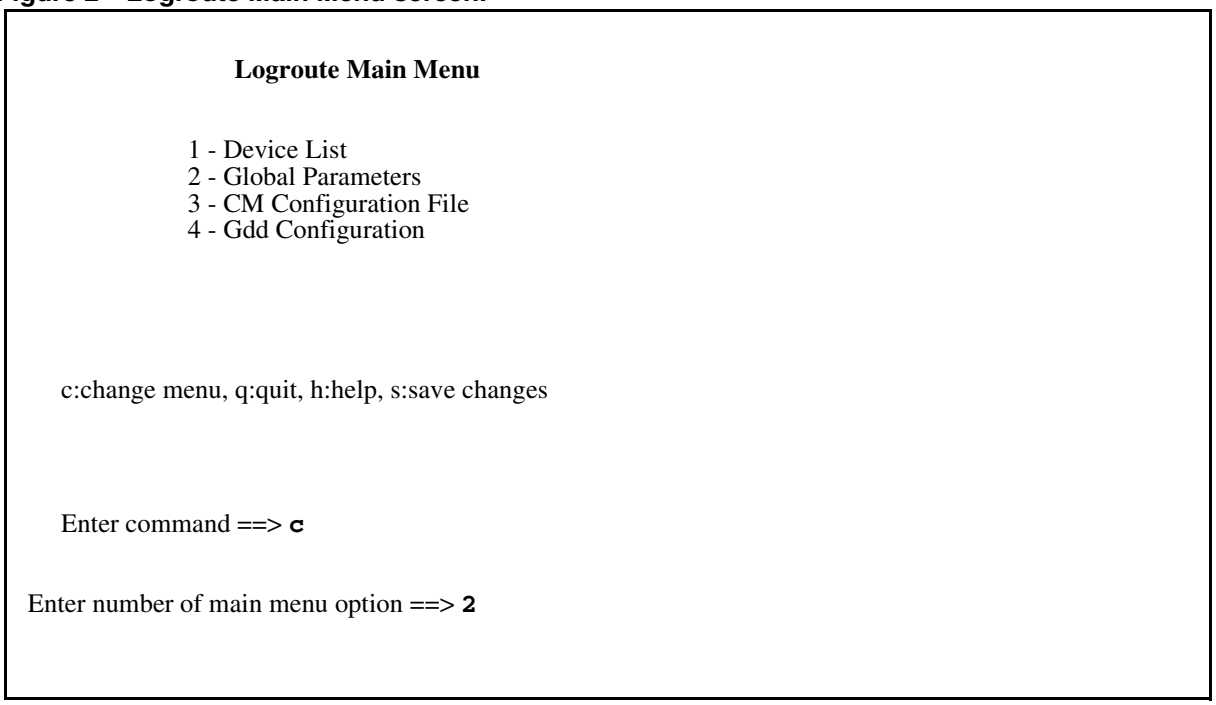
5.3.2 Current Problem scenarios

The Current Log Delivery application contains the following problem scenarios.

5.3.2.1 Logroute Command Line User Interface

The User Interface of Logroute is not very user-friendly currently. For example, consider the Main menu screen as shown in figure 2.

Figure 2 Logroute Main Menu screen.



The user has to first enter “c” and then the number of the main menu option to access any sub-menu. The same is the case for all sub-menu screens. This is a strenuous way to access the sub-menus and information in the logroute tool.

5.3.2.2 Lost Log Detection

The Log Delivery application, currently does not have a mechanism to detect stoppage or any gap in the delivery of logs from a given Element Manager or a Network Element Application. Hence, the client is not notified regarding the loss of logs.

5.3.2.3 Conforming to Standards Specified

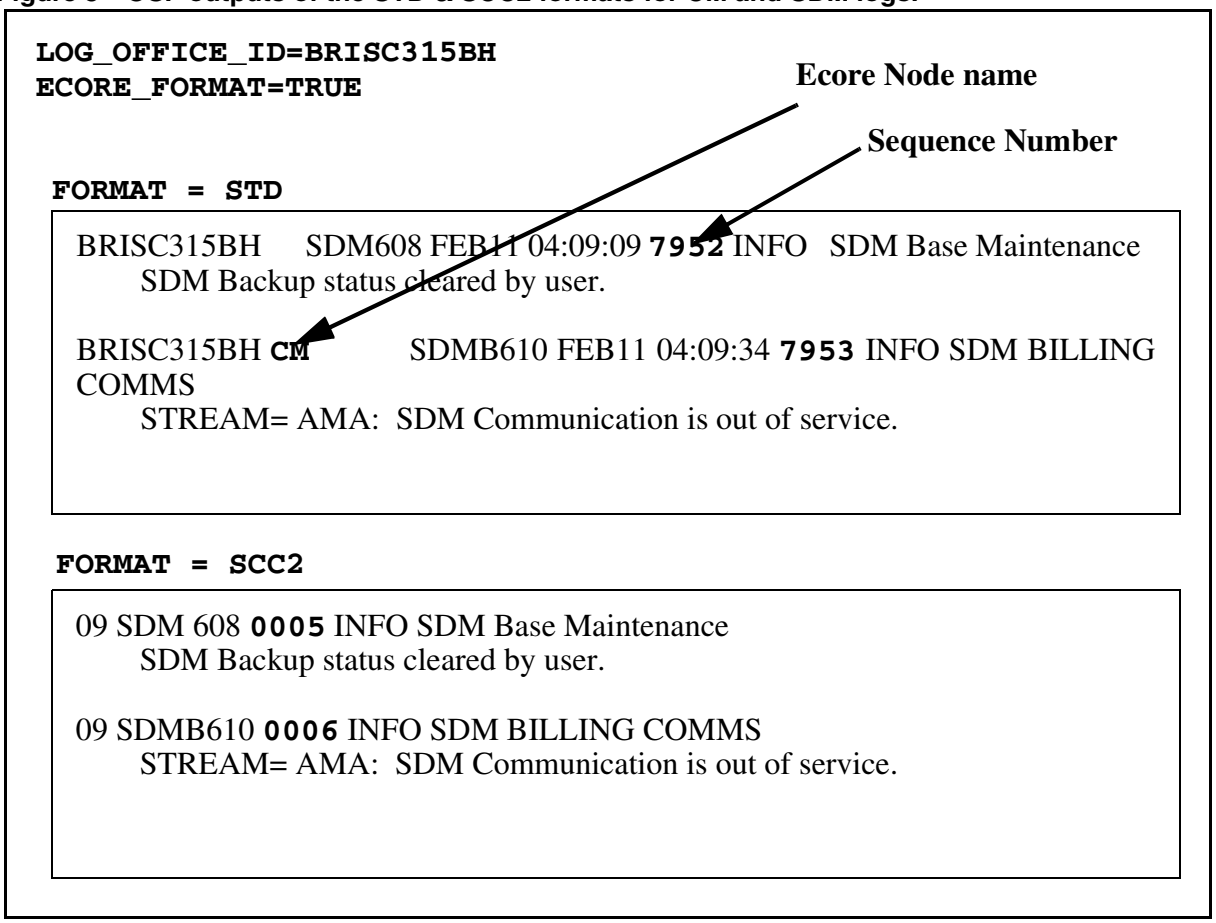
The Logroute tool is used to define the parameters of each individual OSS feed.

- Format : STD or SCC2
- Who originates connection : OSS (TCP), OSS (TCPIN)
- Port number used : <xxxxx>
- Filtering rules (by log name and number) :

OSF retrieves this information and based on the configured format, converts them into STD or SCC2 logs. The inconsistency of the OSF output for different formats can be noticed in Figure 3.

Assuming that the LOG_OFFICE_ID (that identifies the switch generating the log) and ECORE_FORMAT (flag used to decided the display of the node name) in the DMS table OFCVAR have been set.

Figure 3 OSF outputs of the STD & SCC2 formats for CM and SDM logs.



From the above figure it can be clearly seen that the application does not follow the same format for all logs.

- The Node name (ECORE Node name) is not displayed for logs generated on Non-CM node.
- Logs generated in SCC2 format do not display the originator of the log (Example :- CM or SDM).
- The generated Sequence number does not conform to the Dual Sequence Number (Global and Device Sequence Number) format specified in the log standards. Currently the Global and Device Sequence number format is not implemented. The number is implemented as a single four digit Sequence Number.

- The logs generated in the configured format (STD or SCC2) by the Log Delivery Application do not conform to the customer document.

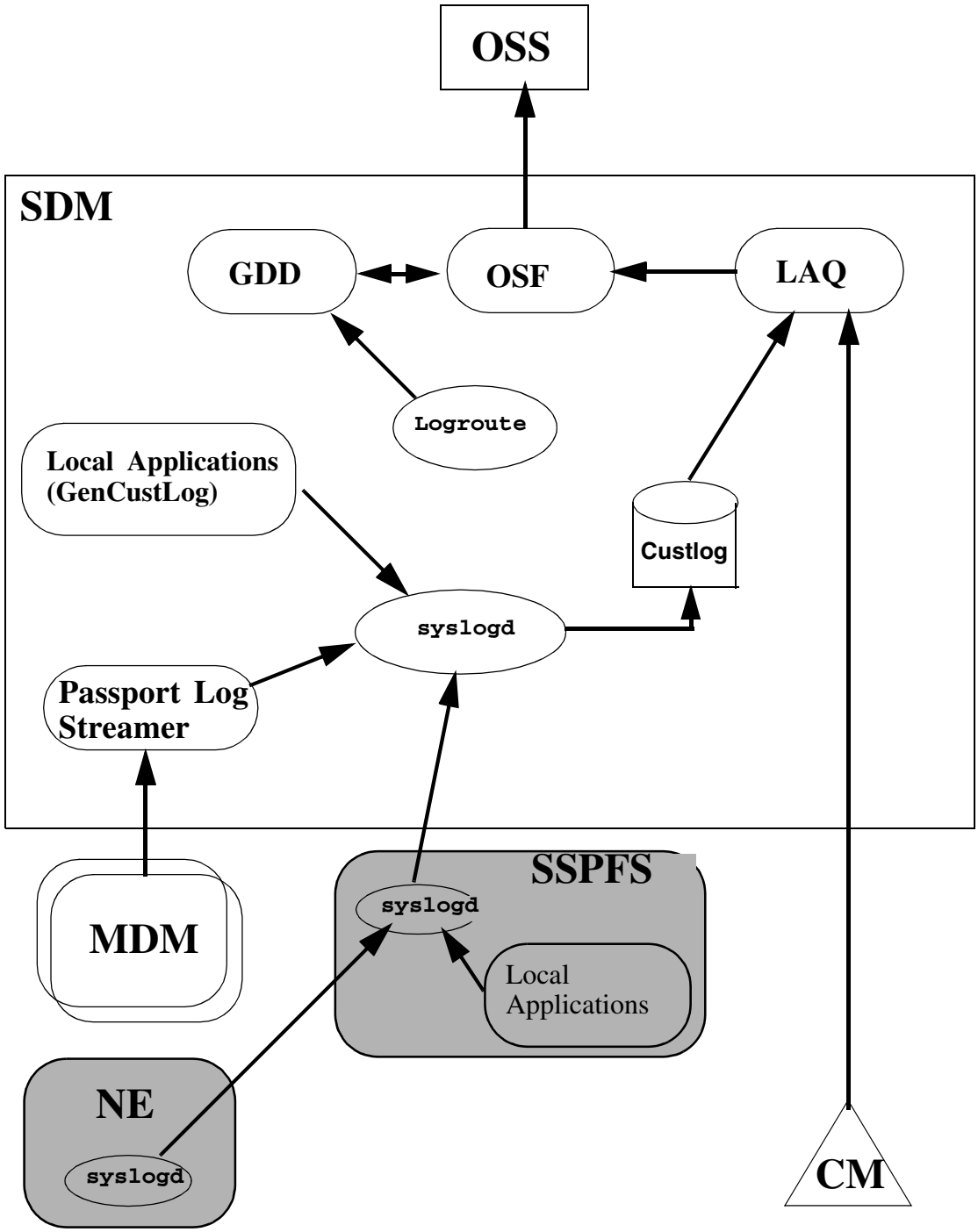
The OSF needs to be upgraded to support the standard log format (either STD or SCC2).

The purpose of the feature is to resolve the current problem scenarios mentioned above.

5.3.3 Functional Components.

The proposed architecture to support customer logs being fed into the syslogd daemon from remote syslogd daemons is as below.

Figure 4 Interaction Between Components



The implementation of this feature can be broken down into the following main components.

5.3.3.1 Logroute Command Line User Interface (Logroute CLUI).

- Modify the existing screens to enable the user to access and modify the existing information more easily.
- Add new menus and screens to make the Logroute CLUI more user-friendly.

5.3.3.2 Upgrade all SDM applications to use GENCustLog API Version 2 to generate custlogs.

- Enhance the current custlog to contain information required for lost log detection.
- Upgrade SDM applications to reflect the new custlog format.

5.3.3.3 Implement initial phase of lost log detection in Log Delivery for Non-CM logs.

- Poll logs from custlog file.
- Detect whether any logs have been lost.
- If lost logs detected, generate log to indicate lost log detection.

5.3.3.4 Enhance lost log indication mechanism for CM logs.

- Enhance Log Delivery so that an internal log is generated when a lost log scenario is detected for CM logs.

5.3.3.5 Enhance Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD formats with ECORE node id enabling and Dual Sequence numbering.

- Enhance Log Delivery to support LOG_OFFICE_ID enabling from SDM.
- Enhance Log Delivery to support ECORE Node Id enabling from SDM.
- Enhance Log Delivery to support Dual Sequence Numbering for logs.
- Enhance STD and SCC2 formats to incorporate the above enhancements (LOG_OFFICE_ID, ECORE Node ID, Dual Sequence Numbering).
- Retain the Pre-SDM20 behaviour of Log Delivery with respect to formats.

5.3.3.6 Handle bursty generation of logs.

- Ensure that the new functionality does not adversely impact the Log Delivery performance and also ensure that the application stays in conformance to the specified limits.

5.4 Feature Description

5.4.1 Introduction

As mentioned above, the main task of this feature consists of

- Implementing code changes to make Logroute CLUI more user-friendly.
- Upgrading all SDM applications to use GenCustLog API version 2 to generate custlogs.
- Implementing initial phase of lost log detection in Log Delivery for Non-CM logs.
- Enhancing the lost log indication mechanism for CM logs.
- Enhancing Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD formats with ECORE node id enabling and dual sequence numbering.
- Handling bursty generation of logs.

5.4.2 Enhancing Logroute CLUI

Logroute tool used for configuration of device and log routing information. This information is used to collect the data in the desired format (STD or SCC2) and send the collected logs to the configured destination. The tool can also be used for configuring the device such that, it receives only the desired logs.

Currently the Logroute tool is not very user-friendly (as described in section 2.3.2.1). This feature seeks to enhance the Logroute tool, so that the user is able to obtain or modify the information more easily.

The enhanced user interface is explained in more detail in the configuration document (optcn.fm) of this feature.

5.4.3 Upgrading SDM applications to use GenCustLog API version 2 to generate custlogs.

5.4.3.1 Enhancement to SDM log generation API

On the SDM, the SDM Log Generation (SLG) API will be upgraded to generate the new custlog format GenCustLog version 2. This new custlog format will enhance the content of the logs flowing through syslogd and stored in custlog to include the following data.

- Node Id :- Identifies where the log originated.
- Host Name :- Identifies the machine which generated the log.
- Application Name :- The application which generated the log.
- Sequence Number :- The number of the log which the application has generated.

To initialize and generate the above data, the following options are provided.

- init_cust_log :- This function is used to set/reset the sequence number and application name of a particular application.
- gen_cust_log_v2 :- This function is used by the applications to generate custlogs in the new GENCustLog Version 2 format.
- gen_foreign_cust_log_v2 :- This function is used by applications that generate a custlog on behalf of a remote system.

5.4.3.2 Updation of all SDM applications

The SDM applications will be updated so that they will call the GenCustLog Version 2 function to generate a custlog.

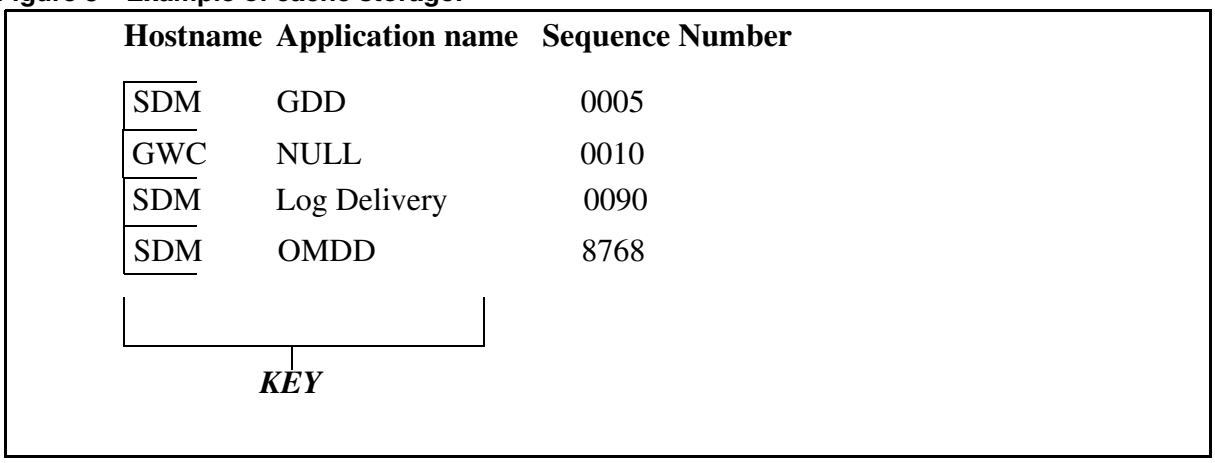
As part of this updation, the application will provide the application name as one of the parameters of the new CustLog version. The application name must be unique.

5.4.4 Implementing initial phase of lost log detection for Non-CM logs

This requirement is achieved by implementing a new lost log detection functionality.

- Create a cache (data structure) to store the latest Hostname, Application name and Sequence number of the custlog generated by each application.

Figure 5 Example of cache storage.



- Log Delivery polls for logs in the custlog file and retrieves the logs.
- While formatting the logs, retrieve the Host name, Application name and Sequence number of the log.
- If the Sequence number of the log has been set to zero abruptly, the LAQ recognizes it as a reset log for that application. accordingly it re-initializes the application details in the cache.
- Validate the sequence number retrieved from the log to the sequence number stored in the cache.
- If the sequence number is found to be breaking the flow (i.e it has skipped by more than one number). Then it is assumed that the following events could have happened.
  a. The logs missing could have been lost.
  b. The logs have arrived out of sequence and the missing logs can be expected to arrive immediately.

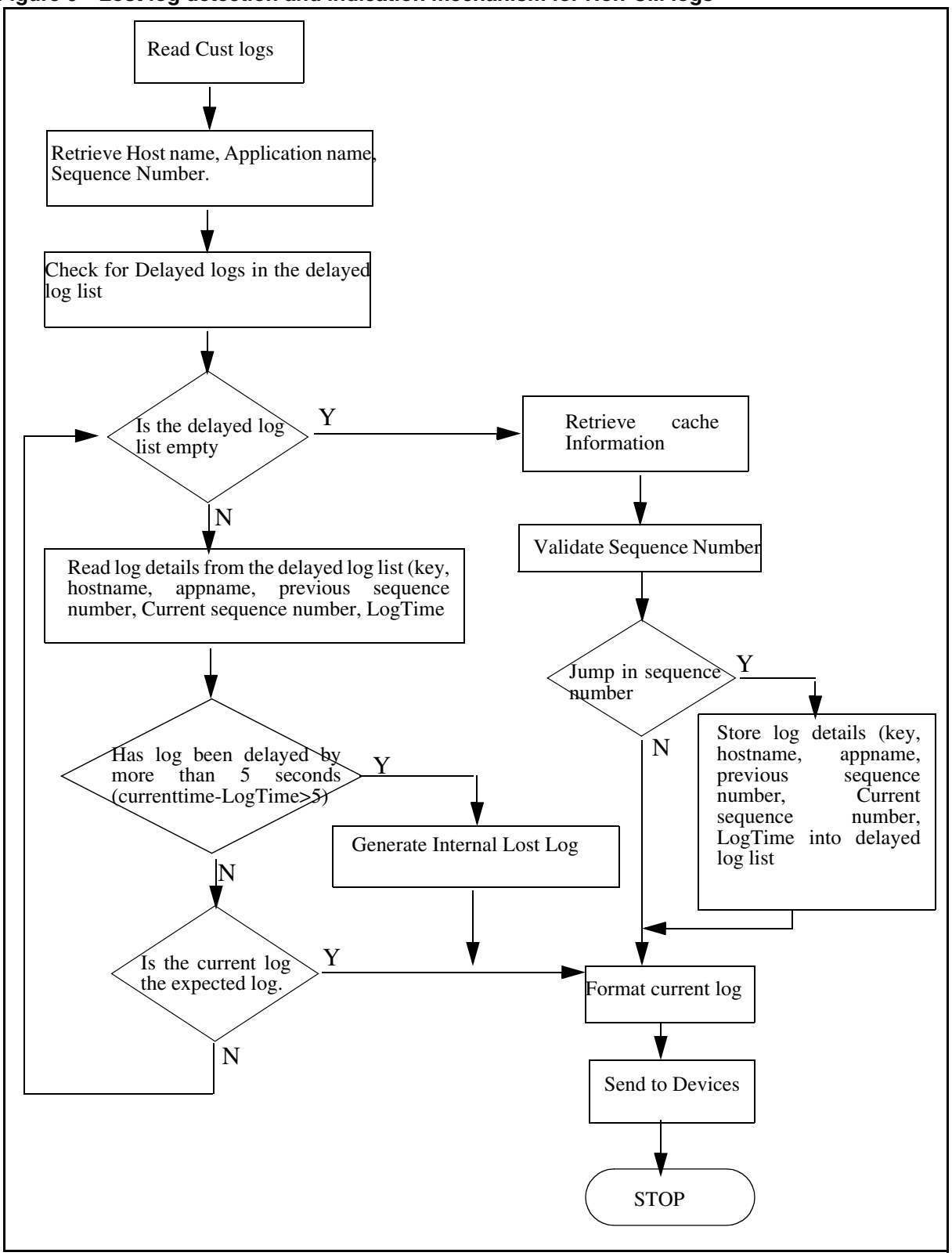
In order to take the above scenario into consideration, the details of the latest log (Key, hostName, appName, previous sequence number, current sequence number) received are stored as a list in a RWSlistCollectables structure “RWDelayedLogCheckList” along with the time when the log was received. When the next log is received, the following steps are followed.

i. The list is checked to see if the log is an expected log or not.
ii. If the log is expected then it is generated.
iii. If the LAQ does not receive the log in less than 5 seconds, an internal log is generated to indicate that a log has been lost.

If LAQ detects that a lost log scenario exists, it will generate a “<number> Logs lost for application <application name> on host <hostname>” log, else it will increment the sequence number.

If the search is not successful, LAQ assumes that log is the first log from that application and accordingly inserts the log details into the RogueWave structure.

Figure 6 Lost log detection and indication mechanism for Non-CM logs



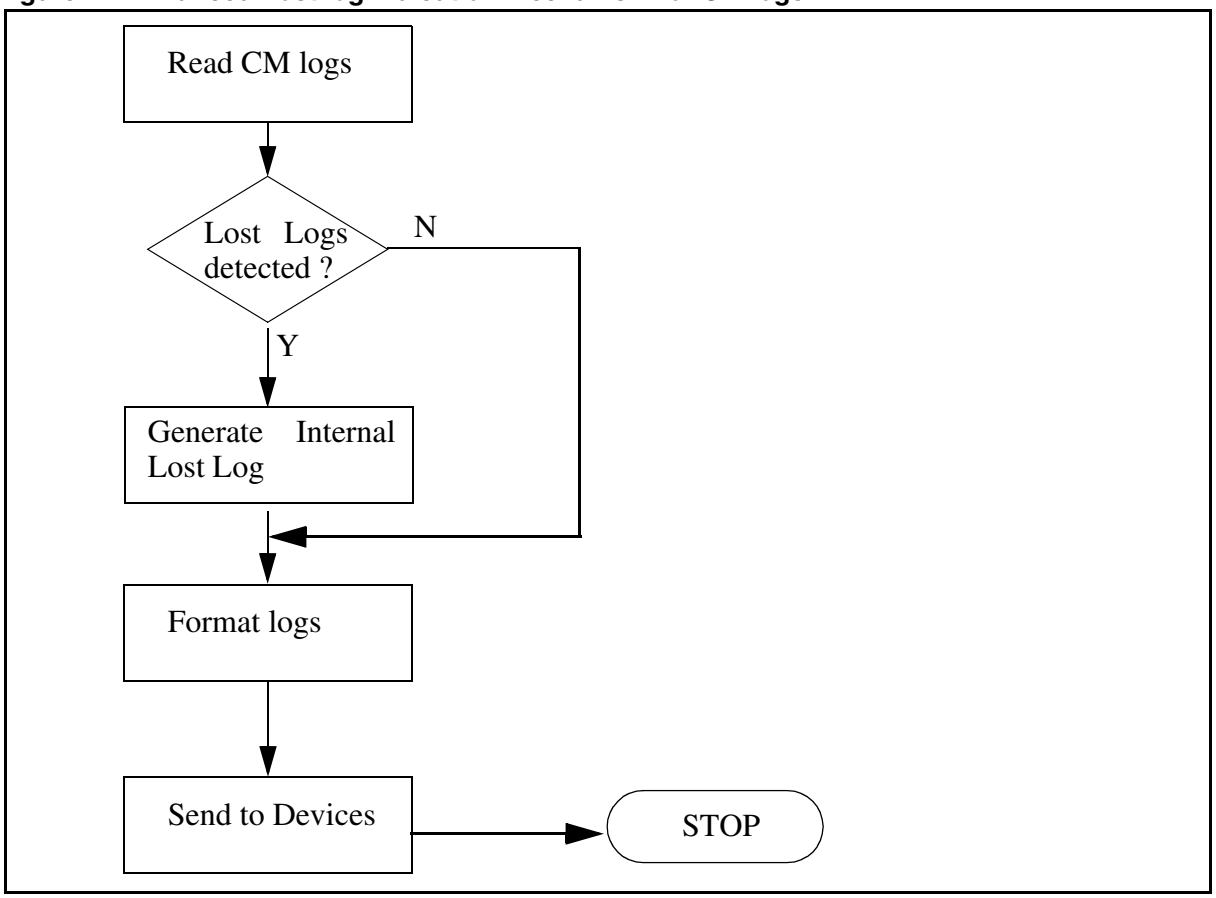
5.4.5 Enhancing the lost log indication mechanism for CM logs.

The current lost log indication mechanism existing for CM logs is enhanced as below.

- Log Delivery application detects a lost log scenario.
- The application generates an internal log indicating the number of logs lost.
- The internal log is passed to the OSF to be sent to all the devices.

This will ensure that the user will be intimated regarding lost logs immediately.

Figure 7 Enhanced Lost log indication mechanism for CM logs



5.4.6 Enhancing Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD format with ECORE node id enabling and Dual Sequence numbering.

5.4.6.1 LOG_OFFICE_ID enabling

The `LOG_OFFICE_ID` parameter currently existing on the core will henceforth be configured from the "`Global Parameters`" level of the logroute tool. This parameter will be the same for all logs and streams. The LOG_OFFICE_ID will be configured as shown in the following figure.

Figure 8 Logroute tool for configuring LOG_OFFICE_ID option.

```
                    Global Parameters

 1 - LOG_OFFICE_ID                : BRISC315BH
 2 - Buffer size (number of logs)   : 150
 3 - Reconnect timeout value (secs)  : 15
 4 - Lost logs threshold (NT only)   : 100
 5 - Incoming end of line character  : 10
 6 - Outgoing end of line characters  : 10 13
 7 - Start of log characters         : 10 13
 8 - End of logs characters          :  10 13
 9 - Number of days to keep log files  : 5
10 - Maximum size of a log file (Meg)  : 40
11 - Maximum size action             : STOPDEV
12 - Help
13 - Return to Main Menu

        Select Option ==> 1

Enter Log_office_Id [CORE-COMPAT]==> BRISC315BH
```

5.4.6.2 Ecore node id enabling

In order to provide the Ecore Node Name for all the logs, the option shall be provided on the SDM through the Logroute tool.

The option to set the **`Ecore`** ON/OFF is to be on a per stream (device) basis and will be provided through the logroute tool. For example, if the user is configuring a TCP-IN device, the device parameters needed for configuring are as shown in the following figure.

Figure 9 Logroute tool for configuring Ecore option.

```
                    TCP-IN Device


                1 -  REMOTE IP      : any
                2 -  PORT           : 8550
                3 -  FORMAT         : STD
                4 -  ECORE          : ON
                5 -  Log Routing
                6 -  Help
                7 -  Return to Main Menu.


          Select Option :- 4

Enter Ecore option (ON or OFF) ==> ON
```

5.4.6.3 Dual Sequence Numbering

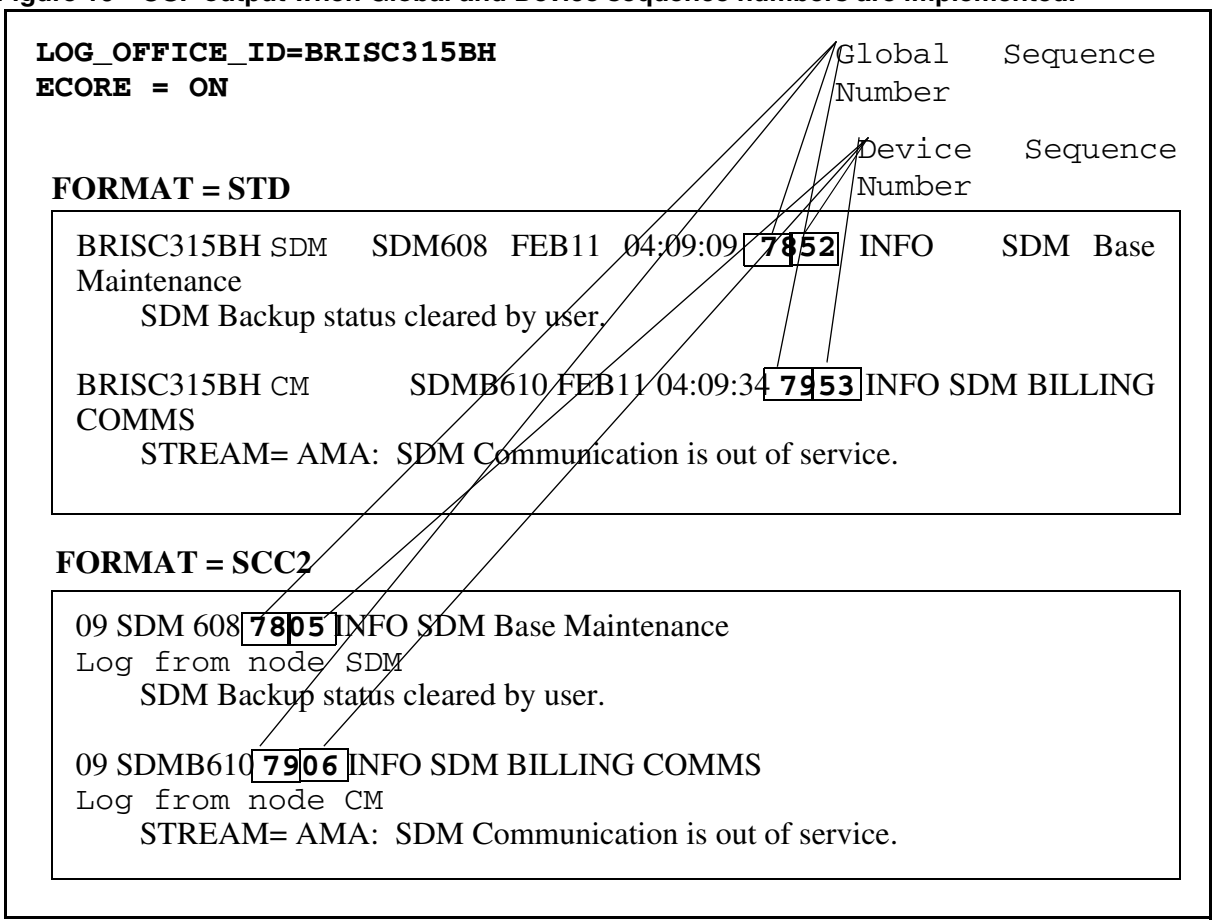
The sequence number field will be implemented as two distinct fields that will be incremented from 0 to 99.

Global Sequence number as a field of 2 digits (from 0 to 99) and
Device Sequence number as a field of 2 digits (from 0 to 99).

The Global Sequence number of the log will be the same for all the devices and the device sequence number varies based on the device. The LAQ will generate the Global Sequence number and the OSF will generate the Device Sequence number for all logs. These number have a maximum value of 99 after which they are reset to 0.

The diagram below illustrates the usage of the Global Sequence number and the Device Sequence number

Figure 10 OSF output when Global and Device sequence numbers are implemented.

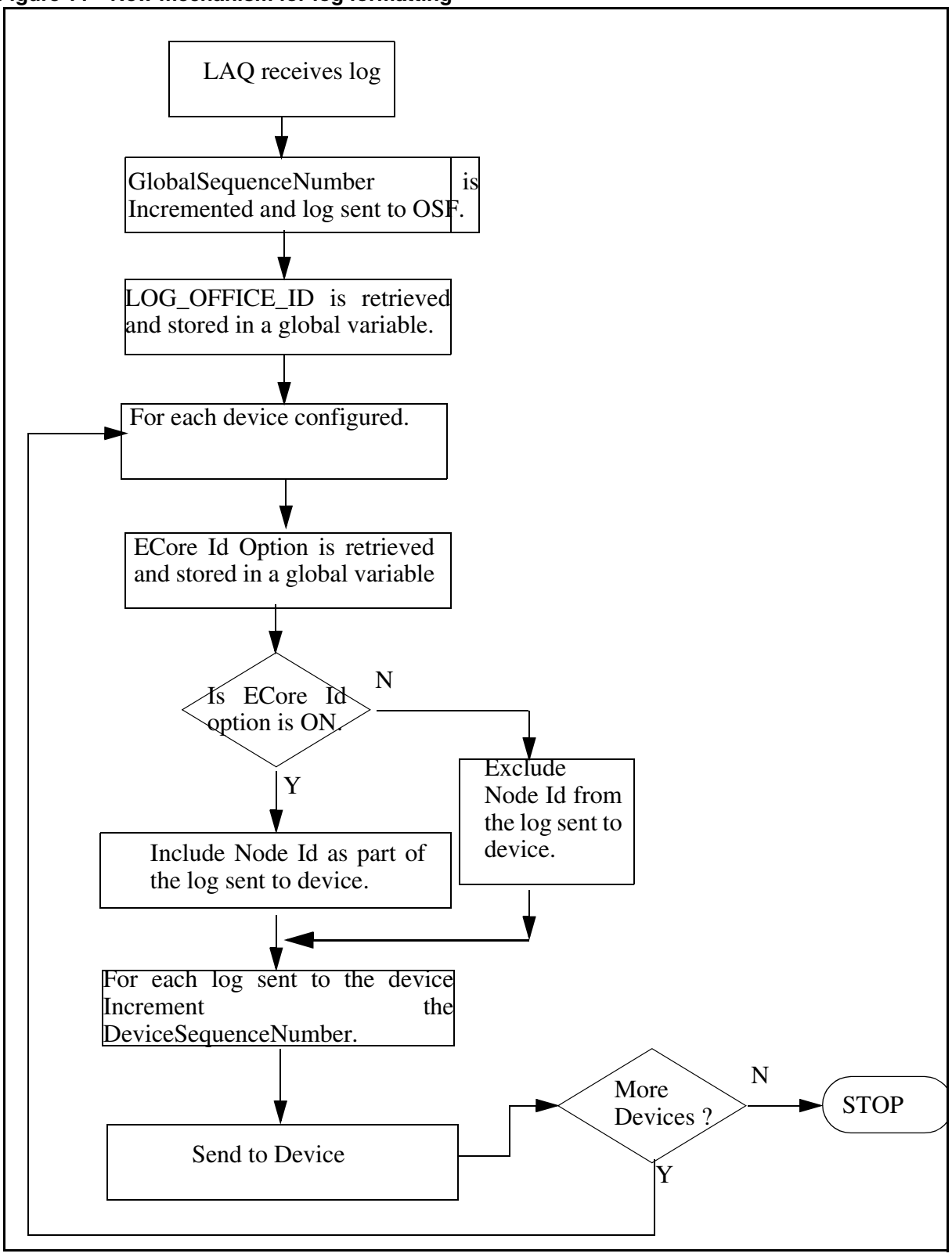


5.4.6.4 Update current formats to support proposed changes

The following changes will be made to Log Delivery to support the ECore Node Id and Dual Sequence numbering.

- When the LAQ receives a new log, the Global Sequence number will be retrieved, incremented and stored.
- After formatting the log, LAQ will send the log to the OSF. Upon receival of the log the OSF will retrieve LOG_OFFICE_ID and ECORE node id option.
- If the Ecore option is ON, then the node name which is part of the log information received by OSF will be included in the log sent to the device.
- If the Ecore option is OFF, then the node name is ignored.
- For each log which is to be sent to the particular device, the corresponding device sequence number is retrieved and incremented.
- The data is then updated into the log information and sent to the device.

Figure 11 New mechanism for log formatting



5.4.6.5 Retain the Pre SDM20 behaviour of Log Delivery.

The Pre SDM20 behaviour of Log Delivery will be retained in the new formats STD_OLD and SCC2-OLD. User who wish to receive logs without the above changes can select the format to be either STD-OLD or SCC2-OLD.

5.4.7 Handling bursty generation of logs.

This feature ensures that the new functionality does not adversely impact the Log Delivery performance and also ensure that the application stays in conformance to the specified limits

5.5 Hardware Requirements or Dependencies

- Fault tolerant SDM with SDM20/CS2E07 load.
- CM (XACORE / BRISC / 3PC)
- Succession Network Elements like GWC, MDM.
- NSDM

5.6 Software Requirements or Dependencies

- Connectivity between various Network Elements and SDM should be up.
- Connectivity between SDM and CM should be up.

5.7 Limitations and restrictions

5.8 Interactions

5.9 Applicable customer facing sections

Fault Management

Logs	___X___
Alarms	_____

Configuration

Data Schema	_____

User Interface ___X___

Element Management _____

Security _____

Service Order _____

Office Parameters ___X___

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

5.10 Glossary

Term	Description
API	Application Programming Interface
OSF	Operation System Interface
LAQ	Loq Acquisition
CLUI	Command Line User Interface
NE	Network Element
OSS	Operation Support System
DMS	Digital Multiplex System
CPU	Central Processing Unit
MDM	Multi-Service Data Manager
CM	Computing Module
SDM	SuperNode Data Manager
SSPFS	Succession Solaris Platform Foundation Software
STD	Standard
SCC2	Switching Control Centre 2
STD - OLD	PRE-SDM20 STD format Compatible
SCC2 - OLD	PRE-SDM20 SCC2 format Compatible

6: Functional Description (FN): A00001847

Note: The FN/CN sections for activity A00001847 include the related information for a number of activities due to the close association of all these activities. The activities that are included in this group are:

- A00001847 - ABI Expansion Datafill
- A00001909 - ABI Trunk Support for RCC
- A00001936 - MG9K ABI Expansion - Node and Link Mtc

Note: Within this document the terms LTC and LGC are used, which the terms LTCI and LGCI are not used. The use of the term LGC or LTC implies both the ISDN and non-ISDN capable versions of these peripherals unless otherwise stated. This is done to avoid confusion as the LGCI and LTCI do not actually exist from a datafill perspective, they are simply LGCs and LTCs with an ISDN capability.

6.1 Feature name

A00001847 - ABI Expansion Datafill

6.2 Description

This activity expands the set of supported Peripheral types that can be provisioned off an ABI card in a MG9000 gateway. In SN05 the initial ABI work provided support for the LGC (ISDN only) and SMA2 peripheral types. With this activity we will provide the capability for customers to provision not only SMA2 and LGC (ISDN only) peripherals off the ABI card, but also LTC and LGC (non-ISDN) peripherals on the ABI.

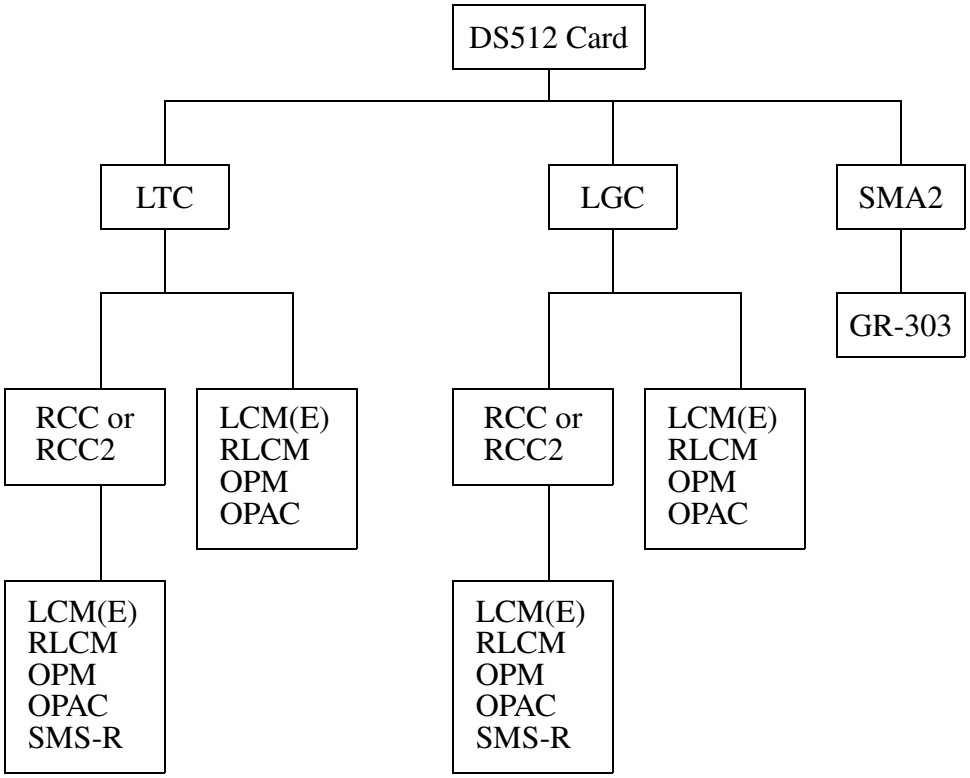
Also, as part of this activity the set of line concentrating devices (LCDs) supported off the above list of host peripherals has been expanded. When this activity is complete the set of supported LCDs will include:

1. LCM
2. RLCM
3. OPM
4. OPAC
5. RSC
6. RSCS

Also, the remotes (RSC/RSCS) will support the SMS-R (Mode I or II) as a subtending device, along with the LCM, RLCM, OPM, and OPAC. It should also be noted that whenever the RSC and RSCS are mentioned both the single and dual configurations are implied. The following figure shows the allowed

configurations for SN06.2. Note that this is a logical not a physical representation, and that it is not possible to host all these devices on a single DS512 card in the MG9000.

Figure 1 Supported SN06.2 Configurations



The main customer visible changes for this activity will be the ability to provision the EXTDS512 optional field as part of the tuple in table LTCINV for the LTC Peripheral Type (the LGC was already supported in SN05 although only for ISDN lines). This optional field is used to identify the IP Address of the ABI Card and the Gateway Controller that the peripheral is "hosted" off (the GWC must be datafilled in table SERVRINV prior to entering this information). Prior to this release if this optional field was added to an LTC tuple an error would result.

Note: Although only ISDN lines were supported on the ABI-based LGC in SN05, the EXTDS512 attribute could be added to any LGC (including normal LGCs without ISDN lines) without an error resulting. Thus this is unchanged in SN06.2 except that we have added official support for the other LCCs on the LGC.

A full description of the table control changes is available in the Data Schema section of this document (part of the Configuration chapter).

6.2.1 Supported Line Class Codes and Features

The following tables lay out the supported Line Class Codes (LCCs) and features that are supported on the new ABI XPMs as well as what is currently supported. This table includes the terms LTCI and LGCI, but it should be noted that the LCCs supported are the same as for the LTC/LGC with the exception of the ISDNKSET.

Note: Although the subtending devices are not listed in the following list, they will support all the LCCs applicable for their host peripheral. For example, an RCC subtending an ABI based LTC will be able to support all the LCCs listed for the LTC in the table below, assuming that the RCC supports that LCC in a legacy environment.

Table 7 LCC Support

	MG9000	MG9000 ABI Supported Peripherals			
LCC	**Lines**	**ESMA**	**LGCi**	**LTCi**	**LGC/LTC**
1FR	S	SN05	SN06.2	SN06.2	SN06.2
1MR	S	SN05	SN06.2	SN06.2	SN06.2
2WW	SN05	SN05	SN06.2	SN06.2	SN06.2
CDF	S	SN05	SN06.2	SN06.2	SN06.2
CFD	S	SN05	SN06.2	SN06.2	SN06.2
EOW	SN05	SN05	SN06.2	SN06.2	SN06.2
ETW	SN05	SN05	SN06.2	SN06.2	SN06.2
IBN	S	SN05	SN06.2	SN06.2	SN06.2
ISDNKSET	-	SN05	SN05	SN06.2	-
INW	S	SN05	SN06.2	SN06.2	SN06.2
M5008	S	SN06.2	SN06.2	SN06.2	SN06.2
M5009	S	SN06.2	SN06.2	SN06.2	SN06.2
M5112	S	SN06.2	SN06.2	SN06.2	SN06.2
M5208	S	SN06.2	SN06.2	SN06.2	SN06.2
M5209	S	SN06.2	SN06.2	SN06.2	SN06.2
M5212	S	SN06.2	SN06.2	SN06.2	SN06.2
M5216	S	SN06.2	SN06.2	SN06.2	SN06.2
M5312	S	SN06.2	SN06.2	SN06.2	SN06.2

Table 7 LCC Support

	MG9000	MG9000 ABI Supported Peripherals			
LCC	**Lines**	**ESMA**	**LGCi**	**LTCi**	**LGC/LTC**
M5316	S	SN06.2	SN06.2	SN06.2	SN06.2
OWT	S	SN05	SN06.2	SN06.2	SN06.2
PBM	S	SN05	SN06.2	SN06.2	SN06.2
PBX	S	SN05	SN06.2	SN06.2	SN06.2
PSET	S	SN06.2	SN06.2	SN06.2	SN06.2
RES	S	SN05	SN06.2	SN06.2	SN06.2
TWX	SN05	SN05	SN06.2	SN06.2	SN06.2
ZMD	S	SN05	SN06.2	SN06.2	SN06.2
ZMZPA	S	SN05	SN06.2	SN06.2	SN06.2

Note: An “S” under the MG9000 Lines column means that this LCC was supported on the MG9000 prior to SN05 (SN05 was the first release for ABI XPMs).

Note: A “-” in any cell of the above table means that the LCC is not supported for that XPM type. For example, ISDNKSET is not supported on LGC/LTC XPMs as these XPMs are not ISDN capable.

The following LCCs are only supported on legacy, not on the MG9000 or ABI based XPMs:

1. 10FR - Ten-party flat rate, residence and business
2. 2FR - Two-party flat rate, residence and business
3. 4FR - Four-party flat rate, residence and business
4. 8FR - Eight-party flat rate, residence and business
5. ATA - Coin, coin first (prepay)
6. CSD - Circuit-switched digital service
7. CSP - Coin, semi-postpay
8. DATA - Data unit
9. PDATA - POTS data unit

Here is the list of supported services on ABI peripherals.

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
18-Button Add-On for Meridian M5000 Series	-	S	-
900 Client	SN06	SN06	SN06
Access to Messaging	SN05	SN05	SN06
Access to Messaging Deny	SN05	SN05	SN06
Additional Call Offering Unrestricted	-	-	SN05
Additional Functional Calls	-	-	SN05
Advanced Intelligent Network	S	S	SN05
Advanced Intelligent Network DN	S	S	SN05
Aggregate CND Recording	-	-	SN05
Aggregate RND Recording	-	-	SN05
Agent Status Lamp	-	S	-
AIN Message Waiting	-	S	SN05
Alternate Service Provider		SN05	SN06
Analog Display Services Interfaces		-	-
Anonymous Caller Rejection	S	S	SN05
Answer Agent Key	-	S	-
Answer Emergency Key	-	S	-
Associated Group Assignment	-	-	SN05
Auto Lamp Refresh	-	-	SN05
Automatic Answer Back	-	S	SN06
Automatic Call Back	S	S	SN05
Automatic Call Distribution	S	S	-
Automatic Call Distribution Not Ready	S	S	-
Automatic Dial	-	S	SN05
Automatic Display	-	S	-
Automatic Line	S	S	SN05
Automatic Message Accounting Test Call Capability	S	S	SN05
Automatic Recall	S	S	SN05
Automatic Recall Dialable Directory Number	S	S	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Automatic SPID Selection	-	-	SN05
Automatic Time and Charges	S	S	SN05
Basic Business Group ISDN	-	-	SN05
Bearer Capability	-	-	SN05
Block Called Party Number	-	-	SN05
Block Callling Party Number	-	-	SN05
Bridged Night Number	S	S	SN05
Bulk Calling Line Identification	SN05	SN05	SN06
Busy Lamp Field for Meridian Business Sets	-	S	-
Call Agent	-	S	-
Call Appearance Call Handling	-	-	SN05
Call Busy Intragroup or Channel Bus Interface	S	S	SN05
Call Covering	-	SN05	-
Call Forward / Interface Busy	-	-	SN05
Call Forward Fraud Prevention Override	S	S	-
Call Forward Indication (CWT only prior to SN06)	SN06	-	-
Call Forward Timed for CFB	S	S	SN05
Call Forward Timed for CFD	S	S	SN05
Call Forwarding	S	-	-
Call Forwarding Busy	S	S	SN05
Call Forwarding Busy Internal Calls Only	S	S	SN05
Call Forwarding Busy Line	S	-	-
Call Forwarding Busy Unrestricted	S	S	SN05
Call Forwarding Do Not Answer (Business Sets)	S	S	SN05
Call Forwarding Do Not Answer (RES)	S	-	-
Call Forwarding Do Not Answer for Hunt Group	S	S	-
Call Forwarding Do Not Answer Unrestricted	S	S	SN05
Call Forwarding Do Not Answer Variable Timer	S	S	SN05
Call Forwarding Fixed	S	S	SN05
Call Forwarding Group Do Not Answer	S	-	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Call Forwarding Intragroup	S	S	SN05
Call Forwarding MADN Secondary Member	S	S	SN05
Call Forwarding on a Per Key Basis	-	S	-
Call Forwarding per DN per call type	-	-	SN05
Call Forwarding Remote Access	S	S	SN05
Call Forwarding Simultaneous/Screening	S	S	-
Call Forwarding Universal	S	S	SN05
Call Forwarding Usage Sensitive Denial	S	-	-
Call Forwarding Validation per DN call type	-	-	SN05
Call Hold	S	-	-
Call Logging	SN05	-	-
Call Management Group	SN05	-	-
Call Park	S	S	SN05
Call Pickup	S	S	SN05
Call Redirect	S	-	-
Call reference busy limit	-	-	SN05
Call Screening, Monitoring, and Intercept	SN06	SN06	-
Call Supervisor	-	S	-
Call Transfer	S	S	SN05
Call Transfer Warning	S	S	-
Call Waiting	S	S	SN05
Call Waiting Conference	S	-	-
Call Waiting Exempt	S	S	-
Call Waiting Intragroup	S	S	SN05
Call Waiting Originating	S	S	-
Call Waiting Ringback	S	S	-
Called party address	-	-	SN05
Called Party Hold	SN05	-	-
Calling Id Delivery and Suppression Delivery	-	-	SN05
Calling Id Delivery and Suppression Suppression	-	-	SN05

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Calling Line Identification	S	S	SN05
Calling Line Identification with Flash	S	-	-
Calling Name Delivery	S	-	SN05
Calling Name Delivery Blocking	S	-	SN06
Calling Number Delivery	S	-	SN05
Calling Number Delivery Blocking	S	-	-
Calling Number Delivery Blocking Override	-	SN05	SN05
Calling party address	-	-	SN05
Calling Party Identification	S	S	-
Cancel Call Waiting	S	S	-
Carrier Toll Denied	S	S	SN05
Circuit mode data	-	-	SN05
Circular Hunt	S	S	SN05
Common Control Switching Arrangement	S	-	-
Conference and call-to-call transfer	-	-	SN05
Conference Join	-	SN05	-
Control Multiple Call Forwarding	S	S	SN05
Controlled Interflow	-	S	-
Convert	S	-	-
Customer Originated Trace	S	S	SN05
Customer Originated Trace with AMA	S	S	-
Customer Data Change	SN06.2	SN06.2	-
Cutoff on Disconnect	S	-	-
Default Logical Terminal	-	-	SN05
Default bearer capability	-	-	SN05
Default directory number	-	-	SN05
Denied Call Forwarding	S	S	SN05
Denied Incoming Calls	S	S	SN05
Denied Origination	S	S	SN05
Denied Termination	S	S	SN05

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Deny Access to CLASS Features	S	-	-
Deny Call Redirect	S	-	-
Deny Call Waiting	S	-	-
Deny Call Waiting Conference	S	-	-
Deny CSMI	SN06	-	-
Deny In-Session Activation	S	S	SN06
Deny Suppressed Ringing Access	S	-	-
Deny three-way calling?usage sensitive	S	-	-
Detailed privacy change allowed recording	-	-	SN05
Dial Call Waiting	S	S	-
Dialable Directory Number	S	-	-
Dialed Number Identification Delivery	S	S	-
Digitone	S	-	-
Directed Call Park	S	S	SN05
Directed Call Pickup	S	S	SN05
Directed Call Pickup Barge-In	S	S	SN05
Directed Call Pickup Barge-In Exempt	S	S	SN05
Directed Call Pickup Exempt	S	S	SN05
Directory Number Hunt	S	S	SN05
Display	-	S	-
Display Agent Status	-	SN05	-
Display Option for Aries	-	S	-
Display Queue Status	-	SN05	-
Display Queue Threshold	-	SN05	-
Distinctive Ringing	S	S	SN05
Distinctive Ringing/Call Waiting	S	S	-
Distributed Line Hunt	S	S	SN05
DN Sharing Multi Terminal	-	-	SN06
Do Not Disturb	S	S	SN05
Downloadable softkeys for ADSI set	SN05	-	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Drop last add-on member	-	-	SN05
EKTS Hold	-	-	SN05
Electronic key Telephone System	-	-	SN05
Emergency Key	-	S	-
Enhanced WATS Access Line	S	-	-
Enhanced WATS Access Line for IntraLATA	S	-	-
Essential Line	S	S	SN05
Exclude External Calls from Call Forwarding	S	S	SN05
Exclude Intragroup Calls from Call Forwarding	S	S	SN05
Executive Busy Override	S	S	SN05
Executive Busy Override Exempt	S	S	SN05
Executive Message Waiting	S	S	-
Extended Call Management	S	S	-
Extension Bridging	S	-	-
Extension/Add-On	-	SN05	-
Fast Transfer	-	S	-
FAX-Thru Service	S	-	-
Feature Group	S	S	SN05
Feature Group S	S	S	-
Feature Keys	-	S	SN05
Flash Ignore	S	-	-
Flexible calling	-	-	SN05
Flexible calling deactivate conference facility	-	-	SN05
Forced Agent Availability	SN05	SN05	-
Free Number Terminating	S	S	SN05
Full Carrier Toll Deny for International Carriers	S	S	-
Ground Loop Test Cancel	SN06.2	-	-
Ground Start	S	-	-
Group Intercom	S	S	SN05
Group Intercom All Calls	-	S	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
High layer compatibility	-	-	SN05
Hotel/Motel	S	-	-
In Call Service Deactivation	S	S	-
Inhibit Line Busy	S	S	SN05
Inhibit Ring Reminder	S	S	SN05
In-Session Activation	S	S	SN06
In-Session Activation Deactivation	S	S	SN06
Inspect Key	-	S	-
Intercom (Business Sets)	-	S	SN05
Intercom (Single-Party Revertive Calling)	S	-	-
InTER-LATA Full Carrier Toll Denied	S	S	SN05
Internal/External Call Forwarding Busy	S	S	SN05
Internal/External Call Forwarding Do Not Answer	S	S	SN05
International Primary Carrier	S	S	SN05
Intra-LATA Full Carrier Toll Denied	S	S	SN05
IntraLATA PIC	S	S	SN05
ISDN Bearer Capibility Routing	=	-	SN05
ISDN service recording recording in AMA	-	-	SN05
Key Set Music on Hold	-	S	SN06
Key Short Hunt	-	S	SN05
Last Number Redial	S	S	SN05
Last Number Redial Associated with Set	-	S	SN05
Leave Message	-	S	SN05
Line Music on Hold	S	S	SN06
Line of Business	-	S	-
Line Overflow to DN	S	S	SN05
Line Overflow to Route	S	S	SN05
Line Study	S	S	SN05
Local Call Detail Recording	S	S	SN05
Local Number Portability Test	S	-	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Local Service Provider Account Owner	S	-	SN05
Local Service Provider Switch Owner	S	-	SN05
Long Distance Signal Activate	S	-	-
Long Distance Signal Option	S	-	-
Long Distance Signal Ring	S	-	-
Long Distance Signal Tone	S	-	-
Lower Layer compatibility	-	-	SN05
M536 36-Button Add-On for Meridian M5000 Series	-	S	-
MADN (Multiple Appearance Directory Number)	S	S	SN05
MADN Ring Forwarding Manual	-	S	SN05
Make Set Busy	S	S	SN05
Make Set Busy Intragroup	S	S	SN05
Malicious Call Hold	-	S	SN05
MDN Lamp	S	S	-
MDN Member Display	S	S	SN05
MDN Member Name	S	S	SN05
MDN Release	S	S	SN05
MDN Ring Forwarding	S	S	SN05
Meridian Business Set Station Camp-On	-	S	-
Message Deactivation	SN05	SN05	SN06
Message Waiting	S	S	SN05
Message Waiting Indication	-	S	-
Message Waiting Query	-	S	-
Migrate	SN06	SN06	SN06
Multi-Line Hunt	S	S	SN05
Multi-Party Bridging	S	-	-
Multi-point End Office Configuration	-	-	SN05
Mute	Legacy	S	-
Name Display	S	S	SN05
Negate Partial Ground Start Diagnostics	SN06.2	-	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Network Facilities Access	SN05	SN05	-
Night Service	-	S	-
No Double Connect	SN06.2	SN06.2	SN06.2
No Hazard Test	SN06.2	-	-
No Line Insulation Test	SN06.2	-	-
No Cancel Call Waiting Without Call Waiting	S	-	-
No Deny	S	-	-
No Receiver Off-Hook Tone	S	S	SN06
Number of calls allowed	-	-	SN05
Number of DN appearances	-	-	SN05
Observe Agent	S	S	-
On Demand B-channel	-	-	SN06
Operator Number Identification	S	S	SN05
Originating Line Select	-	S	-
OUTWATS	S	-	-
Overflow Register (Software)	S	-	-
Overide Call Forward on Account Codes	S	-	-
Parameter Donwloading	-	-	SN05
Permanent Hold	S	-	SN05
Pilot DN Billing	S	S	-
Plug-Up (Trouble Intercept)	S	S	SN05
PORT	S	S	SN05
Power Features	-	S	-
Preferential Hunting	S	S	-
Prevent Delete Option	S	S	SN05
Primary InterLATA Carrier	S	S	SN05
Privacy Change Allowed CIDS	-	-	SN05
Privacy for MADN	-	S	SN05
Privacy Release	-	S	SN05
Private Business Line	-	S	SN05

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Protocol Version Control	-	-	SN05
Provide charge number for calling number	-	-	SN05
PVN Priority Line	S	S	SN06
Query Busy Station	-	S	-
Query Time and Date	-	S	-
Quick Conference Key	-	S	-
Rapid Messaging BRI	-	-	SN05
Rate Area	S	-	SN05
Reason Display	-	S	SN05
Received Digits Billing	S	S	-
Redirecting number delivery	-	-	SN05
Redirecting number pivacy for ISDN CFW	-	-	SN05
Remote Message Indicator	S	-	SN06
Remote Message Register for Local Calls	SN06	-	-
Remote Message Register for Toll Calls	SN06	-	-
Repeated Alert	-	S	-
Requested Suspension	S	S	SN05
Residential Call Hold	S	-	-
Restricted Sent Paid	S	S	SN05
Ring Again	S	S	SN05
SCWID with Disposition	S	-	-
Secondary Directory Number	S	-	-
Secondary Language	S	S	SN05
Security	S	S	SN05
Selective Call Acceptance	S	S	SN05
Selective Call Forwarding	S	S	SN05
Selective Call Rejection	S	S	SN05
Series Completion	S	S	SN05
Service Group	S	S	SN05
Set Based Lamp Field	-	S	-

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Set Model	S	S	-
Short Timed Release Disconnect	S	-	-
Simplified Message Desk Interface	S	S	-
Simultaneous Ringing	SN05	SN05	-
Single Line BRI	-	-	SN05
Single-line Queuing	-	S	-
Single-Line Variety Package	S	-	-
SMDI-SMDI Calling Number Delivery	S	-	-
Special Billing	S	S	SN05
Special Delivery Service	S	S	SN06
Special Delivery Service Deny	S	S	SN06
Speed Calling Long	S	S	SN05
Speed Calling Long List L30	S	-	-
Speed Calling Long List L50	S	-	-
Speed Calling Short	S	S	SN05
Speed Calling Short List	S	-	-
Speed Calling User	S	S	SN05
Spontaneous Call Waiting Id	S	-	-
Station Controlled Conference	S	S	SN05
Station Message Detail Recording	S	S	SN05
Station Origination Restriction	S	S	-
Station Origination Restrictions Controller	S	S	-
Station Specific Authorization Codes	S	S	SN05
Subscriber Activated Call Blocking	S	S	-
Subscriber Line Usage	S	S	SN05
Subscriber Programmable Ringing	S	-	-
Supervisor	S	S	-
Suppress Line Identification Information	S	S	SN05
Suppressed Ringing Access	S	-	-
Suspended Service	S	S	SN05

Table 8 Service Support for ABI XPMs

Service	Non-PSET	PSET	BRI
Talking Call Waiting	SN05	-	-
Terminal Limit	-	-	SN05
Terminal Service Profile Identifier	-	-	SN05
Terminating Billing Option	S	S	SN05
Terminating DN Billing	S	S	-
Terminating Fault Option	S	S	SN06
Terminating Line Select	-	S	-
Terminator Billing Option on Hunt Group	S	-	-
Three-Way Calling	S	S	-
Three-Way Calling Public Announcement	S	S	-
Toll Denial	S	-	-
Toll Diversion	SN05	-	-
Toll Essential	S	S	SN05
Transfer a conference call	-	-	SN05
Translations Plan	S	-	SN05
Uniform Call Distribution	S	S	-
Uniform Call Distribution Logged In Indication	S	-	-
Uniform Call Distribution Login	-	S	-
Voice Mail Easy Access Deny	S	-	SN05
Voice Mail Easy Access Directory Number	S	-	SN05
Voice band information	-	-	SN05
Wake up call ring timeout	S	S	-
Wake-Up Call	S	-	-
Warm Line	S	S	SN05

The following list of services are only supported on Legacy Lines (these services are supported when the associated line is served by a DMS-100

Family host or remote line access peripheral subtended from the CS2000 ENET).

Table 9 Legacy Only Services

Service	Line Option	Comment
1-Meg Modem Service	1MMS	
22-Key Add-On for Aries	M522, M0022	
Asymmetric Digital Subscriber Loop	ADSL	Associated with legacy-side ADSL service Hybrid Centrex groups planned for support in SN05. Allows the console to be legacy served while other group members are on legacy and/or MG9000 lines.
Attendant console and service set	-	
Automatic Identification of Outward Dialing	AIOD	
Automatic Location Identification	ALI	
BRI Caller ID	BRICLID	
Circle Digit	CD0-CD9	Option associated with 8-party and 10-party lines
Closed User Group	CUG	Option associated with DataPath service
Critical Path REStoration	CPR	Option associated with DataPath service
Deny Call Transfer Fraud Prevention	DENYCTFP	
Disconnect Timeout	DISCTO	Option associated with DataPath service
Data Unit Profile	DPR	Option associated with DataPath service
Emergency Service Line	ESL	
Fire Reporting System (Orig and Term)	FRO	
Fire Reporting System (Termination Only)	FRS	
Frequency Selective Ringing	FSR	Associated with multi-party line service
G-Lite	GLITE	
Hands-Free	HF	Option for Nortel proprietary ISDN sets (MD)
Hands-Free Mute	HFMUTE	Option for Nortel proprietary ISDN sets (MD)
Inhibit Make Busy	IMB	
Line Appearance on Digital Trunk PSAP	LDTPSAP	
Line-Ended Public Safety Answering Point	LINEPSAP	
Make Busy Key	MBK	
Man Machine Interface	MMI	Support for Nortel P-Phone Power Feature test tools

Table 9 Legacy Only Services

Service	Line Option	Comment
Manual Line	MAN	Automatic Line service on MG9000 is a suitable substitute
Mute (non-Pset)	MUTE	
Multiple Position Hunt	MPH	
Network Resource Selector	NRS	Option associated with DataPath service
Night Service Directory Number	NSDN	
Overflow Register (Hardware)	OFR	
Packet mode data	PMD	
Random Make Busy	RMB	
Remote Message Register (SD Point)	RMS	
Remote Meter Pulsing	RMP	
Reverse Coin Disposal	RCD	
Softkey	SOFTKEY	Option for Nortel proprietary ISDN sets (MD)
Soft Key Display	SKDISP	Option for Nortel proprietary ISDN sets (MD)
Stop Hunt	SHU	
Subscriber Loop Carrier	SLC	Identifies coin lines resident on a SLC-96 remote
Terminal Management Environment	TME	Support for Nortel P-Phone Power Feature test tools
Uniform Call Distribution Signal Distributor	UCDSD	

2.2.2 Support of ABI RCC Trunks

Also, as part of this activity, trunks will be supported off of RCC/RCC2s subtending any of

- LGC
- LTC

The following trunk types will be supported off of an RCC/RCC2:

- TI
- TO
- T2
- IBNTI
- IBNTO
- IBNT2
- PBX
- PX
- ES

As well, intra-switching will be supported on these RCC trunks.

Note: Trunks are not supported directly on the LTC. Trunking is only supported on RCCs hosted on ABI XPMs. Please see the documentation for activity A00001909 for more information on ABI RCC Trunk support.

2.2.2.1 Trunk Services Support

All Trunk services that are currently supported on the listed trunk types in section 2.2.2, such as ANI outpulsing and operator signals on ES trunks (rering, etc.), will continue to be supported when those trunk are hosted off of an ABI RCC.

2.3 Hardware Requirements or Dependencies

There is no hardware impact associated with this activity.

2.4 Software Requirements or Dependencies

This activity will be implemented in the SN07 stream in the CM, but due to customer requirements will be patched back into the SN06 CM release (officially this is called the SN06.2 release).

There are several other acetifies that are required to complete the support of the additional peripheral types. They include A00001979 - ABI Expansion GWC,

A00001909 - ABI Trunk Support for RCC, and A00001936 - MG9K ABI Expansion - Node & Link Mtc.

2.5 Limitations and restrictions

The following restrictions exist on the new External XPM types added by this activity (it should be noted that all of these restrictions apply to the existing External XPMs as well as the new XPMs and are not new in SN06.2):

- Special Connections are not supported on any External XPM.
- External XPMs do not support broadcast loading or patching, although they do support parallel loading. Broadcast loading and patching are not supported due to the lack of support for IPMLs between the External XPMs.
- The MONTALK LINK command of the Trunk Test Position (TTP) is NOT supported on ABI RCC Trunks. When the MONTALK level is entered with an ABI RCC Trunk posted at the TTP, the MONTALK LISTEN mode is immediately entered. A conference resource is acquired, a two-way connection between the ABI RCC Trunk and conference circuit is made, a two-way connection between the other party in the call and the conference circuit is made, and a one-way listen-only connection is made between the HSET and the conference circuit (i.e. normal MONTALK LISTEN operations). MONTALK TALK is supported on ABI RCC Trunks.
- The T108 and BERT tests of the TTP level of the MAP are supported for ABI RCC Trunks. When the trunk posted at the TTP connects to an ABI RCC Trunk (incoming or two-way), then the loop-back connection will be made at the ABI card of the MG9K Gateway.
- Trunking is not supported directly on an ABI LTC. Trunks should not be provisioned directly on an ABI LTC as they are not supported at this time. Trunks can be provisioned off an RCC hosted on an ABI XPM.

2.6 Interactions

- An MG9000 entering ESA will cause an RCC subtending an ABI-base XPM off the MG9000 to enter into ESA as well. When the MG9000 exits ESA and the C-side links come back into service, then the RCC will also exit ESA.

2.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

- Data Schema ___X__
- User Interface ___X__
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

2.8 Glossary

Term	Description
New term	Definition

7: Functional Description (FN): A00001888

7.1 Feature name

CS2000 Line Test for MG9000 Lines

7.2 Description

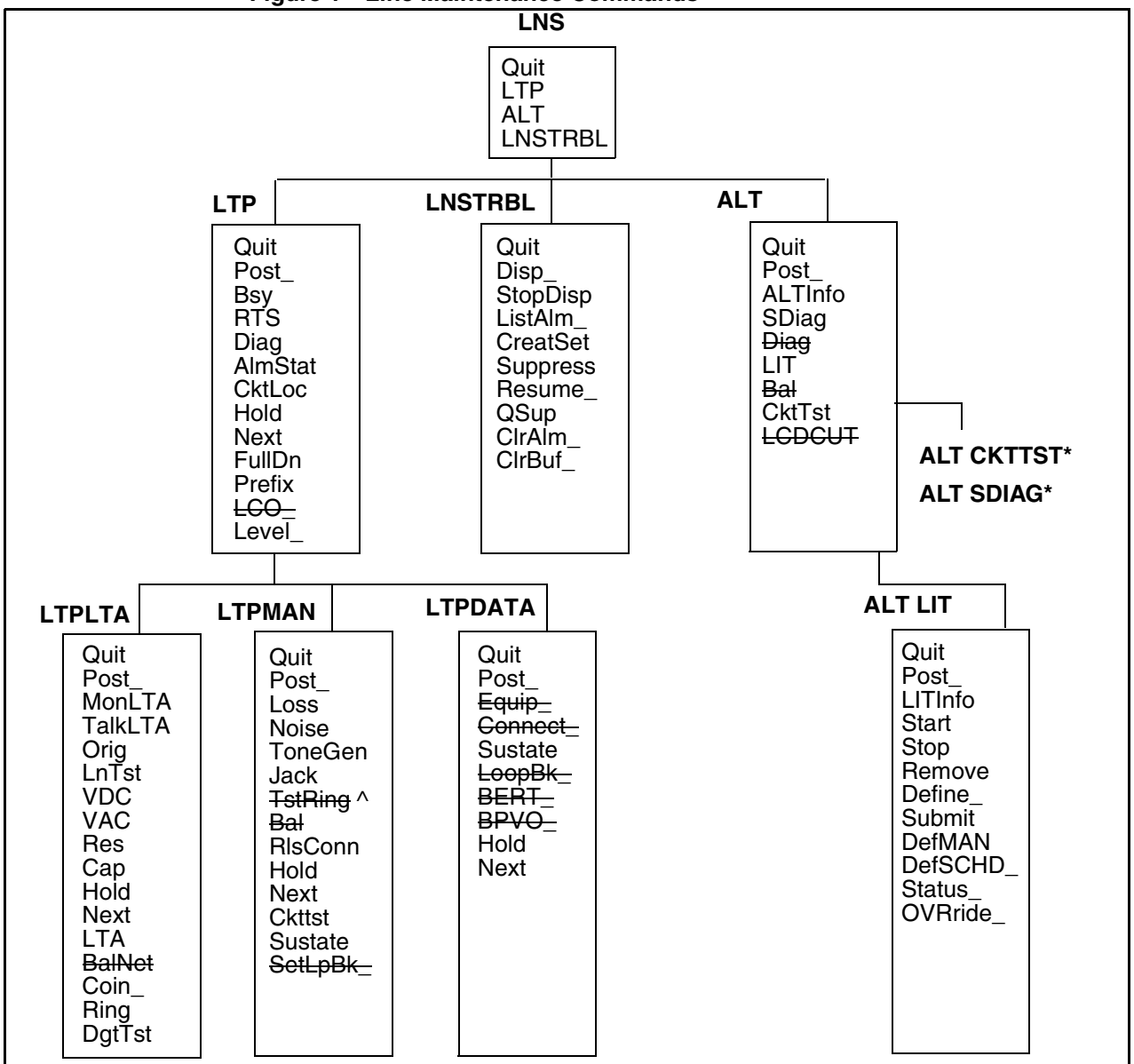
Testing and troubleshooting of line faults are traditionally done using a Maintenance and Administration Position (MAP) user interface at the levels below the LNS MAP level. The LNS MAP level contains the lines test position (LTP) menu commands, the automatic line testing (ALT) menu commands and the lines service trouble (LNSTRBL) commands. Prior to this feature, only a few MAP commands, such as BSY, RTS, and FRLS, were supported for Succession lines off of LGRPs from the MAP. As the primary component of this feature, the majority of the MAP commands in the LTP, ALT and LNSTRBL level for Succession MG9000 POTS, Ground Start, Coin and EBS lines are provided for the Universal Access solution which are available for legacy RDT lines. In addition to the MAP commands, ShowerQ support and Subscriber Premise Test support are provided for these types of Succession lines. Support of No Test Trunk (NTT) is already provided. This feature is for the SN06.2 release and is for the Maintenance Trunk Module (MTM) and Remote Maintenance Module (RMM) configurations.

7.2.1 Overview of Line Maintenance Commands

Figure 1 contains a list of the line maintenance commands shown at their respective levels which are supported for native MG9000 lines. Figure 1 does not include commands which are or are not supported for MG9000 Access Bridge Interface (ABI). To get to the LNS MAP level on a DMS MAP window which is at the top of the hierarchy in the figure, enter the mapci;mtc;lns level.

Most commands shown in the figure are supported for native MG9000 lines. The unsupported commands are indicated by a strike through. Check the legend for additional clarification.

Figure 1 Line Maintenance Commands



Legend:

*** :**The menu of commands for the other ALT levels are the same as the commands for the ALT LIT level.
^ : Indicates that a message is displayed referring the user to use the DIAG command.
A strike through indicates that the command is not supported.

Note 1: The LTP levels IBNCON and DCTLTP are not shown since they do not apply to Succession MG9K.
Note 2: The ALT LCDCUT and ALT SDIAG sub-levels are not shown since it is not applicable to Succession MG9K.
Note 3: The ALT BAL sub-level is not shown since it is not valid for RDTLSG, RDTCON, or RDTEBS lines.
Note 4: The LTP level LTPISDN is not shown since it only applies to ISDN lines and does not apply to native MG9K.

The following sections highlight the basic functionality provided by this activity. For more information, please refer to the DMS-100 Family Lines Maintenance Guide.

7.2.2 LTP Menu Commands

Following are the valid commands at the LTP level for native MG9000 lines:

- **Quit**: The QUIT command is used to leave the current level and return to a higher level.
- **Post**: Posts a line or set of lines to the LTP.
- **Bsy**: The BSY command changes the state of the line in the control position, or optionally all lines that are posted, to a specific state.
- **RTS**: The RTS command changes the state of the line in the control position, or optionally the complete set of posted lines, from MB to IDL.
- **Diag**: The DIAG command performs an extended diagnostic on a line in the control position that is in the MB or IDL state, and displays the results on the LTP screen.
- **AlmStat**: The ALMSTAT command triggers the alarm system of the LNS subsystem and displays the status of alarms in the full switch by type of alarm, when used without parameters. The command is used with parameters to display all or selected alarms at specified units in the host or remote sites, or to change the thresholds of the alarm classes in the full switch.
- **CktLoc**: The CKTLOC command locates and identifies the circuit card used for the line circuit in the control position, and displays circuit characteristics. Some of the displayed information for the Floor and Row Position, which consists of both the row and frame position, is dependent on the datafill of the SN06.2 LGRPLOC option in table LGRPINV. See SN06.2 activity A00002607. If this option is not provided, this information is displayed with default values of “00” for the Floor and “A00” for the Row Position. The Bay ID consists of the frame type, which is displayed as “MG9F”, and the frame number. LEN information that is stored in table LNINV is also displayed.
- **Hold**: The HOLD command moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position.
- **Next**: The NEXT command moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in a specified hold position; and exchanges, saves, or drops the replaced line from LTP control.
- **FullDn**: The FULLDN command displays the full National Number.
- **Prefix**: The PREFIX command clears the LTP of prefix digits. Optionally it sets or changes prefix digits.
- **Level_** : The Level command gives the user access to the sublevels LTPLTA, LTPMAN, LTPDATA, IBNCON, and DCTLTP at the MAP.

7.2.2.1 LTPLTA Menu Commands

Following are the valid commands at the LTPLTA sub-level for native MG9000 lines:

- **Quit**: The QUIT command is used at the LTPLTA sublevel in the same way as it is described at the LTP level.
- **Post_**: The POST command is used in the LTPLTA sublevel in the same way as it is described at the LTP level.
- **MonLTA**: The MONLTA command connects a headset circuit to the MG9000 line in the control position for listening purposes.
- **TalkLTA**: The TALKLTA command connects a talk circuit to a subscriber on a MG9000 line, and optionally connects a talk battery so that the tester can converse with the subscriber when the CO relay is operated.
- **Orig**: The ORIG command configures the loop side of a line circuit in either the off-hook mode or the on-hook mode, or alternates between modes.
- **LnTst**: The LNTST command performs resistance, capacitance, and voltage tests on a MG9000 line.
- **VDC**: The VDC command performs a dc voltage measurement on a subscriber loop.
- **VAC**: The VAC command performs an ac voltage measurement on a subscriber loop.
- **RES**: The RES command performs resistance measurements on a subscriber loop.
- **CAP**: The CAP command performs a capacitance measurement on a subscriber loop.
- **Hold**: The HOLD command is used at the LTPLTA sublevel in the same way that it is described at the LTP level.
- **Next**: The NEXT command is used at the LTPLTA sublevel in the same way that it is described at the LTP level.
- **LTA**: The LTA command connects the LTA to a line card, or releases the LTA from a line card.
- **Coin_**: The COIN command sends a +130 V pulse on the subscriber loop to operate the coin collect mechanism in the coin station, or a -130 V pulse to operate the coin return mechanism.
- **Ring**: The RING command places ringing voltage on the loop of a MG9000 line.

- **DgtTst**: The DGTTST command tests the DIGITONE pad or dial on the subscriber station.

7.2.2.2 LTPMAN Menu Commands

Following are the valid commands at the LTPMAN sub-level for native MG9000 lines:

- **Quit**: The QUIT command is used at the LTPMAN sublevel in the same way as described in the LTP level.
- **Post_**: The POST command is used at the LTPMAN sublevel in the same way as described in the LTP level.
- **Loss**: The LOSS command measures the insertion loss of a test tone sent from the subscriber end of a loop to its line circuit.
- **Noise**: The NOISE command measures the C-message weighted circuit noise on a subscriber loop.
- **ToneGen**: The TONEGEN command transmits a tone on a subscriber loop.
- **Jack**: The JACK command connects a jack-ended trunk to a subscriber line, or a jack to a subscriber loop while bypassing the line card.
- **TstRing**: The TSTRING command tests the ringing relay in the line card for proper functioning. Since this functionality is performed during the Diag command, a message referring the craftsperson to run the Diag command is displayed.
- **RlsConn**: The RLSCONN command releases test equipment that is connected to a line.
- **Hold**: The HOLD command is used at the LTPMAN sublevel in the same way that it is described at the LTP level.
- **Next**: The NEXT command is used at the LTPMAN sublevel in the same way that it is described at the LTP level.
- **Ckttst**: The CKTTST command sends test messages to test the posted line.
- **Sustate**: The SUSTATE command determines the status of the MBS that is connected to the Business Set line in the control position.

7.2.2.3 LTPDATA Menu Commands

Following are the valid commands at the LTPDATA sub-level for native MG9000 lines:

- **Quit_**: The QUIT command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.
- **Post_** : The POST command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.

- **Sustate**: The SUSTATE command reports on the loop status of the subscriber data line.
- **Hold**: The HOLD command is used at the LTPDATA level in the same way as it is described in the LTP level.
- **Next**: The NEXT command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.

7.2.3 LNSTRBL Menu Commands

Following are the valid commands at the LNSTRBL level for native MG9000 lines:

- **Quit**: The QUIT command is used at the LNSTRBL level in the same way as it is described in the LTP level.
- **Disp_**: The DISP command displays call processing trouble entries in the upper buffer that is allocated to a LCD.
- **StopDisp**: The STOPDISP command discontinues the periodic updating of the call processing trouble displays that were initiated by the command DISP.
- **ListAlm_**: The LISTALM command displays a list of LCD that have call processing fault alarms, and the class of alarm that exists in each LCD.
- **CreatSet**: The CREATSET command posts a set of call processing trouble upper buffer entries.
- **Suppress**: The SUPPRESS command causes specified trouble types to be ignored by the buffering process and by alarm generation
- **Resume_**: The RESUME command discontinues the suppression of specified types of call processing troubles.
- **QSup**: The QSUP command lists the code number and description of the types of troubles which are currently suppressed.
- **ClrAlm_**: The CLRALM command clears the call processing alarms in a specified LCD and resets attempt and failure counters to zero.
- **ClrBuf_**: The CLRBUF command deletes part or all of the contents of the upper buffer that is allocated to a specified LCD.

7.2.4 ALT Menu Commands

Following are the valid commands at the ALT level for native MG9000 lines:

- **Quit**: The QUIT command causes the system to leave the current level and return to a higher level of the MAP.
- **Post_**: The POST command posts the scheduled ALT TESTID that is stored in memory (in Table ALTSCHED)
- **ALTInfo**: The ALTINFO command checks test data stored in memory (Table ALTSCHED)
- **SDiag**: The SDIAG command accesses the SDIAG sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.
- **LIT**: The LIT command accesses the LIT sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.
- **CktTst**: The CKTTST command accesses the CKTTST sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.

The following ALT commands are not supported for native MG9000 lines:

- **DIAG**
- **BAL**
- **LCDCUT**

All MG9000 linecard types are support by ALT in the SN06.2 release.

7.2.4.1 ALT Sublevel Commands

Following are the valid commands at the ALT sub-levels for native MG9000 lines:

- **Quit**: The QUIT command causes the system to leave the current level and return to a higher level of the MAP.
- **Post_** : The POST command posts the scheduled ALT TESTID that is stored in memory and corresponds to the current sublevel.
- **LITInfo**: The LITINFO command displays the system default values for the LIT parameters. Note: This command only applies to the ALTLIT menu level.
- **Start**: The START command sets the posted scheduled ALT test in a state such that it is ready to run at the next scheduled time.
- **Stop**: The STOP command stops a test and changes the status of the TESTID.
- **Remove**: The REMOVE command removes the data associated with the posted TESTID from memory (table ALTSCHED). If the TESTID is for a scheduled test, the system prompts for a YES or NO confirmation.

- **Define_**: The DEFINE command defines test data for the specified TESTID.
- **Submit**: The SUBMIT command submits the defined test data for the posted TESTID into memory (table ALTSCHED).
- **DefMAN**: The DEFMAN command is used to assign a TESTID to the test that corresponds to the current ALT sublevel. For example, the DEFMAN command entered at the LIT level of MAP device number 7, will be assigned a TESTID of MANUAL07.
- **DefSCHD_**: The DEFSCHD command is used to assign a TESTID to the scheduled test that corresponds to the current ALT sublevel.
- **Status_**: The STATUS command checks the status of the posted TESTID.
- **OVRride_**: The OVERRIDE command overrides a scheduled test so that testing will not start until a specified day and time has passed.

7.2.5 ShowerQ

Failure of some conditions, such as line card not in place, test register not functioning, and message signaling not successful, causes the MG9000 line to be registered in the shower queue (a CS2000 originated diagnostic schedule) and released for a second call attempt. If any of the tests fail a second time, the MG9000 line is subjected to diagnostic tests for fault identification. Shower queue results are reported to the log system.

All MG9000 linecards are supported by the ShowerQ in the SN06.2 release.

For more information on the shower queue process, please refer to the DMS-100 Family Lines Maintenance Guide.

7.2.6 Subscriber Premise Tests

The silent switchman test (SSMAN), station ringer test, and the dialable short circuit test are usually conducted on subscriber premises by installation or repair personnel.

The **SSMAN test** checks the subscriber loop for facility faults. The test circuit is accessed by dialing a service code or a seven digit number. After a confirmation tone is returned, the MG9000 line is disconnected from office battery and ground for a defined interval as datafilled in table OFCENG as SILENT_SWITCHMAN_TIMEOUT, allowing facility faults to be checked.

The **station ringer test** is used to verify that a subscriber's station set is functioning correctly. The station ringer test is initiated by dialing a customer defined access code. When the station ringer test is initiated, it allows the user to verify the following set functions:

POTS, Coin or Groundstart

- DP or DTMF Digits
- Flash Key or Flash Hook
- RLS Key or Onhook
- Talk Key or Offhook
- Set Ringer

PPhone

- Meridian Set Function Keys
- Meridian Set Lamps
- Meridian Set Display

The circuit test part of Station Ringer test for KSET lines is not supported in this release. The result for circuit test are shown by LED displays 1, 2 and 8 turning on. The number of messages is not displayed also. The test can be exited during circuit test by pressing the "Hold" key.

The **dialable short circuit test** involves placing a short circuit to the loop of the MG9000 line when a code is dialed to access the short circuit. The short circuit persists on the line under test for a period of time as established by the operating company via OFCENG office parameter CABLE_SHORT_TIMEOUT, or for the default period of 3 min. When the short circuit ends its established duration, the subscriber's line is returned to regular service.

For more information on the sequence of tasks for these type of tests, please refer to the NTP 297-1001-594, DMS-100 Family Lines Maintenance Guide. This document contains additional details on the subscriber premise tests and translations required to support these tests.

7.2.6.1 Note on Digit Maps

In H.248, gateways can use digit maps when collecting digits. When the collected digits match an applied digit map, the gateway will report the collected digits to the call server. The subscriber premise tests are typically provisioned with a three digit access code in translations.

When the user dials a three digit access code to initiate a subscriber premise test, it may not match the standard digits maps used with MG9000 lines. The

MG9000 has a 10 second timeout and will report collected digits to the CS2000 even if the dialed digits do not match an applied digit map.

When a craftsperson is initiating the subscriber premise tests on MG9000 lines, this may cause a 10 second delay between the dialing of the access code and the application of the confirmation tone to indicate that the test is starting. For KSET lines, there is no delay between the dialing of the access code and the application of the confirmation tone since KSET lines do not use digit maps.

7.2.7 Line Diagnostics

The CS2000 line diagnostics are intended to verify that a line is capable of providing service. The CS2000 line diagnostics are integrated with the embedded MG9000 circuit diagnostics. When an MG9000 circuit is diagnosed from the CS2000, the embedded MG9000 line diagnostics are executed and additional network tests are performed to ensure that the circuit is providing service. The following shows the tests the CS2000 line diagnostics will perform for MG9000 lines, and compares the MG9000 line diagnostics to the diagnostics supported for HOST lines and GR-303 lines.

CS2000 Line Diagnostics

Test	HOST	TR-303	LGRP
Provisioning Data	Note 1	x	x
Missing Card Test	x	x	Note 2
Trans Hybrid Loss	x	x	x
PadsFigure 3, "Functional Description (FN): A00001650"	x	Note 3	x
Weighted and Notch Noise	x	x	x
Flux Cancellation / Echo Return	x	x	Note 4
Offhook Detection	x	x	x
Onhook Detection	x	x	x
Ringing	x	x	x
Ground Start	x	x	x
TR Reversal	x	x	x
Coin Collect	x	x	x
Coin Return	x	x	x

CS2000 Line Diagnostics

Test	HOST	TR-303	LGRP
PPhone Opcode Signalling	x	x	x
PPhone Provisioning Audit	x	x	x
Battery Feed	x	Note 5	Note 5
Cutoff Relay	x	Note 5	Note 5
Test Access Relay	x	Note 5	Note 5
Facility Check	x	Note 5	Note 5

X - denotes tests that are supported

1. GR-303 digital loop carriers and H.248 gateways have provisioning that must match the provisioning in the CS2000 to provide service. HOST lines do not have remote provisioning data and the provisioning data test is not required.
2. The MG9000 does not support a missing card tests. MG9000 lines can affect the CS2000 line state. If the linecard is missing or disabled, the CS2000 line state will be set to SB to indicate that the line is in a trouble condition.
3. The CS2000 does to support analog pad control for GR-303 lines; therefore, the analog padding test is not supported for GR-303 lines.
4. The MG9000 has echo cancellers for all line types; therefore, a echo return test is not performed at this time.
5. GR-303 and MG9000 line diagnostics do not include facility and linecard relay tests.

7.3 Configuration Requirements

7.3.1 Hardware Requirements

7.3.1.1 CS2000 Hardware

The following hardware is required to provide the CS2000 line test support:

7.3.1.1.1 Trunk Modules

The CS2000 supports an array of test heads and supporting hardware. These circuit packs are contained in trunk modules. Examples of the supported trunk modules are the TM8, ISM, MTM and RMM.

7.3.1.1.2 Test Circuits

The following CS2000 test heads and supporting hardware are required to support MG9000 line testing:

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)
- NT2X10/NT2X11 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)

The CS2000 also requires the following supporting equipment for MLT test trunks:

- NT2X57 SD Card

Additional details on the circuit packs listed above are provided in TAM-1001-018 DMS-100 Family Quick Reference Guide. This is available through Helmsman.

7.3.1.1.3 MTA Matrix

The CS2000 supports two types of test heads: transmission test heads and metallic test heads. The transmission test heads connect to the line under test through the bearer network. The metallic test heads connect to the line under test through a metallic test access matrix.

The metallic test access matrix is a matrix with the metallic test heads connected to the horizontal leads on the matrix and the line concentrating devices connected to the vertical leads on the matrix. This matrix allows any test head to be cross connected to any line, thus allowing the test heads to be shared across all line access devices.

The CS2000 supports the following cards for implementing the MTA matrix:

- NT3X09BA 8x8 Matrix Card

The trunk modules also contain the MTA matrix cards.

7.3.1.1.4 Horizontal Connectivity

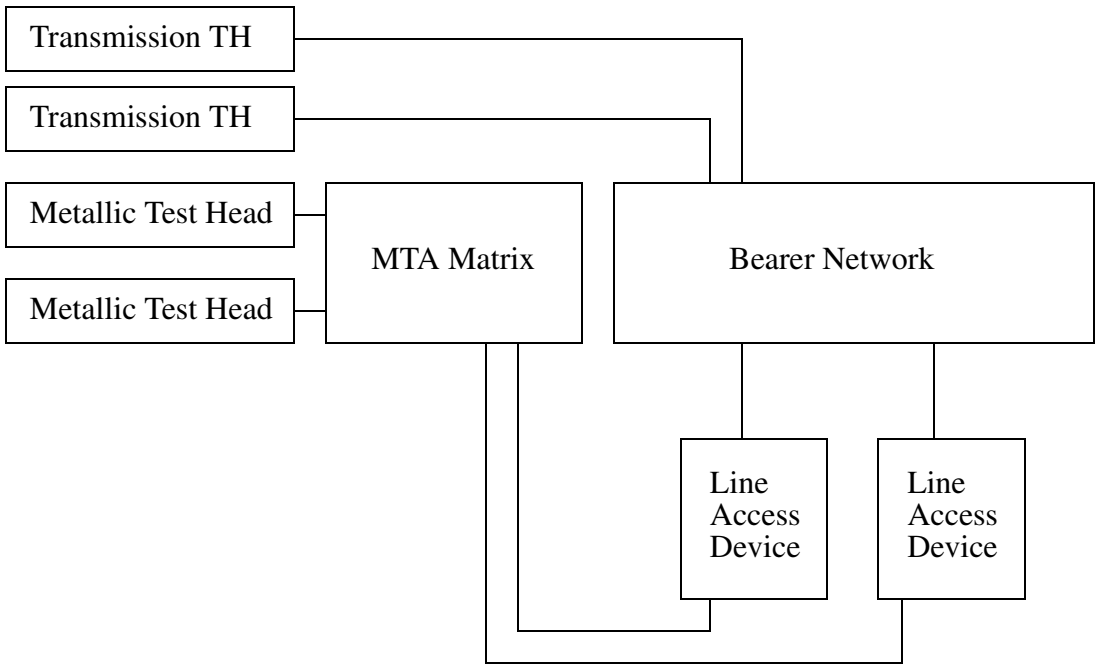
As noted above, the metallic test heads must be wired to the horizontal leads on the MTA matrix.

7.3.1.1.5 Vertical Connectivity

As notes above, the test access ports on the line concentrating devices must be wired to the vertical leads on the MTA matrix.

7.3.1.1.6 Test Configuration Diagram

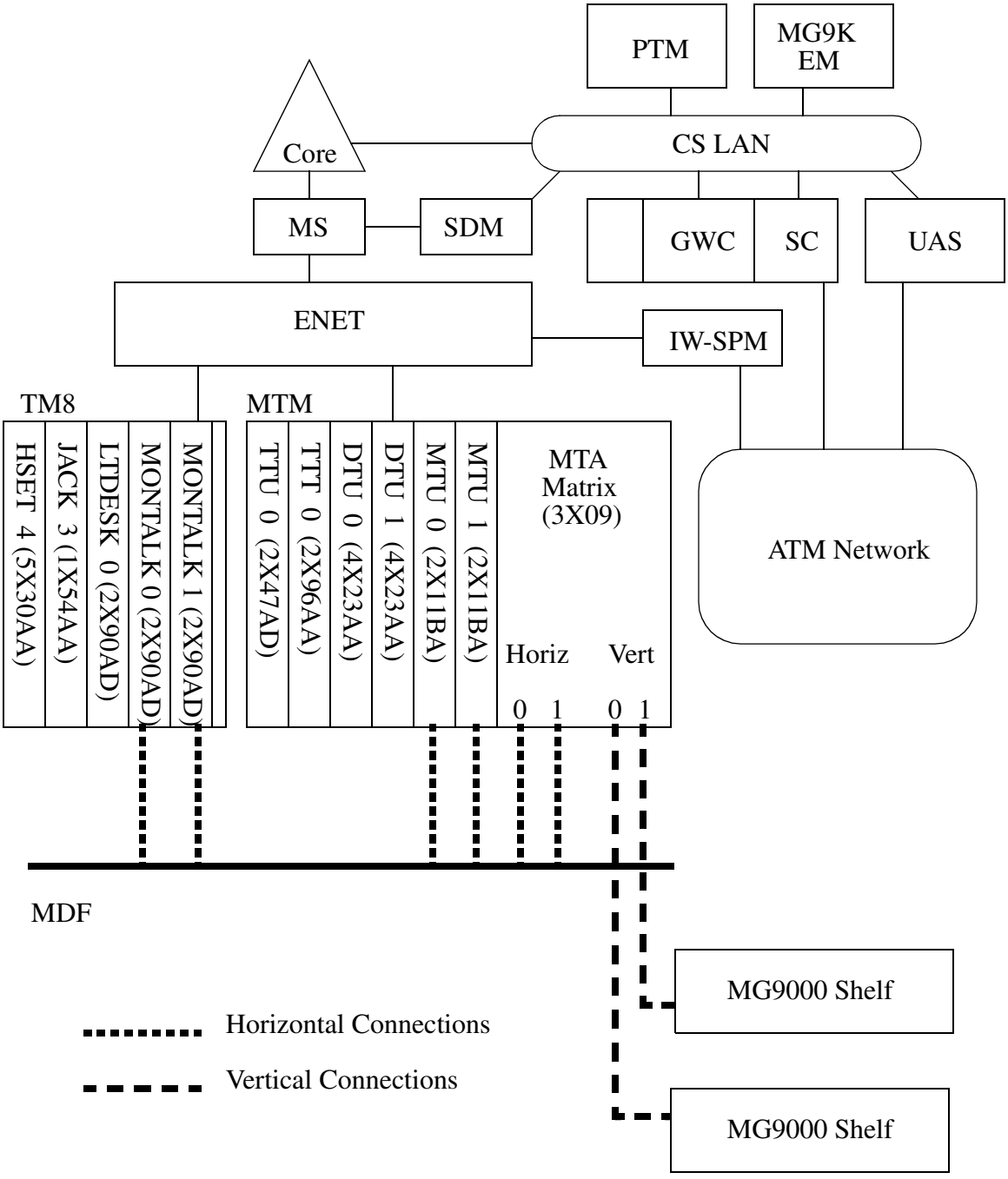
The following diagrams illustrate the hardware configuration required to support CS2000 based line testing for MG9000 lines.



The above diagram is a logical view of the test equipment.

- The transmission test heads have access to the bearer network. These test heads are connected to the line access devices through the bearer network.
- The metallic test heads are connected to the horizontal leads on the MTA matrix. The line access devices are connected to the vertical leads on the MTA matrix. In this configuration, any metallic test head can be cross connected to any line on any line access device.

The following figure gives a more detailed view of the physical implementation.


PTM
MG9K EM
Core
CS LAN
MS
SDM
GWC
SC
UAS
ENET
IW-SPM
TM8
MTM
HSET 4 (5X30AA)
JACK 3 (1X54AA)
LTDESK 0 (2X90AD)
MONTALK 0 (2X90AD)
MONTALK 1 (2X90AD)
TTU 0 (2X47AD)
TTT 0 (2X96AA)
DTU 0 (4X23AA)
DTU 1 (4X23AA)
MTU 0 (2X11BA)
MTU 1 (2X11BA)
MTA Matrix (3X09)
Horiz
Vert
0 1 0 1
ATM Network
MDF
MG9000 Shelf
MG9000 Shelf
Horizontal Connections
Vertical Connections

7.3.1.1.7 References

NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides a more complete description of the test equipment and the provisioning of the test equipment.

NTP 297-8991-805 DMS-100 Family Hardware Description Manual provides additional details on the hardware described above.

NTP 50041.08 DMS-100/200 Hardware Planning Guide

7.3.1.2 MG9000 Hardware

The MG9000 requires the following hardware to support the SN06.2 line test content provided by activities A00001888 and A00001890:

- MTA-TRC pack per node per frame
- SIC card per shelf.

7.3.1.3 3rd Party Gateways

The CS2000 line test functionality will support any 3rd party gateway that supports the H.248 extension added by activities A00001890 and A00001888. However, this document does not provide specific information on the hardware requirements for 3rd party gateways.

7.3.2 Software Requirements

There are 5 types of equipment/connectivity datafilled required to support the CS2000 line test functionality provided by activities A00001888 and A00001890.

- First the trunk modules that contain the CS2000 test equipment are provisioned.
- Second, the CS2000 test heads and supporting hardware are provisioned.
- Third, the MTA (Metallic Test Access) matrix for the CS2000 is provisioned.
- Fourth, the metallic test head connectivity to the horizontals on the MTA matrix are provisioned.
- Fifth, the line concentrating device connectivity to the verticals on the MTA matrix are provisioned.

Note that additional datafill is required for individual line test applications. For example, the subscriber premise tests are supported for MG9000 lines in the SN06.2 release (DSCKT, SSMAN, Station Ringer). The subscriber premise tests require translations in the CS2000 to function correctly.

This document does not provide details on the provisioning and translations required for the individual line test applications. The provisioning and translations for individual line test applications are already documented in NTP 297-1001-594 DMS-100 Family Line Maintenance Guide, and the existing provisioning and translations methods apply to LGRP lines on the CS2000.

7.3.2.1 Trunk Module Provisioning

The trunk modules are provisioned in table TMINV and RMMINV. The CS2000 uses the same trunk module provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provide details on trunk module provisioning for the CS2000.

7.3.2.2 Test Head and Supporting Hardware Provisioning

The test heads and supporting hardware are provisioned in tables TRKGRP and TRKMEM. The CS2000 uses the same test head provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on test head provisioning for the CS2000.

7.3.2.3 MTA Matrix Provisioning

The MTA matrix is provisioned in table MTAMDRVE. The CS2000 uses the same MTA matrix provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on MTA matrix provisioning for the CS2000.

7.3.2.4 Horizontal Connectivity Provisioning

The horizontal connectivity is provisioned in table MTAHORIZ. The CS2000 uses the same horizontal connectivity provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on the horizontal connectivity provisioning for the CS2000.

7.3.2.5 Vertical Connectivity Provisioning

Vertical connectivity provisioning for LGRPs differs from the vertical connectivity provisioning for existing DMS-100 peripherals. Additional details on LGRP vertical connectivity are provided below.

Table LGRPINV and MTAVERT are used to provision the metallic connections from MG9000 shelves to verticals on the MTA matrix. The following figure shows examples of provisioning these tables for MG9000 to MTA matrix connectivity.

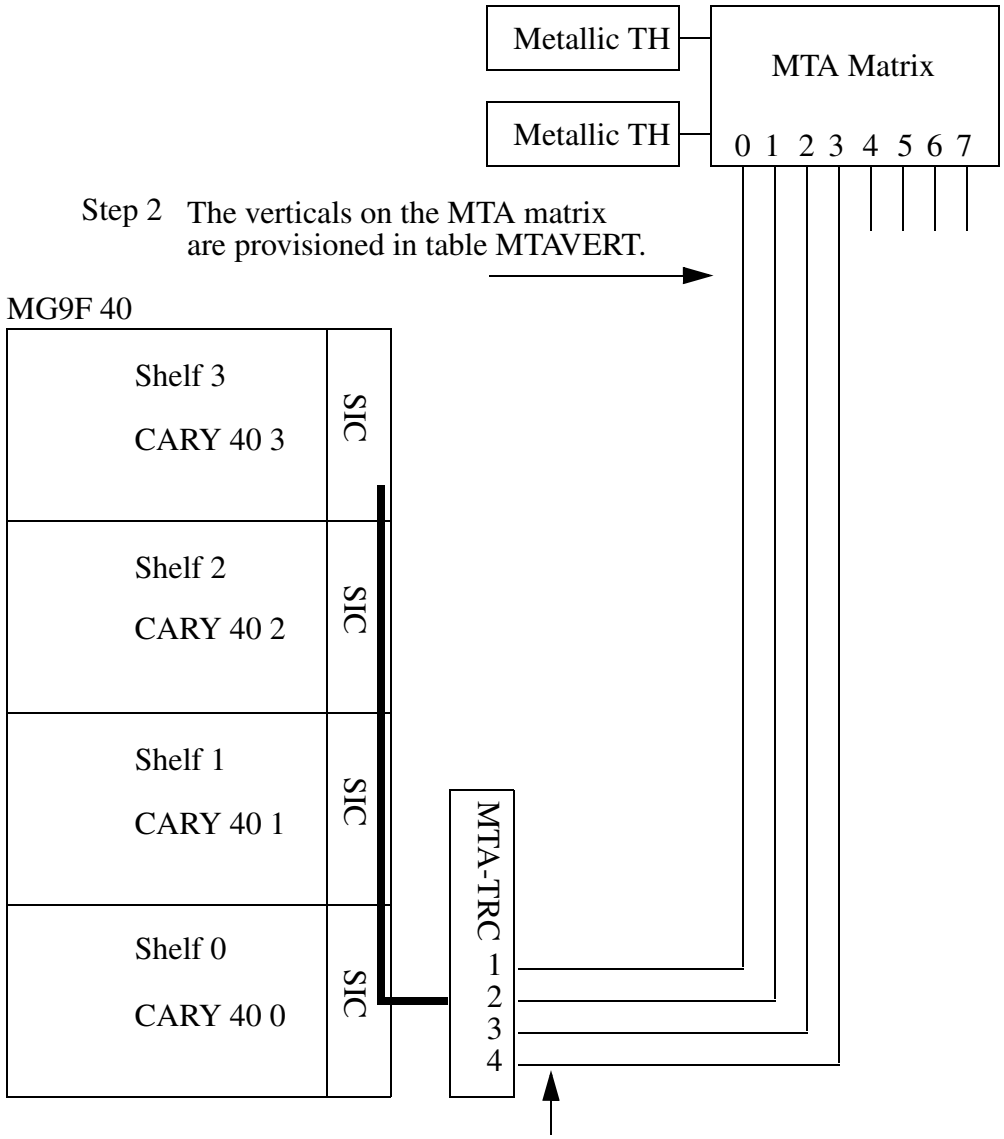


Table LGRPINV

```
CARY 40 0  GWC 0  S  MTSTAPT  CARY  (0  1) $
CARY 40 1  GWC 0  S  MTSTAPT  CARY  (1  2) $
CARY 40 2  GWC 0  S  MTSTAPT  CARY  (2  3) $
CARY 40 3  GWC 0  S  MTSTAPT  CARY  (3  4) $
```

Table MTAVERT

```
0  G  (O  CARY  40  0) $
1  G  (O  CARY  40  1) $
2  G  (O  CARY  40  2) $
3  G  (O  CARY  40  3) $
```

Vertical
Metallic Test Access Point

Provisioning Rules for MG9000 Verticals

1. The metallic test access connections for the MG9000s are provisioned in table LGRPINV first, and then in table MTAVERT.
2. Table LGRPINV allows up to 8 metallic test access points (with verticals) to be provisioned per LGRP. This is for future flexibility to increase the number of simultaneous tests per MG9000. **At this time, the user should only provision a single metallic test access point per LGRP in table LGRPINV (each LGRP being a single MG9000 shelf**).
3. LGRPs are assigned to verticals in table MTAVERT. Before an LGRP is assigned to a vertical in table MTAVERT, the tuple for the LGRP in table LGRPINV must have a metallic test access point associated to the vertical.

As noted in the rules, only a one metallic test access point and vertical should be assigned to an LGRP in the SN06.2 release. A single physical MG9000 can support up to 16 shelves; however, a single physical MG9000 can only support 8 metallic test access points. When an MG9000 grows beyond 8 shelves, verticals must be shared across multiple shelves. The provisioning recommendations for SN06.2 are as follows:

a. For MG9000 nodes that have 8 or less shelves, each shelf on the MG9000 should be assigned to a unique metallic test access point and vertical.

b. As an MG9000 grows beyond 8 shelves, the metallic test access points and verticals used on shelves 0-7 should be reused on shelves 8-15 in sequential fashion.

c. If wideband testing is required on the MG9000 to support DSL lines, then one (or more) of the metallic test access points should be reserved for the wideband test head.

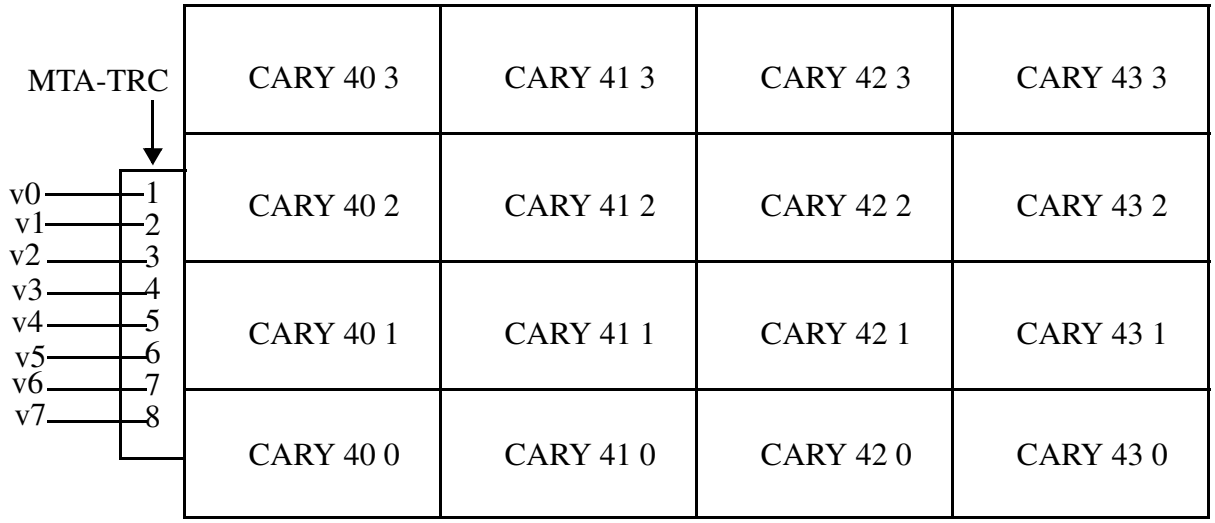
Example 1 : All 8 metallic test access points assigned to verticals.

The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node is in the CARY site and it occupies frame 40 41 42 and 43. This example shows all 8 metallic test access points wired to verticals on the MTA matrix.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
------------------------------------------------------------------------
CARY 40 0  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2  GWC 0  S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3  GWC 0  S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0  GWC 0  S (MTSTAPT CARY (4 5) $ ) $
```

```
CARY 41 1  GWC 0  S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2  GWC 0  S (MTSTAPT CARY (6 7) $ ) $
CARY 41 3  GWC 0  S (MTSTAPT CARY (7 8) $ ) $
CARY 42 0  GWC 1  S (MTSTAPT CARY (0 1) $ ) $
CARY 42 1  GWC 1  S (MTSTAPT CARY (1 2) $ ) $
CARY 42 2  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 42 3  GWC 1  S (MTSTAPT CARY (3 4) $ ) $

CARY 43 0  GWC 1  S (MTSTAPT CARY (4 5) $ ) $
CARY 43 1  GWC 1  S (MTSTAPT CARY (5 6) $ ) $
CARY 43 2  GWC 1  S (MTSTAPT CARY (6 7) $ ) $
CARY 43 3  GWC 1  S (MTSTAPT CARY (7 8) $ ) $

TABLE: MTAVERT

VERT VERTCONN
------------------------
0  G  ( O CARY 40 0 ) (O CARY 42 0) $
1  G  ( O CARY 40 1 ) (O CARY 42 1) $
2  G  ( O CARY 40 2 ) (O CARY 42 2) $
3  G  ( O CARY 40 3 ) (O CARY 42 3) $
4  G  ( O CARY 41 0 ) (O CARY 43 0) $
5  G  ( O CARY 41 1 ) (O CARY 43 1) $
6  G  ( O CARY 41 2 ) (O CARY 43 2) $
7  G  ( O CARY 41 3 ) (O CARY 43 3) $
```



In this configuration, a single vertical will be shared across as many as 1024 lines.

Example 2 : Two metallic test access points reserved for wideband testing

The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node is in the CARY site and it occupies frame 40 41 42 and 43. This example shows only 6 metallic test access points wired to verticals on the MTA matrix.

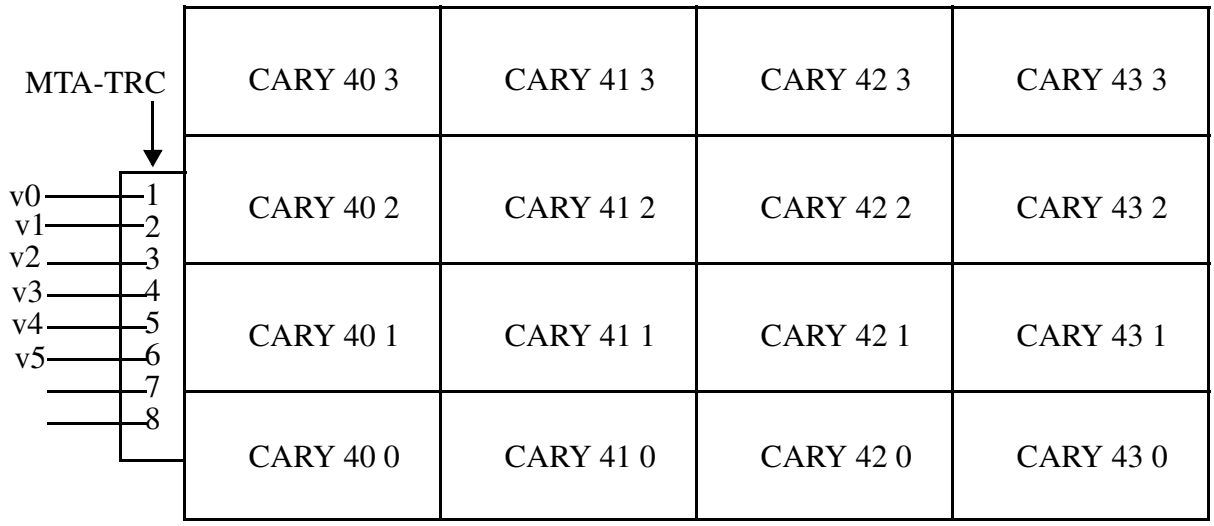
TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
------------------------------------------------------------------------
CARY 40 0  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2  GWC 0  S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3  GWC 0  S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0  GWC 0  S (MTSTAPT CARY (4 5) $ ) $
CARY 41 1  GWC 0  S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 41 3  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 42 0  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 42 1  GWC 1  S (MTSTAPT CARY (3 4) $ ) $
CARY 42 2  GWC 1  S (MTSTAPT CARY (4 5) $ ) $
CARY 42 3  GWC 1  S (MTSTAPT CARY (5 6) $ ) $
CARY 43 0  GWC 1  S (MTSTAPT CARY (0 1) $ ) $
CARY 43 1  GWC 1  S (MTSTAPT CARY (1 2) $ ) $
CARY 43 2  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 43 3  GWC 1  S (MTSTAPT CARY (3 4) $ ) $
```

TABLE: MTAVERT

```
VERT VERTCONN
-----------------------
0  G  ( O CARY 40 0 ) (O CARY 41 2) (O CARY 43 0)$
1  G  ( O CARY 40 1 ) (O CARY 41 3) (O CARY 43 1)$
2  G  ( O CARY 40 2 ) (O CARY 42 0) (O CARY 43 2)$
3  G  ( O CARY 40 3 ) (O CARY 42 1) (O CARY 43 3)$
4  G  ( O CARY 41 0 ) (O CARY 42 2) $
5  G  ( O CARY 41 1 ) (O CARY 42 3) $
```

In this example, a single vertical can be shared by up to 1536 lines.



7.3.2.6 Provisioning Example

7.3.2.6.1 Trunk Module Provisioning

First, the trunk modules must be provisioned. This includes shelves such as the TM8, MTMs and RMMs. In the example given, RMMs are not shown. However, RMMs can be used in the remote sites for MG9000 line testing. The sample datafill given shows a single MTM and TM8 shelf for this CS2000.

Note: all tables are shown in packeted format.

TABLE: TMINV

TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS LKDATA EQPEC LOAD EXECS SCTMLOC

TM8 0 TME 0 18 1 D 28 0 32 0 0 2X52AG BTMKA02 TM8EX SHELF
MTM 0 TME 0 52 1 D 28 0 32 5 0 2X58CB MTMKA02 MTMEX SHELF

7.3.2.6.2 Test Head and Supporting Hardware Provisioning

The test heads and supporting hardware are provisioned next. These circuits are provisioned through tables TRKGRP and TRKMEM. The following test heads and interface circuits are required to support MG9000 line testing:

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)
- NT2X10/NT2X11 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)

TABLE: TRKGRP

GRPKEY GRPTYP TRAFSNO PADGRP NCCLS GRPINFO

TTU MAINT 0 NPDGP NCIT 2X47AD
TTT MAINT 0 NPDGP NCIT 2X96AA
DTU MAINT 0 NPDGP NCRT 4X23AA
MTU MAINT 0 NPDGP NCRT 2X11BA
MONTALK MAINT 0 NPDGP NCRT 2X90AD
HSET MAINT 0 NPDGP NCRT 5X30AA
JACK MAINT 0 NPDGP NCRT 1X54AA
LTDESK TD 0 NPDGP NCOT NIL MIDL IC NPRT NSCR 613 613 LCL N N BASIC N

TABLE: TRKMEM

CLLI EXTRKNM SGRP MEMVAR

TTU 0 0 MTM 0 21
TTT 0 0 MTM 0 16
DTU 0 0 MTM 0 18
DTU 1 0 MTM 0 19
MTU 0 0 MTM 0 10
MTU 1 0 MTM 0 11
MONTALK 0 0 TM8 0 8
MONTALK 1 0 TM8 0 10
HSET 4 0 TM8 0 2
JACK 3 0 TM8 0 18
LTDESK 0 0 TM8 0 6

7.3.2.6.3 MTA Matrix Provisioning

After the test heads and supporting circuits are provisioned, the MTA (Metallic Test Access) matrix is provisioned for the CS2000. The MTA matrix is provisioned through table MTAMDRVE. This example shows an MTA matrix with a single MTA matrix card. The CS2000 supports an MTA matrix that is

significantly larger. The MTA matrix for a CS2000 is created by linking together multiple MTA cards in both the vertical and horizontal directions.

TABLE: MTAMDRVE

```
MTAMEM VERT HORIZ TMTYPE TMNO TMCKTNO MTACARD
-------------------------------------------
0 0 0 MTM 0 6 3X09BA
```

7.3.2.6.4 Horizontal Connectivity Provisioning

After provisioning the MTA matrix for the office, the test heads are assigned to horizontals on the MTA matrix. The example shows a pair of MTU (Metallic Test Units) connected to the first two horizontals on the MTA matrix along with a single analog test trunk for supporting external test systems such as: Access Care, 4TEL and Loop Care.

TABLE: MTAHORIZ

```
HORIZ HORIZGRP HORIZAGT MTAGRP
-----------------------------
0 0 L MTU 0 Y (0 0) $
1 0 L MTU 1 N (0 1) $
3 0 T LTDESK 0 (0 3) $
```

7.3.2.6.5 Vertical Connectivity Provisioning

After provisioning the test head connectivity to the horizontals on the MTA matrix, the line concentrating devices are assigned to verticals on the MTA matrix. For LGRPs, verticals are assigned to specific MG9000 metallic test access points and shelves through tables LGRPINV and MTAVERT.

The following example shows two separate LGRPs. For CARY 77 1, the entry in LGRPINV associates vertical 0 with metallic test access point 1 on the gateway. For CARY 40 2, the entry in LGRPINV associates vertical 1 with metallic test access point 1 on the gateway.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
-------------------------------------------------------------------------
CARY  77 1  GWC   5   S (MTSTAPT CARY ( 0 1) $)$
CARY  40 2  GWC   5   S (MTSTAPT CARY ( 1 1) $)$
```

TABLE: MTAVERT

```
VERT VERTCONN
-------------
0 G (O CARY 77 1 ) $
1 G (O CARY 40 2 ) $
```

7.4 Line States

This section provide information on the MG9000 lines states. This includes the interfaces for checking the line states and what they represent.

7.4.1 CS2000 Line States

The following is a list of CS2000 line states and their meaning. This is the complete list of CS2000 line states. Not all states are currently used for MG9000 lines. The states that are not used for MG9000 lines are in italic.

- CPB (Call processing busy)
  - — The line is in use by a subscriber (call processing is taking place).
- CPD (Call processing deload)
  - — The line is in use by a subscriber, and a maintenance request to place the line in the deloaded (DEL) state is pending. The state changes momentarily to DEL when call processing ends, and then to state MB.
- *CUT (Cutoff)*
  - — *The cutoff relay in the line circuit is operated, disconnecting the subscriber loop from the line circuit.*
  - — *Not used for MG9000 lines.*
- DEL (Deloaded)
  - — The line is removed from availability for call processing by a maintenance order, in preparation for testing activity. This is a temporary state after the state CPD and before the state MB.
- *DMB (Applicable to ISDN lines. See Integrated Services Digital Network)*
  - — *Basic Rate Interface Maintenance Guide, 297-2401-501.*
  - — *Not used for MG9000 lines.*
- *HAZ (Hazard)*
  - — *A line hazard condition (foreign line voltage, leakage resistance) has been detected; the line's cutoff relay is operated.*
  - — *Not used for MG9000 lines.*
- IDL (Idle)

— The line is in service and available to process calls.

- INB (Installation busy)

  — The line is not available for call processing for one or more of the following reasons:

  – some required data has not been assigned

  – a data change has been made

  – a LTP operator has entered an instruction

  During this state tests can be conducted.

- LMB (Line module busy)

  — Call processing cannot take place because the LGRP that represent the MG9000 shelf for the posted line is out of service.

- LO (Lock-out)

  — The line has been removed from service by the CS2000, preventing call processing. Manual action is required to change the state.

- MB (Maintenance busy)

  — The line has been removed from service by maintenance personnel or by the CS2000. Call processing cannot take place.

- NEQ (Not equipped)

  — The LEN has not been datafilled. Call processing cannot take place.

- PLO (PSPD lock-out)

  — This is a particular variety of the state LO. The line has been removed from service by the CS2000 because of a PSPD condition. Call processing cannot take place until the condition no longer exists and the CS2000 restores the line state to IDL.

- SB

  — The line has been removed from service by the CS2000. There are a range of error conditions that can cause an MG9000 line to be set to the SB state in the CS2000. If the CS2000 can set the line to the SB state if it detects an error condition for the line. The CS2000 can also set the line to the SB state if it receive an indication from the GWC that the line is not capable of providing service. This could represent a data error in the GWC or MG9000, or it could represent a fault condition for the line at the MG9000 such as an overcurrent protection condition. For lines in the SB state, the craftsperson should check the state of the circuit at the MG9000 EM.

- *SZ*

  — *Future line state*

— *Not used for MG9000 lines.*

7.4.2 MG9000 Line States

The state of the MG9000 circuits are checked at the MG9000 EM. The MG9000 EM shows the status of the physical line circuit and it shows the status of the H.248 line termination.

7.4.2.1 Line Circuit

The state of the physical line circuit is checked by opening the line card at the MG9000 EM and then opening the port on the line card. The following state information is shown for the MG9000 physical line circuit.

- Administrative Status
  - — The administrative status shows the requested user state. The values can be locked and unlocked.
    - – Locked indicates that the circuit has been manually taken out of service.
    - – Unlocked indicates that the circuit has not been manually taken out of service.
- Operational Status
  - — The operational status shows the current service state. The values can be enabled, disabled.
    - – Enabled indicates that the circuit is in the working state.
    - – Disabled indicates that the circuit is not in the working state.
- Fault State
  - — This state indicates that the line maintenance subsystem on the MG9000 has determined that the selected circuit is in a fault condition and is not providing service. The CS2000 state will be set to SB.
- Protection State
  - — This state indicates that excess voltage/current was detected for the selected circuit. MG9000 line maintenance has placed the circuit in the protect state. Lines in this state will not provide subscriber service. When MG9000 lines are in the protection state, the CS2000 line state is set to SB.
- Babble State
  - — This state indicates that the line maintenance subsystem on the MG9000 has determined that the selected circuit is a babbler. The circuit is generating excessive circuit state indications. Line maintenance will disable babbling circuits to protect the MG9000.

Lines in this state will not provide subscriber service. When line maintenance takes the circuit to the disabled state, the CS2000 line state will be set to SB.

- Cut Off Relay
  - — This state indicates that the cut off relay has been operated for the selected circuit. The user will not have service when the cutoff relay is operated to disconnect the loop for the circuit.

7.4.2.2 H.248 Line Termination

The state of the H.248 line termination is shown at the Switched Lines Services Manager on the MG9000 EM. The H.248 line termination represent the logical call processing service for the subscriber circuit. The state of the H.248 line termination is tied to the CS2000 line state.

If the service is turned down on the CS2000, the CS2000 will set the H.248 line to the disabled state. When service is restored for a line at the CS2000, the CS2000 will set the H.248 line termination to the enabled state.

The H.248 line termination state is also dependent on the physical line circuit. If the physical line circuit is in the disabled state (not able to provide service), the gateway will move the H.248 line termination to disabled state. This will inturn set the CS2000 line state to the SB state.

The Switched Lines Services Manager shows the following state information for the H.248 line terminations:

- Operational Status
  - — The operational status shows the current service state of the H.248 line termination. The values can be enabled, disabled and test.
    - – Enabled indicates that the H.248 line termination is in the working state and providing service.
    - – Disabled indicates that the H.248 line termination is not in the working state and is not providing service.
    - – Test indicates that the line is currently under test.
- Termination Test Status
  - — For terminations that are under test, the termination test status provides additional information. The value can be Not Testing, Testing via Call Server, Testing via EM.
    - – Not Testing indicates that the line is not currently under test.
    - – Testing via Call Server indicates that the line is currently under test from the Call Server.

– Testing via EM indicates that the line is currently under test from the MG9000 Element Manger.

7.5 Line Options Support

The following line options affect the CS2000 line test subsystem are supported for MG9000 lines:

- No Double Connect (NDC)

  The No Double Connect (NDC) option prevents a line from being connected to a verification or test circuit when the line is off-hook.

- No Hazard Test (NHT)

  The No Hazard Test (NHT) option does not allow the user to test the line for a line hazard condition. Line hazard conditions are low resistance or high voltage on the subscriber loop.

- No Line Insulation Test (NLT)

  The No Line Insulation Test (NLT) option allows the automatic line insulation test to skip a line.

7.6 Diagnostic Users Guide

7.6.1 Diagnostic Results

The line diagnostic results are delivered through a combination of the following:

- Printing results at the MAP
- Generating the appropriate logs
- Setting or clearing alarm flags for the line

7.6.1.1 Line Log

The MG9000 line diagnostic uses the following existing logs:

The LINE100 log indicates a line diagnostic has passed.

```
RTP206BH ***+LINE100 MAR21 08:06:49 3600 PASS LN_DIAG
        CARY 05 0 02 21    DN 6195200000
        DIAGNOSTIC RESULT   Card Diagnostic OK
        ACTION REQUIRED  None
        CARD TYPE  RDTLSG
```

The LINE101 indicates that a line diagnostic has failed.

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Single-party ringing
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTLSG
```

7.6.1.2 Alarm Flags

Various errors and actions in the CS2000 can mark failure flags against an MG9000 line. These failure flags provide information to the craftsperson on lines that are in trouble and need corrective action. The alarm flags supported for MG9000 lines are listed below.

- D - Long diagnostic has failed
- S - Short diagnostic has failed
- N - Needs long diagnostic
- Q - Line is in the ShowerQ
- L - Line has failed loop signaling at the linecard
- l - Line has failed loop signalling at the terminal

7.6.2 Line State Supported for the Line Diagnostics

7.6.2.1 For LTP Diags

The LTP diagnostic is supported on MG9000 lines in the following state:

- INB
- DMB
- MB
- LO
- IDL
- HAZ

7.6.2.2 ALT SDIAG

ALT SDIAG will test lines in the following states:

- INB
- MB
- IDL

7.6.2.3 ShowerQ

The ShowerQ tests lines in the following states:

- INB
- MB
- SB
- IDL
- LO
- DMB
- CUT
- PLO
- HAZ

7.6.3 Diagnostic Results

This section shows the most common diagnostic result indications and the actions the user should take for each result.

7.6.3.1 Diagnostic Passed

Display / Log

```
RTP206BH ***+LINE100 MAR21 08:06:49 3600 PASS LN_DIAG
        CARY 05 0 02 21    DN 6195200000
        DIAGNOSTIC RESULT   Card Diagnostic OK
        ACTION REQUIRED  None
        CARD TYPE  RDTLSG
```

Description

- The line tested is functioning correctly.

Alarm

- When a circuit diagnostic passes for a given line, all diagnostic failure flags for the line will be cleared.

Users Action

- No user action is required.

7.6.3.2 CS2000 Software Errors

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
CARY 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Call server software error
ACTION REQUIRED Check Logs
CARD TYPE RDTEBS

Description

- A CS2000 software error has occurred.

Alarm

- The line failure flag is not affected.

Users Action

- Capture the CS2000 SWERR log and try the test again.

7.6.3.3 GWC Processing Errors

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
CARY 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT GWC processing error
ACTION REQUIRED Chk GWC logs
CARD TYPE RDTLSG

Description

- A gateway controller software error has occurred.

Alarm

- The line failure flag is not affected.

Users Action

- Capture the GWC logs and try the test again.

7.6.3.4 GWC Provisioning Faults Detected

7.6.3.4.1 Missing Node Data

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
CARY 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Node data missing in GWC
ACTION REQUIRED Chk GWC data
CARD TYPE RDTLSG

Description

- In H.248, a node is represented by a termination called the root termination. The Gateway Controllers can support many MG9000 shelves. Each MG9000 shelf is provisioned in the GWC and represented as a root termination. This logical node is also referred to as the VMG (Virtual Media Gateway) in the MG9000 documentation. This diagnostic result indicates that there is a provisioning problem in the GWC. The GWC is missing the node provisioning data for the MG9000 shelf. This will prevent the entire MG9000 shelf from providing service.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- Check the node provisioning data for the GWC.

7.6.3.4.2 Missing Line Data

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Line data missing in GWC
    ACTION REQUIRED   Chk GWC data
    CARD TYPE   RDTLSG
```

Description

- The line termination for the line under test does not exist in the GWC. In H.248, each line is represented by a line termination. For MG9000 lines to provide service, the line termination must be provisioned in the GWC and it must be provisioned at the MG9000. This diagnostic failure indicates that the provisioning data for the line under test is missing in the GWC. The line will not provide service with this error condition.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- Check the line provisioning data in the GWC.

7.6.3.5 Node State Faults Detected in the GWC

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21                DN   6195200000
    DIAGNOSTIC RESULT   Gateway is out of service in GWC
    ACTION REQUIRED   Chk GW state
    CARD TYPE   RDTLSG
```

Description.

- A Gateway Controller can support many MG9000 shelves. Each MG9000 shelf is represented as a unique node in the Gateway Controller. This node is referred to as the root termination in H.248, and it also referred to at the VMG in the MG9000 documentation. The fault indicates that the node that represents the MG9000 shelf state is Out of Service in the Gateway Controller. When this occurs, the lines should be transitioned to the LMB state in the CS2000. If the line is not in the LMB state, this indicates that a node state mismatch exists between the C2000 and the Gateway Controller.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The user should check the line state in the CS2000. If the line state is not LMB and this diagnostic error persists, the user should attempt to correct

the MG9000 shelf state mismatch between the CS2000 and the Gateway Controller.

7.6.3.6 Line Termination is Out of Service in the GWC

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
CARY 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Line out of service in GWC
ACTION REQUIRED Chk ln state
CARD TYPE RDTLSG

Description

- The H.248 line termination for the line under test is in an out of service state in the GWC.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The user should check the state of the line circuit at the MG9000 element manager to ensure that the line circuit is in the enabled state.
- If the line circuit is in the enabled stated at the MG9000 EM, the user should BSY and RTS the line to attempt to bring the line termination back to a working state. After the BSY and RTS, repeat the diagnostic. If the problem persists, contact the next level of support.

7.6.3.7 Gateway Controller to Gateway Messaging Error

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
CARY 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT No response from gateway
ACTION REQUIRED Try again
CARD TYPE RDTLSG

Description

- This indicates that the Gateway Controller timed out waiting on a response from a test request sent to the gateway.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The users should try the diagnostic again. If this problem persists, it indicates a messaging problem between the Gateway Controller and the Gateway that could affect call processing.

7.6.3.8 Gateway Processing Error

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Gateway processing error
    ACTION REQUIRED   Chk GW logs
    CARD TYPE   RDTLSG
```

Description

- This indicates that the gateway failed to process a line test request.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The users should check the MG9000 logs for SWERRs and try the test again. If this problem persists, contact the next level of support.

7.6.3.9 Gateway Test Resources Unavailable

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test resources unavailable at gateway
    ACTION REQUIRED   Chk Gateway
    CARD TYPE   RDTLSG
```

Description

- This indicates that the MG9000 line test resources are out of service.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The user should check the state of the line test hardware at the gateway. For the MG9000, the users should check the state of the MTA-TRC pack

and the SIC cards. Those cards provide the line test functions within the MG9000.

7.6.3.10 Gateway Test Resource Busy

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test resources busy at gateway
    ACTION REQUIRED   Try Again
    CARD TYPE   RDTLSG
```

Description

- This indicates that the MG9000 line test resources are currently in use.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- This does not indicate any type of equipment fault. The line test resources in the gateway are all currently in use. The user should attempt the test again.

7.6.3.11 Line Provisioning Mismatch in the Gateway

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Line data mismatch in gateway
    ACTION REQUIRED   Chk GW data
    CARD TYPE   RDTLSG
```

Description

- The H.248 line terminations in the MG9000 can be provisioned as POTS, coin and PPhone services. This error indicates that the diagnostic detected a mismatch between the line termination provisioning data in the MG9000 and the provisioning data in table LNINV.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.

- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print

- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The users should correct the line data mismatch at the MG9000.

7.6.3.12 Line Provisioning Missing in the Gateway

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Line data missing in gateway
    ACTION REQUIRED   Chk GW data
    CARD TYPE   RDTLSG
```

Description

This Indicates that there is a line data missing in the gateway and the user should check the provisioning data in the gateway.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.

- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print

- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The users should check the line provisioning data in the gateway.

7.6.3.13 Line Card Diagnostic Failures

7.6.3.13.1 Offhook Detection Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Off-hook
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTLSG
```

Description

- Indicates that the linecard does not detect and report subscriber offhook condition correctly.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The line circuit should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.2 Onhook Detection Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  On-hook
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTLSG
```

Description

- Indicates that the linecard does not detect and report subscriber onhook condition correctly.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The line circuit should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.3 Single Party Ringing Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Single-party ringing
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTLSG
```

Description

- Indicates that the linecard does generate the correct ringing voltage and frequency.

Alarm

- The line failure flag for the line is set D to indicated that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print

- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The line circuit should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.4 Tip Ring Reversal Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Reverse battery
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTCON
```

Description

- Indicates that the linecard does not provide tip ring reversal correctly. Note: tip/ring reversal signaling is used by coin lines only.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print

- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The line circuit should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.5 Coin Collect or Coin Return Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Coin collect/return
    ACTION REQUIRED    Replace card
    CARD TYPE   RDTCON
```

Description

- Indicates that the linecard does not generate coin collect or coin return voltages correctly.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

Users Action

- The line circuit should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.6 Transhybrid Loss Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:40:48 6900 FAIL LN_DIAG
     CARY 05 0 02 21    DN 2145201001
     DIAGNOSTIC RESULT  -11.6-10.7  0.6  1.4 THL Test
     ACTION REQUIRED  Replace Card
     CARD TYPE  RDTLSG
```

Description

- The transhybrid loss test passes a series of tones through a linecard in both directions to verify that the linecard will encode and decode speech correctly for voice frequencies. This test also verifies the hybrid circuit in the linecard is not defective. The transhybrid loss tests uses the following frequencies: 304, 704, 1504 and 4305 Hz. The above display/log indicates that the transhybrid loss test has failed. The measured transhybrid loss at each test frequency is displayed in the diagnostic failure log.

- The transhybrid loss test will fail if too much loss or gain is detected when the tones are passed through the line under test. Different linecard have different transmission characteristics. The following shows the ranges that are considered a test pass for the MG9000 linecards.

POTS-32 and 8x8 DSL

	304 Hz	704 Hz	1504 Hz	3204 Hz
Minimum (Loaded)	Not Supported	Not Supported	Not Supported	Not Supported
Maximum (Loaded)	Not Supported	Not Supported	Not Supported	Not Supported
Minimum (Non-Loaded)	-5.0 dB	-4.5 dB	-4.5 dB	-5.0 dB
Maximum (Non-Loaded)	1.0 dB	1.5 dB	1.5 dB	1.0 dB

SAA-12

	304 Hz	704 Hz	1504 Hz	3204 Hz
Minimum (Loaded)	Not Supported	Not Supported	Not Supported	Not Supported
Maximum (Loaded)	Not Supported	Not Supported	Not Supported	Not Supported
Minimum (Non-Loaded)	-8.0 dB	-7.5 dB	-7.0 dB	-7.5 dB
Maximum (Non-Loaded)	-2.0 dB	-1.5 dB	-1.0 dB	-1.5 dB

- The example log shows a linecard that does not pass low frequency tones correctly.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print

- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- If the diagnostic failure shows excess loss or gain in the linecard, the linecard should be replaced or the subscriber should be moved to another circuit.

User Notes

- The MG9000 does not supported loaded lines. If a MG9000 line is provisioned as a loaded line in table LNINV, the transhybrid loss test will fail. If this occurs, the user should correct the provisioning error in table LNINV.

7.6.3.13.7 Continuity Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    CARY 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Bearer continuity not detected
    ACTION REQUIRED   Try Again
    CARD TYPE   RDTLSG
```

Description

- When the transhybrid loss test indicate -88.8 for all frequencies, then it may not be the linecard. It is more likely a bearer path problem.

Alarm

- The line failure flag is not affected by this error condition.

Users Action

- The user should attempt the test again. If multiple lines show the same behavior, the user should troubleshoot the bearer network connection faults.

7.6.3.13.8 Weighted or Notched Noise Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:50:13 6200 FAIL LN_DIAG
     CARY 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Noise Level 44.1DB Notch Noise
```

ACTION REQUIRED Replace Card
CARD TYPE RDTLSG

RTPU07BC ***+LINE101 OCT26 09:53:55 7100 FAIL LN_DIAG
CARY 00 0 00 14 DN 2145201001
DIAGNOSTIC RESULT Noise Level 36.5DB Weight Noise
ACTION REQUIRED Replace Card
CARD TYPE RDTLSG

Description

- The weighted or notched noise tests have failed for the linecard. The noise limits for the MG9000 linecards are as follows:

  Notched Noise must be less than 42.0 dB

  Weighted Noise must be less than 30.0 dB

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- The linecard should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.9 Linecard Pads Failure

Display / Log

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
CARY 00 0 00 14 DN 2145201001
DIAGNOSTIC RESULT -.7 -2.2 -.4 -.4 Pad 1DB Test
ACTION REQUIRED Replace Card
CARD TYPE RDTLSG

Description

- Indicates that linecard pad test failed. The CS2000 supports per call gain control, referred to as padding. This linecard pad test will verify that the CS2000 can adjust the pads in an MG9000 linecard. The linecard pad test measures the gain applied by a linecard when a 1, 3, 5, and 7 dB pad are applied to the line under test. The linecard pad test verifies that the correct gain in applied at 304, 704, 1504 and 4305 Hz.
- The example log given shows a diagnostic that failed the 1dB pad test. The diagnostic will allow a 1 dB variance from the requested gain. In the example given, the 704 Hz frequency had a loss of -2.2 dB when a -1.0 dB pad was requested.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- The linecard should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.10 Linecard Messaging Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     CARY 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  No Signalling to Card 5/10
     ACTION REQUIRED  Replace Card
     CARD TYPE  RDTEBS
```

Description

- PPhones, also referred to as EBS (Electronic Business Sets) lines, use out of band signaling. This signalling is called OPCODE signalling. The linecard diagnostic for an MG9000 PPhone line will verify the OPCODE signaling to the linecard and to the PPhone set itself. The given diagnostic

error log indicates that the OPCODE signaling test to the linecard has failed.

- The diagnostic failure log also contains the number of OPCODE message sent to the of message received back from the linecard.

Alarm

- The line failure flag for the line is set to L to indicate that the linecard diagnostic has failed the OPCODE signaling test to the linecard itself. Lines marked with the L failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a L failure flag:

  mapci nodisp;mtc;lns;ltp;post df lcard print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- The user can use the CKTTST command to perform additional manual OPCODE signaling tests on the suspect line.
- The linecard should be replaced or the subscriber should be moved to another circuit.

7.6.3.13.11 Mainset Messaging Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
    CARY 00 0 00 14    DN 2145201001
    DIAGNOSTIC RESULT  No Signalling to Set 5/10
    ACTION REQUIRED  Chk Card&Set
    CARD TYPE  RDTEBS
```

Description

- PPhones, also referred to as EBS (Electronic Business Sets) lines, use out of band signaling instead of analog signaling. This signalling is called OPCODE signalling. The linecard diagnostic for an MG9000 PPhone line will verify the OPCODE signaling to the linecard and to the PPhone set itself. The given diagnostic error log indicates that the OPCODE signaling test to the set has failed.

- The diagnostic failure log also contains the number of OPCODE message sent to and received back from the set.

Alarm

- The line failure flag for the line is set to l to indicate that the linecard diagnostic has failed the OPCODE signaling test to the phone set. Lines marked with the l failure flag have been identified by the CS2000 as lines that are not providing service. For this failure flag, there is a working PPhone assigned to the line under test, and the CS2000 can not successfully exchange OPCODE messages with a set on the loop.
- The following command line will print a report containing all the lines served by the CS2000 with a l failure flag:

  mapci nodisp;mtc;lns;ltp;post df lset print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- The user should verify that the set is connected to the loop.
- The user can use the CKTTST command to perform additional manual OPCODE signaling tests.
- If the CKTTST command verifies that the signaling to the mainset is not working and the set is connected to the loop, the user should replace the linecard. If the problem persists, the set should be replaced.
- The user can use the Station Ringer test to verify that the new set is fully functional from the subscriber premise.

7.6.3.13.12 Addon / Extension Provisioning Mismatch

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
      CARY 00 0 00 14    DN 2145201001
      DIAGNOSTIC RESULT  Ext. Not Responding
      ACTION REQUIRED   Sustate
      CARD TYPE  RDTEBS

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
      CARY 00 0 00 14    DN 2145201001
      DIAGNOSTIC RESULT  Addon Not Responding
      ACTION REQUIRED   Sustate
      CARD TYPE  RDTEBS
```

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     CARY 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Ext. Not Datafilled
     ACTION REQUIRED   Sustate
     CARD TYPE  RDTEBS

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     CARY 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Addon Not Datafilled
     ACTION REQUIRED   Sustate
     CARD TYPE  RDTEBS
```

Description

- The linecard diagnostic on an MG9000 PPhone line will audit the hardware on the loop and compare the hardware to the provisioning in the CS2000. The CS2000 can support up to 3 addons and 3 extensions per PPhone line. If the line diagnostic finds a mismatch between the hardware and the provisioning in the CS2000, the diagnostic will fail.
- The first example log shows a line that has an extension provisioned in the CS2000 but can not be detected on the loop.
- The second example log shows a line that has an addon provisioned in the CS2000 but can not be detected on the loop.
- The third example log shows a line where the diagnostic has detected an extension on the loop being testing, which is not provisioned in the CS2000.
- The fourth example log shows a line where the diagnostic has detected an addon on teh looop being testing, which is not provisioned in the CS2000.

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.
- The following command line will print a report containing all the lines served by the CS2000 with a D failure flag:

  mapci nodisp;mtc;lns;ltp;post df d print
- The following command line will print a report containing all the lines served by the CS2000 with any failure flag set:

  mapci nodisp;mtc;lns;ltp;post df print

User Action

- The user should use the SUSTATE command to evaluate the CS2000 provisioning versus the hardware connected to the line. Once the mismatch is identified, the provisioning or hardware error should be corrected.

7.6.4 Multicircuit Linecards

7.6.4.1 Managing Faulty Circuits

When the diagnostics detect a fault that requires intervention by a craftsperson, the CS2000 will raise a failure flag against the line. See the list of supported diagnostic failure flags listed in section "3.6.1.2 Alarm Flags" on page 209.

The diagnostic failure flag can be cleared by replacing the linecard and reexecuting the diagnostic. When the diagnostic passes, the CS2000 will automatically clear the failure flag. For multicircuit linecards, the user may not replace the entire pack if only one a few circuit on the linecard are defective. In this scenario, the user will not be able to clear the diagnostic failure flag by reexecuting the diagnostic.

The following procedure should be used to manage individual defective circuits on a multicircuit linecard.

- If a subscriber is assigned to the defective circuit, move the subscriber off the defective circuit to a working circuit.
- Select the circuit at the gateway element manager.
- Lock the individual defective circuit. If a circuit is in the locked state, the CS2000 will not attempt to test the line. The CS2000 will also not be able to return the line to the IDL state if service is reassigned to the defective circuit by mistake.
- Enter the LGLTT (LGRP Line Test Tool). Type LGLTT at the CI prompt. Use the ClrFlag command to clear the failure flag against the line. See section "3.13.2 LGLTT" on page 241.
- Post the line at the LTP level of the map. Verify that the failure flag has been cleared for the circuit. Verify that the DIAG command is not allowed for the line.

Note: the user must track the defective circuits to ensure that they are not unlocked at the gateway element manager. The user must also manage the defective circuits in their inventory system to ensure that service is not assigned to the defective circuit again.

7.7 Routine Maintenance

The following NTPs provide extensive information on the recommended routing maintenance and trouble shooting procedures for CS2000 lines:

297-1001-594	DMS-100 Family Lines Maintenance Guide
297-8991-500	Maintenance and Operations Manual
297-1421-503	Subscriber Services Maintenance Guide

This section provides some specific recommendations for MG9000 lines.

7.7.1 Subscriber Service

ALT SDIAG should schedule and executed on MG9000 lines. ALT SDIAG will routinely run the line diagnostics to detect functional, state or provisioning errors that would prevent subscriber service.

7.7.2 Facility Tests

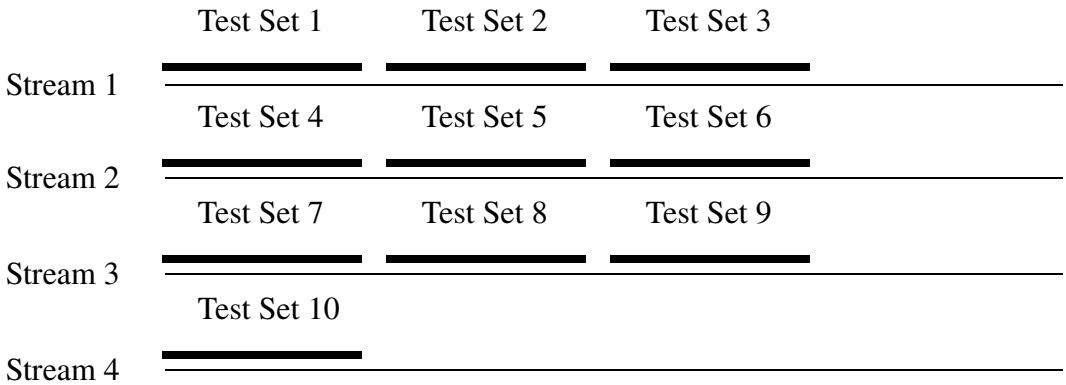
ALT LIT or a loop testing system should be scheduled to routinely test subscriber loops.

7.7.3 ALT Provisioning Recommendations for MG9000 Lines

7.7.3.0.1 MG90000 Tests Sets

ALT is designed to provide as much testing concurrency as possible. The user enters into ALT the range of LENs to test, which can span multiple nodes. ALT will run through the range of LENs to determine the “test sets” for the range of LENs.

ALT then creates a set of “test streams”. The test streams represent the resources that can be used to perform ALT tests. ALT will attempt to create as many streams a possible and divide the test sets up among the streams for maximum testing concurrency. This is illustrated in the diagram below. The diagram shows a configuration where ALT calculates 10 possible test sets for a range of LENs and divides the test sets over 4 test streams.



ALT SDIAG

Each MG9000 shelf is represented as an LGRP in the call server. As stated above, ALT test sets are calculated on a per node basis. A single MG9000 frame is represented in the call server as four distinct nodes. Therefore, a single MG9000 frame will be divided into 4 separate ALT test sets (one for each shelf).

ALT SDIAG, is dependent on the TTU resources in the MTM and the MTA-TRC resources in the MG9000. The TTU resources are required to perform transmission tests on the MG9000 linecards, and the MTA-TRC pack provides the supervision and ringing test resources. When ALT SDIAG is calculating the test streams for MG9000 lines, it will calculate the test streams based on the available TTUs. Specifically, ALT will create a single test stream for each TTU available for ALT SDIAG testing.

The combination of the way ALT test sets and ALT test streams are calculated can create a resource contention in the MG9000. A given MG9000 frame has a single MTA-TRC pack. Each MTA-TRC pack only provides two TRC circuits. Therefore, for a single MG9000 frame, only two MG9000 linecard diagnostics can be executed simultaneously.

The following example illustrates the issue:

- A craftsperson requests ALT to perform diagnostics for all the MG9000 lines in a single frame.
- Each MG9000 shelf is represented in the core as an LGRP. As stated above, each node in the CS2000 is assigned to a unique test set. Therefore, each MG9000 shelf will be assigned to a unique test set.

- As the linecard diagnostic only requires a TTU in the CS2000, ALT will attempt to create 4 test streams, one for each test set, and assign a TTU to each stream.
- ALT will then assign each test set, one for each shelf, to the 4 test streams.
- Once the test sets are assigned to test streams, ALT will begin processing the ALT test streams in parallel. This will create a scenario where ALT is attempting linecard diagnostic on all 4 shelves in a MG9000 frame concurrently. As the MG9000 can only support 2 simultaneous linecard diagnostics, there will be resources contention in the MG9000. Two of the ALT test streams will execute correctly, and two of the ALT test streams will fail due to unavailable resources at the MG9000.

To avoid the resource contention, the user should create tests on a per MG9000 shelf basis and ensure that ALT SDIAG is not scheduled on more than shelves shelf per frame concurrently.

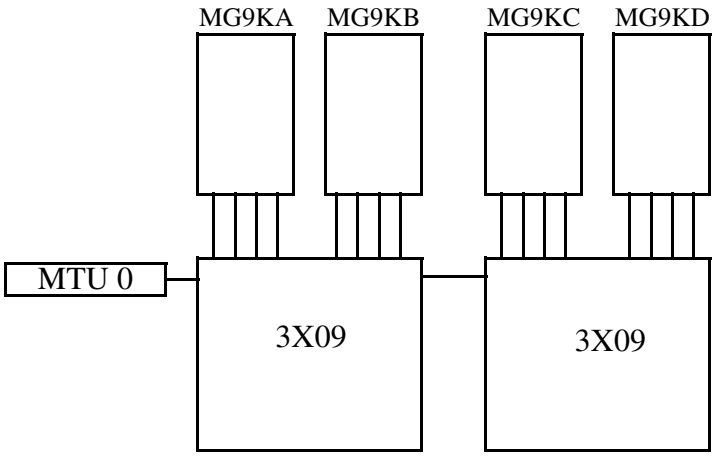
ALT LIT

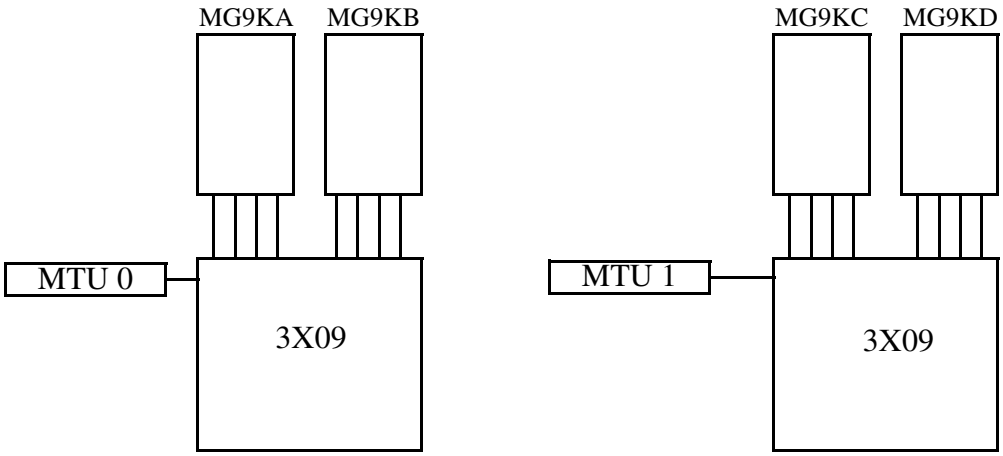
ALT LIT requires an MTU to test the subscriber's loop. ALT uses the "dedicated" MTUs in the switch. There are two test configuration options which are supported for MG9000 lines. If the customer uses the WTA (Wideband Test Access) panel, there will be a single dedicated MTU for a pair of 3X09s. If the customer wires the test equipment together through the MDF (Main Distribution Frame) a dedicated MTU can be assigned to each 3X09. These configurations are shown in the following diagrams.

As documented in the engineering rules, a MG9000 node should not span across multiple 3X09 circuit packs. Therefore, in either configuration shown, a given MG9000 can only use one possible dedicated MTU for performing ALT LIT tests.

When ALT LIT creates its test streams, it will create a test stream for each MTU in the switch that has the ALT option set to Y. As ALT LIT is assigning MG9000 test sets to the test streams, the engineering rules will ensure that the MG9000 test sets for a single MG9000 (one for each shelf) will go into the same test stream, because all the shelves for a given MG9000 must use the same MTU. Therefore, all the shelves in a MG9000 physical node will be tested in a serial fashion. This will ensure that there is no contention for MG9000 resources while ALT LIT is testing MG9000 lines.

Note: the option the customer chooses to deploy for the 3X09 configurations will be dependent on the maintenance window that is allowed for ALT LIT testing.





ALT CKTTST

ALT CKTTST performs messaging to the MG9000 to check the ability to loopback PPhone messages at the linecard or phone set. For the MG9000, each shelf is represented as a node in the core. Each MG9000 LGRP will be considered a single test set. There is no test equipment required to perform a

CKTTST, therefore, ALT can create a unique test stream for each test set up to the maximum number of ALT test streams allowed.

ALT CKTTST can run concurrently across all MG9000 shelves in the office

7.8 Trouble Shooting

The following NTPs provide extensive information on the recommended routing maintenance and trouble shooting procedures for CS2000 lines:

297-1001-594	DMS-100 Family Lines Maintenance Guide
297-8991-500	Maintenance and Operations Manual
297-1421-503	Subscriber Services Maintenance Guide

This section provides some specific recommendations for MG9000 lines.

7.8.1 No Dial Tone

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- If the fault is not outside plant, post the line at the CS2000 and check the CS2000 line state.
- If the line is an manually busy state, stop trouble shooting.
- If the line is in the SB state, that can indicated that the CS2000 has taken the line to the SB state, or it could indicated that the Gateway has taken the line to the SB state.
  - — The user can attempt to BSY and RTS the line. If the line returns to the IDL state, verify that dial tone is restored.
  - — If the line remains SB, check the line at the MG9000 EM. Check the line circuit for faults. The line circuit must be in the enabled state before the CS2000 line state will return to IDL. If there is a circuit fault at the MG9000, resolve the MG9000 circuit fault. Once resolved and the line circuit is restored to the enabled state, verify that the line has returned to the IDL state in the CS2000. Verify that dial tone is restored.
- If the CS2000 line state is IDL and there is not dial tone, execute the DIAG command on the line. The DIAG command will verify the line provisioning date in the CS2000, GWC and the MG9000. Once the provisioning data is verified, the DIAG will request the MG9000 to execute the embedded circuit diagnostics. This will execute the following tests:

- — Offhook detection
- — Onhook detection
- — Ringing
- — Coin Collect / Coin Return / Reverse Battery (for coin lines)
- — For PPhone lines, OPCODE signaling is verified instead of analog signaling.

- If the line diagnostic fails, resolve the issue reported in the diagnostic.
- If the line diagnostic passes check for dial tone at T/R pair coming off the face place on the linecard. If dial tone does not exist and the line diagnostic passes for the line, escalate to the next level of support. The TALKLTA and ORIG commands can be used to remotely pull dial tone from the T/R of the linecard.

7.8.2 Poor Speech Quality

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- Post the line at the CS2000 MAP position and execute the DIAG command. This will verify the transmission characteristics of the line.
- If the DIAG fails, move the subscriber to a different circuit.
- If the DIAG passes, the TONGEN, LOSS and NOISE commands can be used to perform manual transmission tests on the subscribers linecard and loop.
- If the problem can not be isolated, escalate to the next level of support.

7.8.3 Line Does Not Ring

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- If the fault is not outside plant, post the line at the CS2000 and check the CS2000 line state.
- If the line is an manually busy state, stop trouble shooting.
- If the line is in the SB state, that can indicated that the CS2000 has taken the line to the SB state, or it could indicated that the Gateway has taken the line to the SB state.
  - — The user can attempt to BSY and RTS the line. If the line returns to the IDL state, verify that dial tone is restored.

— If the line remains SB, check the line at the MG9000 EM. Check the line circuit for faults. The line circuit must be in the enabled state before the CS2000 line state will return to IDL. If there is a circuit fault at the MG9000, resolve the MG9000 circuit fault. Once resolved and the line circuit is restore to the enabled state, verify that the line has returned to the IDL state in the CS2000. Verify that dial tone is restored.

- If the CS2000 line state is IDL terminating calls will not RING the line, execute the DIAG command on the line. The DIAG command will verify the line provisioning date in the CS2000, GWC and the MG9000. Once the provisioning data is verified, the DIAG will request the MG9000 to execute the embedded circuit diagnostics. This will execute the following tests:
  - — Offhook detection
  - — Onhook detection
  - — Ringing
  - — Coin Collect / Coin Return / Reverse Battery (for coin lines)
  - — For PPhone lines, OPCODE signaling is verified instead of analog signaling.
- If the line diagnostic fails, resolve the issue reported in the diagnostic.
- If the line diagnostic passes check for ringing voltage at T/R pair coming off the face place on the linecard. If ringing voltage does not exist and the line diagnostic passes for the line, escalate to the next level of support.

7.8.4 Call Not Completed Correctly

- Use TRAVER to verify that translations will correctly route the dialed digits for the line being tested.
- If the translations are verified to be good, determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- Post the line at the CS2000 MAPCI. Execute the DIAG command on the line. This will execute the following tests:
  - — Offhook detection
  - — Onhook detection
  - — Ringing
  - — Coin Collect / Coin Return / Reverse Battery (for coin lines)
  - — For PPhone lines, OPCODE signaling is verified instead of analog signaling.

— Transhybrid Loss

— Weighed and Notched Noise

— Padding

The diagnostic will verify the transmission characteristics of the linecard.

- If the line diagnostic fails, resolve the issue reported in the diagnostic.
- If the diagnostic passes, test the lines ability to collect and report digits to the CS2000. The TALKLTA, ORIG commands be used to simulate a test call. The TALKLTA, DGTTST commands can be used to capture and observe any digits actually collected for the line under test.
- If the diagnostic passes for the line under test, and manual trouble shooting can not isolate the problem, escalate to the next level of support.

7.8.5 PPhone Lines Not Functioning Correctly

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- Post the line at the CS2000 MAPCI. Execute the DIAG command on the line. This will execute the following tests:

  — Offhook detection (analog lines)

  — Onhook detection (analog lines)

  — Ringing (analog lines)

  — Coin Collect / Coin Return / Reverse Battery (for coin lines)

  — OPCODE signaling (for PPhone lines)

  — Transhybrid Loss (for analog lines)

  — Weighed and Notched Noise (for analog lines)

  — Padding (for analog lines)

  The line diagnostic on a PPhone line will verify the provisioning in the CS2000 matches the set hardware, and it will verify the signaling between the CS2000, the linecard and the PPhone set.
- The Station Ringer test can be executed on site to verify the PPhone set itself.
- If the issue can not be isolated, escalate to the next level of support.

7.9 Logs

7.9.1 Existing Logs Applicable to CS2000 Line Test

NTP 297-1001-594 DMS-100 Family Lines Maintenance Guides, section 3 contains the line maintenance related logs for the CS2000.

7.9.2 Modified Logs

7.9.2.1 ALT SDIAG

There are two types of diagnostics supported by the ALT (Automatic Line Test) subsystem: long diagnostics and short diagnostics. The long diagnostics use external metallic test resources to test the line, and traditionally have provided more coverage than the short diagnostics which do not use external metallic test equipment.

For LGRP lines, the linecard diagnostics are not dependent on external metallic test equipment; therefore, only short diagnostics are supported. Note, the short diagnostics do not provide a reduced fault coverage for LGRP lines. They have been designed to provide the same fault coverage as the manual linecard diagnostics without the use of external metallic test equipment.

ALT SDIAG has been modified to use the ALT101 log for LGRP lines. As stated above, ALT SDIAG provides full fault coverage for LGRP lines so it has been modified to give a more detailed report on the diagnostic failures for LGRP lines. The following shows an example ALT101 log for an LGRP line that has failed diagnostics.

```
RTPU07BC      ALT101 NOV18 11:35:35 7900 FAIL ALT
       SLOA 77 1 19 18          NO DIRN    1st CYCLE
       TEST TYPE SDIAG DIAGNOSTIC RESULT Test failed: Off-hook
       ACTION REQUIRED  Replace card  CARD TYPE  RDTLSG
```

7.10 OMs

7.10.1 Line Troubles

NTP 297-1001-594 DMS-100 Family Lines Maintenance Guides provides recommendations for CS2000 OMs the users should monitor for lines troubles.

7.10.2 Equipment Troubles

NTP 297-1001-595 DMS-100 Family Trunks Maintenance Guide provides information on CS2000 OMs for the CS2000 test equipment.

7.11 Alarms

MG9000 lines support the CS2000 line failure flags in the SN06.2 release. This enables the ALMSTAT command for MG9000 lines. The ALMSTAT command allows the user to query the line alarms for an office. The user can also set thresholds for updating office alarms for excessive line failures.

7.11.1 ALMSTAT QUERY

The following shows sample output of an almstat query.

```
                OFFICE LINE FAILURE TOTALS

                          OFFICE   OFFICE OFFICE OFFICE
                          CURRENT  MINOR  MAJOR  CRITICAL
Ext   Diag Fail  (D)       3       10     20      30
Facility Fault   (F)       0       10     20      30
Short Diag Fail  (S)       31      10     20      30
Needs Ext  Diag  (N)       0       10     20      30
Set Missing   (MSET)       1       10     20      30
Card Missing (MCARD)       13      100    150     200
Shower Queue (QUEUE)       0       100    150     200
Major ICMOLINE(IMAJ)       0       100    150     200
Minor ICMOLINE(IMIN)       0       100    150     200
Loop Sig Set  (LSET)       1       100    150     200
Loop Sig Card(LCARD)       0       100    150     200
TCM sync loss    (T)       0       100    150     200
Loop Performance (P)       1       100    150     200
Major CPERROR (CMAJ)       0       5      10      15
Minor CPERROR (CMIN)       0       5      10      15
Major RapidMSG(OMAJ)       0       10     20      30
Minor RapidMSG(OMIN)       0       10     20      30
Utility Card     (U)       0       100    150     200
State = PLO   (PSPD)       1       10     20      30
State = HAZ (HAZARD)       0       0      1       10

              OFFICE LINE TOTALS

Number of working lines (total)    in this office is : 1400
Number of working DTMF lines       in this office is : 960
Number of working dial pulse lines in this office is : 3
Number of working EBSs (total)     in this office is : 327
Number of working PSET terminals   in this office is : 1
Number of working M5312 terminals  in this office is : 193
Number of working M5212 terminals  in this office is : 1
```

```
Number of working M5316 terminals  in this office is : 132
Number of working Data Units       in this office is : 0
Number of working ISDN loops       in this office is : 110
Number of working BCLID Data Links in this office is : 0

             OFFICE DIAL TONE DELAY (DTSR) INFORMATION

Present time   Oct30 08:27:29
Active time    Oct30 08:20:00
Holding time   Oct30 08:20:00

Dial Tone Delay Counts And Percentages

                Pulse  Signalling
           Attempted  Delayed  Percentage
Active           0         0        0.0%
Holding          0         0        0.0%

                DTMF   Signalling
           Attempted  Delayed  Percentage
Active        2351         0        0.0%
Holding       2816         0        0.0%

              Keyset Signalling
           Attempted  Delayed  Percentage
Active           0         0        0.0%
Holding          0         0        0.0%
```

7.11.2 ALMSTAT SET

The user can also use the ALMSTAT command to set the thresholds for the MINOR, MAJOR and CRITICAL office alarms.

7.12 User Error Responses

The complete list of user error responses are located in the configuration section under activity A00001890. Following are some of the more common error responses.

7.12.1 Line State Errors

When testing an MG9000 line, the line terminations is set to the TEST state. If the CS2000 fails to set to the termination to the TEST state, the user will get one of the following error responses.

Failed to determine the termination state

The CS2000 failed to determine the current state of the line at the gateway. The user should attempt the test again. If the problem persists, the users should contact the next level of support.

Failed to put the termination in the test state

The CS2000 requested the gateway to place the line in the TEST state and the request was not successful. The user should check the state of the line termination in the gateway.

The line is an ESA call

The CS2000 has determined that the line is involved in ESA call.

The line is out of service at the gateway

The CS2000 has determined that the line is in an out of service state at the gateway. The users should check the state of the line at the element manager for the gateway to isolate the fault on the gateway.

7.12.2 Line Test Provisioning Errors

Unable to determine metallic test equipment provisioned
Verify the MTSTAPT option exists for the entry in table LGRPINV

When a line test was attempted on an MG9000 line, the CS2000 failed to access the metallic test point provisioning data for the MG9000 in table LGRPINV. Check the provisioning in table LGRPINV.

Unable to get the test point index from LGRPINV
Test cannot be performed

When a line test was attempted on an MG9000 line, the CS2000 failed to access the metallic test point provisioning data for the MG9000 in table LGRPINV. Check the provisioning in table LGRPINV.

Vertical is not datafilled in MTAVERT
Test cannot be performed

When a line test was attempted on an MG9000 line, the CS2000 failed to access the vertical provisioning data for the MG9000 in table MTAVERT. Check the provisioning in table MTAVERT.

7.13 Tools

7.13.1 NFF

The No Fault Found utility allows the user to capture and query results from individual tests performed during the line diagnostics. The NFF utility is entered by typing NFF at the CS2000 CI prompt. The following shows the command help reference.

```
No Fault Diagnostic (NFF) utility.

This allows the intermediate results of the line
diagnostics to be sent to a file.

Valid commands are:

NFF START (fd) (fn) - Start recording NFF tst result onto
                      specified device and file name.
NFF STOP            - Stop NFF recording and close file
NFF QUERY           - Query the NFF recording status,
                      device and file name.
NFF PRINT           - Print the closed NFF file.

Parms: <Function> {START <device_name> DEVICE name
                   <file_name  > STRING,
                  STOP,
                  QUERY,
                  PRINT}
```

7.13.1.1 NFF Results for an MG9000 line

The following shows the data provided by the NFF utility for an MG9000 line.

```
>mapci nodisp;mtc;lns;ltp;post l ud17 5 3 2 0
MAPCI:
MTC:
LNS:
LTP:
>nff start sfdev diag1
>diag
RTD ***+LINE100 OCT30 08:52:43 1200 PASS LN_DIAG
        UD17 05 3 02 00    DN 6136211701
        DIAGNOSTIC RESULT  Card Diagnostic OK
        ACTION REQUIRED  None
        CARD TYPE  RDTLSG
>nff stop
NFF stopped
>nff print
```

```
No fault found diagnostic result
-
Diagnostic intermediate result for LEN: UD17 05 3 02 00 on
   OCT-30 08:52:33
Transhybrid loss test result:
                 304    704   1504   3204    Hz
     Max          10     15     15     10    db*10
     Actual      -22    -16    -15    -18    db*10
     Min         -50    -45    -45    -50    db*10
-
Test pads in line card result:
                 304    704   1504   3204    Hz
     1 db pad:   -10    -10    -10    -10    db*10
     3 db pad:   -30    -30    -30    -30    db*10
     7 db pad:   -70    -70    -70    -70    db*10
     0 db pad:     0      0      0      0    db*10
-
     Noise test result:  56   db*10 noise level
-
     Noise test result:  282   db*10 noise level
```

7.13.2 LGLTT

The LGRP Line Test Tool (LGLTT) can be used to clear the failure flag against a defective MG9000 circuit. To do so, enter the ClrFlag command at the CS2000 CI prompt, followed by the DN or LEN of the defective circuit. Below is an example of the use of the command:

```
CI:
>
>lgltt
LGRP Line Test Tool (LGLTT):
>help
LGRP Line Test Tool (LGLTT)
Commands:
  Help     - Display summary
  ClrFlag  - Clear failure flag for a given MG9000 DN/LEN
  Quit     - To return to CI
>clrflag sloa 77 1 19 10
>clrflag 5202090
>quit
```

7.14 Restart Behavior

All CS2000 line test activities are terminated by element restarts.

- After a CORE restart, any line test in progress is aborted and the line is returned to the IDLE state.
- After a Gateway Controller restart, any line test in progress times out and a failure message is displayed at the MAP. If the line test requires manual action at the CORE, the line test will remain in the test state until that action is complete.
- After a Gateway restart, any line test in progress is aborted and a failure message is displayed at the MAP.

7.15 MG9000 ESA Entry

All CS2000 line test activities are terminated by the MG9000 when a shelf enters ESA.

7.16 Limitations and restrictions

- The CS2000 line test functionality is only supported for MG9000 lines.
- The CS2000 line test functionality is only supported for MG9000 lines when using the following cardcodes:: RDTLSG, RDTCON, RDTEBS.
- Some of the SN06.2 CS2000 line test functionality delivered for MG9000 lines requires the collocation of DMS metallic test equipment with the MG9000. The functions that require collocated metallic test equipment are not supported in remote sites that do not contain ABI peripherals.

7.17 Interactions

Not applicable.

7.18 Applicable customer facing sections

Fault Management

Logs	__N/A_
Alarms	__N/A_
Configuration	
Data Schema	__N/A_
User Interface	__X_(see A00001890 for CM Configuration)
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	__N/A_
Accounting (includes AMA billing)	__N/A_
Performance (includes operational measurements)	__N/A_

7.19 Glossary

Term	Description
ABI	Access Bridge Interface
ALT	Automatic Line Test
EBS	Electronic Business Set
EDTU	Enhanced Digital Test Unit
LNSTRBL	Lines Service Trouble
LTP	Lines Test Position
LTU	Line Test Unit
MAP	Maintenance and Administration Position
MBS	Meridian Business Set
MTM	Maintenance Trunk Module
MTU	Metallic Test Unit
NTT	No Test Trunk
RDT	Remote Digital Terminal
RMM	Remote Maintenance Module

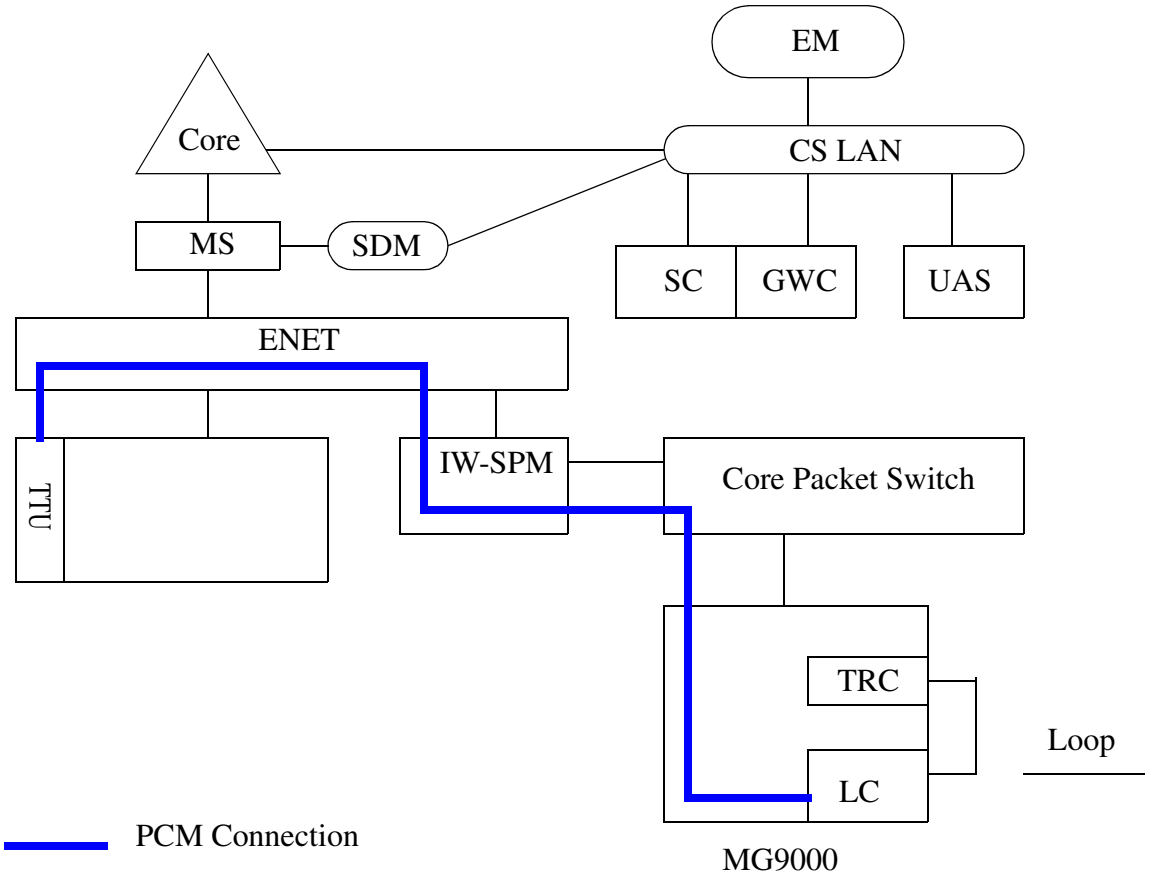
Term	Description
SSMAN	Silent SwitchMAN test
TTT	Transmission Test Trunk
TTU	Transmission Test Unit

Appendix 1: Test Configuration Diagrams

This appendix contains configuration diagrams for the various CS2000 line test functions. This information is intended to aid in trouble shooting testing issues. The commands that are not listed do not require any test equipment. For example the SUSTATE command does not require line test equipment so a configuration diagram is not shown.

DIAG

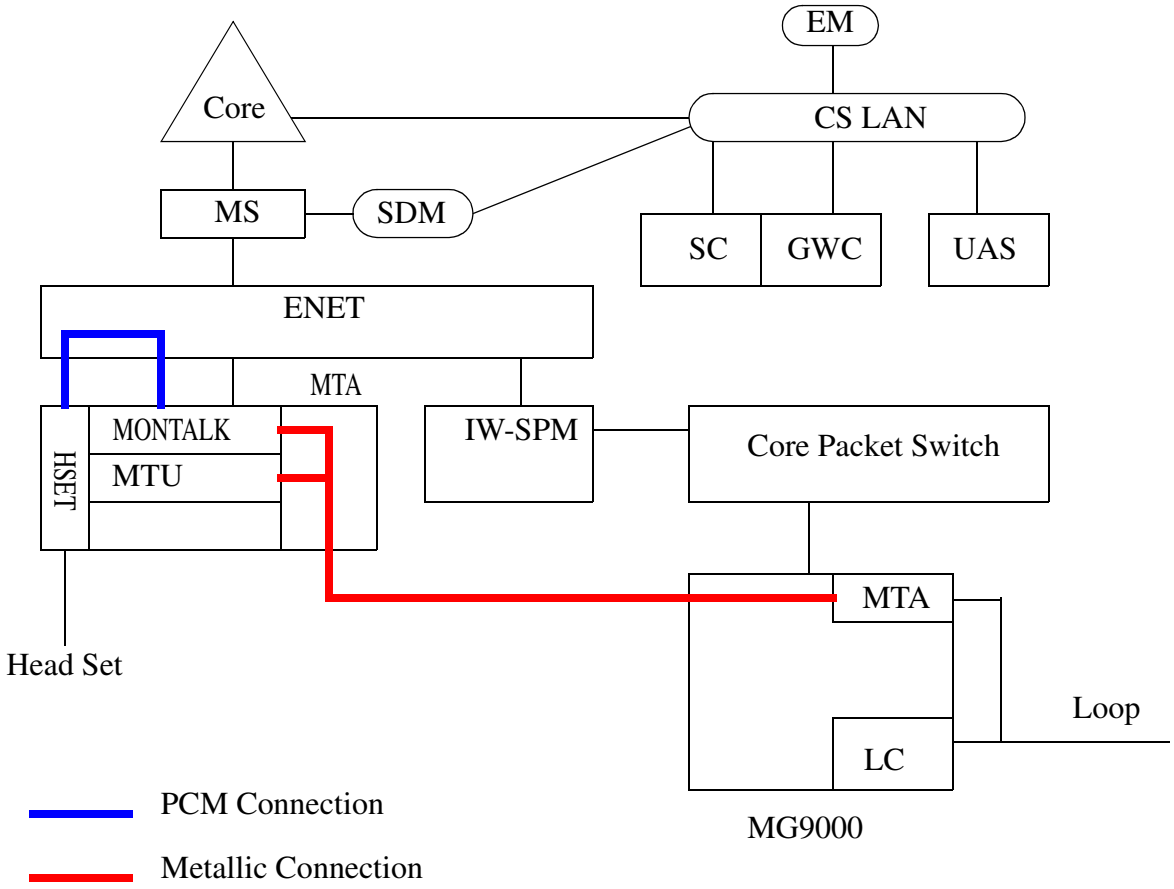
For POTS, Coin and groundstart lines, a TTU located in an ISM/MTM shelf is used during the linecard diagnostic.



The transmission tests are not supported for PPhone lines in the SN06.2 release. Therefore, no external test equipment is required when executing a diagnostic on a MG9000 PPhone line.

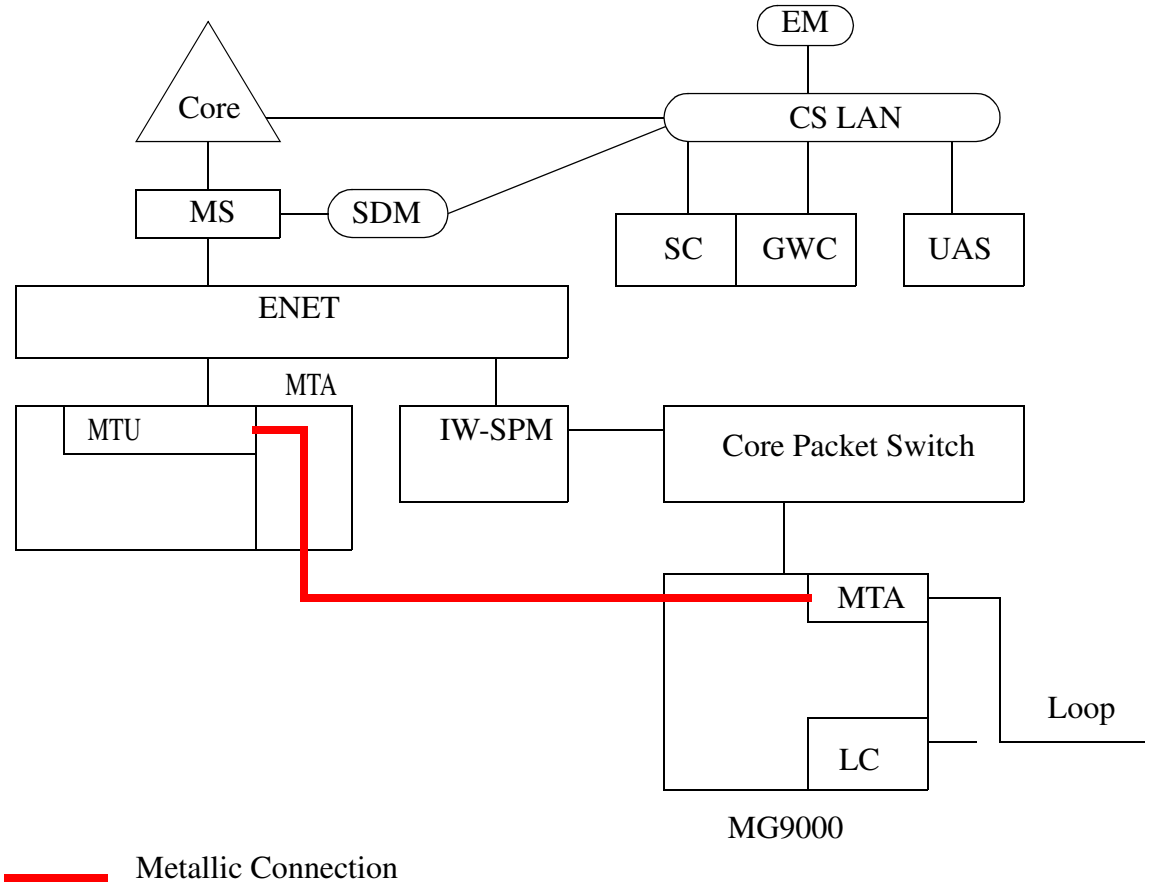
MONLTA, TALKLTA, ORIG, COIN, RING, DGTTST

The following diagram shows the configuration used when the above listed commands are performed on an MG9000 line.



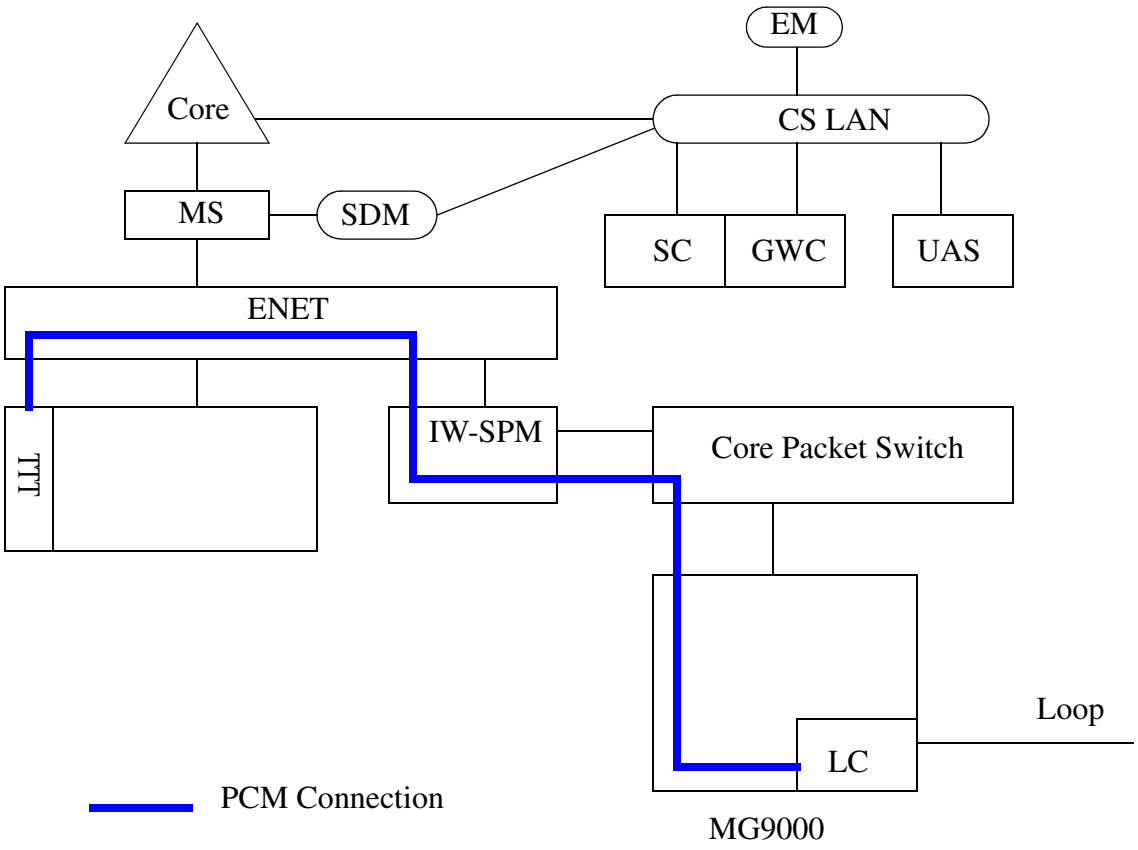
LNTST, VDC, VAC, RES, CAP, LTA

The following diagram shows the configuration used when the above listed commands are performed on an MG9000 line.



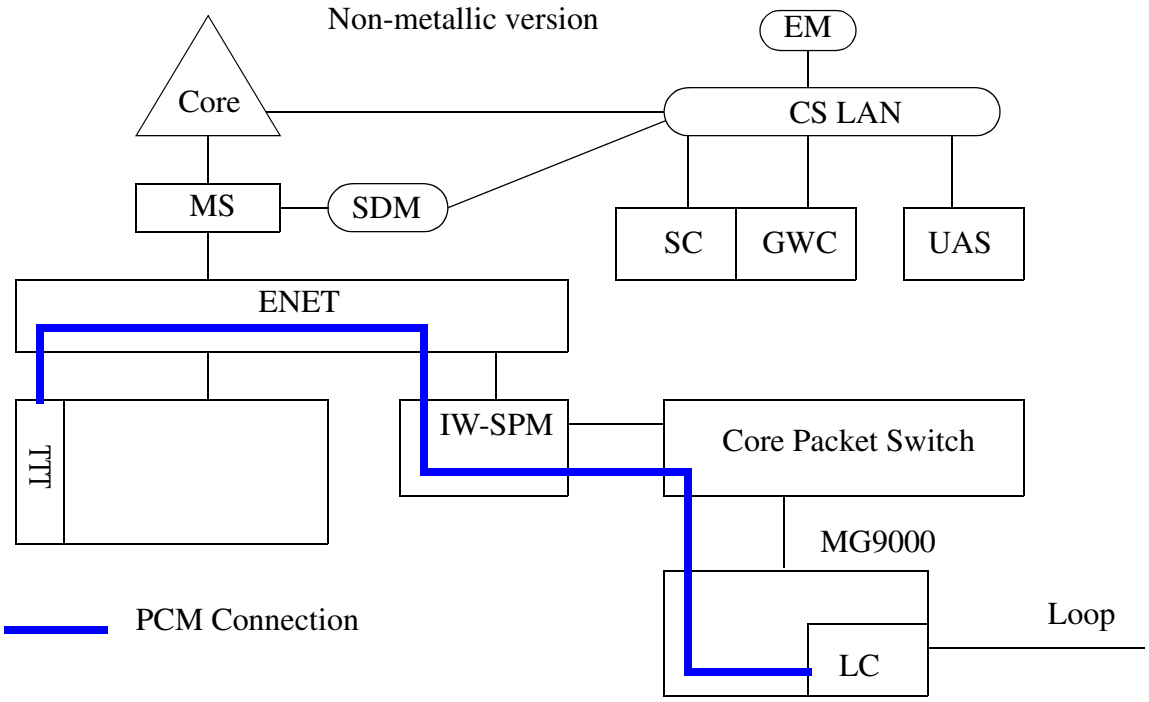
LOSS, NOISE

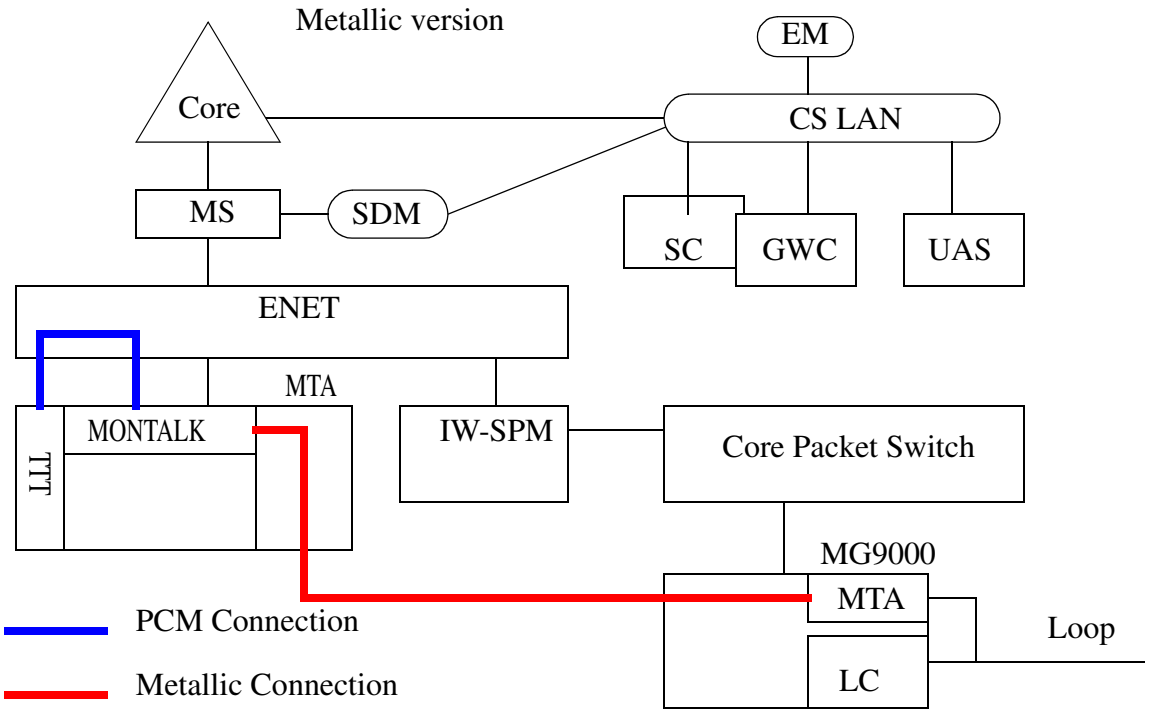
The following diagram shows the configuration used when the above listed commands are performed on an MG9000 line.



TONEGEN

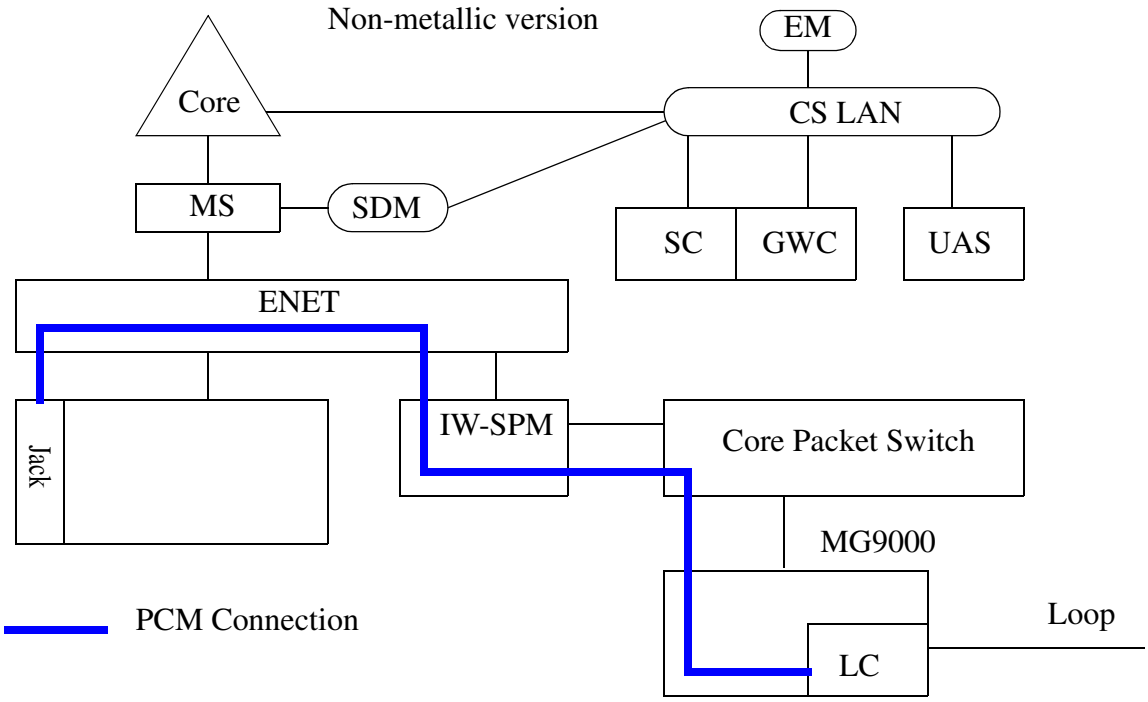
There are two versions of the TONEGEN command, the metallic and non-metallic version.

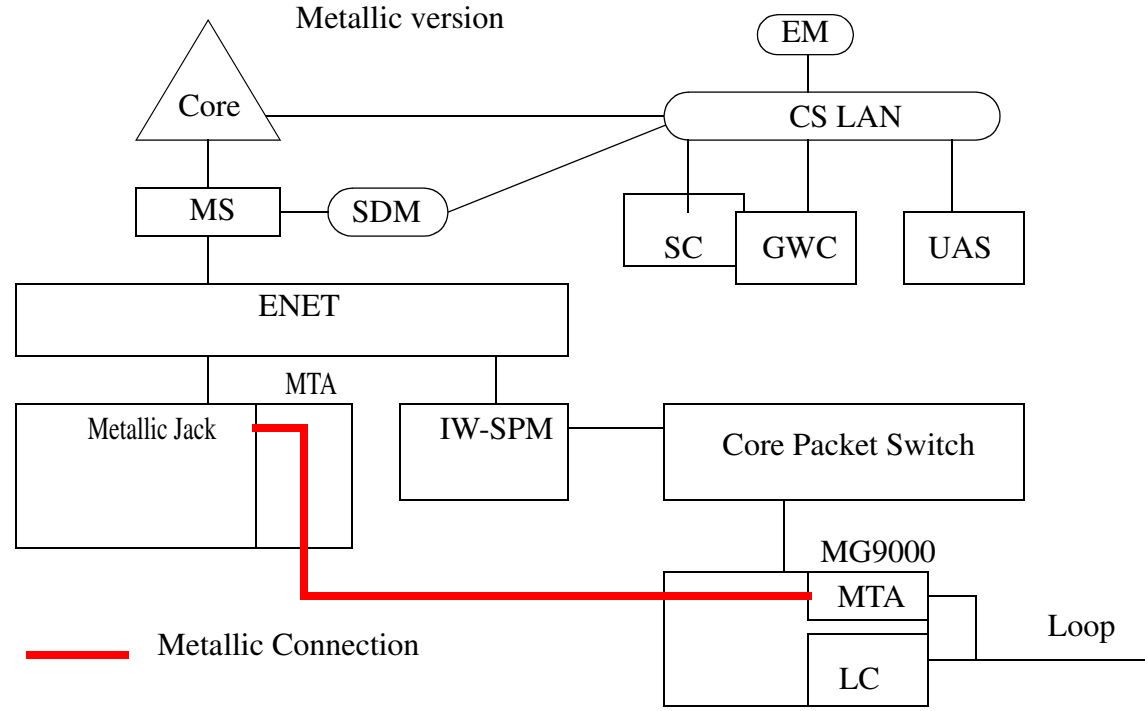




JACK

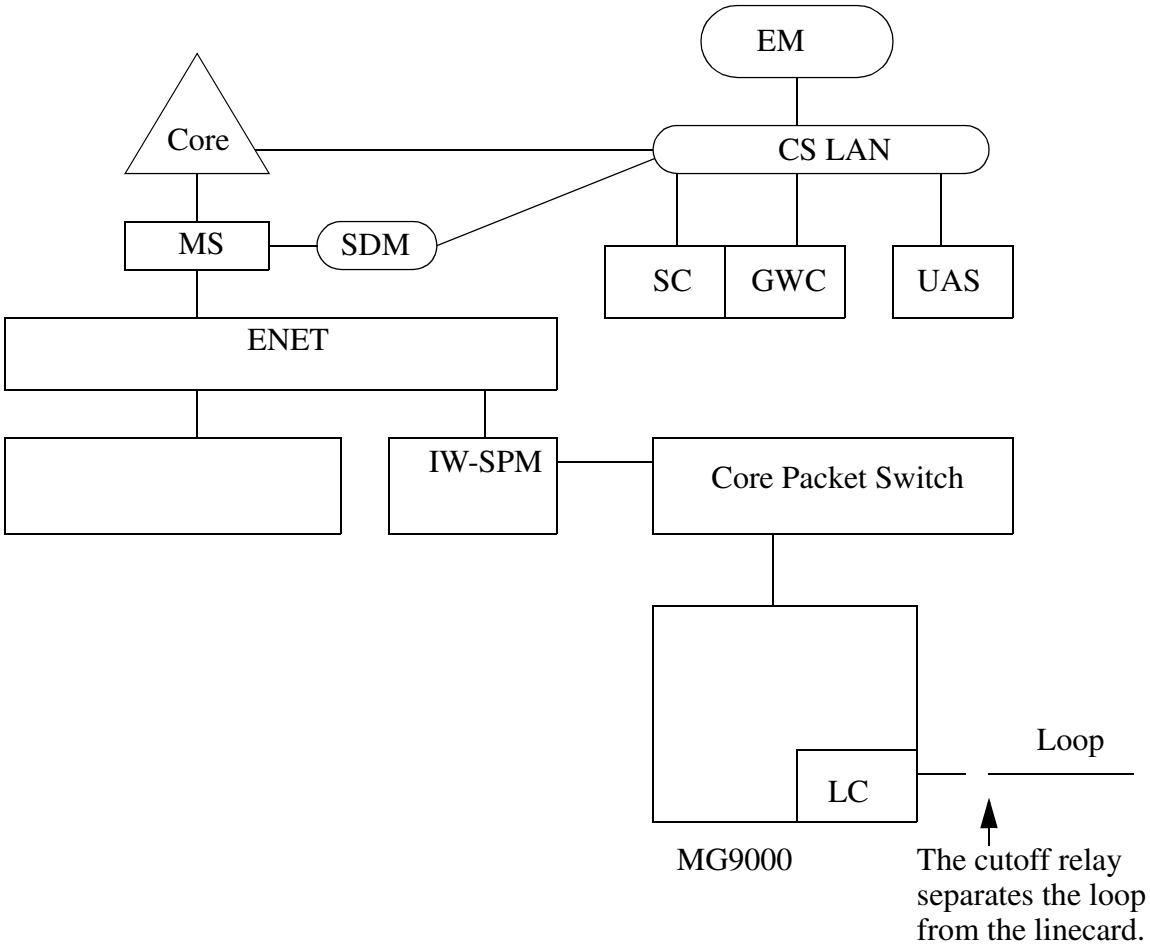
There are two versions of the JACK command, the metallic and non-metallic version





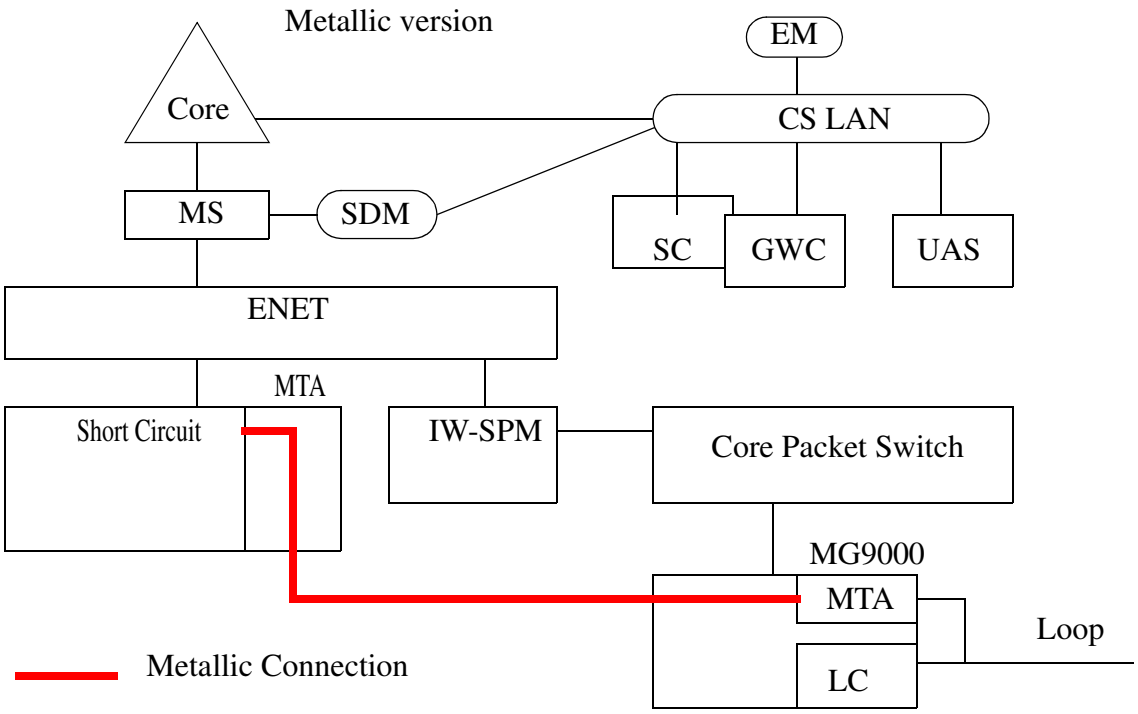
SSMAN

The silent switchman test allows a craftsperson to dial an access code and have the switch automatically apply an open condition to the subscriber loop for a provisioned period of time. No external test equipment is used. However, the metallic test resources in the MG9000 are used. Therefore the SSMAN test can be blocked if the metallic test resources in the MG9000 are already in use.



DSCKT

The dialable short circuit allows a craftsperson to dial an access code and have the switch automatically apply a short to the subscriber loop for a provisioned period of time.



ALT SDIAG

ALT SDIAG for MG9000 lines use the same equipment as LTP DIAG. Refer to the DIAG section for the test equipment configuration diagram.

ALT LIT

ALT LIT use the same equipment as the LNTST, VDC, VAC, RES, CAP commands. Refer to the test configuration diagrams for those commands.

ShowerQ

The ShowerQ diagnostic runs the same diagnostic as the LTP and ALT diagnostics; therefore, the same equipment is used. Refer to the DIAG section for the test equipment configuration diagram.

8: Functional Description (FN): A00001890

The FN islocated under the activity A00001888.

8.1 Feature name

8.2 Description

8.3 Hardware Requirements or Dependencies

8.4 Software Requirements or Dependencies

8.5 Limitations and restrictions

8.6 Interactions

8.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

8.8 Glossary

Term	Description
New term	Definition

9: Functional Description (FN): A00001893 and A00001894

9.1 Feature name

The name of this feature is MG9K Imaging, A00001893 and A00001894.

9.2 Document version

/main/pnmdoc/4

9.3 Description

Currently, there is not a concept of imaging a Media Gateway 9000 (MG9K) device load from the Media Gateway 9000 Element Manager (MG9K EM) or any other application. This means that after a new load is loaded into a Supercore OC3, ITX, ITP, DS1, or ABI device, each device must then be patched up to date. This process can take hours, days and some times months depending on the size of the office, the number of patches and the maintenance window.

This feature will provide a means for the customer to upgrade an MG9K Device, patch the device up to date, image the MG9K Device load with the patches applied and then upgrade the rest of the devices in the office with the imaged load.

This feature will also provide a means for imaging to occur automatically so that after the upgrade, if more patches arrive to the site, the customer can continuously keep a stored, up to date, imaged load.

This feature introduces MG9K device imaging from the following Succession applications:

- MG9K Element Manager (MG9K EM)
- Network Patch Manager (NPM)

The MG9K EM will provide an interface for the user to image one MG9K Device at a time. The NPM will provide a mechanism for the user to image a device via a maintenance command through the NPM user interfaces as well as schedule an imaging task through the NPM scheduler.

Note: the NPM will provide a mechanism for the user to request images of multiple device loads, but the MG9K EM will only be able to image one device at time per Network Element.

9.3.1 Media Gateway 9000 Element Manager

This feature will change the MG9K Element Manager Graphical User Interface (GUI) at the card level as well as asking the user to provide additional information at start up time for the MG9K EM Server.

9.3.1.1 Security

This feature does not change any of the login procedures or security level access for the MG9K EM, however, this feature does require that the user have emsadm or emsrw level of security in order to execute the Software Image command.Otherwise the command will be greyed out indicating that the user does not have access to execute the command.

9.3.1.2 Logs

This feature will introduce a new Information log that will indicate a success or failure of an image as well a a new Audit log that will indicate user access of the image command.

However, it is not the responsibility of this document to discuss the log information as it will be provided in a separate log document for this feature. This information is being provided here so the reader of this document can be aware of the new logs.

9.3.1.3 MG9K EM Server Configuration

Configuration for the MG9K EM will change when a user executes the mg9kconfig.sh script from the /opt/nortel/mg9ksrv_xx/bin directory on the SSPFS platform.

When a user executes the mg9kconfig.sh script before start up of the MG9K Server, the user will be asked to provide the following information:

- Image Server - the load server where the load images will be stored
- Image Server User ID - the user id for the load server that has ftp access
- Image Server password - the password for the load server user id
- Supercore IMA Image Directory - directory where the image for this load type will be stored.
- SuperCore OC2 Image Directory - directory where the image for this load type will be stored.
- ITP Image Directory - directory where the image for this load type will be stored.
- ITX Image Directory - directory where the image for this load type will be stored.

- DS1 Image Directory - directory where the image for this load type will be stored.
- ABI Image Directory -directory where the image for this load type will be stored.

The mg9kconfig.sh script will provide a default Image Directory for the user that will be located at: /swd/mg9k.

The user can change this information by executing the ./mg9kserver config script located in /opt/nortel/mg9ksrv_xx/bin. This command can be executed after the MG9K server is running. This feature will provide a "*Change Imaging Server Settings*" Menu in this script so that the default software imaging parameters can be changed without executing the entire mg9kconfig.sh script again.

9.3.1.4 MG9K EM GUI

This feature changes the MG9K EM GUI at the card level only. An additional item named *Software Image* will be added to the *Actions* menu. The Software Image function is performed on a **per card basis** and is only available for the SuperCore OC3, SuperCore IMA, ITP, ITX, DS1 and ABI cards.

As part of manual imaging, the MG9K EM will obtain patch information from the Network Patch Manager. This information will help the user to determine if there is any reason the device load should not be imaged. If the NPM determines any of the following conditions, a *Warning* message will be sent to the user:

- the device load contains obsolete patches
- the device load contains patches that are on hold
- the device itself is on hold
- the device load is at a lower patch level then the previously image load.

A *Failure* message will be sent to the user if communication with the NPM cannot be obtained. However, in all of these instances, the user will have the ability to override these conditions and continue with the image.

9.3.1.5 Image File

The name of the image file created by imaging is pre-determined and **CANNOT** be configured. The imaged file name will be based on the name of the load file with a ".tar" extension. For example, if the file name of the load is SCOA07AA_GZ, the imaged load file name will be SCOA07AA_GZ.tar. This is the name of the load file that should be used when the user is ready to upgrade or re-load devices from disk.

9.3.1.6 FTP Configuration

This feature requires that the FTP server that is used for images have an FTP user configured that has read AND overwrite access to the server. After an image file is created once, every subsequent image of that load will be overwritten. NOTE: only the image file will be overwritten, not the original load file.

9.3.2 Network Patch Manager

The NPM will offer the ability to image an MG9K Device via a new maintenance command; *SmartImage*. This new maintenance command will "look and feel" like the other maintenance commands in the NPM.

Unlike manual imaging from the MG9K EM, the *SmartImage* command utilizes a patching criteria that will determine if the devices that the user wishes to image *should* be imaged.

9.3.2.1 NPM PreDefined Device Sets

This feature will introduce two new predefined device sets to the NPM:

- MG9KDEVICES
- GWCDEVICES

Each of these sets will include all of the devices of the device type they reference. For example, MG9K Devices will include all of the MG9K type devices; OC3, ITP, ITX, DS1, and ABI. It will be recommended that the user utilize these sets when executing the *SmartImage* command.

9.3.2.2 NPM Patching Criteria

Basically, the criteria for the SmartImage command boils down to which device(s) contains the highest patch content.

Because this is the "focus" of the criteria, it is essential that the user be aware of what they are doing when they image a device from the NPM. It is **highly** recommended that the user only use the "device sets" that will be provided as part of this feature. Otherwise, an image of a device could be taken that does not contain the highest patch content.

This criteria is the same criteria that is used today for auto imaging ISN and Gateway controller devices.

9.3.2.3 NPM GUI/CLUI

This feature will add a new command called *SmartImage* to the NPM GUI and CLUI. The new SmartImage command will appear under maintenance commands in the Task window for the GUI and will be part of the maintenance group of commands listed in the CLUI.

9.3.2.4 Scheduling

The *SmartImage* command can be saved as a task and can be scheduled as part of the NPM System Plan via the NPM GUI or CLUI for auto imaging. It is recommended that when scheduling the SmartImage task, auto apply be scheduled and executed before the *SmartImage* task.

9.3.2.5 Security

This feature requires the user to have a security level of emsadm in order to execute the *SmartImage* command.

9.3.2.6 Logs

This feature will not add new log numbers for the SmartImage command. This feature will utilized the NPM maintenance log numbers that are currently available for maintenance commands.

9.4 Hardware Requirements or Dependencies

None

9.5 Software Requirements or Dependencies

This feature requires the SN07 MG9K EM, NPM and MG9K Device Software.

9.6 Limitations and restrictions

The following items are listed here as limitations from this feature:

- **SmartImage is dependant on the default information that is input at configuration time of the MG9K EM Server. If this information is not available, the user will not be able to SmartImage or auto image.**
- **SmartImage or auto imaging for the customer who does not *specialize* his office. It is for the customer who patches all devices with the same patches.**
- **The patching criteria looks at the levels of patches in a device load. Therefore is a user patches a device with 4 patches, images the device, then removes the patches and then applies 4 different patches; the level of patches since the last image has not changed and the device will not be imaged.**
- **Due to the fact that two MG9K EM Servers execute on the same SSPFS box at one time during upgrades; the customer must be aware that when the mg9kconfig.sh script asks for the image user id and image server password, they must be the same for both MG9K EM Servers executing. This is due to the fact that there will only be one secure password file for the imaging server per SSPFS platform. However, the additional information the user provides via the**

mg9kconfig.sh script can be different, including the image server IP and load image directories.

9.7 Interactions

None

9.8 Applicable customer facing sections

Fault Management	
Logs	_X____
Alarms	NA____
Configuration	
Data Schema	_NA___
User Interface	_X___
Element Management	_NA___
Security	_NA___
Service Order	_NA___
Office Parameters	_NA___
Accounting (includes AMA billing)	_NA___
Performance (includes operational measurements)	_NA___

9.9 Glossary

MG9K EM - Media Gateway 9000 Element Manager

NPM - Network Patch Manager

GUI - Graphical User Interface

CLUI - Command Line User Interface

10: Functional Description (FN): A00001895

10.1 Feature name

H323 Base Application

10.2 Description

Please refer to FN sections of feature A00001913 and A00002225.

10.3 GWC Logs

Log report GWC600 is an information log for an H.323 failure. The log entry identifies the H.323 failure condition and describes the specific reason for the failure. Please refer to FM section of feature A00001895.

10.4 Hardware Requirements or Dependencies

None

10.5 Software Requirements or Dependencies

None

10.6 Limitations and restrictions

10.6.1 CS2K H.323 limitations

1 CS2K H323 system does not support silence suppression codecs (e.g. G.729b or G.729ab, G.723).

2 Comfort noise on CS2K-H.323 is not supported.

3 ~~CS2K H323 system cannot currently support T.38. Any support for FAX or Modem operations SHOULD be provided via Mediatrix 1104/1124.~~

4 ~~The capacity of an H323 GW cannot be changed after initial installation without taking the GW OOS. Bsy/INB the trunks in order to change capacity or ip address.~~

5 The NAT dynamic mapping timeout in the router should be set high enough in order to keep those long duration calls active - where user tries to invoke a feature after talking for a long period of time. See Config notes.

6 DISA Services :

- For CS2K H.323, DISA DN hosted off of BCM is NOT supported.
- When a Carrier Based Line (CICM, MediaTrix, etc) dials a DISA DN hosted on the CS2K, the DISA DN grants access to a Hosted IPPBX Enterprise (e.g. S1000) without any workaround.

- DISA is NOT supported when a Carrier Based Line (CICM, MediaTrix, etc) dials a DISA DN hosted on the S1000/S1000M/BCM.
- When an H.323 IPPBX Line (BCM, S1000, S1000M etc) dial a DISA DN hosted on the S1000/S1000M DISA call works without any work around.
- When an H.323 IPPBX Line (BCM, S1000, S1000M etc) dial a DISA DN hosted on the CS2K, the call should route to ISUP looparounds (on a PVG) before terminating to DISA.

7 To preserve DPNSS VPN network capabilities calls between the Westell H323-DPNSS trunks and other agents (line or PVG) must be routed via SIP-T IBN7(DFT) looparound trunks to preserve DPNSS VPN network capabilities. Also trunks and lines should be in the same network (i.e. the customer groups of the line and trunk have the same NETNAME value) and the CLID option for the line's customer group set to ONNET to get CLI display for all VPN calls (or OFFNET if you want CLI display for all calls).

8 Currently CS2K H.323 use H.450 for DPNSS tunneling only and it does not support any H.450 based supplementary features.

9 The TCP keepalive is disabled by default to prevent the active calls after the warm swact from dropping (except when the call involves Cisco GW, in which case call drops after the warm swact).

10 Inter-working between H.323 and the IW SPM is not supported. Loop around trunk should be used instead.

11 Slow start calls will be supported with G.711 only.

12 Any call which involves both APG and Media portal is not supported.

13 CNDB (Calling Number Delivery Blocking) and CNNB (Calling Name and Number Delivery Blocking) Features work with following datafill:

Table LTDATA should have the following datafill for the H.323 PRI Trunk:

"Serv Serv Y N Screened Always PRI_IP_PROT H.323"

14 In order to prevent Glare on the H.323 trunk, trunk selection order should be set as ASEQ and NOT MIDL.

15 When a call originates from either Cisco GW, BCM or M1/ S1000, where originator has blocked his calling party number and name then those fields are NOT delivered to the CS2K marked as 'private' instead those field are sent to the CS2K marked as 'unavailable'. This causes feature e.g. ACRJ not to work, where a terminator had chosen to reject all incoming private calls.

16 When a BCM is configured to route calls to lines (MG9K, Mediatrix, or native) using the Private route type on the BCM, the calling number will be delivered as 'unknown' number. To allow the calling number to be presented to lines when calling from a BCM a route type other than Private should be used.

10.6.2 H.323 Gateway limitations

1 For the calls terminating on the S1000M1 and S1000 NET_RINGBACK_ON option must be provisioned in the TABLE LTDATA for all S1000M1 and S1000 trunk CLLIs in order to get the audiable ringback tone during the Call Setup (at the time of ALERTing).

2 ~~S1000M and S1000 do not support Calling Name Delivery to Non-MCDN endpoints.~~

3 ~~S1000M and S1000 do not support Calling Name Display on S1000M/ S1000 phones from Non-MCDN endpoints either.~~

4 The BCM GW does not support SlowStart signalling on origination.

5 The CS2K H323 System currently interoperates with Cisco's H323 IOS-version 12.2(13b) GWs , however there are a number of restrictions to be addressed in a future load release from Cisco:

a. Cisco calls are terminated by the GW 1 minute after a GWC warm SWACT.

b. Cisco GWs must be configured in a 1:1 static bind NAT configuration

c. For call scenarios where the Cisco GW is to connect to the UAS, and the Media Portal is present in the call topology due to NAT/FW traversal, the Cisco GW must be configured to transmit/receive immediately.

~~d. Slow start termination on Cisco GW is not supported with H245 tunneling enabled~~

6 For Core Cold and Reload restarts and for GWC Cold SWACT H.323 calls may not get dropped in the H.323 GWs and will be dropped in the Core. After a warm SWACT on the GWC, any attempted tcp messaging caused by a feature activation or dtmf key press (if it is conveyed by out of bandmsgs) will cause a warm swacted call to drop.

7 The following are few features which are not currently supported on the CS2K H.323 IPPBX

- Executive Busy Override (EBO)
- Automatic Call Back (ACB), however Network Ring Again is supported for calls within the same customer group
- Release Link Trunk (RLT)
- Malicious Call Hold (MCH), however MCH is supported on the Carrier Based Lines (CICM, MediaTrix, etc)
- Network ACD

8 Codec Provisioning: If a H.323 GW can support both G.711 and G.729 then G.711 should be provisioned as a defualt codec and G.729 should be provisioned as a preferred codec. No GW should be configured as have only G.729 codec. Configure BCM3.5 to have no preferred codec & to have G711 as the default codec. For the BCM3.5 Unified Manager, there is a need to set G711 as the default codec for Nortel IP terminal. **Configure BCM 3.6 gateways to have G.711 as default & G.729 preferred.**

9 H.323 calls with only Symmetric codec and ptime are supported (H.323 GW must receive what send - i.e. if send G711 must receive G711, if send 20ms must receive 20ms).

10 ~~When the ethernet cable at the back of the Westell GW is disconnected (for longer than 3 time-to-live periods, each of which is 30 secs) the Westell GW fails to automatically re-register with the CS2K upon reconnection of the cable. In these cases, manual recovery action is required to bring the Westell GW back into service.~~

11 M1 Conference Keys only works after the conference party answers the call.

12 S1000M do not send any packets till the CONNECT. So we need to change to the loss timer on the PVG to 0 - see config notes #3.

13 There are three different ways to carry DTMF digits:

— DTMF digits are carried as inband DTMF tone. But low bit-rate voice codecs such as G.729 cannot be guaranteed to reproduce these tone signals accurately enough for automatic recognition

— Out of band DTMF digits in signaling

— Using RTP payload to carry DTMF digits, Telephony Tones and Telephony Signals as specified in RFC2833.

As listed above, inband DTMF tone is not sufficient for certain codecs such as G.729. RFC 2833 solves the problem by carrying DTMF digits in the RTP Payload with special encoded RTP packets, but currently certain H.323 GWs such as BCM, S1000M/S1000 do not support RFC 2833.

Following is a list of ways to carry DTMF digits between different GWs:

Table 1 Method Used to carry DTMF digits between different GWs:

Termination Origination	**To H.323 GWs which Supports RFC 2833**	**H.323 GWs which do Not supports RFC 2833**
From H.323 GWs which Supports RFC 2833	RFC 2833	Out of Band DTMF Signaling
From H.323 GWs which do Not Support RFC 2833	Out of Band DTMF Signaling	Out of Band DTMF Signaling

Table 1 Method Used to carry DTMF digits between different GWs:

Termination Origination	**To H.323 GWs which Supports RFC 2833**	**H.323 GWs which do Not supports RFC 2833**
From PVG Supports (PVG RFC 2833)	RFC 2833	DTMF digits pressed on the phone off H.323 GW are delivered to PVG in out of band dtmf signaling, PVG will play out the tone DTMF digits pressed on the phone off PVG: - G.711 Codec H.323 does not request to collect DTMF digits, so DTMF from PVG will be delivered as in band tone - G.729 Codec H.323 does request PVG to collect DTMF digits, so DTMF from PVG will be delivered as out of band signaling
Mediatrix Supports (Mediatrix supports RFC 2833)	RFC 2833	DTMF digits pressed on the phone off H.323 GW are delivered to mediatrix GWC in out of band dtmf signaling, but Mediatrix side will NOT play out the tone H.323 does not request mediatrix to collect DTMF digits, so DTMF pressed on mediatrix will be delivered as in band tone

10.6.3 H.323 Protocol limitations

1 H.323 protocol does not support providing audible ringback tones to the H.323 subscriber after a call has been answered. Due to this, the H.323 subscriber will hear silence in certain feature interaction scenarios instead of audible ringback. These scenarios include:

- a line gateway (such as Mediatrix) invokes call park on a call that it received from an H.323 subscriber. In this scenario, the H.323 subscriber will hear silence until the call is retrieved.
- a line gateway (such as Mediatrix) is involved in a call with an H.323 subscriber, followed by the line gateway initiating a conference to another party. If the third party is conferenced into the call while still alerting, the H.323 subscriber will not receive audible ringback. (Note: If the third party is connected via a TDM ISUP trunk, then audible ringback will be provided by the terminating office and will be heard.)

- a line gateway (such as Mediatrix) performs a call transfer of an answered call from an H.323 subscriber to an alerting party.
- certain ACD/UCD scenarios where the call is queued after answer.

In these scenarios, the service interaction will function as normal, except for the fact the H.323 subscriber will hear silence as opposed to audible ringback. Since all of these scenarios involve answered calls, the H.323 subscriber will most likely know that they're on hold and waiting for some action to complete.

10.7 Configuration Notes

1 Add the NET_RINGBACK_ON in the table ltdata to the get the network ringback for the S1000M terminating call.

```
Examples:
```

ISDN 13 SERV

SERV Y Y ALWAYS ALWAYS (NET_RINGBACK_ON) (PRI_IP_PROT H323) $

ISDN 14 SERV

SERV Y Y ALWAYS ALWAYS (NET_RINGBACK_ON) (PRI_IP_PROT H323) $

2 Media proxy (RTP Portal) must be associated in SESM -> GWC# ->Provisioning -> Media Proxies -> for all GWCs (line, trunk, UAS and H.323 GWCs).

3 S1000M do not send any packets till the CONNECT. So we need to change to the loss timer on the PVG to 0.

Telnet to your PVG

and check the card slot you are using on the PVG :

St prov

set nsta/13 vgs brag/1 loss 0

set nsta/13 vgs brag/2 loss 0

…..

set nsta/13 vgs brag/16 loss 0

act prov

confirm prov

4 Make sure that the RFC 2833 is clicked in the SESM ‘Configure Network’ GUI, if the RFC 2833 support is required for the In-band DTMF tones.

5 Make sure that the appropriate DEFAULT CODEC is selected for a particular market (e.g. G.711 u-Law is selected for North America and G.711 a-Law is selected for International). Also make sure that G.729 is selected in the SESM ‘Configure Network-> Compression Codec’ GUI, if the G.729 codec support is required.

6 The two configuration rules must be setup for each H.323 GW which in the Enterprise IP-VPN on the NAT router. The first rule maps the RAS port of the GW (UDP transport) to NATed IP(of the NAT router) + port (X open on the NAT router). The second rule maps the Call signalling port of the GW (TCP transport) to the NATed IP(of the NAT router) + port (X+1open on the NAT router).

Example:
10.19.199.195(NAT Router IPAddress):7000(port on the NAT router)<-> 10.88.88.55(H.323 GW IP address):1719(RAS port on the GW)

10.19.199.195(NAT Router IPAddress):7001(port on the NAT router)<-> 10.88.88.55(H.323 GW IP address):1720(Call Sig. port on the GW)

7 For gateways -e.g. Cisco GWs- that do not provide a static RAS port, N:1 addressing is not an option as mapping the port must be done dynamically. This is a NAT 1:1 configuration and although supported in a limited fashion, devices requiring this configuration may require code changes, which is already supported for Cisco GWs, in the CS2K to support registration and call processing.

8 If a H323 gateway in International market does not support overlap signaling for termination, then the translation in the core should be set to do en-bloc signaling by using the TABLE PXCODE and minmax mm option to control for the en-bloc sending.

9 The “INTER DOMAIN" bool is in the TABLE TRKOPTS for the SIP-T Trunks should be set as follows

- "INTER DOMAIN" bool should be set to Y (i.e. inter-domain) for all SIP-T trunks except loop-around trunks.
- "INTER DOMAIN" bool should be set to N (i.e. intra-domain) for SIP-T loop-around trunks.

10 To hear the busy tone when calling from S1000M/S1000 phone to a A Busied Line. Apply the BHC19 patch and ensure AUDTRMT is set to "Y" on the TABLE LTID for S1000M/S1000 trunks.

11 Do not enable e.164 registration in the H.323 GW as this kind of registration is not supported by GWC.

12 For NATs with per-protocol timeouts, recommend timer values are

- For TCP (for Call Signaling) bind timeout of 35 minutes.
- For UDP (for RAS) bind timeout of 3 minutes.

For NATs that have a single global timeout value, a bind timeout value of 35 minutes is recommended.

10.8 Interactions

10.9 Applicable customer facing sections

Fault Management

Logs ____Y__

Alarms ____ Y_

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

10.10 Glossary

Term	Description
GWC	Gateway Controller
GK	H.323 Gatekeeper

Term	Description
RAS	Registration Admission Status H.323 message
RRQ	Registration Request

11: Functional description (FN): A00001898

11.1 Feature name

A00001898 - ABI RMM Support

11.2 Description

This activity adds support for hosting a Remote Maintenance Module (RMM) off of ABI-based XPMs, specifically the LTC, LTCI, LGC, LGCI, and SMA2. The need for an RMM hosted off peripherals other than the RCC/RCC2 type peripheral has come about due to the office collapse scenarios in which central office based XPMs such as LTCs, LGCs, and SMA2s are no longer co-resident with the Call Server. In these collapsed office sites there is a need to perform metallic line testing on these peripherals, but the existing MTM test resources are no longer available (MTMs must be hosted off of the ENET and hence cannot be present in the collapsed sites as there is no longer an ENET in these sites).

To fill this gap the RMM will be used for test access, but it needs to be reconfigured to be properly supported in the new environment where it is not part of the RSC/RSCS setup. The RMM uses DS30A links to connect to it's host peripheral, which is perfectly fine for the LTC/LGC type XPMs, but is a problem for the SMA2. The SMA2, prior to this activity, did not support a DS30A type interface on it's P-side. With this activity we will add the capability for the SMA2 to host DS30A based subtending RMMs. This means that core provisioning, core maintenance, and the SMA2 load itself need to be altered to support the new DS30A interface.

Another issue with the RMM involves the hardware configuration. Specifically, the RMM has in the past always been sold by Nortel as a component of the RSC/RSCS, not as a stand-alone piece of hardware. For this activity the RMM needs to be supported in a new frame, and new cabling needs to be configured to allow it to be connected to the new host peripherals. This new hardware setup needs to be documented and made available to the customer to be installed in the collapsed office sites.

11.3 Hardware Requirements or Dependencies

There are two new hardware requirements for this project, the RMM frame and the DS30A card and cable to the RMM.

11.3.1 RMM Frames

The RMM will be housed in a MIS frame. This is an existing frametype, but prior to this feature, was not used to house RMM shelves. This frame type will be used regardless of whether the RMM subtends the SMA2 or LTC/LGC.

11.3.2 RMM Circuit Packs

The following circuits packs will be supported in an RMM in the ABI configuration. . The pack are:

- 0X10: Scan Detector
- 2X11: MTU, (Mult-Line Test Unit)
- 2X57: Signal Distribution Card
- 2X90: Datafilled as a Montalk or NTT (No Test Trunk)
- 3Z09: MTA (Metallic Test Access)

11.3.3 DS30A Cards and Cables

See the Engineering Information section of this feature for more details than the summary below.

An RMM requires a DS30A interface to its host XPM. The SMA2 requires a MX74 DS30A card to interface the RMM. Prior to this feature, a DS30A card could not be provisioned on an SMA2 in LTCPSINV.

In addition a new cable is required to interface from the MX74 on the SMA2 to the RMM.

The LGC/LTC XPMs already supported a DS30A interface (6X48 card) prior to this feature. This card will be used for interfacing the RMM, but a new cable is required to connect from the LTC/LGC to the RMM.

11.4 Software Requirements or Dependencies

This activity will be implemented in the SN07 stream in the CM, but due to customer requirements will be patched back into the SN06 CM release (officially this is called the SN06.2 release).

There are several other acitivies that are required to complete the support of the RMM. They include A00001847 - ABI Expansion, and A00001936 - MG9K ABI Expansion - Node & Link Mtc.

11.5 Limitations and restrictions

The following limitations and restrictions exist for this activity:

- The RMM will only be supported on the LGC/LTC , and SMA2. The RMM will not be supported on the SMS in SN06.2.
- Only a single RMM will be supported hosted off an SMA2. This is due to the provisioning restriction whereby only a single DS30A link is allowed on the P-side of the SMA2.

- Only the circuits listed in section “11.3.2 RMM Circuit Packs” on page 204 are supported on an ABI RMM. No effort has been made to prevent the datafill of other circuits packs, but they will not be supported.
- The RMM Selector field in table RMMINV will be set to RMMLTC for both LTCs and LGCs. This is done because the two types of peripherals are treated exactly the same (and are essentially alike from a hardware perspective) in their handling.

11.6 Interactions

None

11.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema __X___

User Interface __X__

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

11.8 Glossary

Term	Description
New term	Definition

12: Functional description (FN): A00001935

12.1 Feature name

Provisioning Support for Centrex-IP Nodes and Lines

12.2 Description

Feature A0001935 will deliver the lines flow through and pre-provisioning functionality in the Succession Element and Sub-element Manager (SESM) required for the Centrex IP Client Manager (CICM) integration with Succession. The design will be split into Nodes provisioning for CICM Gateways (GWs), and lines provisioning for CICM terminations.
The Nodes provisioning feature component will provide for the provisioning of CICM GWs. Nodes provisioning will also provide functionality to pre-provision the CICM terminations in the GWC-EM and to pre-provision LENs (Line Equipment Numbers) in XACore table LNINV. The Lines Provisioning component will provide flow through of service information entered at OSSGate (SERVORD+ commands). New line provisioning functionality will be delivered to allow line data to be transmitted to the CICM Element Manager (CICM-EM).

12.3 Hardware Requirements or Dependencies

Not applicable.

12.4 Software Requirements or Dependencies

Not applicable.

12.5 Limitations and restrictions

None.

12.6 Interactions

This feature will integrate the Centrex-IP client provisioning with the existing Succession SERVORD+ system. Centrex-IP client ommands/data will distributed to the CICM-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the CICM-EM from SESM SERVORD+:

- NEW, EST, ADD, OUT, DEL, CDN, CHDN, CLN/CTP, CKLN/CKTP, ADO, DEO, CHF

This list is subject to change until final DSUM approval.

12.7 Applicable customer facing sections

Fault Management

- Logs __N/A_
- Alarms __N/A_

Configuration

- Data Schema ___X__
- User Interface __N/A_
- Element Management __N/A_
- Security __N/A_
- Service Order ___X__
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

12.8 Glossary

Term	Description
New term	Definition

13: Functional Description (FN): A00001990

13.1 Feature name

CAIN via CICROUTE PEP Sourcing

13.2 Description

13.2.1 Background

Currently, CAIN subscriptions can be achieved through tables TRKGRP, AINSCUSP, UNIPROF, AUTHCODU, AUTHCDX and STDPRTCT. The sourcing of this patch will allow CAIN subscriptions to be added to table CICROUTE enabling subscription on a per CIC (Carrier Identification Code) basis. This new subscription point will allow carriers to use the SCP to route calls based on their CIC.

This functionality was originally patched into the UCS12 load. That patch has been propogated to more recent UCS loads. This activity will source the patching into the SN07 load and put it under SOC (Software Optionality Control) control.

13.2.2 Functional Description

The new subscription point will be created by adding the CAINGRP option to tuples of table CICROUTE, just as in other CAIN subscription tables. The CAINGRP option takes one argument, the service name, as defined in table CAINGRP. In the example below, CIC 333 is subscribed service SRVC1.

Table 1 CICROUTE Example with CAIN Subscription

KEY	NATLSTS	INTLSTS	MLTCOSID	OPCHIDX	PRTNM	IDPRTNM	ADIN	CICDELV	OPTIONS
333 1	611	212	0	2	CIC	EAPT	3	ALWAYS	**CAINGRP SRVC1**

CAIN precedence levels determine the order in which specific subscription types are checked for applicability at a particular TDP. The new CICROUTE subscription point will have a new precedence level of CARRIER which will fit in the current order as below:

Table 2 Precedence Level Between Subscription Types

Order	Subscription Type	Subscription Tables
1	SCP	Requested by SCP
2	Address	subtable STDPRT of STDPRTCT
3	Authorization Code	AUTHCODU, AUTHCDU*

Table 2 Precedence Level Between Subscription Types

Order	Subscription Type	Subscription Tables
4	ANI	ANICUSP, ANIVAL, UNIPROF
5	TR533_CIC	
6	Agent	TRKGRP, CALLATTR, TRKFEAT
7	**Carrier**	CICROUTE
8	Office-wide	CAINPARM

13.2.2.1 Subscribing to CAIN via table CICROUTE

The originating agent types supported by this feature are PTS FGD, SS7 FGD, and SS7 Inter IMT.

All originating trunks wishing to use the CAIN functions must have the CAIN option defined in table TRKGRP, CALLATTR, or TRKFEAT. The CICRTE option also needs to be included in TRKGRP so translations will use table CICROUTE and encounter the new subscription point.

A service and its associated triggers must be added to table CAINGRP and the triggers must have their criteria defined in the relevant subscription tables.

Once the above datafill is in place, the CAINGRP option can be added to individual tuples in table CICROUTE. The CAINGRP option takes the name of a service defined in table CAINGRP.

More general information on CAIN datafill can be found in NTPs 297-2621-370*, the UCS DMS-250 NetworkBuilder Application Guides.

13.2.2.2 CallP Behavior

When a specific TDP (Trigger Detection Point) is encountered during call processing (see NTP 297-261-370 Network Builder Application Guide, Vol. 2), each subscription method is checked in the precedence order defined above. If a subscription to a CAIN service is defined via the CAINGRP option, and the service includes a trigger of this TDP, and the trigger's criteria is met, then the trigger will have its action performed.

Adding a new subscription point to CAIN does not affect the procedure described above. A service subscribed via table CICROUTE will have its triggers evaluated at the proper TDPs.

13.2.2.3 Traver

The traver tool simulates a call from the user specified originating trunk to the user specified address. Traver displays the following CAIN-specific information at each TDP encountered:

1 The name of the TDP encountered (e.g. ORIGATT)

2 The CAIN subscription method, if any (e.g. CARRIER)

3 The tuple from table CAINGRP detailing the subscribed to service

4 The tuple from the trigger table detailing the criteria being evaluated

5 The action, if any, taken if the trigger's criteria is met

Traver will be enhanced to display the subscription method of CARRIER, the CAINGRP data and the trigger table data if a call subscribes to CAIN via CICROUTE.

The following traver snippet shows the SCP being queried when it is determined that the call is subscribed to the SPECGRP service via table CICROUTE. This example was run via

> UVTSTS 611; traver tr dal221twdtls 2201234 t

Table 3 Example Traver Output

--> ENTER TDP INFOANLZ <--
+++ CAIN SUBSCRIPTION VIA CARRIER +++
TABLE CICROUTE
110 DEF 611 611 0 11 EAN EAPT 1 ALWAYS (CAINGRP TESTGRP) (CIC_CASU) $
TABLE CAINGRP
TESTGRP 72 CAIN02 TCAP_SCCP (ANLZINFO INFOANLZ CUSTDP) $ $ (ADIN) (CAINGRP) (ORGTINFO) $ $
TABLE CUSTDP
TESTGRP ADDR 2386213513 2386213513 QUERY TREAT $
UserID: CAIN 2503EANT2WS7 111
BearerCapability: SPEECH
CalledPartyID: 2386213513
TriggerCriteriaType: CUST_INT
CallingPartyID: 619
+++ TRAVER: SUCCESSFUL CALL TRACE +++

13.2.2.4 Log Changes

Logs that indicate the subscription method will be updated to display the CIC information.

13.2.2.4.1 CAIN902 Logs

CAIN902 logs show the subscription method and other relevant details when a call subscribes to CAIN (not when the query is sent to the SCP). The

METHOD field of the log indicates the subscription type (e.g. ANI, OFFICE) and the precedence level. CAIN902 logs will indicate a METHOD of CICROUTE and a precedence level of 7 when appropriate.

13.2.2.4.2 VAMP902 Logs

VAMP902 logs are output when the VPTrace CI tool is enabled and an outbound message is sent through the VAMP framework to the SCP.

The VAMP902 log may display the subscription type via the SUBINFO field. The SUBINFO field will be enhanced by this activity to include CARRIER as a possible value.

13.2.2.5 SOC Control

This feature will be controlled by a State SOC (State is either IDLE or ON). The SOC id will be CAIN0612. Using the SOC CI command to activate or deactivate a order code is covered in NTP 297-8991-901.

Datafilling a CAINGRP option will be allowed regardless of the state of SOC CAIN0612. However, if the SOC is IDLE, the CAIN software will not recognize subscriptions via CICROUTE either during CallP or in the Traver Tool.

13.2.2.6 ONP

Reformat procs will be written as part of this feature to garauntee the validity of CICROUTE tuples whether the swtich has patch HIJ00 activated or not.

13.3 Hardware Requirements or Dependencies

N/A.

13.4 Software Requirements or Dependencies

No new dependencies are introduced by this work beyod the new SOC order code detail above. However, using the functinality of this activity depends on a number of basic CAIN SOCs detailed below.

Table 4 CAIN SOC Codes of Note

Order Code	Function
CAIN0100	Usage Option for all CAIN msgs to SCP
CAIN0200	Extenstion Paramaters
CAIN050*	SOCs to enable Specific Trigger
CAIN0600	Conversational Digit Collection
CAIN0601	SCP Trigger Subscription
CAIN0602	EDPs Enabled

Table 4 CAIN SOC Codes of Note

Order Code	Function
CAIN604	Inter IMT Support

13.5 Limitations and restrictions

Originating trunk types supported by this feature are PTS-FGD, SS7-FGD and SS7 Inter IMT. Other trunk types are incapable of passing the CIC information.

13.6 Interactions

13.6.1 Normal CIC Routing Suspended

13.6.2 If a CAINGRP is datafilled against a CICROUTE CIC, normal CIC routing will be suspended and CAIN processing will begin. For example, if the DEFCIC option is datafilled against a trunk in table TRKGRP that is supported by table CICROUTE with the DFCICRTE sub-option set (when this field is Y, the DEFCIC can be used as an index into table CICROUTE), call processing will exit and the CIC routing feature will begin CAIN processing. If a CAIN “no action” or continue response is encoutered, normal CICROUTE call processing will continue.**CAINCIC Not Affected**

The functionality of table TRKGRP option DEFCIC, sub-option CAINCIC will not be affected by this activity.

13.6.3 No Affect on CAIN Standard Routing

Standard routing paramaters CARRIER, ALTERNATECARRIER and SECONDALTERNATECARRIER will continue to be used to identify a route by obtaining an STS value through table CICROUTE.

However, if the following scenario occurs, an extra CAIN902 log will be generated.

An Analyze_Route message containing CARRIER and ALTERNATECARRIER is recieved. Table CICROUTE is accessed for the CARRIER and a CAINGRP is picked up. The subsequent route selection results in a busy condition and the call route advances to the ALTERNATECARRIER. Table CICROUTE does not have a CAINGRP option for the ATLERNATECARRIER. Carrier subscription is undone and a CAIN902 log will be output to indicate this.

13.7 Applicable customer facing sections

Fault Management

- Logs __X___
- Alarms __N/A_

Configuration

- Data Schema _____
- User Interface __N/A_
- Element Management __N/A_
- Security __X___
- Service Order __X___
- Office Parameters __X___

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) _____

13.8 Glossary

Term	Description
CAIN	Carrier Advanced Intelligent Network
CIC	Carrier Identification Code
FGD	Feature Group D (Dial Plan for EANT trunks)
ONP	One Night Process (for software upgrade)
PEP	Product Enhancement Patch
PTS	Per-Trunk Signaling
SCP	Service Control Point
SOC	Software Optionality Control
SSP	Service Switching Point
UCS	Universal Carrier Software
VAMP	Variable AIN Messaging Platform

14: Functional description (FN): A00002008

14.1 Feature name

SBA:CBM Introduction[A00002008]

14.2 Description

This document will be broken into two sub sections for each section. The first sub section will describe **Adding a Logical volume for SBA**. The sub section second will describe the procedure for **DVD Billing record backup**.

14.2.1 Adding a Logical volume for SBA

For AIX:

- The instructions have not changed and can be found in Accounting module, chapter, “Adding a logical volume for SBA“
- Alternatively, the “makelv” command described below for CBM can also be used on AIX to create a Logical Volume for SBA billing files
- The recommended "logical_volume_name" remains the same on AIX: "/sba/<stream name>".
  - i.e. /sba/ama;

For CBM:

- the "makelv" command can also be used on CBM to create a Logical Volume for SBA billing files. Consult the configuration section for the actual instructions on how to do this.

14.2.2 DVD Billing record backup

The purpose of this subsection is to describe a manual procedure for backing up billing data from the CBM to a DVD. Three procedures will be described. The First procedure will be how to blank a DVD-RW disk. The Second procedure will be what the customer will do to back up the closed sent and closed not sent billing directories using a script that is provided to them. The third procedure will document how to create a DVD without the aid of the script. This could be of use in emergency scenarios or when only specific files are to be backed up.

Note: These actions should be performed only during non-peak hours unless a DVD backup is an urgent in special case.

Note: It is worth pointing out that the tape functionality has been removed for the CBM(Solaris) system. Only DVD functionality is supported. And DVD functionality has not been added to SDM (FX) systems. Users of this system should continue to use the current tape backup procedure.

Note: It is necessary to be a root user to execute these procedures

Note: These are best effort procedures. No locking is done on the files being copied

Note: On a CBM850, if a swact occurs during any of the following procedures the action will fail and must be started again on the newly active side.

14.2.2.1 Blanking a DVD-RW

Blanking the DVD-RW erases the contents of the DVD. It is a necessary step before a DVD-RW can be written to if it has previously been written to. It is unnecessary and not possible to do this to DVD-R type DVD's.

Note: This procedure is not specific to billing. It is an sspfs general procedure.

- You first must insert the DVD-RW which you intend to blank into the DVD drive.
- First, issue the UNIX command "cdrw -l" (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdrw -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

  #> /usr/bin/cdrw -l
- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

  #> /usr/bin/eject cdrom
- After successfully inserting your DVD, list the contents of the DVD-RW with the following UNIX command to ensure that it is the DVD you intend to blank.

  #> /usr/bin/ls /cdrom/cdrom0
- If you are satisfied that this is the disc you intend to blank, then enter the following UNIX command. This step can take a significant amount of time to complete. possibly more than one hour.

  #> /usr/bin/cdrw -b all
- To confirm the DVD is now blanked. Ensure the DVD is inserted. Then enter the UNIX command below. It should return some device information and the statement "Media is blank"

  #> /usr/bin/cdrw -M

14.2.2.2 Using script to back up billing records

This is the procedure the craft person would most likely use to back up the closed sent and closed not sent directories. This method is non selective in the files that it chooses to back up. It backs up the entire contents of the selected directories. It writes the files to the DVD in the following directory format "/<Stream name>/<Directory name>/files".

> **Note:** This procedure does not move the files from closed not sent to closed sent

- The craft person should ensure that he/she has a large enough supply of blank DVD's at least one for each stream they intend to back up. possibly more if the streams are larger than 2GB. The script will alert the craft person as to the number of disks that are required for each stream before proceeding to write the records to the DVD. Note that the DVDs should be blank. Consult the blanking procedure if the DVD's are not blanked.
- You first must insert the DVD-RW which you intend to write into the DVD drive.
- First, issue the UNIX command "cdrw -l" (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdrw -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

  #> /usr/bin/cdrw -l

- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

  #> /usr/bin/eject cdrom

- The next step is to enter sbadvdwrite at a UNIX prompt to start the script. you will get the following result

```
#> sbadvdwrite
Billing Data DVD Backup
--------------------------------------------------------------------------------
This is a utility to back up closed sent and closed not sent billing records.
A blank DVD should be in inserted in the DVDRW drive.


Press Enter to proceed, or type Abort to abort:
```

- Then press enter to proceed or abort to stop the scripts execution

- Next you will be asked to select the stream you would like to back up as is shown in the following result. If no streams are configured the script will print out and error message stating so and exit.

```
Billing Data DVD Backup Stream Display
--------------------------------------------------------------------------------
The following streams are available to be backed up.

AMA
OCC
SMDR

Billing Data DVD Backup Stream Selection
--------------------------------------------------------------------------------

>AMA

Enter the stream that you would like to back up and hit return.
```

- Now enter the stream that you would like to back up or abort to stop the scripts execution.
- Then press enter to proceed or abort to stop the scripts execution

```
Press Enter to proceed, or type Abort to abort:
```

- Next you will be prompted for which directories you would like to back up. Make your selection.

```
Billing Data DVD Backup Directory Selection
--------------------------------------------------------------------------------

enter the number corresponding to the directory(s) that you want backed up
and hit return:

1    - Closed Sent
2    - Closed Not Sent
3    - Both Closed Sent and Closed Not Sent

>3
Closed sent and Closed Not Sent have been
selected for backup.
```

Press Enter to proceed, or type Abort to abort:

- Then press enter to proceed or abort to stop the scripts execution
- Then you will advised of the number of DVD's that will be required to back

'1' blank DVD(s) will be required.

Press Enter to proceed, or type Abort to abort:

- Then press enter to proceed or abort to stop the scripts execution
- Next the DVD(s) are written to. Follow the on screen instructions with regards to when to insert DVDs into the DVD tray if more than 1 DVD is required. The DVD tray will eject automatically when the DVD is finished being written to.

creating scratch /tmp/.tar 2046m d97

creating scratch /tmp/.iso 2048m d98

Looking for CD devices...

Checking for media...

Please insert a blank cd and hit <enter> OR type <abort>:

Checking for media...

Media is blank

Start cdwrite of /tmp/.tar/billingdir/, iso_space=/tmp/.iso.

Please wait...

executing /usr/bin/mkisofs -r -J -o /tmp/.iso/iso.img /tmp/.tar/billingdir/

Using P0403021.000;1 for /tmp/.tar/billingdir/closedSent/P040302182716AMA (P040302182715AMA)

Using P0403021.001;1 for /tmp/.tar/billingdir/closedSent/P040302182715AMA (P040

302182614AMA)

Using P0403021.002;1 for /tmp/.tar/billingdir/closedSent/P040302182614AMA (P040302181113AMA)

Using P0403021.003;1 for /tmp/.tar/billingdir/closedSent/P040302181113AMA (P040302181112AMA)

Using P0403021.004;1 for /tmp/.tar/billingdir/closedSent/P040302181112AMA (P040302181011AMA)

Using P0403021.005;1 for /tmp/.tar/billingdir/closedSent/P040302181011AMA (P040

302173310AMA)

Using P0403021.006;1 for /tmp/.tar/billingdir/closedSent/P040302173310AMA (P040

302173309AMA)

Using P0403021.007;1 for /tmp/.tar/billingdir/closedSent/P040302173309AMA (P040

302173108AMA)

Using P0403021.008;1 for /tmp/.tar/billingdir/closedSent/P040302173108AMA (P040

302172307AMA)

Using P0403021.009;1 for /tmp/.tar/billingdir/closedSent/P040302172307AMA (P040

302172306AMA)

Using P0403021.00A;1 for /tmp/.tar/billingdir/closedSent/P040302172306AMA (P040

U302172205AMA)

Using P0403021.00B;1 for /tmp/.tar/billingdir/closedSent/P040302172205AMA (P040

302165504AMA)

Using P0403021.00C;1 for /tmp/.tar/billingdir/closedSent/P040302165504AMA (P040

302165503AMA)

Using P0403021.00D;1 for /tmp/.tar/billingdir/closedSent/P040302165503AMA (P040

302165402AMA)

Using P0403021.00E;1 for /tmp/.tar/billingdir/closedSent/P040302165402AMA (P040

302164901AMA)

Using P0403021.00F;1 for /tmp/.tar/billingdir/closedSent/P040302164901AMA (P040

302164100AMA)

Using P0403021.00G;1 for /tmp/.tar/billingdir/closedSent/P040302164100AMA (P040

302153832AMA)

Using P0403021.00H;1 for /tmp/.tar/billingdir/closedSent/P040302153832AMA (P040

302153831AMA)

Using P0403021.00I;1 for /tmp/.tar/billingdir/closedSent/P040302153831AMA (P040

302153730AMA)

35.63% done, estimate finish Wed Mar 3 16:29:21 2004

71.26% done, estimate finish Wed Mar 3 16:29:21 2004

Total extents actually written = 14049

Total translation table size: 0

Total rockridge attributes bytes: 2364

Total directory bytes: 6144

Path table size(bytes): 42

Max brk space used c000

14049 extents written (27 Mb)

```
Looking for CD devices...
Initializing device...done.
Preparing to write DVD
Writing track 1...done.
Finalizing (Can take upto 4 minutes)...done.
write /tmp/.tar/billingdir/ succeeds
cdwrite exiting with return code 0
removing scratch /tmp/.tar d97
removing scratch /tmp/.iso d98


Billing Data DVD Backup Finished
--------------------------------------------------------------------------------
you have now completed the DVD backup operation. Please ensure all requested
files have been written to the DVD(s)
```

- You have now completed the script based backup procedure.Label the DVD(s) with a CD/DVD safe pen and repeat until all of the required streams are backed up. When finished writing all disks use the ls command to confirm that all of the desired files have been copied and are of the correct size.

14.2.3 Manual procedure for writing to DVD

This is a procedure intended mainly for GNPS when they have been contacted by a customer to purge billing files. Probably due to down stream network connectivity problems. Or for a customer who wishes to back up specific files. The sbadvdwrite script is the preferred method for customers who intend to do general back ups

Note: This is not a billing specific procedure it is a general sspfs procedure

Note: This procedure does not move the files from closed not sent to closed sent

Note:

- You first must insert the DVD-RW which you intend to write into the DVD drive.
- First, issue the UNIX command “cdrw -l” (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdrw -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

#> /usr/bin/cdrw -l

- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

  #> /usr/bin/eject cdrom

- Next you want to confirm that all of the data which you want to put on the DVD will fit. You will need to use the cd and ls UNIX commands as follows. First use the cd command to set the current directory to the directory which contains the files you want to back up. In this case the files are in the /export/tmatt/closedsent directory. so the following command is issued.

  #> cd /export/tmatt/closedsent

  Next use the ls command as follows. This command lists all of the files in the current directory. The size of the files in bytes is listed in the fifth column of the output (in bold bellow). Add the size of each file you intend to back up together and ensure that the total size of all files does not exceed 2000000000 bytes. If it does you will need to use more than one DVD. Divide the files up to make the most efficient use of each DVD.

  #> /usr/bin/ls -l
  total 270524
  -rw-r--r-- 1 maint maint **7034800** Feb 3 16:56 data1
  -rw-r--r-- 1 maint maint **4915002** Jan 26 18:55 data2
  -rw-r--r-- 1 maint maint **10000000** Feb 2 15:21 data3
  -rw-r--r-- 1 maint maint **57590000** Jan 23 11:59 data5

- Next you need to create a ISO9660 file system from the files you intend to back up. To do this you use the UNIX command mkisofs. Use it as folllows.Where <destination file> is the name of the binary file that contains the ISO9660 file system. This is selected by the crafts person. <pathspec> represents the full path of the files that are to be backed up. It is very important to ensure that the directory in which you are creating the ISO9660 binary file has at least 2000000000 bytes of free space or the mkisofs command will fail.

  #> /usr/bin/mkisofs -o <destination file> -a -J -L -R <pathspec>

  For example if you wanted to create the <destination file> /export/home/maint/tmatt/tempiso out of the two files data1 and data2 from above you would issue the following UNIX command

  #> /usr/bin/mkisofs -o export/home/maint/tmatt/tempiso -a -J -L -R /export/tmatt/closedsent/data1 /export/tmatt/closedsent/data2

  Note: this command will fail if the files in the path spec total more than 2000000000 bytes in size

- Next you will write the binary that you have created to the DVD. For this you will use the UNIX command cdrw as follows.

  #> /usr/bin/cdrw -C -i <iso9660 file>

  Where <iso9660 file> is the binary you just created above. So for example you would use the following command to write the Binary to the DVD.

  #> /usr/bin/cdrw -C -i export/home/maint/tmatt/tempiso

- Now delete the iso9660 file which was created previously with the rm UNIX command as follows. This is an important step which allows you the regain disk space.

  #> /usr/bin/rm export/home/maint/tmatt/tempiso

14.3 Software Requirements or Dependencies

14.4 Hardware Requirements or Dependencies

DVDRW must be installed in the system

14.5 Limitations and restrictions

none

14.6 Interactions

none

14.7 Applicable customer facing sections

Fault Management	
Logs	___N___
Alarms	___N___
Configuration	
Data Schema	___N___
User Interface	___N___
Element Management	___N___
Security	___N___
Service Order	___N___
Office Parameters	___N___
Accounting (includes AMA billing)	___N___
Performance (includes operational measurements)	___N___

14.8 Glossary

Term	Description
New term	Definition

14.9 References

cdrw man page
http://docs.sun.com/db/doc/816-0210/6m6nb7m5m?a=view

mkisofs man page
http://www.netsys.com/cgi-bin/solaris9?mkisofs(8)

15: Functional Description (FN): A00002009

15.1 Feature name

Enhance Display on PSET

15.2 Description

This feature activity is to migrate an existing line option, NAME24, from the MSL layer to the CCM layer.

NAME24 was created in the MSL layer under feature “Name Display Character Extension”. The documentation about the option creation are located in PLS DOC under names of AX1228 (CCM) and AX1240 (MSL).

The NAME24 line option enables subscribers to provide a name up to 24 characters for their private network. This NAME will be displayed on a MBS that supports 24 character display at the other end of the call. The display format will be following:

NAME24 --- Top line

DN --- Bottom line.

A SOC will be associated with this feature in CCM. After the migration, NAME24 will be a SOCed line option in the CCM layer and a non-SOCed line option in the MSL layer.

The SOC will have two functionalities. It controls the NAME24 line option processing and the display when NAME24 doesn’t apply to the originator. See section 2.6, 2.7 and 2.8 for details.

The SOC_FTR_ ID for this activity is “00002009” with OrderCode “MDC00075”

This feature activity involves changes to the MSL layer as well as the CCM layer. But the changes will not affect the behavior of the existing Name Display Character Extension (NAME24) feature in the MSL layer.

15.3 Hardware Requirements or Dependencies

There is no hardware requirement.

15.4 Software Requirements or Dependencies

CCM20

15.5 Limitations and restrictions

- This display feature will only be applied to MBS sets with 24 character display.
- IVD sets will be supported in MSL as well.
- NAME24 is limited to inter-custgrp or intera-custgrp calls in the same switch.

15.6 Servord

15.6.1 Assignment

The NAME24 line option can be assigned to a MBS via the SERVORD ADO, NEW, and COPYSET commands. Since the NAME24 options depends upon the NAME option, it must be assigned to a MBS that already has the NAME option on it or when NAME is being added to the set.

15.6.2 SO prompt

Here shows a simple assignment of this option in SERVORD. see Surveyor section for more examples.

```
>ado
SONUMBER:     NOW   3  9 16 PM
>
DN_OR_LEN:
>7234532
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>name24on7234532
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 9 16 PM 7234532 ( 1 NAME24 NAME24ON7234532 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

15.7 Interactions

15.7.1 Interaction with REASON

Since NAME24 provides a name up to 24 characters it preserves all of the spaces on the top line of the display phone for the name and moves DN to the bottom line.

When a REASON display is delivered to a set the NAME24 feature will simply quit processing because of the limited display space. The display will be the same as if NAME24 is not on the originating line.

15.7.2 Interaction with NAME feature

NAME24 works on top of NAME option. It overrides the private network name provided by NAME option.

With NAME option two names can be datafilled for two different networks, private and public. T

With the NAME24 option, a name up to 24 characters can be datafilled. It is intended to be used as a “private” name for people with long surnames.

In the original design, NAME24 overrode either of the two names datafilled by NAME option.

This activity will limit NAME24 only to override “private name” if it is datafilled by NAME option. This change will not affect MSL customers.

The following two tables summarizes the interactions with NAME option before and after this activity.

Table 1 Example Datafill

	Party A	**Party B**	**Party C**	**Party D**
CUSTGRP	IBNTST	IBNTST	BNR	CLASSDSP
CSUTNTWK	PRIVATE	PRIVATE	PUBLIC	--
NAME option	private: Nice public: Nortel	private: Kevin public: Nortel	public: JCPenny	public: JCPenny
NAME24 option	Nice_PictureFrames	Kevin_Alex_ Blazejewski	JCPenny_CaryTown	JCPenny_Crabtree

Table 2 NAME Display Two Names (without NAME24)

Calls	**Network ID of the Call**	**Display on A**	**Display on B**	**Display on C**	**Display on D**
A <-> B	private	Kevin	**Nice**	n/a	n/a
A <-> C	public	JCPENNY	n/a	**Nortel**	n/a
A <-> D	public	JCPENNY	n/a	n/a	**Nortel**
C<-> D	public	n/a	n/a	JCPENNY	JCPENNY

Table 3 MSL Implementation: NAME24 Overrides Two Names

Calls	Network ID Of the Call	Display on A	Display on B	Display on C	Display on D
A <-> B	private	Kevin Alex Blazejewski	*Nice PictureFrames*	n/a	n/a
A <-> C	public	JCPenny CaryTown	n/a	*Nice PictureFrames*	n/a
A <-> D	public	JCPenny Crabtree	n/a	n/a	*Nice PictureFrames*
C<-> D	public	n/a	n/a	JCPenny Crabtree	JCPenny CaryTown

Table 4 CCM Implementation: NAME24 only Overrides Private Name

Calls	Network ID of the Call	Display on A	Display on B	Display on C	Display on D
A <-> B	private	Kevin Alex Blazejewski	*Nice PrictrueFrames*	n/a	n/a
A <-> C	public	JCPenny	n/a	*Nortel*	n/a
A <-> D	public	JCPenny	n/a	n/a	*Nortel*
C<-> D	public	n/a	n/a	JCPenny	JCPenny

15.7.3 Interaction with TCAPNM

NAME24 will not override TCAPNM but will display the TCAPNM and the DN on two separated lines.

NAME24 interacts with TCAPNM in the same way as NAME option. When it detects that TCAPNM applies to the line it will not check if the TCAPNM is retrieved successfully. If no TCAPNM is retrieved no name will be displayed.

15.7.4 Interaction with AUTODISP

NAME24 will display KEY# with DN on the bottom line of the display for incoming calls.

ALEXANDER BLAZEJEWSKI
KEY -1 6841000

15.7.5 Interaction with other features

The NAME24 will not work with features that require extra messages being displayed because of the limited display space. Also, NAME24 will not work with features that have their own specific name to be displayed.

When any one of following features is applied to the line NAME24 will quit its processing. The display will be the same as if NAME24 is not on the line.

a. An E911 call.

b. Attendant is attached to the call.

c. Call is forwarded/redirected/transferred/picked-up

d. The agent is an ACD agent

e. Originating agent is a MADN with the NAME24 assigned.

f. NAME24 will not function when the INSPECT feature is used on the terminating MBS.

15.8 Move DN to the bottom line - Controlled by NAME24 SOC

15.8.1 Background -- DN being dropped from display

When only the Name and DN are going to be displayed and NAME24 does not apply to the originator, the Name and DN will be displayed on the same top line of the terminator's display, and the bottom line will be left empty.

There are some cases that DN will be dropped from display and the bottom line will be left empty on the terminator's display.

Without NAME24 option / SOC MDC00075 = IDLE

- DN will not be displayed on the terminator if originator's Name + DN is over 15 characters long and terminator has a 2x16 display window
- DN will not be displayed on the terminator if originator's Name + DN is over 24 characters long and the terminator has a display window of 2x16 or 2x24.

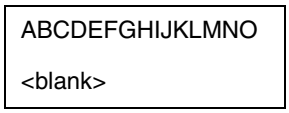
With NAME24 option / SOC MDC00075 = ON

Since the NAME24 works only NAME and DN are going to be displayed (except AUTODISP), it will display the DN on the bottom line on the terminator's display if NAME24 SOC is ON, and the NAME24 doesn't apply to the originator because of the following reason(s):

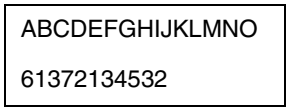
- The originator doesn't have the NAME24 line option on it.
- The originator has NAME24 option on it but the terminator has a display window of 2x16.
- The originator has the NAME24 line option on it but it is not to be displayed (possibly, the call is on the public network).
- TCAPNM applies to the originator

Example:

- Party A (6137234532) has the NAME line option with a name of "abcdefghijklmno".
- Party B has a 2x16 display KSET,
- Party A calls party B
- Display on B:
  - — NAME24 SOC Idle



  - — NAME24 SOC On



15.9 Applicable customer facing sections

Indicate with an “X” if you are completing the sections of the DDOC listed below. Indicate with “NA” if these sections do not apply to this functionality

Fault Management

- Logs _NA__
- Alarms _NA__

Configuration

- Data Schema _X___
- User Interface _NA__
- Element Management _NA__
- Security _NA__
- Service Order _X____
- Office Parameters _NA__

Accounting (includes AMA billing) _NA__

Performance (includes operational measurements) _NA__

15.10 Glossary

Table 5 list of abbreviations

Acronym	Expansion of Acronym
PSET	Proprietary Business Set
KSET	Key Set
IVD	Integrated Voice and Data
MBS	Meridian Business Set
ISDN	Integrated Services Digital Network
CCM	DMS 100 Common Layer
MSL	Meridian Stored Logic
PLS	Product Library System
SOC	Software Optionality Control

Acronym	Expansion of Acronym
CUSTGRP	Customer Group
CUSTNTWK	A table name in DMS
IPL	Initial
PRIVATE	A network ID
PUBLIC	A network ID
IBNTST	A customer group name
BNR	A customer group name
CLASSDSP	A customer group name

16: Functional Description (FN): A00002011

16.1 Feature name

DMS-100: Virtual Office Worker

16.2 Description

The intent of this activity is to migrate the Virtual Office Worker (VOW) software from the MSL DRU into the CCM DRU.

The function of the VOW software is not changing as a result of this feature with the exception that it will now be available to all DMS-100 customers instead of limited to MSL-100 PBXs. The function of the VOW feature will be controlled by SOC for those customer who are not using MSL-100 loads.

For a functional description of the VOW feature, please refer to the FN of the original feature. It can be found in the PLS DOC library under AX1236FN.AA20.

16.3 Hardware Requirements or Dependencies

Not Applicable. See section 1.5.1 of AX1236FN.AA20 in PLS DOC library.

16.4 Software Requirements or Dependencies

None.

16.5 Limitations and restrictions

See section 1.7.2 of AX1236FN.AA20 in PLS DOC library.

16.6 Interactions

See section 1.7.1 of AX1236FN.AA20 in PLS DOC library.

16.7 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	__N/A__
Configuration	
Data Schema	___X___
User Interface	___X___
Element Management	__N/A__
Security	__N/A__
Service Order	___X___
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	___X___

Note: The chart above represents the customer facing sections which were created for the original feature. The corresponding sections in this document will NOT be created. For information on these sections, see the following:

Logs - Section 1.6.1 of AX1236FN.AA20 and/or AX1236LG.AA20 in PLS DOC library.

Data Schema - Section 1.6.2 of AX1236FN.AA20 and/or AX1236DS.AA20 in PLS DOC library.

User Interface - Section 1.6.4 of AX1236FN.AA20 and/or AX1236MM.AA20 in PLS DOC library.

Service Order - Section 1.6.3 of AX1236FN.AA20 and/or AX1236SO.AA20 in PLS DOC library.

Performance (OMs) - Section 1.6.5 of AX1236FN.AA20 and/or AX1236OM.AA20 in PLS DOC library.

16.8 Software Optionality Control (SOC)

For non-MSL customers, this feature will be regulated by standard SOC control. VOWs and VOWDNs can be datafilled, but will not be permitted to log-in unless the feature is activated in SOC. If the SOC is turned off, attempts to log-in by a VOW user will be routed to FNAL treatment.

Table 1 SOC

SOC option name:	TBD
SOC option title:	TBD
SOC option control type:	state
New SOC option?	Yes
SOC option order code	TBD
Option defined in DRU:	CCM
Affected products:	CCM20

In loads built for the MSL market, the SOC should always be ON.

16.9 Glossary

Term	Description
FNAL	Feature Not Allowed
SOC	Software Optionality Control

17: Functional Description (FN): A00002012

17.1 Feature name

XA-Core CMIC/RTIF HIOP Maintenance Software.

17.2 Description

17.2.1 Overview

This document provides an overview of the functionality provided by the Operations, Administration, and Maintenance (OAM) software for the High Performance Input Output Processor card (HIOP) with CMIC, RTIF, TOD, and ETHR functionality (CMIC/RTIF HIOP).

This HIOP card supports the following functionalities:

- Core to Message Switch (MS) InterConnect (CMIC), providing high speed access to the DMS Message Switch via OC3 links,
- Reset Terminal InterFace (RTIF). The RTIF local ports support XA-Core connectivity to Video Display Terminals (VDT) (EIA RS232 standard). The RTIF remote ports provide connection to remote terminals via modem (EIA RS422 standard).
- Time Of Day (TOD) support, and
- Ethernet, providing high speed access to the Succession Network via 100Mb/s full duplex ethernet links.

  Note: the OAM changes related to the Ethernet functionality were delivered by the XA-Core Ethernet Maintenance feature and are described in document AT.59019176 in fmdoc.

  Note: this feature does not introduce any changes to the Reset Terminal Interface (RTIF) behavior. The RTIF components are backwards compatible to the packlet.

This software provides the maintenance interface to the craft person for monitoring and manipulating the state of the HIOP common equipment, the CMIC, RTIF, ETHR ports and links, and TOD. For more information on the HIOP circuit pack, please refer to document ‘HIOP Maintenance Software’ (AT.59029980).

The components of the interface to the XA-Core are consistent with the XA-Core OAM interface. These include the maintenance administration position (MAP), logs, alarms, and operational measurements (OMs). All maintenance, fault handling, redundancy checking, and event reporting functionalities provided by this feature are consistent with established XA-Core maintenance procedures and guidelines.

The software associated with XA-Core CMIC/RTIF HIOP OAM Software provides the following functionality:

- changes the existing CMIC MAP level and MAP commands in order to maintain the new CMIC ports,
- changes the existing RTIF MAP level and MAP commands in order to maintain the new RTIF links (local and remote),
- changes the existing alarms, logs, and operational measurements that report on the maintenance status of the CMIC and RTIF ports and links.

17.2.2 HIOP card description

The CMIC/RTIF HIOP card is similar to the NTLX04CA HIOP card that supports AMDI, ETHR, and RTIF functionality. The main hardware difference between the two is the transmitter used in the OC3 hardware:

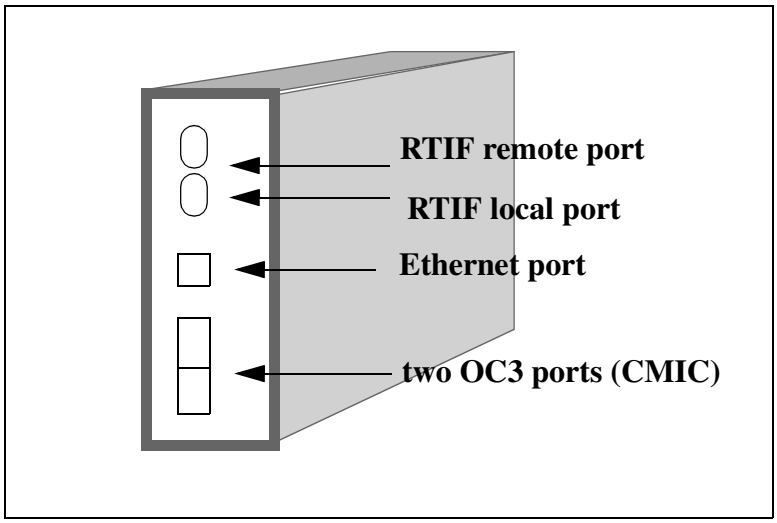
- the NTLX04CA HIOP card has single-mode transmitter (OC3 used for AMDI),
- the CMIC/RTIF HIOP card has multi-mode transmitter (OC3 used for CMIC).

The XA-Core CMIC/RTIF HIOP circuit pack is equipped with:

- two OC3 ports,
- one ethernet port, and
- two RTIF ports: one RS232 RTIF local port and one RTIF remote port.

Unlike circuit pack NTLX03 (IOP), the HIOP card does not support packlets. Please refer to “Figure 1 HIOP card” on page 238.

Figure 1 HIOP card



The HIOP LED strategy follows established XA-Core guidelines: the card is equipped with one red and one green LED which show the status of the card. Three additional amber LEDs represent presence or loss of signal on RTIF, ETHR, and CMIC links respectively.

The XA-Core Visual Indicator (LED) Strategy is described in XA0015FN.

17.3 Interactions

- XA-Core HIOP Maintenance Software: AT.59029980,
- XA-Core Ethernet Maintenance feature: AT.59019176,
- XA-Core Visual Indicator (LED) Strategy: XA0015,
- XA-Core provisioning feature: AT.59009527.

17.4 Applicable customer facing sections

Fault Management

Logs	__X____
Alarms	__X____

Configuration

Data Schema	___N/A___
User Interface	___X___

Element Management ___N/A___

Security ___N/A___

Service Order ___N/A___

Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___X___

17.5 Glossary

Term	Description
AMDI	ATM Multimode Data Interface
CMIC	Core to MS InterConnect
DMS	Digital Multiplex Switch
ETHR	Ethernet
HIOP	High performance Input Output Processor
MAP	Maintenance Administration Position
MS	Message Switch
OAM	Operations, Administration, and Maintenance
OM	Operational Measurement
PIDR	P side IDentification Register
RTIF	Reset Terminal InterFace
SN	SuperNode
SNSE	SuperNode Shelf Extension
TOD	Time Of Day
VDT	Video Display Terminals
XA-Core, XAC	eXtended Architecture Core

18: Functional Description (FN): A00002013

18.1 Feature name

Intelligent Network T1 Timer Expiry Message Suppression

18.2 Description

The T1 Timer specifies a length of time, in seconds, the SSP waits for response from an off-board processor after sending it a query message before the call is routed to treatment. When routing the call to treatment, a ‘T1 Timer Expiry’ message is generated by the SSP.

This feature, when enabled, will suppress ‘T1 Timer Expiry’ messages from being generated. Suppressing the ‘T1 Timer Expiry’ messages from being generated will prevent the messages from flooding the network should an SCP go down.

However, suppressing the ‘T1 Timer Expiry’ messages violates the standard procedure for this situation and is therefore adding optional functionality.

This feature depends on SOC INW00001 to switch the functionality ON/OFF and uses office parameter T1_TIMER_EXPIRY_MSG_SUPPRESS to provide feature optionality control.

The office parameter contains four fields, the first of which allows the user to switch the ‘T1 Timer Expiry’ message generation ON/OFF. When the feature is on, the remaining three fields allow the user to switch log generation ON/OFF, alarm generation ON/OFF and specify a threshold value. The threshold value is related with the alarm generation and is explained later on.

If the suppress option is switch on, no “T1 Timer Expiry” messages will be generated.

If the log option is switched on, then a GAME101 log will be created when the RSPTMOUT OM count is greater than zero. The RSPTMOUT is an OM peg that is incremented everytime the SSP generates a ‘T1 Timer Expiry’ message.

If the alarm option is switched on, then a GAME102 log will be created when the RSPTMOUT OM count is greater than or equal to the threshold value specified in the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS. This log generates an external minor alarm. It will stay activated while the RSPTMOUT OM count is greater than or equal to the threshold value, as previously described. Or, until an operator clears the minor alarm from the banner. The RSPTMOUT OM count will be checked against the threshold value everytime the RSPTMOUT OM transfer period expires. If the

RSPTMOUT OM count drops below the threshold value and the minor alarm was generated in the previous RSPTMOUT OM transfer period, then this feature will clear the minor alarm.

For more details on the log or alarm, please refer to the relevant documentation.

18.3 Hardware Requirements or Dependencies

None.

18.4 Software Requirements or Dependencies

None.

18.5 Limitations and restrictions

This feature will impact DMS-100 (including TDM, Succession, MSL), MMP and SSR. All other markets are not affected by this feature.

18.6 Interactions

None.

18.7 Applicable customer facing sections

Fault Management	
Logs	_X____
Alarms	_X____
Configuration	
Data Schema	_N/A__
User Interface	_N/A__
Element Management	_N/A__
Security	_N/A__
Service Order	_N/A__
Office Parameters	_X____
Accounting (includes AMA billing)	_N/A__
Performance (includes operational measurements)	_N/A__

18.8 Glossary

Term	Description
SCP	Service Control Point
SOC	Software Optionality Control
OM	Operational Measurement

19: Functional Description (FN): A00002016

19.1 Feature name

A00002016: AINDENY Enhancements

19.2 Description

19.2.1 Background

AINDENY currently exists as both a line and customer group option. Its purpose is to block the triggering of Vertical Service Code (VSC) triggers to lines and customer groups. The VSC triggers are Specific Feature Code (SFC), Public Feature Code (PFC) and Office-Wide PFC (OFCPFC). These triggers are all hit by the originator dialing a digit string starting with a * or #. The AINDENY line option blocks SFC, PFC and OFCPFC triggers. The CUSTSTN option only blocks OFCPFC triggers.

AINDENY options are lists of {ACTION, SCOPE} pairs where ACTION is either DENY or RESTORE and SCOPE specifies a specific tuple in table TRIGITM or a whole trigger-type. An AINDENY option of “AINDENY DENY TIID 4 OPFC3, DENY TIID 4 SFC2” will deny triggering to the triggers defined in table TRIGITM as “4 OPFC3” and “4 SFC2”. The option can block entire triggers types, e.g. “AINDENY DENY ALL SFC”. Furthermore, the option can specifically allow triggers that have been blocked by AINDENY. “AINDENY DENY ALL OFCPFC, RESTORE TIID 4 OFCPFC2” denies all Office-Wide PFC triggers except the “4 OFCPFC2” trigger.

19.2.2 Functional Description

Verizon has requested the ability to deny AIN Prefix triggers (Specified_Carrier, One_Plus_Prefix, International, Operator_Services) on a per trunk group basis. This can be accomplished by enhancing table TRKAIN to store AINDENY information. In addition, this activity will expand the CUSTSTN AINDENY option to hold 15 triggers to bring it in line with the AINDENY line option.

19.2.3 Enlarging the CUSTSTN AINDENY Option

Currently the AINDENY option of table CUSTSTN can only hold 10 elements; that is, only 10 DENY or RESTORE actions can be taken per customer group. The AINDENY line option can hold 15 elements. This activity will enlarge the storage capacity of the CUSTSTN AINDENY option to 15 elements.

19.2.4 Denying Prefix Triggers

The four Prefix triggers (Specified_Carrier, One_Plus_Prefix, International, Operator_Services) are all detected at the Info_Analyzed TDP. The AINDENY line and customer group options cannot currently block these trigger types. This activity will allow the CUSTSTN, line and the newly created TRKAIN AINDENY options to hold the four Prefix triggers and block their triggering at the Info_Analyzed TDP.

19.2.4.1 Datafill for blocking Prefix triggers

The Prefix triggers are detected at the Info_Analyzed TDP (TDP 4). One or more Prefix triggers need to be added to table TRIGITM as below.

Table 1 Example Datafill for the Prefix triggers in table TRIGITM

TDP	Name	Trigger	Criteria	State	Action	MSGSET	TRANSPRT	GTT
4	PRFXEX1	*SPECARR*	$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX2	*ONEPLUS*	$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX3	*INTERNTL*	$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX4	*OPERSRV*	$	ULK	EVENT	R02	SS7	AINPOP

Secondly, individual agents need to subscribe to the Prefix triggers. This can be accomplished in tables OFCTIID, CUSTIID, TRKAIN or through Servord.

Table 2 Subscribing Agents to AIN Prefix Triggers

Agent	Datafill
Office	table OFCTIID; add 4 PRFXEX1 ON
Customer Group	table CUSTTIID; add RESGRP 4 PRFXEX1 ON
Line	servord; ado $ 6213519 ain tiid 4 PRFXEX1 ON $
Trunk	table TRKAIN; add CLLI3 AIN TIID 4 PRFXEX1 ON $

Next, the AINDENY option can be added to the line, table CUSTSTN or table TRKAIN.

Table 3 Adding the AINDENY option

Agent	Datafill
Customer Group	table CUSTSTN; add RESGRP AINDENY AINDENY DENY TIID 4 PRFXEX1 $

Table 3 Adding the AINDENY option

Agent	Datafill
Line	servord; ado $ 6213519 AINDENY DENY TIID 4 PRFXEX1 $
Trunk	table TRKAIN; add CLLI3 AINDENY DENY TIID 4 PRFXEX1 $

Finally, the SOCs relevant to the trigger being detected need to turned on. Table 4 details the SOC Codes for PFC, SFC, OFCPFC, and the Prefix triggers.

Table 4 SOC Order Codes for VSC and Prefix Triggers

Trigger	SOC
SFC	AIN00294
PFC	AIN00294
OFCPFC	AIN00309
SPECARR	AIN00252
ONEPLUS	AIN00251
INTERNTL	AIN00253
OPERSRV	AIN00254

19.2.5 Blocking Prefix Triggers for Trunks

Trunks can be subscribed to AIN triggers through table TRKAIN or through office-wide subscriptions. However, there is currently no way to block the triggering for specific trunk groups.

Currently, table TRKAIN is keyed by CLLI. This activity will reformat the TRKAIN table to be keyed by a combination of CLLI and option name. This new format will allow a new AINDENY option to be added against CLLIs. The existing subscription information will be keyed by CLLI and the option name ‘AIN’.

The new AINDENY option will be functionally similar to the line and customer group options except that it will only block Prefix triggers. It will not be capable of holding SFC, PFC, or Office-Wide PFC triggers. It will allow 15 DENYs or RESTOREs just as the line and customer group options.

19.2.5.1 Datafilling AINDENY option in table TRKAIN

Table TRKAIN will be indexed by a combination of trunk group and option name. To deny all Operator Services triggers, except trigger “4 OPSRV1” for trunk group ISUP2WITEA, add the tuple seen below.

Table 5 Example Datafill for an AINDENY Option in table TRKAIN

OPTKEY	OPTINFO
ISUP2WITEA AINDENY	AINDENY (DENY ALL OPSERV) (RESTORE TIID 4 OPSRV1) $

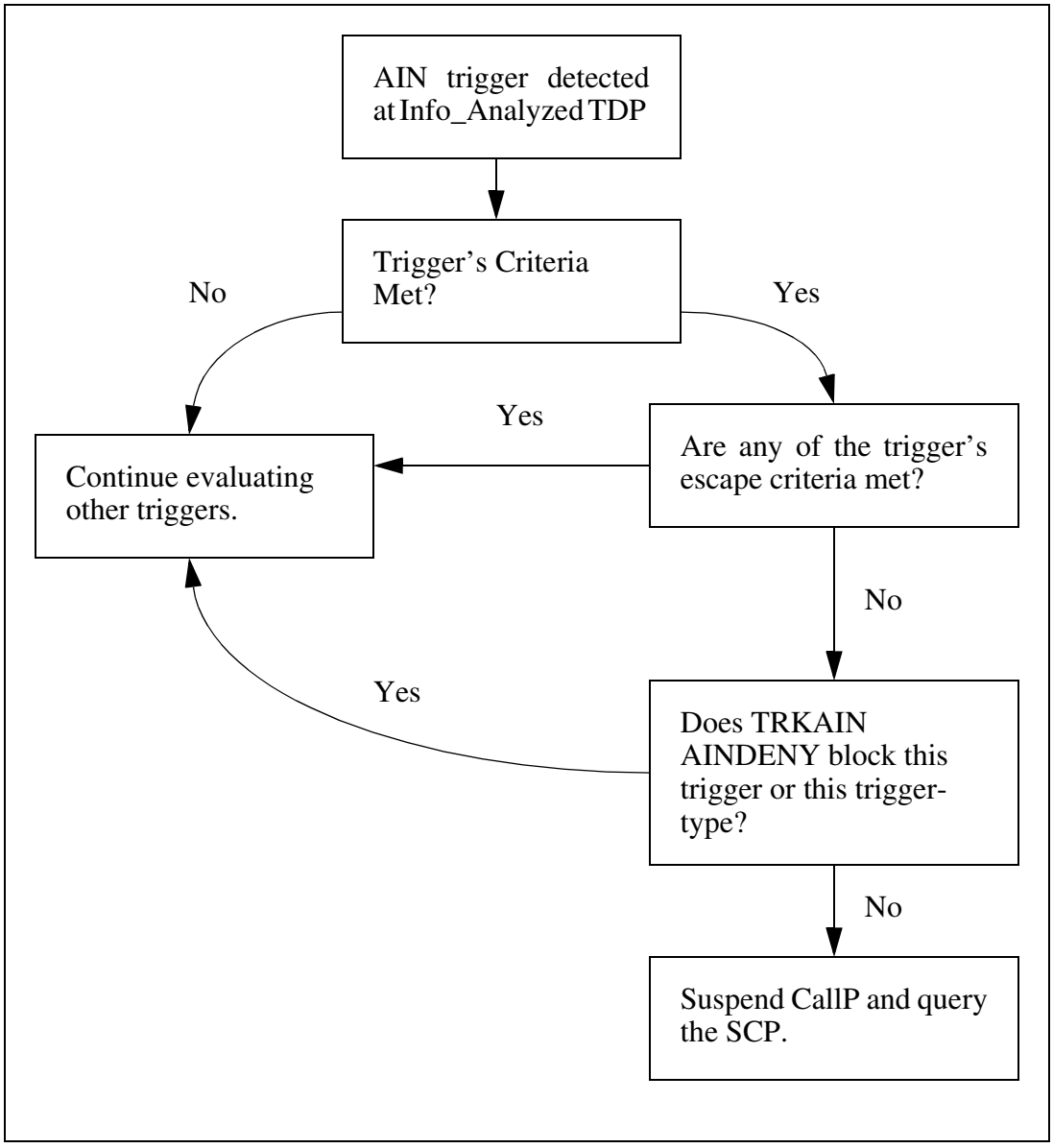
The existing AIN subscription information will be reformated to add an option name of 'AIN'. See table 6 for an example.

Table 6 Example Datafill for AIN Option in table TRKAIN

OPTKEY	OPTINFO
ISUP2WITEA AIN	AIN TIID (4 INTRL1 ON) (4 OPSRV3 ON) $

19.2.5.2 TRKAIN AINDENY CallP Behavior

When an originating trunk encounters the INFO_ANALYZED TDP and is subscribed to any AIN triggers at this TDP, it will evaluate the criteria for each subscribed trigger. If all the trigger criteria are met (including escape criteria), call processing will be suspended while the SCP is queried. If there is a TRKAIN AINDENY option datafilled against the originating trunk and the option specifies that the specific trigger or trigger-type is denied, the SCP will not be queried and AIN will continue evaluating any other subscribed triggers at this TDP. This behavior is summarized in the flowchart below.



19.2.6 Traver

The Traver tool simulates a call from the user specified originator with the user specified digits. Traver will display information regarding subscriptions to AIN triggers and will display the criteria associated with those triggers. The tool also respects the AINDENY line and customer group options and will tell the user if the SCP query was blocked due to AINDENY. Traver code will be enhanced to consider AINDENY for Prefix triggers and trunk origination.

Example of line being denied a One_Plus trigger by AINDENY line option:

```
>traver l 6213512 16199451478 b
TABLE IBNLINES
HOST 01 0 00 23 0 DT STN RES 6213512 0 613_P621_0 L613_LATA1_0 613 (AR) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 NSCR 613 P621 NONE Y RESGRP 0 0 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
HOST 01 0 00 23 0 AIN AIN TIID (4 MKSFC ON) $
TABLE CUSTSTN
RESGRP AIN AIN TIID
TABLE OFCVAR
AIN_OFFICE_TRIGGRP TIID
AIN Orig Attempt TDP: no subscribed trigger.
TABLE NCOS
RESGRP 0 0 0 RES613 ( XLAS RESX613 STARXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA STARXLA 0 RES
TABLE DIGCOL
RES specified: RES digit collection
TABLE IBNXLA: XLANAME RESX613
TUPLE NOT FOUND
Default from table XLANAME:
RESX613
    (NET N N 0 N RES N Y GEN ( LATTR 0 613_P621_0 L613_LATA1_0)
    (EA NILC Y 0) $ $)$ 9
TABLE DIGCOL
RES specified: RES digit collection
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 NSCR 613 P621 NONE Y RESGRP 0 0 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE STDPRTCT
P621 ( 1) ( 0) 3
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 16 17 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 925 12 ( 122) ( 1) ( 0) ( 0) 2 $
 . SUBTABLE HNPACODE
```

```
. KEY NOT FOUND
. REAL VALUE IS:  VCT VACT N
TABLE TMTCNTL
LNT ( 148)
 . SUBTABLE TREAT
 . VACT Y S T120
AIN Info Collected TDP: no subscribed trigger.
Checking AIN SFC Trigger Items as SFC is compatible with current call
Checking AIN SFC Trigger Items as SFC is compatible with current call
Checking AIN ONEPLUS Trigger Items as ONEPLUS is compatible with current call
 .  . TABLE CUSTTIID
 .  . RESGRP 4 MKONE ON
 .  . TABLE TRIGITM
 .  . 4 MKONE ONEPLUS $ ULK EVENT R02 SS7 AINPOP $
 .  . TABLE IBNFEAT
 .  . HOST 01 0 00 23 0 AINDENY AINDENY (DENY TIID 4 MKONE) $
 .  .TABLE C7GTTYPE
 .  .AINPOP ANSI7 6 $
 .  .  . TABLE C7GTT
 .  .  . AINPOP 1000000000 1000000000 PCSSN (SIMTOOL_RTESET SIMTOOL 0)
$ SSN
AIN Info Analyzed TDP: trigger criteria not met.
Line is subscribed to option AINDENY. Triggering denied.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


AIN Info Analyzed TDP: trigger criteria met.
Querying the database would occur now.
Use the AINMQG option to save the query to a file for use in TstQuery.
Use the AINRES option for further information

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Example of trunk being denied a One_Plus trigger by TRKAIN AINDENY:

```
>traver tr priic 19199451478 b
TABLE TRKGRP
PRIIC PRA 0 PRAC NCRT DSEQ N (ISDN 501) $ $
TABLE LTCALLS
ISDN 501 PUB XLALEC 1 613_P621_1 L613_LATA1_0 $
 .  . TABLE TRKAIN
 .  . PRIIC TIID (4 MKONE ON) $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP TIID
TABLE LINEATTR
1 1MR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_1 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
```

```
613_P621_1 FR01 613 P621 TSPS Y RESGRP 0 0 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE STDPRTCT
P621 ( 1) ( 0) 3
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 191 1920 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 925 12 ( 122) ( 1) ( 0) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D 3BCELL2WMF 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 ( 37) OPTL N N Y
 . SUBTABLE LCASCR
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
TUPLE NOT FOUND.  DEFAULT IS TO LEAVE XLA RESULT UNCHANGED
TABLE CLSVSCRC
KEY NOT FOUND
AIN Info Collected TDP: no subscribed trigger.
Checking AIN ONEPLUS Trigger Items as ONEPLUS is compatible with current call
 .  . TABLE TRIGITM
 . . 4 MKONE ONEPLUS $ ULK EVENT R02 SS7 AINPOP $
 .  . TABLE TRKAIN
 .  . PRIIC AINDENY AINDENY (DENY ALL ONEPLUS) $
 .  .  . TABLE C7GTTYPE
 .  .  . AINPOP ANSI7 6 $
 .  .  . TABLE C7GTT
 .  .  . AINPOP 1000000000 1000000000 PCSSN (SIMTOOL_RTESET SIMTOOL 0) $ SSN
AIN Info Analyzed TDP: trigger criteria not met.
Line is subscribed to option AINDENY. Triggering denied.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


AIN Info Analyzed TDP: trigger criteria met.
Querying the database would occur now.
Use the AINMQG option to save the query to a file for use in TstQuery.
Use the AINRES option for further information


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

19.3 Hardware Requirements or Dependencies

No new hardware requirements are introduced by this feature.

19.4 Software Requirements or Dependencies

The basic AIN SOC options need to be in state ON for the AINDENY option to be encountered during CallP. However, no new software dependencies are introduced by this feature.

19.5 Limitations and restrictions

Only AIN-capable trunks will be allowed AINDENY options in table TRKAIN.

19.6 Interactions

N/A.

19.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	__X__
User Interface	__X__
Element Management	_N/A_
Security	_N/A_
Service Order	__X__
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

19.8 Glossary

Term	Description
AIN	Advanced Intelligent Networks
AINDENY	A line option and an option in table CUSTSTN that blocks specific AIN triggers from querying the SCP.
PFC	Public Feature Code: an AIN trigger
Prefix Triggers	The Specified_Carrier, One_Plus_Prefix, International, and Operator_Services AIN triggers.
SCP	Service Control Point: the machine that the SSP queries with AIN TCAP messaging.
SFC	Specific Feature Code: an AIN trigger
SOC	Software Optionality Control
SSP	Service Switching Point: the DMS-100 in AIN speak.
VSC	Vertical Service Code: SFC, PFC and OFCPFC are VSC-detecting triggers. VSC codes are digit strings starting with * or #.

20: Functional Description (FN): A00002020

20.1 Feature name

ESA Translation Download

20.2 Description

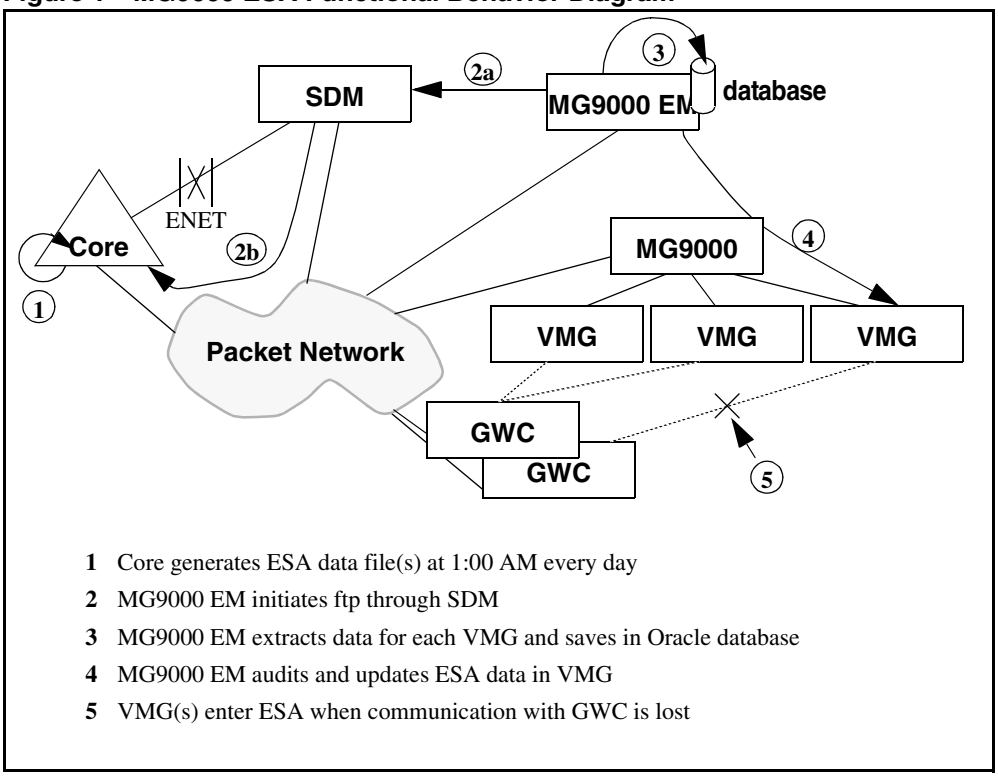
This activity allows the download of information necessary to support Emergency Stand Alone (ESA) call processing across all native (non ABI) lines served by a single MG9000.

The download takes place from the CS2000 core to an MG9000 element manager. The data is generated by the core at 1:00 AM and stored in a file called ESA_SYSTEM_SD$XML on a device specified by OFCENG parameter ESA_GWDATA_DEVICE. It is then downloaded by the MG9000 EM through the SDM.

Prior to this activity, ESA was supported for the MG9000 but all ESA data was provisioned through the MG9000 element manager. This method will continue to be used for VMGs not marked as North American in the MG9000 EM.

Note: Activity “A00002380 - MG9K ABI ESA” is implemented in CCM20 and enhances MG9K ESA to support ABI as well as non native lines. The documentation for that activity affects many of the same areas as this activity but in most cases does not invalidate the documentation found here. One exception is the ESATRAVER command described in the CN section of this document.

Figure 1 MG9000 ESA Functional Behavior Diagram



1 Core generates ESA data file(s) at 1:00 AM every day

2 MG9000 EM initiates ftp through SDM

3 MG9000 EM extracts data for each VMG and saves in Oracle database

4 MG9000 EM audits and updates ESA data in VMG

5 VMG(s) enter ESA when communication with GWC is lost

20.2.1 Related Activities

This activity is one of three activities to enhance ESA for the MG9000 in the SN06.2 time frame. The activity addresses the core code and will be sourced into the SN07 stream and patched back to SN06.2

The other features are

- A00001982 - ESA Enhancements [MG9000]
- A00002019 - ESA EM Enhancements (MG9000 EM]

This activity assumes that deterministic LENs are being used for MG9000 lines. Please refer to

- “A89009298 - MG9000 Lines Preprovisioning” (SN06)

20.3 Hardware Requirements or Dependencies

This activity requires CS2000 with SDM and EIOP.

The maximum size of SFDEV is 5 million words (10 million bytes) so a disk device must be available for large offices. Please see the engineering section of this document.

20.4 Software Requirements or Dependencies

Office must convert to using deterministic LENs for MG9000 as described in SN06 activity “A89009298 - MG9000 Lines Preprovisioning”.

20.5 Limitations and restrictions

ESA data will be built by the core every 24 hours at 1:00 AM or as the result of a manual command. Changes to CS2000 line data will not be reflected in the MG9000 until the data has been

- built by the core
- downloaded by the MG9000 Element Manager (EM)
- downloaded to the MG9000

Individual MG9000 VMGs can drop into ESA independently of other VMGs on the same MG9000. Emergency 911 lines should be provisioned on each VMG with table ESAPXLA provisioned to route 911 calls to these lines.

The ESA_SYSTEM_SD$XML file is not normally viewed by the telco. The DMS PRINT and EDIT commands will only partially display the file. The file must be transferred, using FTP, to a PC or UNIX, to be viewed completely.

20.6 Interactions

The MG9000 EM downloads the ESA data file from the core daily. The time for this download should be set so the data has been freshly built. The default values in the core and MG9000 EM are set to ensure the data is downloaded soon after being built.

20.7 Applicable customer facing sections

Fault Management	
Logs	__X___
Alarms	_____
Configuration	
Data Schema	__X___
User Interface	__X___
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	__X___
Accounting (includes AMA billing)	_____

Performance (includes operational measurements) _____

20.8 Glossary

Term	Description
ABI	Access Bridging Interface
CS2000	Call Server 2000
EIOP	Ethernet Input/Output Packlet
EM	Element Manager
ESA	Emergency Stand Alone
MG9000	Media Gateway 9000
SDM	SuperNode Data Manager
VMG	Virtual Media Gateway

21: Functional Description (FN): A00002047

21.1 Feature name

Double Density Spectrum Backplane

21.2 Feature Synopsis

This feature is being implemented in release SN07, under the following activities:

- A00002047 for DMSSHR(20)
- A00002057 for SP(20)

The feature entails the implementation of a new double density backplane for the Spectrum family of products.

The intent of this feature is to enable space efficiency by collapsing today's two-shelf Spectrum node configuration into a single double density card shelf. This can be accomplished in several ways. One example would be an IW SPM that does not use ECAN, provisioned with two CEMs, two ATM RMs, three DSP RMs, and a Sync RM. This has a straightforward conversion to a single-shelf configuration using the double density backplane. A second example would be a densely configured MG4K node, provisioned with two CEMs, two ATM RMs, two OC3 RMs, four DSP RMs, seven COH RMs, two Sync RMs, two DLC RMs, and an Alarm RM. In this case, when taken together with the new Spectrum resource module, the NTLX45AA Telephony Services Processor (TSP), customers will be able to fit four such Spectrum nodes into a single frame, one node per shelf.

The Double Density SPM program will significantly improve the trunk port density of the Spectrum-based product portfolio. Program benefits are a 50% density increase, achieved by a 50% footprint reduction, and a small yearly operating cost reduction (power and floor-space savings) which lowers the customer cost of ownership. The Double Density SPM program introduces new Spectrum back plane hardware, the NTLX51CA. The new back plane will provide backwards compatibility with the existing Resource Modules. Due to slot limitations, products that use the three-slot LSA complexes will experience slot exhaustion in the Double Density Spectrum-these products currently include MG4K LSA/STS1 and GSM e3 TCU/BSC-and, thus, will not be able to exploit the new backplane.

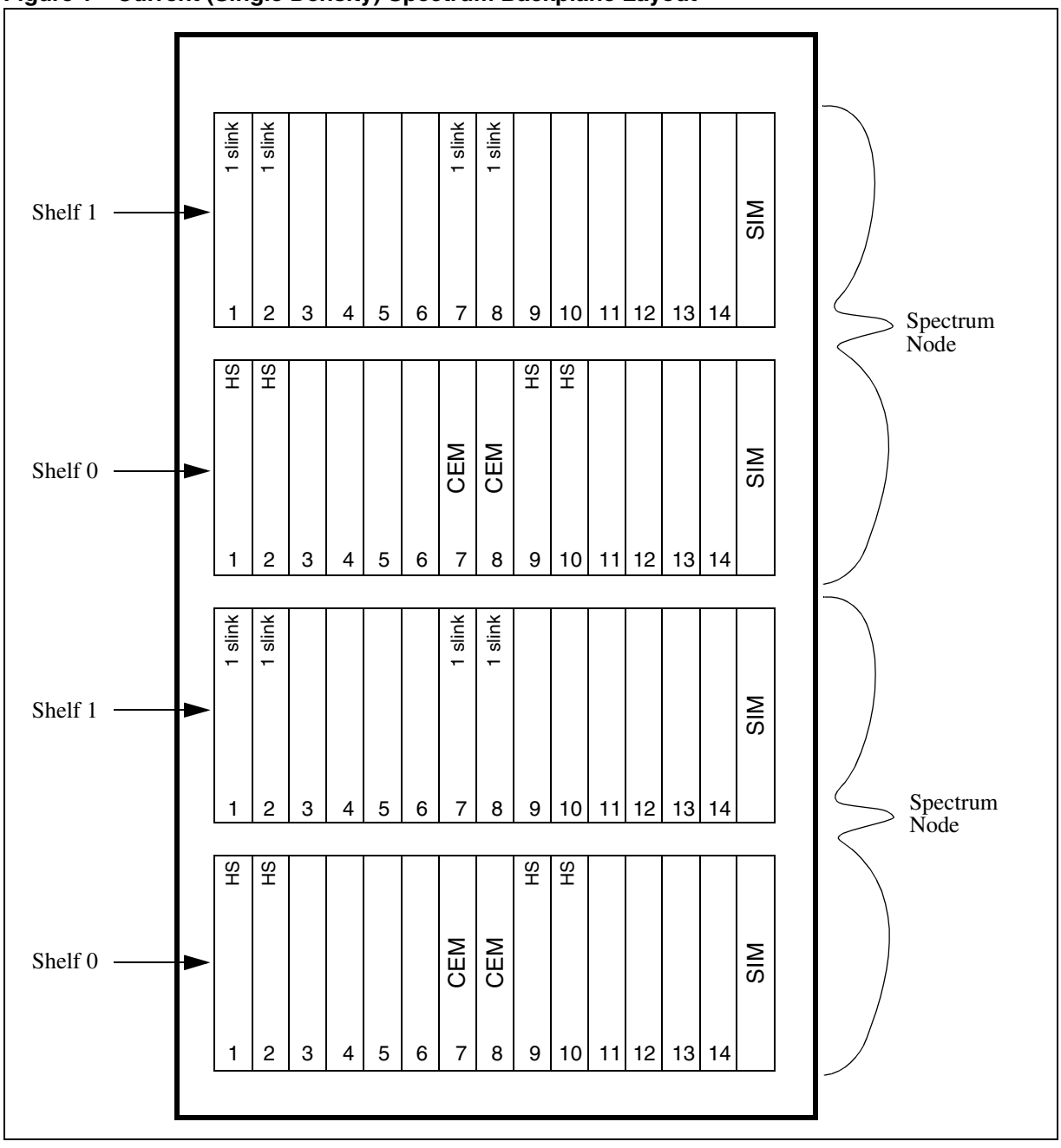
There are two distinct phases to the Double Density Spectrum Program. The first phase (A00002047, covered in this FN) modifies the existing Spectrum backplane hardware, NTLX51BA, to support four 15-slot Spectrum nodes per frame; currently two 30-slot nodes are supported per frame. The second phase, A00002386, constructs a new high-density DSP/ECAN card (the Telephony Services Processor, or TSP card) creating a new ECAN and DSP applications. This second phase also modifies the Spectrum software to support the concept of dynamic resource re-assignment within a single call and allows DSP and ECAN applications to co-exist on a single card.

21.3 Background Information

Today's Spectrum hardware includes a frame with PEC NTLX91BA that houses a backplane with PEC NTLX51BA which in turn supports **two** Spectrum nodes, each spanning two contiguous card shelves. (Please refer to "Figure 1 Current (Single Density) Spectrum Backplane Layout" on page 259.)

As illustrated, each Spectrum node occupies two shelves within the frame, each shelf housing 15 slots. Slot 15 on each shelf is dedicated for the Shelf Interface Modules (SIMs). Slots 7 and 8 of shelf 0 for each Spectrum node are dedicated for the Common Equipment Modules (CEMs).

Figure 1 Current (Single Density) Spectrum Backplane Layout



The remaining slots support various Spectrum resource modules (RMs), each having varying serial link (slink) requirements, depending upon the inter-module communication needs. Four high-speed slots are each serviced by 9 slinks and can be used for RM types such as OC3 or ATM. Low-speed slots are serviced by 3 slinks and can be used for RM types such as DSP or VSP. There are also four slots (1, 2, 7, and 8 on shelf 1) with single slinks which can accommodate DLC, DLC2, and ALM cards.

21.4 Feature Description

The new hardware layout for Double Density Spectrum includes a frame with PEC NTLX91CA (identical to the NTLX91BA frame[1]) that houses a backplane with PEC NTLX51CA which in turn supports **four** Spectrum nodes, each spanning only a single card shelf. (Please refer to “Figure 2 New Double Density Spectrum Backplane Layout” on page 261.)

Slot 15 on each shelf is still dedicated for the SIMs. Also, since each shelf is a “shelf 0”, slots 7 and 8 on each shelf are dedicated for CEMs. Of the remaining slots, ten of them are high-speed (9 slink) slots, slots 5 and 6 are single slink slots.

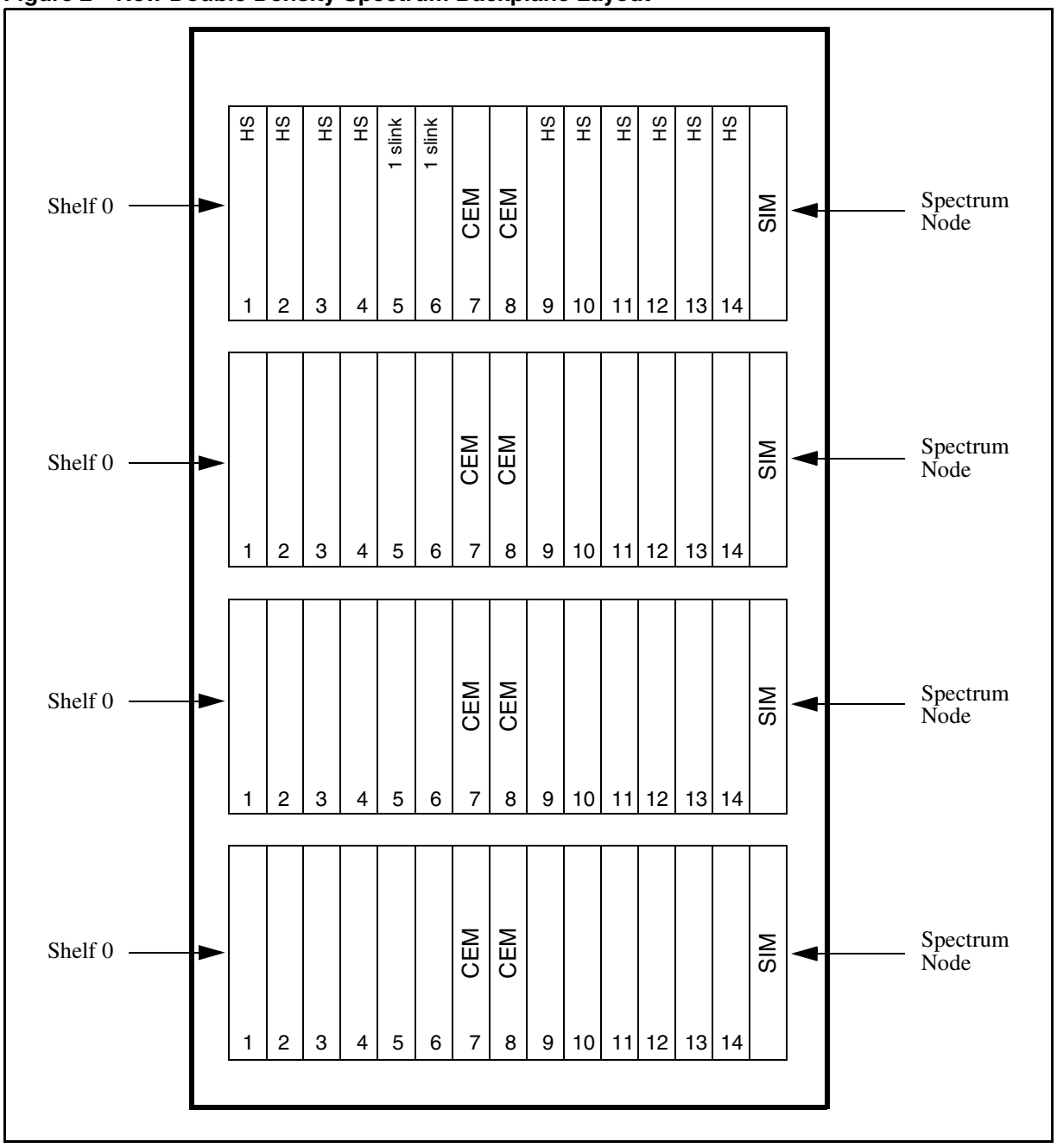
Clock synchronization traces are present in slots 1 and 2 (for use by ATM RMs), slots 9 and 10 (for use by OC3 or ATM RMs), and slots 5 and 6 (for use by Sync RMs, and also suitable for DLC and DLC2 RMs).

The addition of high-speed slots (and consequent reduction in low-speed slots) enable the single-shelf Spectrum layout through compression of DSP and ECAN functionality into a very small number of the new Telephony Services Processor (TSP) RMs.

> ***Note:*** To provide a future migration path for the Spectrum product (e.g., for OC-12 support), a set of Differential Link (D-Link) signals have been added to the double density backplane assembly. These D-link signals route between slots 5 & 6 and the ten high-speed slots; slots 5 & 6 form the hub of the D-link signals which emanate in a star configuration to the high-speed slots.

[1]The new frame PEC code is needed to facilitate ordering, since the frame and backplanes are ordered as a unit.

Figure 2 New Double Density Spectrum Backplane Layout



21.5 Limitations and restrictions

Though high-speed and double density Spectrum backplanes may co-reside in the same office, the two backplanes cannot be mixed within the same Spectrum frame.

21.6 Logs (LG)

N/A

21.7 Data schema (DS)

21.7.1 New/modified tables

Table 1 New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
MNSHELF	changed	unchanged
MNCKTPAK	changed	unchanged

There are no new fields for tables MNSHELF or MNCKTPAK. Rather, the verification rules have changed in support of the double density Spectrum backplane. Tables MNSHELF and MNCKTPAK will be modified to enforce the following restrictions with respect to the double density Spectrum backplane:

- a single frame cannot contain both a traditional (high speed) Spectrum shelf assembly (NTLX51BA) and a new double density shelf assembly (NTLX51CA)
- a single NTLX91CA frame can be provisioned with no more than four Spectrum nodes, using only double density Spectrum shelf assemblies (NTLX51CA)
- frames older than NTLX91CA with backplanes older than NTLX51CA cannot be datafilled with more than two Spectrum nodes
- circuit packs cannot be datafilled on shelf 1 of a Spectrum node that resides on a double density backplane (since shelf 1 cannot exist)
- prevent higher speed cards from being datafilled in slots 5 and 6 (the SRM slots) of a double density Spectrum node
- ATM RMs can be datafilled in slots 1 and 2, or 9 and 10 only
- OC3 RMs can be datafilled in slots 9 and 10 only
- Sync RMs can be datafilled in slots 5 and 6 only

21.8 Office parameters (OP)

N/A

21.9 Service orders (SO)

N/A

21.10 Alarms (AL)

N/A

21.11 Command interface (CI)

21.11.1 MAP Display Changes

Since a double density Spectrum node will only use up one card shelf, rather than the two shelves used up by a traditional Spectrum node, corresponding changes are necessitated to some of the SPM MAP displays. Specifically, the SPM shelf level and CEM/RM protection level MAP displays will be truncated to display only the one card shelf. The following subsections illustrate the changes.

21.11.1.1 SPM Shelf Level MAP Changes

The SPM shelf level MAP summarizes the states of all of the SPM's cards. (Refer to Figure 3 on page 263and Figure 4 on page 264.)

> mapci;mtc;pm;post spm 34

Figure 3 Old Single Density Spectrum Node Display

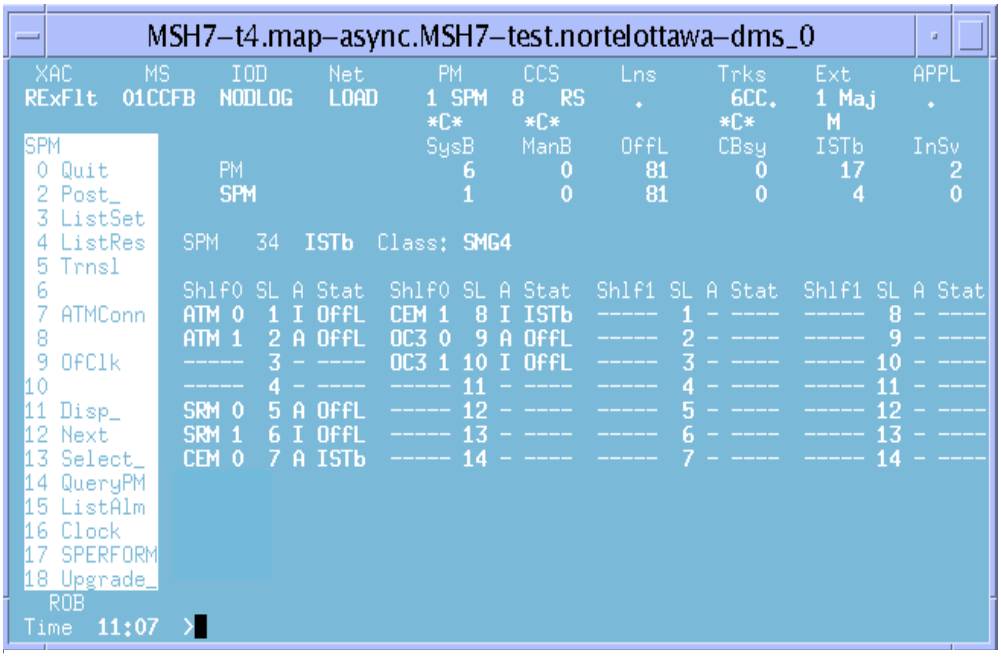
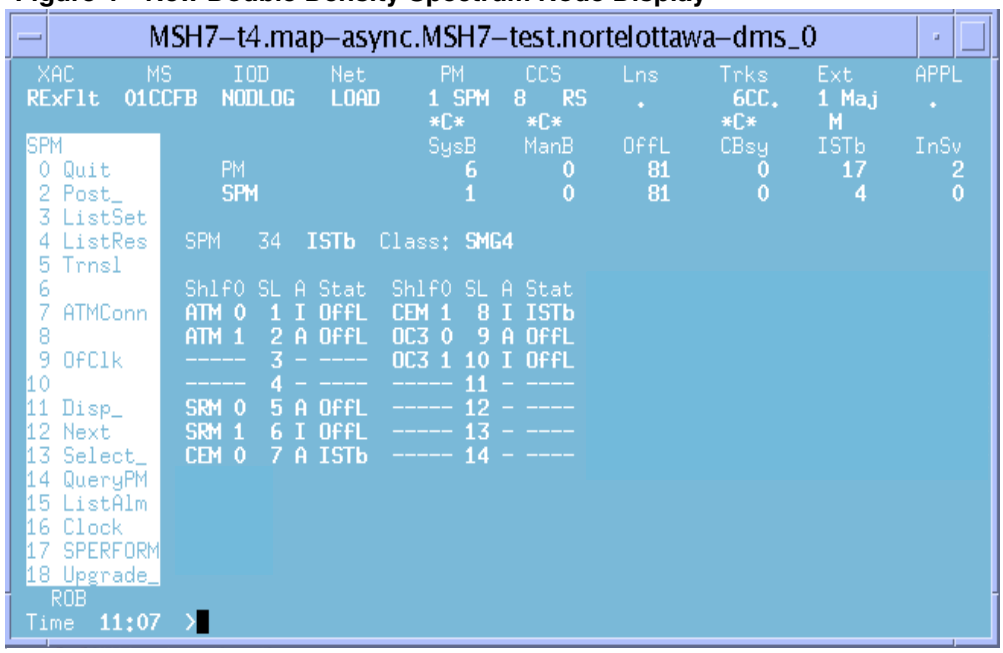


Figure 4 New Double Density Spectrum Node Display



21.11.1.2 SPM Module Protection Level MAP Changes

The CEM (or RM) protection level MAPs are used for manually switching CEM (or RM) activity between units in the same Protection Group. (Refer to Figure 5 on page 264 and Figure 6 on page 265.)

> mapci;mtc;pm;post spm 34;select cem 0; prot

Figure 5 Old Single Density Spectrum Node Display

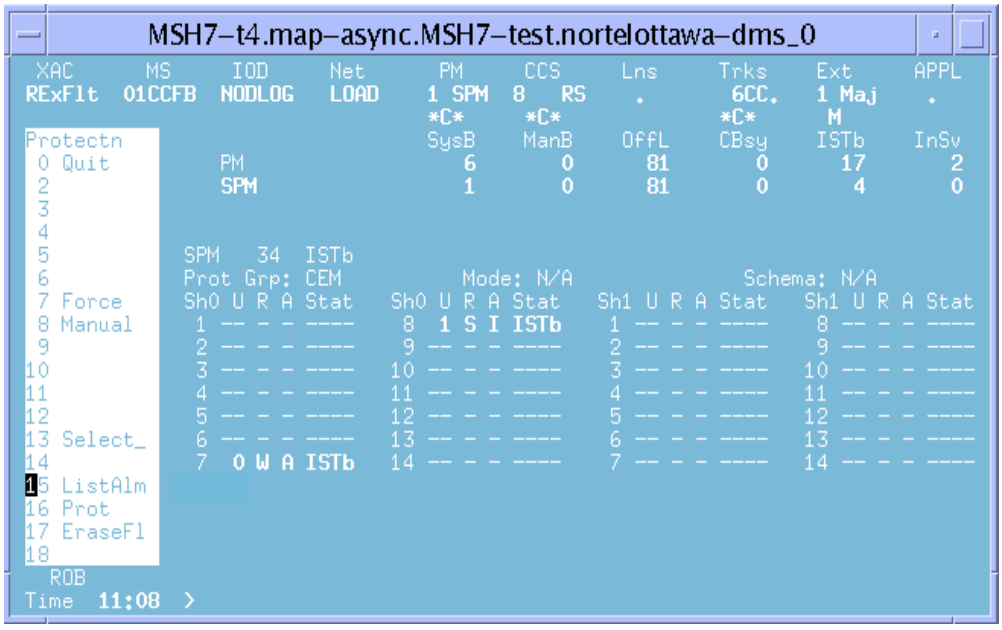
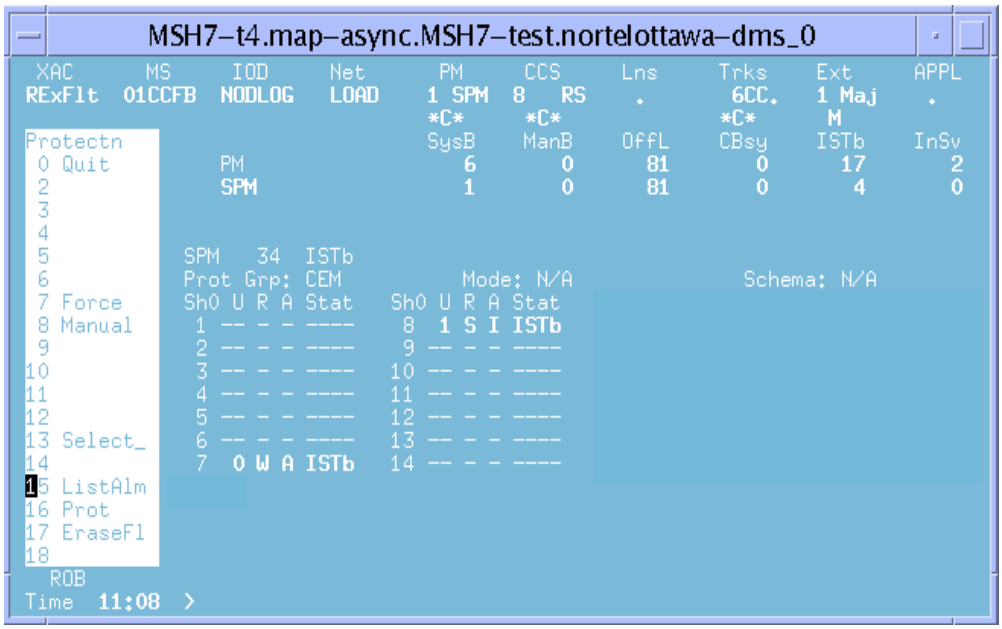


Figure 6 New Double Density Spectrum Node Display



21.12 Glossary

Term	Description
TSP	Telephony Services Processor - a new, high-density Spectrum resource module that can be used to replace multiple VSP, DSP, and COH resource modules.

22: Functional Description (FN): A00002133

22.1 Features name

A00002133:

CBM HA Installation, Patching and SW Delivery

22.2 Description

This feature provides the following functionality:

CBM product functionality:

- Software delivery processes for the CBM product
- Installation for the CBM product in both single and dual server high availability configuration
- Preparation work required in SN07 for CBM upgrades in SN08

Product generic functionality:

- A platform for patching for products based on the Solaris operating system
- An easy to use interface for installing and removing software

Software Delivery

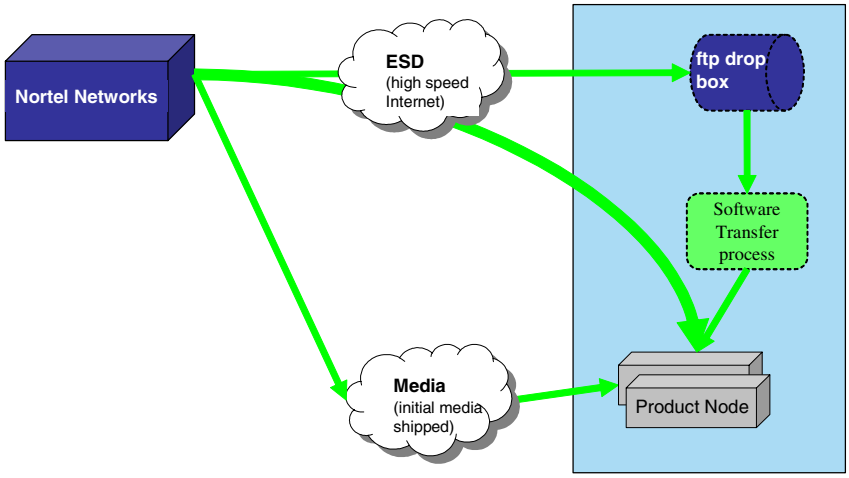
Electronic software delivery (ESD) is the supported method of software delivery for the CBM product. To support ESD, customers will require a high speed internet connection.

ESD provides greater responsiveness than media delivery. ESD provides business value by enabling automatic application of software reducing support costs.

CDROM media will be included with the initial product installation. Patches and maintenance load images will be delivered through ESD

ESD deliveries can be deposited on an intermediary machine, or directly onto the product node if access is provided. The direct access method is preferred as it is simpler.

The following diagram depicts an overview of software delivery.



The CDROM media will contain the final load image for the product and all available packages at the time the CDROM image was mastered. From that point on, the product will be patched using electronic patch delivery.

Installation

Installation procedures will support system preparation prior to shipment to the customer site to add business value. Preparation work includes installation of the SSPFS platform and CBM common software. Value is created by reducing installation technician labour costs as a single technician can perform the common parts of the installation process on many machines at the same time at the factory. This saves installation time and complexity during the install procedure at the customer site.

For two node clusters, the following steps are performed on the active node. Either node can be arbitrarily selected to be the active node for installation.

Installations for a single node cluster are very similar to installations for a two node cluster. Simply skip the last step where the inactive node is cloned.

Installation steps:

1) Install Solaris and the SSPFS platform and the CBM common components

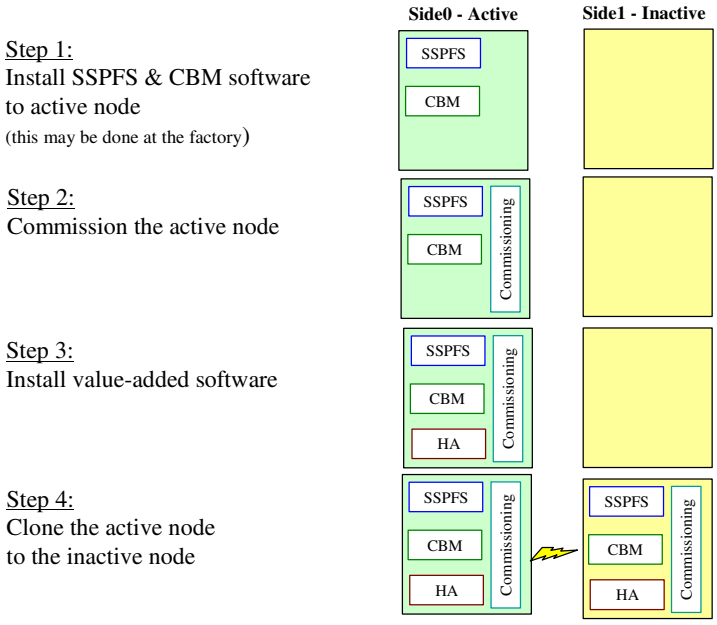
<these steps will be performed at the factory prior to shipment to site>

2) Perform system commissioning

3) Install value added software such as Billing, OM Delivery, or any other purchased software.

If this is a two node cluster, then

4) Clone the inactive node from the active node using the sync mechanism provide with the SSPFS HA framework



CBM Common software installation:

The installation interface is command line driven and common to all CBM based products. The “cbm_setup” installation tool provides a simple interface to initiate, complete, and provide status feedback for the installation.

<Begin screen capture>

```
==================================================
CBM Setup Program

==================================================
Checking available disk space.

Checking SSPFS setup.

Checking base directory.

/opt/nortel/cbm/7 exists.

Examining installed packages ...

Verifying required packages ...

      GNU Compiler and Libraries COMPLETELY INSTALLED

      RogueWave SourcePro Libraries      COMPLETELY INSTALLED

      Platform Base                      COMPLETELY INSTALLED

      SDM Base Maintenance Interface     COMPLETELY INSTALLED

      Platform Utilities                 COMPLETELY INSTALLED

      Generic Data Delivery              COMPLETELY INSTALLED

      Log Delivery Service               COMPLETELY INSTALLED

      Table Access Service               COMPLETELY INSTALLED

      OM Access Service                  COMPLETELY INSTALLED

Verification completed.
```

<End screen capture>

Upgrade preparation work:

cbm_setup will be used to provide a simple command line interface for upgrades. This adds business value by reducing training costs that would be required to learn multiple interfaces.

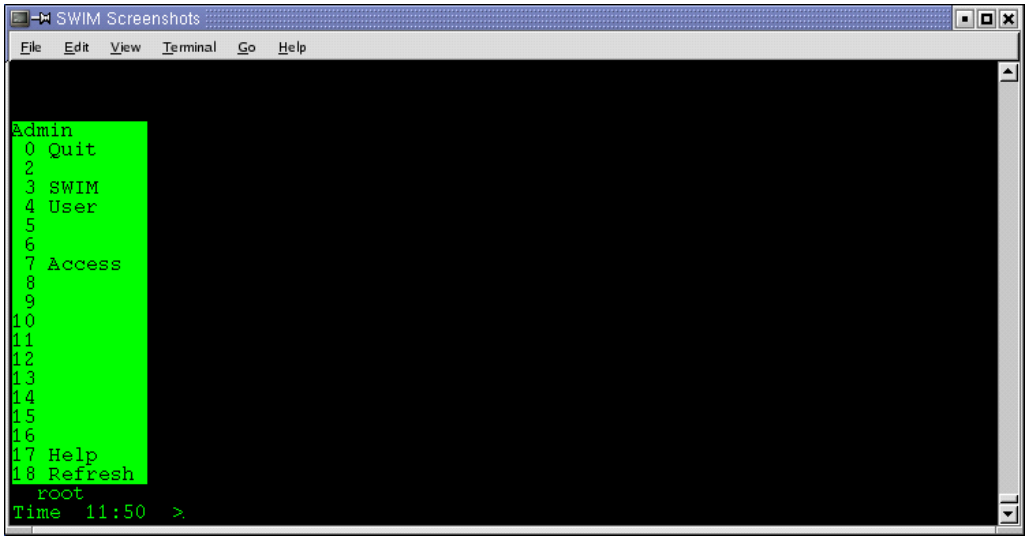
cbm_setup was designed to minimize user interaction prompts which adds business value by preventing user error and reducing labour and training costs.

CBM Upgrades were not completed as part of this activity.

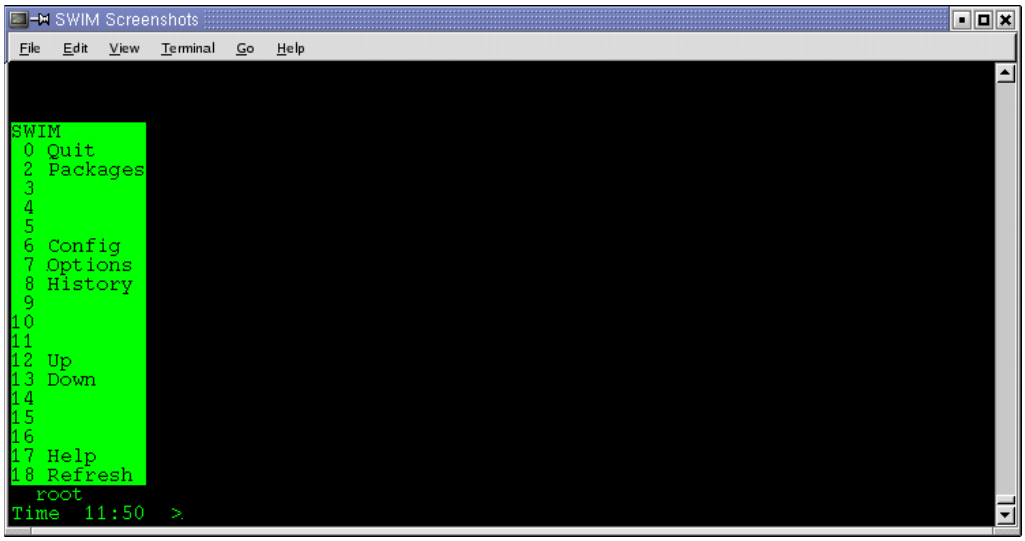
Software management:

Value added applications are installed via the SWIM level of the cbmmtce interface. Applications can be installed or removed at any time after initial installation. Applications must only be installed from the active node cbmmtce interface. This interface provides business value by providing a common interface across products for package removal and installation.

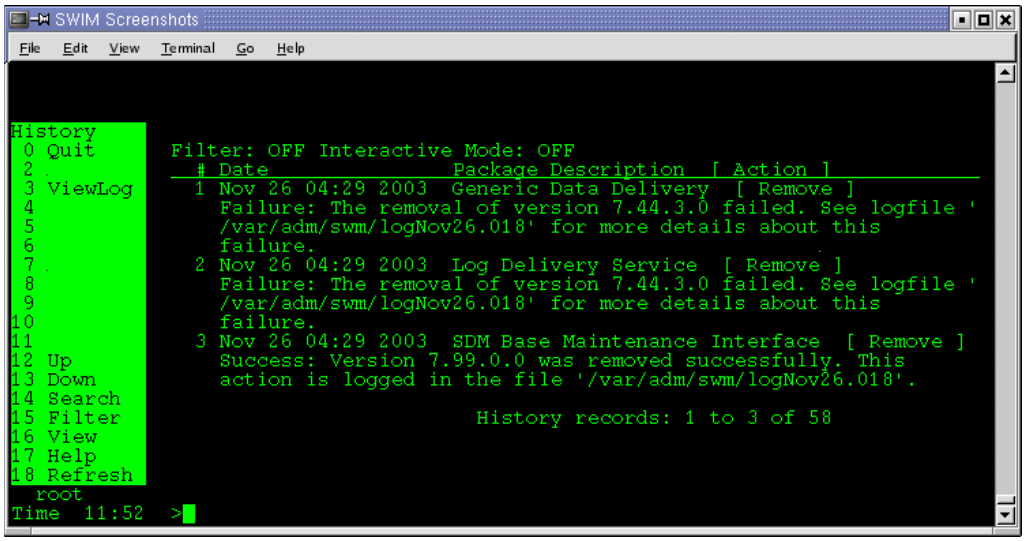
The SWIM level is accessible directly by typing SWIM and then enter in the cbmmtce interface, or through the admin level of the cbmmtce interface as detailed in the following graphic:



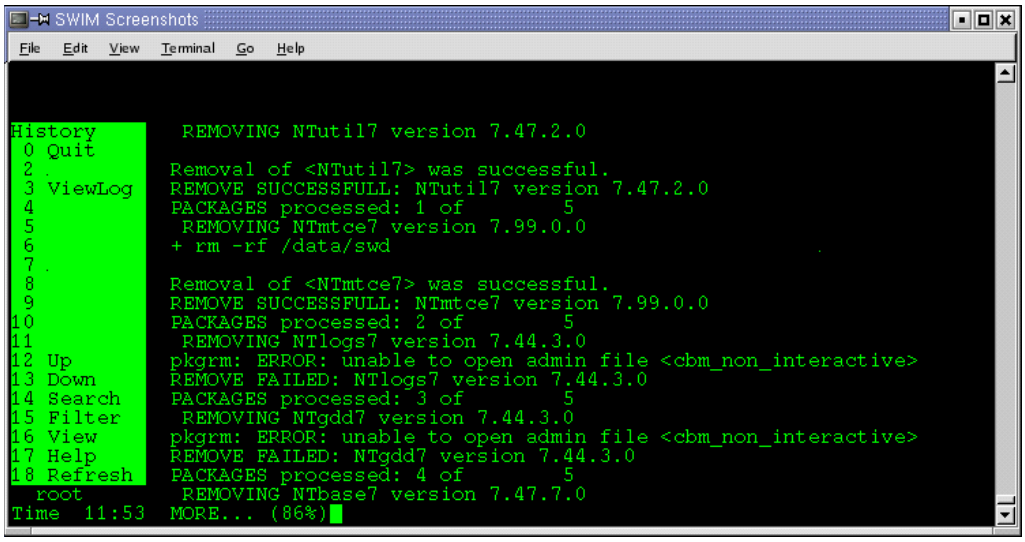
The options provided by the SWIM level are shown in the following graphic:



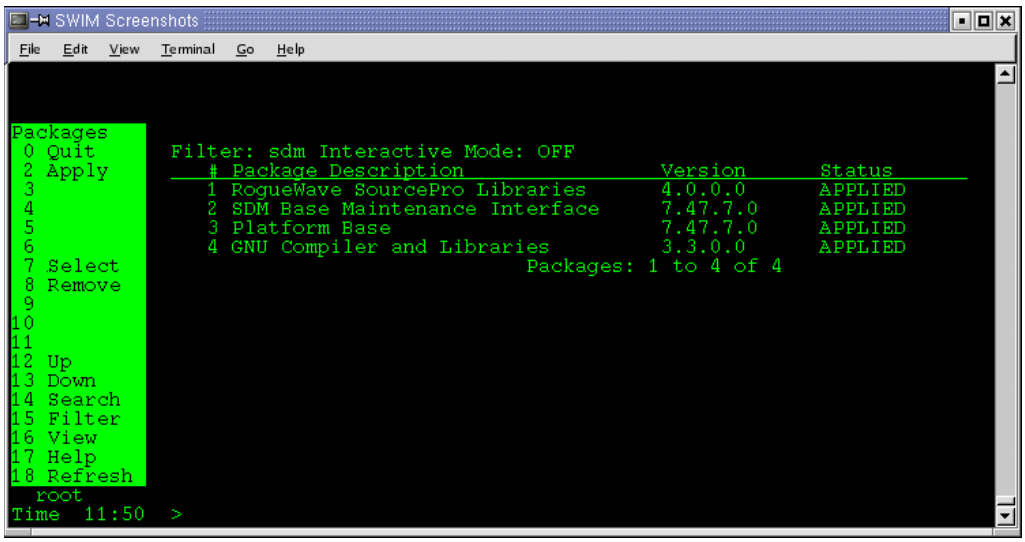
The SWIM -> History level provides a transaction history of packages that were applied using SWIM. These logs are maintained on the system and rotated every week or as disk space requires them to be rotated.



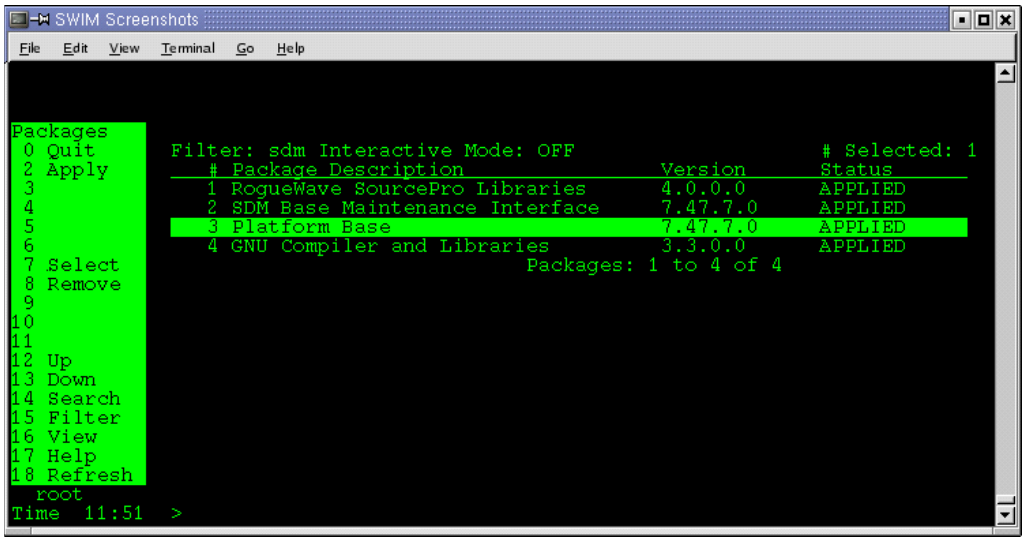
The SWIM -> History -> ViewLog level can be used to view the details from the application of a package using SWIM.



The SWIM -> Packages level shows software that is installed. The SWIM -> Packages -> Apply level should be used to apply software. It will provide a listing of available software Packages in a specified or default directory. The default directory is /swd/.



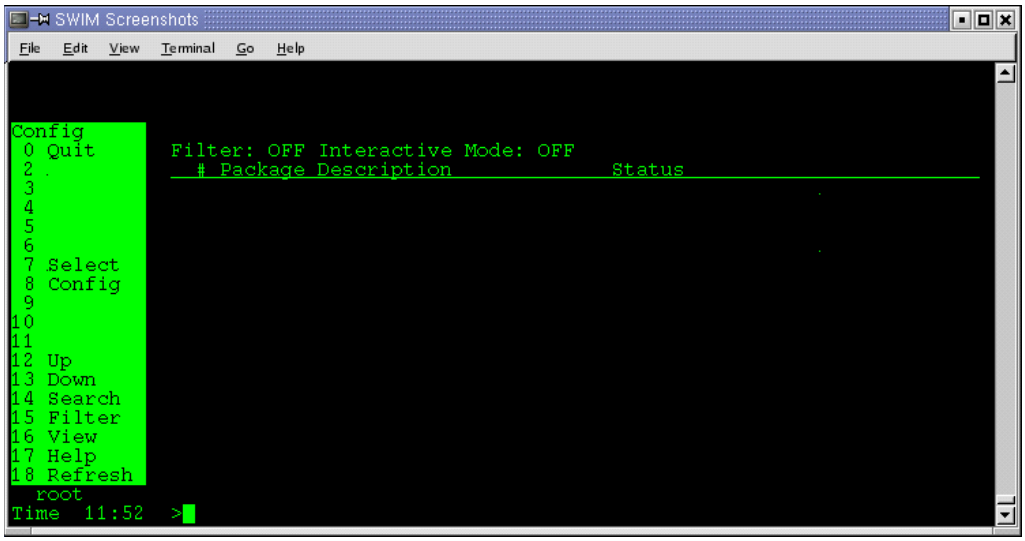
SWIM -> Packages, with an installed package selected



Application configuration:

Applications that require manual configuration will be configured via a command line interface initiated from the cbmmtce interface's config level. This provides business value as the interface and approach are the same across products preventing re-learning to reduce training costs and user error.

The following graphic depicts the config level:



Applications not requiring manual configuration will automatically be configured during installation or as they are brought into service depending on the scenario. The process of configuring these applications will be transparent to the system user.

Applications requiring manual configuration can be configured in two ways:

1) During installation, SWIM will notice the application requires manual configuration and at the end of the installation it will automatically prompt the user for the configuration steps and information.

Multiple installations requiring configuration will be batch queued such that the manual configuration steps are all executed at the end of the software installation cycle.

2) Should the user decide not the configure the application at installation time.They can configure, or reconfigure the application from the config level of the cbmmtce interface.

Patching:

A suite of tools to control patching are built into the SSPFS product. The tools are available to any products built on top of the SSPFS product, including the CBM product.

The patching suite tools create business value by reducing patching & support costs. They provide simple and product generic user interfaces to apply and remove patches as well as query and audit software.

Corrective content will be made available to the customers as individual patches. These will be provided in Solaris patch format contained within a tar and gzipped archive.The patching tools automatically handle processing and applying the patches.

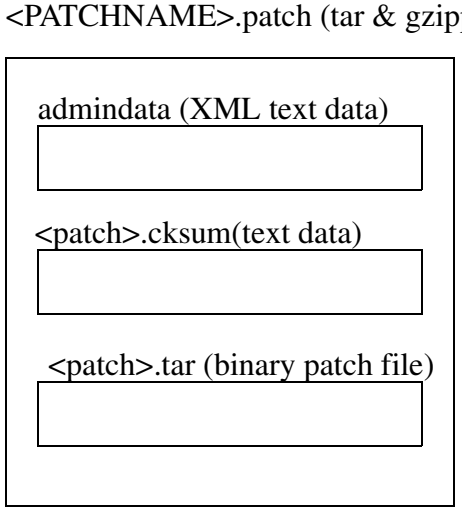
New for the CBM is a mechanism to guarantee the integrity of patches as they are received. The checksum delivered with the patch is used to verify the integrity of the patch archive. Any patch that is damaged in any way on its way to the CBM will be rejected as damaged.The customer will be informed of any such rejection.

Patches will be compressed and transported as a single file. The compression adds value by reducing disk space requirements and ESD transfer times for patches.

The patch archive will contain checksum data to verify the patches integrity. Should the patch file become corrupt in any way, the system will be able to detect, avoid applying, and alarm the corrupt patch.

An administrative file is provided with all patches to provide status information, release notes for the patch, and handling instructions for the patching tools.

The following diagram denotes the structure of patches provided by Nortel:



Patches are designated as one of three types: active node apply, inactive node apply, and manual apply. The patch type is used to trigger the appropriate handling of the patch while being applied in highly available cluster configuration. For single node configurations, inactive apply patches automatically become manual apply patches.

Both active node apply and inactive node apply patches can be applied automatically by setting a schedule with the patchconfig tool.There are separate schedules for each. Manual patches are never automatically applied, and cannot be scheduled. For non-clustered systems, the inactive apply schedule does not exist as patches are either active apply or manual apply.

Patches have an attribute embedded within them to determine whether they require a system reboot to be applied. If they require a reboot, the patching suite software will initiate the reboot. Depending on the scenario triggered by the patch type, the reboot may be handled either automatically, or manually with user prompts.

Patches applied on the active node will only affect service for specific applications modified or updated by the patch. Patches applied on the inactive side will not be enabled until after a SWACT (which involves a loss of service for all applications). However, applying the patch on the inactive side allows a continuation of service on the active side while the patch is being applied on the inactive.

Patches are only applied to the mate node once the patch has successfully been applied to the first node. Patches that fail to apply successfully will be automatically removed and an alarm will notify the user of the unsuccessful apply attempt.

Patch Handling	Applied Automatically	Can be scheduled	Node applied on	Description
Active Apply	Yes	Yes	Active	This handling is ideal for non disruptive or patches for less sensitive applications.
Inactive Apply	Yes	Yes	Inactive	This handling is ideal for disruptive or sensitive application patches.
Manual Apply	No	No – manually initiated	Inactive node with prompts	This handling is ideal for disruptive patches, patches that require manual interaction, or highly sensitive applications.

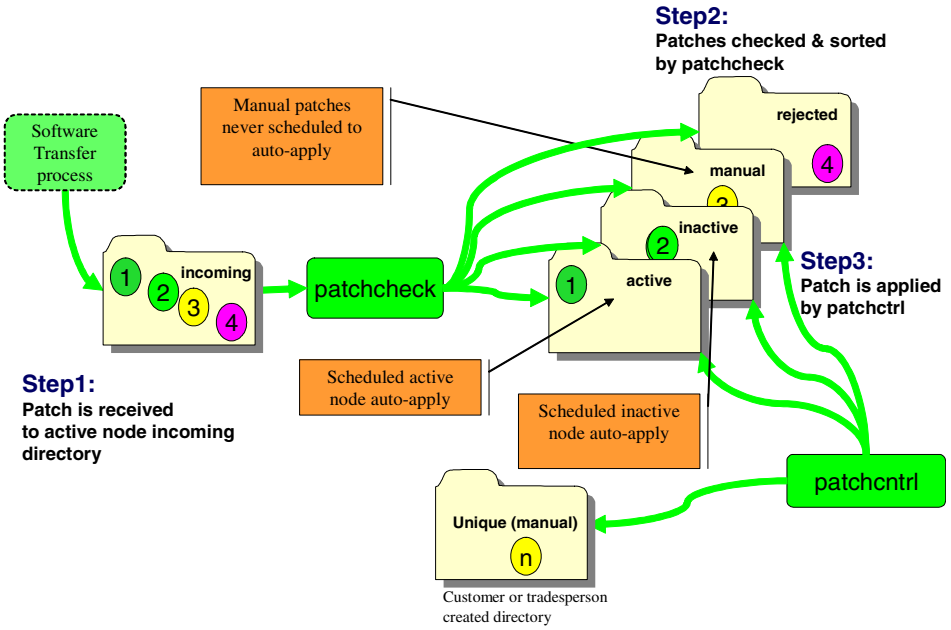
Additional Patch Attributes:

Reboot required: Yes/No Patch Status: S/V/R/Z

RPS States:
Submitted
Verification
Released
Zapped

These attributes trigger special handling. VO patches = manual apply.

The following diagram details how patches will be received in the incoming directory and processed by patchcheck to be sorted into directories according to required apply handling: Multiple patches will be applied in sequence.



Also new for the CBM is the capability to override embedded patching handling with a more cautious handling procedure. This feature is enabled by setting patch filters. Patch filters allow declaration of patches matching criteria to be always inactive apply, or always manual apply. The filters are set, updated, or removed using the patchfilter command. The filtering mechanism is based on the filter pattern matching the patch name, or the name of the package the patch updates, or the category of the patch.

Patch filters always add more conservative handling to patches. For example, making an active apply application such as Billing a strictly manual apply application. Patches requiring special handling cannot be filtered to remove that special handling. For example, a manual patch cannot be filtered to make it active apply.

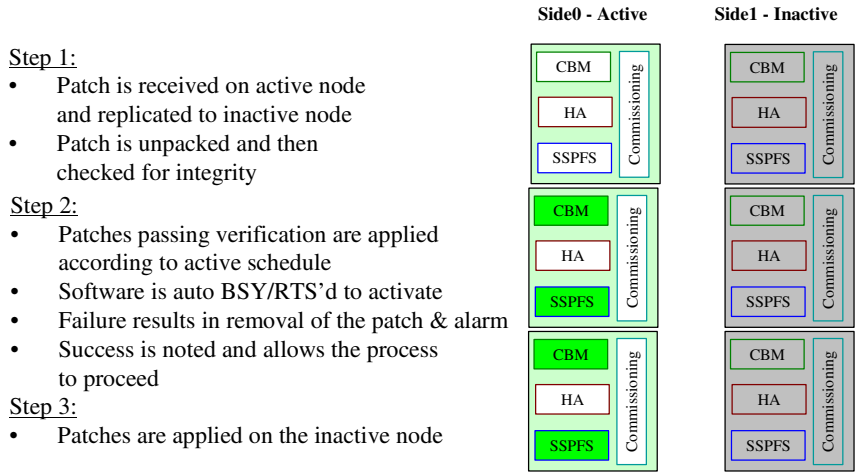
A status field is embedded within the patch to track the deployment state of the patch. This state is referenced to determine the appropriate behaviour for patch application. Verification (V) patches will be automatically classed as manual apply patches only. Release (R) status patches will follow their appropriate handling based on the patch type field, or any defined patch filters.

The configurable patch application schedules provide business value by allowing automatic patch application during less busy periods and reducing support costs as that would have been incurred if manual interaction was required.

The patch format used by the patching suite provides automatic patch application and automatic application restart once the patch has been applied (if required). CBM patches will restart applications autmatically by default.

The patching tools provide high availability cluster support. This feature enables value by automatically handling sensitive or disruptive patches requiring reboots or restart of important applications. These patches are handled automatically by applying them on the inactive node of the cluster and then SWACT'ing. These inactive apply patches will be applied on the inactive node to minimize service disruption.

The following diagram depicts how active apply patches are handled:

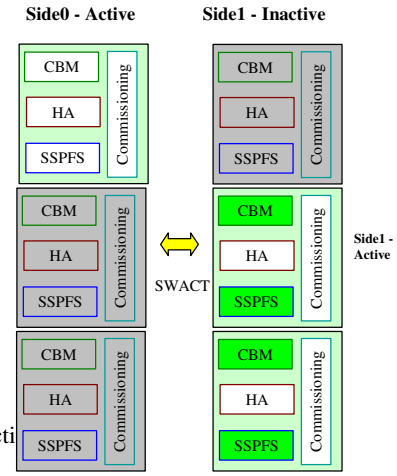


The following diagram depicts how inactive apply patches will be handled:

Step 1:
- Patch is received on active node and replicated to inactive node
- Patch is unpacked and then checked for integrity

Step 2:
- Patches passing verification are applied according to inactive schedule
- Failure results in removal of the patch & alarm
- SWACT and RTS is initiated to activate
- Success is noted and allows the process to proceed

Step 3:
- Patches are applied on the inactive (formerly acti node)



Patching security & robustness features:

The patching suite provides several important security features to enable a high level of security for customer networks.

The patching suite includes automatic integrity checking to screen and alarm corrupt patches & prevent their application. The patching suite supports encrypted file transfers & inter node communication.

The manual patch application type is supported to provide complete control over sensitive patches. Patch filters provide the ability to define more sensitive handling for defined applications to minimize service disruption

Important design considerations were factored to ensure a high level of robustness for the patching suite. No application level software required to apply patches. Patches are applied using low level operating system commands to ensure application of patches will not be blocked by a daemon or service being unavailable.

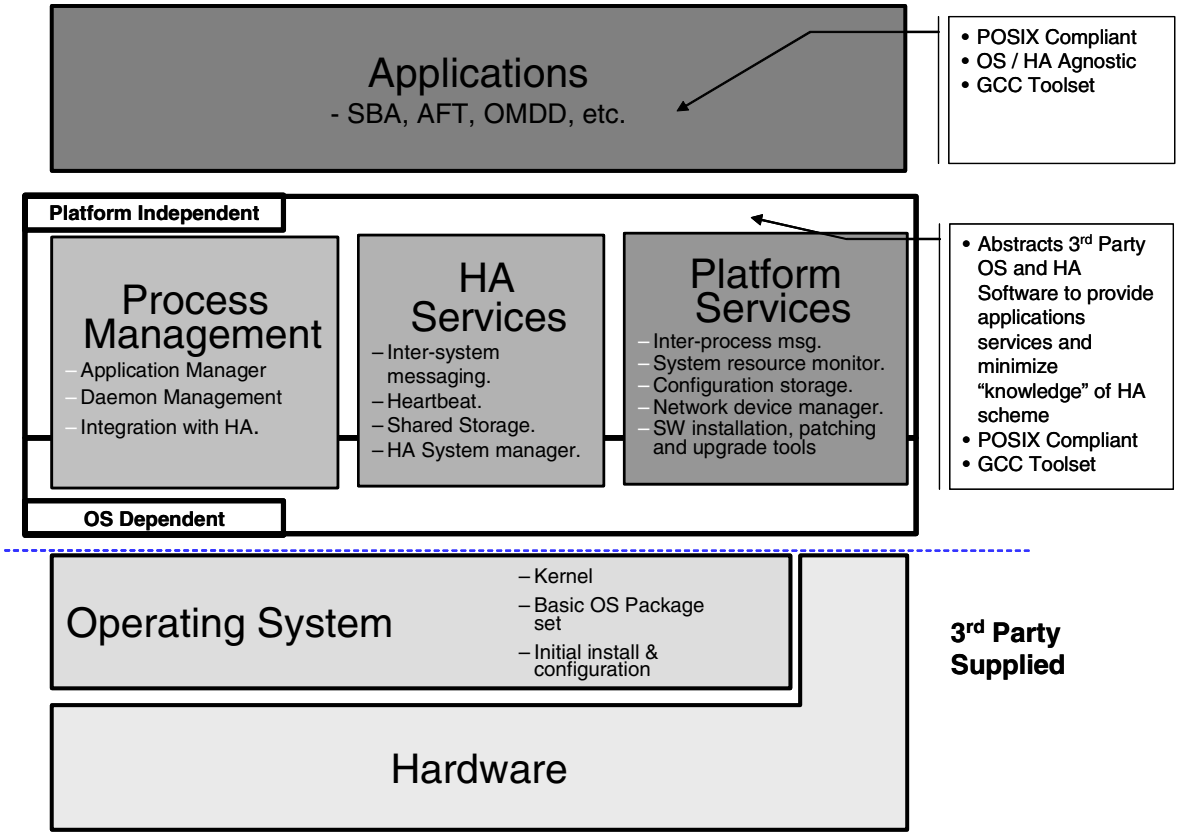
No special daemons required to support patching. For the automatic scheduling functions to work, the cron server must be functioning.

New for this release, the root password not required to control patching. Maintenance users (maint group, or emsadm group) will have access to run patchctrl. This enables them to apply patches without accessing the root password.

Please see the patching limitations section of this document for information regarding a possible security exploit.

22.3 Hardware and Software Requirements or Dependencies

The CBM product requires the Sun Microsystems N240 hardware platform that is provided by the SSPFS platform. The CBM product utilizes the Solaris operating system also provided by the SSPFS platform.



Dependencies for Patching include:

- Solaris patchadd and patchrm tools

- High available software
- Alarming facilities

Dependencies for Installation include:

- SSPFS installation script and commissioning interfaces
- Solaris pkgadd and pkgrm tools
- CDROM or ESD Image (ISO) of CDROM
- HA Cloning tool
- Alarming facilities
- Application registration interfaces
- Application set up automation

Upgrade preparation dependencies:

- HA Cloning tool
- Alarming facilities
- Application registration interfaces

22.4 Limitations and restrictions

General Limitations:

- There are differences between SDM's legacy patching processes and interfaces and the patching suite interfaces developed in A0002133. These differences are not likely to be accepted by customers creating a requirement to enhance the patching suite tools to understand and support SDM patching.The patching suite tools were designed with this goal in mind.

The following limitations are noted for the following components.

Patching limitations:

- Patches must be provided in Sun patch format
- Patch integrity checking requires a checksum to be include with the patch

- For the patch handling mechanisms (active apply, inactive apply, manual apply) to work, an amindata file containing information defining the intended handling must be included with the patch
- Solaris patches must follow a Solaris patch manager supported naming convention.
- Patches are cumulative until completion of a design activity to create incremental patching tools
- Patches must handle restart of dependent applications until a more sophisticated shared library & dependency handing tool is developed
- Z status patches will never be delivered, but are not automatically removed from products installed in the field.
- **Important:** Patches can not be verified to have originated from Nortel Networks without the development of a patch authenticity checking mechanism. Lack of this mechanism provides a significant security hole.

Installation limitations:

- Packages need to be supplied in Sun package format

22.5 Interactions

Installation Interactions:

Installation of CBM core software is completed through using the cbm_setup interface. This tool will automatically install the CBM core (also known as “base”) software. The core software packages will be installed and their installation verified automatically without any prompts.

Value added software such as Billing, OM Deliivery, and other applications that are sold seperately from the code platform software can be installed at any time after the initial installation using the SWIM interface. For two node cluster configurations, the SWIM interface will automatically install the software packages selected onto both nodes.

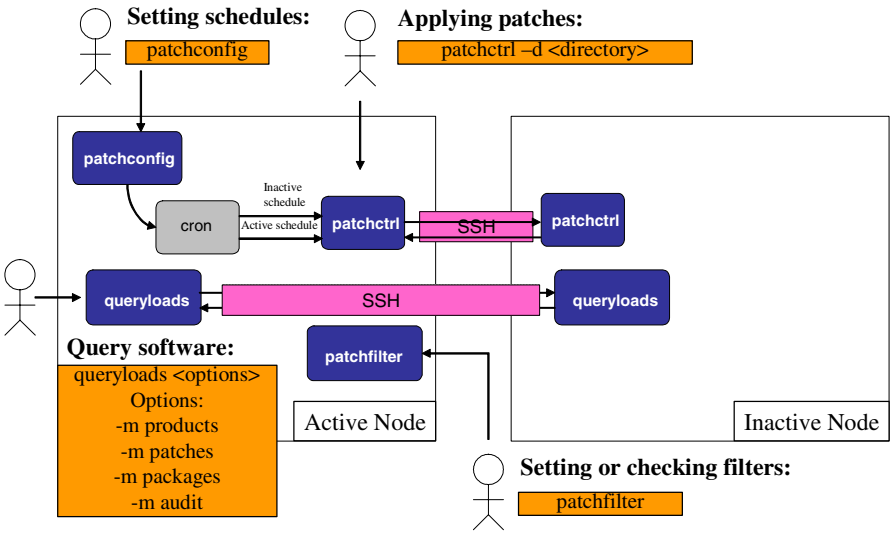
Upgrade Interactions:

The planned interface for CBM ugprades will be cbm_setup.

This work will be completed in a new activity.

Patching Interactions:

There are 4 interfaces for patching. They are depicted in the following graphic:



1) patchconfig

The patchconfig tool is used to set, or reset the patching schedules.

The user will be prompted for two schedules, one for the active apply schedule and one for the inactive apply schedule.These schedules will be used to trigger application of patches for the respective node and patch handling type.

<TODO: Add screen capture for patchconfig>

2) patchctrl

The patchctrl tool provides a single interface for patch application. It automatically handles active patch apply, inactive patch apply, or manual apply scenarios. If patches require a reboot, it will automatically initiate the reboot or prompt when patching manually.

patchctrl will automatically handle triggering a SWACT for patches that require it when the system is a two node cluster. During manual patch application, a SWACT will be preceeded by a prompt.

3) queryloads

queryloads provides an easy to use interface to gather software information about the system. queryloads reports information in one of two formats, a human friendly report, or raw XML data.

queryloads reports information on the Nortel products installed on the system, the software packages installed, and the software patches installed. If provided with a product name, queryloads will automatically filter output to report information for that product rather than all software installed on the system.

4) patchfilter

patchfilter provides an interface to set or remove filter instructions. Patch filters allow customers to define more conservative handling for patches. This enables making patches for designated applications either inactive or manual apply even though the patch itself may be an active apply patch. Filters only allow more conservative handling. For example, a manual patch could not be made an active apply patch.

5) Alarms

A minor alarm (Istb) will be raised on the node when a patch has failed to apply. A command line tool will be provided to manually clear this alarm.

A minor alarm (Istb) will be raised and automatically cleared on the node when a patch fails the integrity check

22.6 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	___X___
Configuration	
Data Schema	___X___
User Interface	___X___
Element Management	___X___
Security	___X___
Service Order	___NA___
Office Parameters	___NA___

Accounting (includes AMA billing) ___NA___

Performance (includes operational measurements) ___NA___

22.7 Glossary

Term	Description
CBM	The Nortel Networks Core and Billing Manager product.
SDM	The Nortel Networks SuperNode Data Manager product.
NPM	Network Patch Manager
Patch	An atomic unit for delivering changes to deployed products. Patches may contain files, directories, and links to affect changes on the system.
SSPFS	Nortel's Succession platform based on the Solaris operating system.
SWACT	SWitch of ACTivity from the active cluster node to have the inactive cluster node take over.
cron	The UNIX cron daemon, a facility for scheduling execution of commands.
Value added software	Software that provides additional capability beyond the core product. (and costs extra)

23: Functional Description (FN): A00002137

23.1 Feature name

A00002137: DS512 Link Mtc Robustness - CM

The work for this feature is documented in module A00002146 in PLS FMDOC.

23.2 Description

23.3 Hardware Requirements or Dependencies

23.4 Software Requirements or Dependencies

23.5 Limitations and restrictions

23.6 Interactions

23.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

23.8 Glossary

Term	Description
New term	Definition

24: Functional Description (FN): A00002146

24.1 Feature name

A00002146: MAPCI ABI Link Test & Legacy Comparison

24.2 Description

Our existing customer base has a large number of legacy XPM peripherals in existing TDM networks. Migrating to a total packet network will be a large undertaking for our customers. Providing a means to gradually migrate will help our customers make the transition to total packet switching.

This feature is part of a larger project goal to subtend legacy XPM peripherals from an MG9000 using the Access Bridge Interface (ABI, pec code NTNY43AA). The XPM peripherals will connect to the MG9000 via DS-512 links instead of connecting to the ENET via DS-512 links. Most of the link mtc. needed to support ABI XPMs was developed in SN05 and SN06 via activities 59038678 and 59039633.

There are 4 parts to this design activity.

- **ABI Link Mtc. Enhancements**

  One purpose of this feature is to enhance the existing link maintenance software for the MG9000-ABI peripheral by filling in some inconsistencies found during testing and by adding the capability to perform single link maintenance on message-capable links.

- **ABI Card Activity Status**

  Unlike the ENET, the ABI cards in an MG9000 have a Master/Slave status. This feature enables the MG9K and the CS2K to report and handle ABI card activity status so that it can be displayed on the Map and (if desired) used by the speech aspect in CS2K software to align the preferred plane selection on the “Master” ABI card for call setup. (See also activity A00002045: ABI Loadsharing.)

- **Manual Link Mtc.**

  In order to facilitate commissioning and testing of ABI XPMs, there is a need to perform manual mtc. actions on the cside links of the XPM from the XA-Core MAP interface. This feature adds a new Map sublevel to the posted LGC map level from which an ABI XPM’s cside links can be Bsyed, RTSed and TSTed. See Figure 1, "ABILink Map level".

  Note: Only message links are supported at this time.

- **Resync capability**

When an XPM is being rehomed from the ENET network to an MG9K/ ABI, there is a need to tell the ABI interface to adjust its frame sync reference to sync to the inactive XPM unit. This capability is provided via new command ADJUST_FRAME_SYNC (AFS for short) from within the ABI Rehome CI tool (ABIREHOME).

Figure 1 ABILink Map level

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .      1 LGC     .        .        .       .        .

ABILink                             SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                    0        0        0        0        1       32
 2               LGC                   0        0        0        0        1        9
 3
 4            LGC     0 ISTb  Links_OOS: CSide  1 , PSide  0
 5            Unit0:   Act   InSv
 6 Tst_       Unit1:   Inact InSv
 7 Bsy_
 8 RTS_       CSide host: GWC 16  ABI IP Address: 10.32.133.194
 9                                DS30                 1 1 1 1 1 1
10                      ABI Status 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
11             Plane 0   Master   . . M . . . . . . . . . . . . .
12             Plane 1   Slave    . . . . . . . . . . . . . . . .
13
14
15
16
17
18
  ADMIN
```

24.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced due to this feature.

24.4 Software Requirements or Dependencies

This feature requires the following loads to function properly:

- MG9000 - SN06.2
- GWC - SN06.2
- XACore - SN06.2 (SN06 with 6.2 patches applied)

Feature A00002746: “ABI XPM Fault Isolation & QueryPM” is dependent upon this one for it’s functionality.

24.5 Limitations and restrictions

In SN06.2, the ABI interface on MG9000 supports the following XPM pm_types only:

- LGC
- LTC
- SMA2

Manual mtc. actions from the ABILink map level are not supported on individual speech-only links in SN06.2.

24.6 Interactions

Not applicable.

24.7 Applicable customer facing sections

Fault Management	
Logs	__X___
Alarms	_____
Configuration	
Data Schema	_____
User Interface	__X___
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

24.8 Glossary

Term	Description
ABI	Access Bridge Interface - a card or board on the MG9K
CM	Compute Module - the CPU of the CS2K
Core	same as CM
CS2K, CS2000	Communications Server 2000 - the CallP engine of the Succession network
DS30	A link protocol used to connect to one port on the cside of a host XPM; consists of 30 speech channels plus 2 msg channels.
DS512	A link protocol used to connect to the cside of a host XPM; consists of 512 channels subdivided logically into 16 DS30 links.
ENET	Enhanced Network
GW	MG9K Media Gateway
GWC	Media Gateway Controller
MG9K, MG9000	Media Gateway 9000
RTS	Return To Service
XA-Core	A CS2K with multi-processor hardware
XPM	Any of the series 2 peripherals, i.e. LTC, LGC, SMA2, etc.

25: Functional description (FN): A00002155

25.1 Feature name

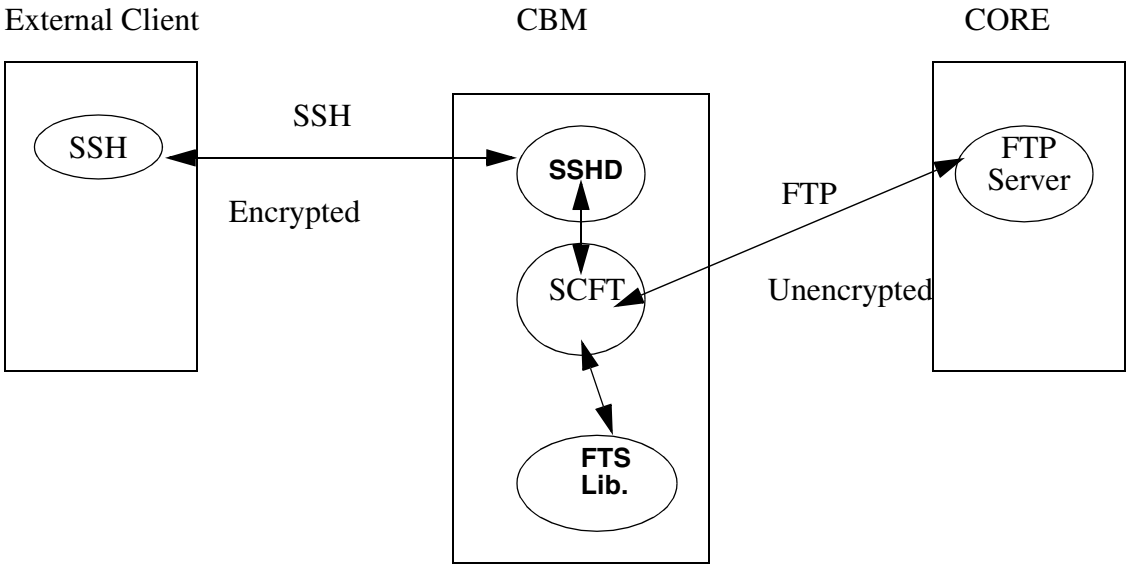
SSH Core File Transfer (SCFT) for CBM and SDM.

25.2 Description

This feature is intended to provide a non-DCE option for secure FTP that will allow secure FTP access to the CORE. through the CBM or SDM.The feature can be used to retrieve files from the core and transfer files to the core from an external workstation through the CBM or SDM. The feature provides the security supplied by the SSH (version 2) so that the core will not be compromised by illegal users. The SCTP code that runs on the CBM or SDM provides much of the standard FTP functionality, enabling the remote client to perform all the FTP operation that may be needed to maintain the CORE through the CBM or SDM.

This feature provides the dynamic creation of the CM FTP users. This is accomplished by the SSH core file transfer authorizing the user executing the command based on their group memberships.

Figure 1 SSH Core File Transfer



25.3 Hardware Requirements or Dependencies

This feature will run both on the CBM platform as well as the SDM.

25.4 Software Requirements or Dependencies

The external client must have standard SSH (version 2) running on his machine. He must also have the SCFT code running on the CBM or SDM. It would also be useful but not necessary to have the Korn shell script created by Nortel for running the SCFT code through SSH loaded on the external client's machine. The SCFT code as well as the Korn Shell script will be delivered to the client as a packaged SDM/CBM load.

25.4.1 Handling SSH authorized_keys file over SWACTs.

If you are using a CBM-850 system that has two CBM clustered together, special care must be take that the SSH authorized_keys file are kept current on both sides. This is particularly important if you do a swact as you may no longer be able to connect password free if the authorized_keys file is different. The authorized_keys file can be copied over to the cbm on the other side by using the syncFile.ksh command.

> /opt/servman/shell/syncFile.ksh /.ssh/authorized_keys

25.5 Limitations and restrictions

Only a restricted subset of FTP commands are supported with the SSH Core File Transfer. However, it should be noted that one of the commands supported is the "command" feature which allows any FTP command to entered as a string that will be performed on the FTP server on the core. With this command virtually any FTP command can be entered.

Core image files can not be transferred from an outside client at this time. There is code within the Core that prohibits this.

It should also be noted that all commands must fit onto one line and must be passed to the SCFT code intact.This is necessary because the FTP connection to the core is created and removed after each command. So you can not, for instance, set the output type to Binary in one command then do a put in the next and expect the type to be binary. The binary command will not be remembered for the put and the type will default back to the standard FTP type of ASCII.

25.6 Interactions

This feature will use the previously existing FTS code to perform the FTP commands that are requested through the SSH Core File Transfer code. Some changes have been made to allow the output to be returned to the external client. The external client will also be required to have a standard SSH installed on their system.

25.7 Applicable customer facing sections

Fault Management

- Logs ___X__
- Alarms __N/A_

Configuration

- Data Schema __N/A_
- User Interface __X___
- Element Management __N/A_
- Security ___X__
- Service Order __N/A_
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

25.8 Glossary

Term	Description
AIX	IBM UNIX operating system on the SDM FX
CBM	Core Billing Manager
CM	Command Module (the CPU of the DMS)
CMFT	Command Module File Transfer Script
AIX	IBM UNIX operating system on the SDM FX
CBM	Core and Billing Manager
Core	DMS switch computing engine
DCE	Distributed Computer Environment
FTP	File transfer protocol
FTS	File transfer System (Nortel proprietary code)
IP	Internet Protocol
SCFT	SSH Core File Transfer
SDM	SuperNode Data Manager

Term	Description
SSH	Secure Shell protocol
SSHD	Secure Shell protocol Daemon

26: Functional description (FN): A00002164

26.1 Feature name

A00002164 - APPLICATION MANAGER FOR HIGH AVAILABILITY (HA)

26.2 Description

This feature provides a framework for running Core and Billing Manager (CBM) applications in a High Availability (HA) computing environment, based on having programs run on distinct computers rather than on a fault tolerant hardware base.

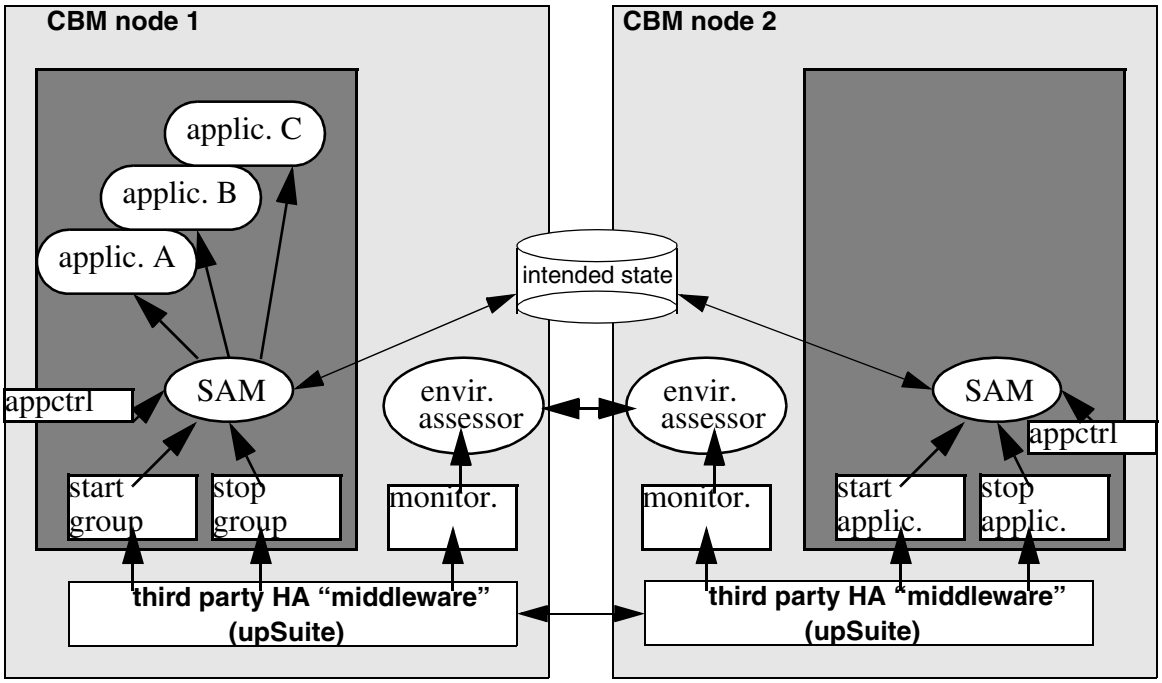
The feature deals with application management. An application is one or more programs that perform an OAM&P functions. Managing applications means starting and stopping them; restarting them automatically if they crash; and in the context of a HA environment switching them between the computers (nodes) in a CBM cluster as required.

In a CBM system applications are managed by a dedicated process the SDM/CBM Application Manager (SAM). The main purpose of this feature is to adapt the proven SAM manager, developed for the synch-matched fault tolerant SDM product, to work in a HA solution made up of two independently running computers.

26.2.1 Major components

Figure 1 depicts the major components involved in managing application on the High Availability CBM product. This feature implements the components that are in the dark gray boxes. The figure depicts the situation where node 1 is the “active” computer in the cluster, where the applications are running.

Figure 1 Application management components in HA CBM



These components and their primary functions are:

Application One or more programs that are performing a CBM Operation, Administration, Management or Provisioning (OAM&P) function. Applications are generally installed by a package, and can be individually managed by a user. Applications are organized in **groups** for the purpose of combined management and HA switchover. In the initial release of this product, only one group is supported: the "active side applications" group. This group will encompass all the CBM applications, and will run on the "active" CBM node.

SAM The management program that is responsible for starting, restarting and stopping applications as appropriate. SAM maintains information about an application and its group. This information contains amongst other things:

Intended state - The state that the user/administrator desires the application or group to be in. SAM will attempt to bring the application to that state, but may not be able to achieve it if there are problems. The intended state of groups and applications is stored on disk, thus it will be remembered if the SAM program dies, or the system restarts. Furthermore, the intended state file is deposited in a **replicated** file

system. This means that the up-to-date intended state information is available to the SAM program of both nodes, which enables SAM to bring the applications up to the same state they were in after an HA activity switch over.

Effective state - This is the real state of the application or group. It reflects degradation or failures of the application and group caused by faults on the system or network. The effective state is the one that is reported to the user via the management tools.

APPCTRL This is a command line user interface (CLUI) program that an administrator uses to control applications individually or as a group. It actually interfaces with SAM. The APPCTRL command supports sub-commands like: offline to set the intended state of a component to Offl; return to service (RTS) to set the intended state to in service (InSv); and busy (BSY) to set the intended state to manual busy (ManB). The cbmmtc page mode interactive management program also offers the same sub-commands in the APPL “level”.

HA middleware The software that controls the operation of the CBM cluster. It is responsible for deciding which node in a CBM cluster is to run a service (application group). It does this by exchanging messages between nodes and running diagnostics on the key hardware components of the computers. When the HA middleware decides to run a service on a node, it will also ensure that the resources that the service needs, like the “floating” CBM IP address, is activated on that node. When the HA framework determines that service must be moved to the other node, then it goes through a procedure known as a “HA switch over”. This involves stopping the services on the active system, transferring the resources to the other system, and starting the services on the other system. The HA framework used on CBM is a third party commercial software product, it uses “scripts” to interface with the software that it is managing. The HA framework is capable of spreading the load by having services active on multiple different nodes. However, in the initial release of this product, we will limit ourselves to two nodes per cluster, and one service: the “active side applications” group. Thus, in practice, for the first release, one of the two nodes will be the active computer, and the other one the inactive computer.

Start group script Run by the HA framework when a node has just become active, indicating that it is time to start the applications. The script passes the request to SAM who will launch the applications.

Stop group script Run by the HA framework when a node is about to become inactive, requesting an orderly shut down of the applications. The script passes the request to SAM who will terminate the applications.

Monitor script The HA framework will call this script regularly to verify the sanity of the application run-time environment. The script will interface with the environment assessor program. The script will return “NOT OK” if the environment assessor has determined that the local system or its network connections have a critical fault that prevents the applications from performing their job. In that case the HA framework will initiate a HA switch over to the other system. The environment assessor performs sanity checks that go beyond the basic hardware checks provided by the HA framework; it also communicates with its peer on the other system to ensure that it doesn’t cause a switch over unless it has determined that the other system is in a better situation. The environment assessor is not part of this feature, it is covered by feature A00002757 CBM FAULT MANAGEMENT.

26.2.2 Group and Application States

Figure 2 shows a flowchart describing the **effective** states that groups and applications can be in on the CBM, it also depicts all the changes between states and the triggers that cause them.

The big encompassing rounded rectangles represent the **group** states, the smaller rounded rectangles represent the **application** states. As mentioned earlier, in the initial release of CBM all the applications will be contained in one group called the “active side applications” group.

The group state and the applications **intended** state are controlled independently by a maintenance operator issuing **appctrl** or **cbmmtc** graphical user interface APPL level commands. However, it is apparent in the picture that the application **effective** state is greatly influenced by the **intended** state of the group that contains it. The general rule is that **SAM will try to bring an application’s effective state to the “lesser” of the group intended state or the application intended state**. However, there are factors that prevent the effective state from reaching the InSv state if that is the goal: like failures, which result in one of the faulty states; or being on the inactive side node, which causes the effective state to be Stby.

For example, if the group intended state is set by the administrator to offline (Offl), then all the applications are forced to go to the offline state regardless of their individual intended state setting. However, if the group state is set to ManB, then the application effective states can only be Offl or ManB. In the later case, an application that had been previously set to Offl (intended state) by the administrator would remain Offl even if the encompassing group was moved to the ManB state by the operator.

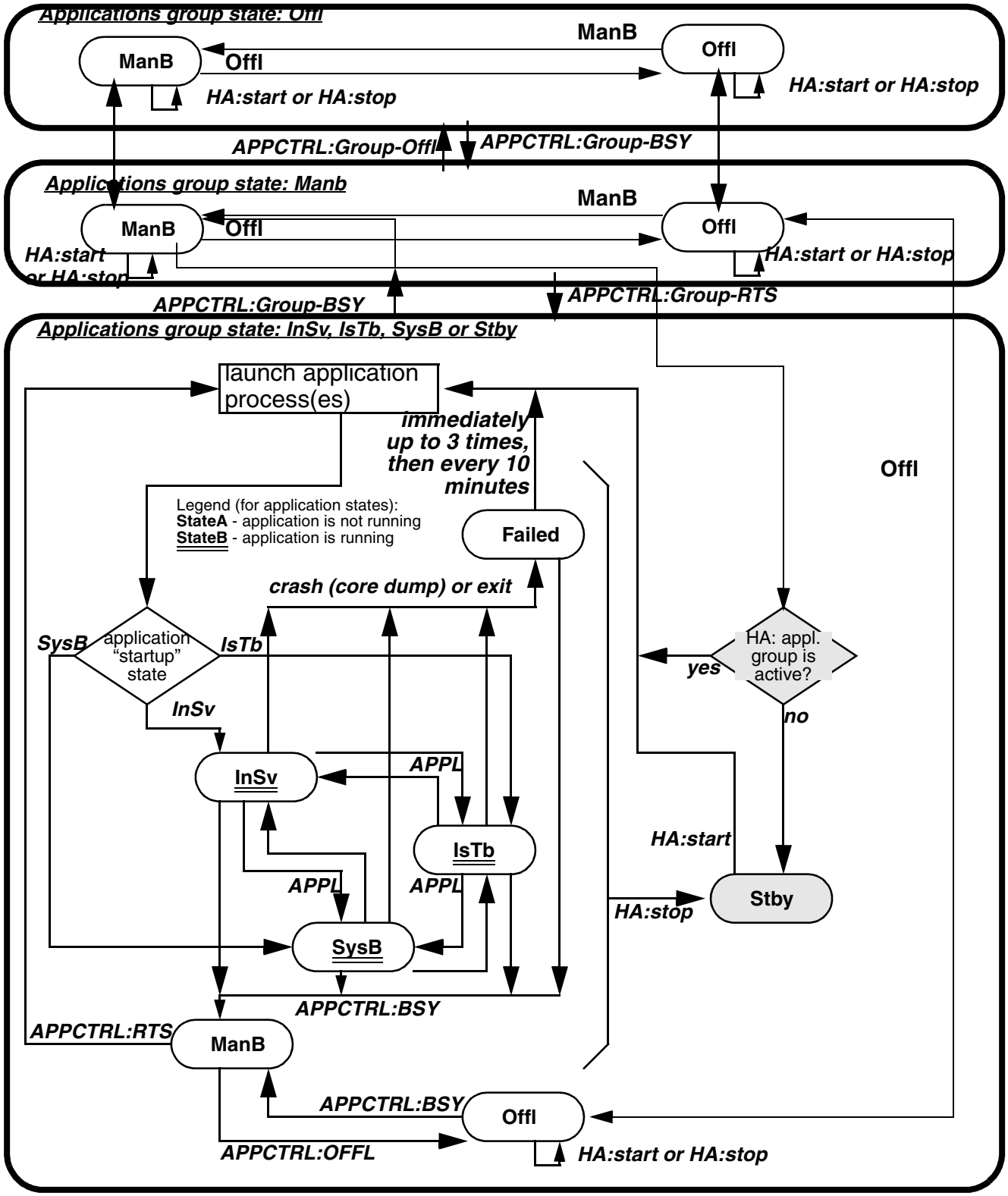
When the administrator issues a Ready to Service (RTS) operation on the group the applications are enabled to start, which ideally means they go to in service (InSv) state; unless they have been explicitly offlined. After the application process(es) is started, it will spontaneously move between the in

service (InSv), in service trouble (IsTb) and system busy (SysB) based on status reports issued by the running application. These states describe whether the application is respectively fully operational, partially operational, severely degraded. If the application fails to start and exits, then it is put in the failed state. SAM will attempt to restart applications in the failed state on a regular basis.

The CBM application state paradigm follows the exact same behavior that prevails on the SDM fault tolerant product from which it is derived. The major difference is the introduction of the standby state (Stby), which is required to support the High Availability (HA) configuration. The additions to the state machine flowchart introduced by the HA paradigm are depicted in gray in the figure. In essence, if an application is administratively enabled to start, but cannot do so on the local system because the HA framework has determined that the local system is inactive, then the application will be put in the Stby state. As soon as the HA framework invokes the start script, then all the applications that were in Stby state, will be launched and will go to one of the active states.

It is worthwhile to note that if an application is put by the administrator to the manual busy (ManB) state via a busy (BSY) command; the application would not remain in ManB state after a HA switch over. This is consistent with the behavior of the SDM product where an application that was in ManB state would be returned to service in the event of a system reboot. The rational for this behavior is that the ManB state is a temporary state, only used to do punctual maintenance. If an application needs to be permanently disabled, then it needs to be put in the Offl state.

Figure 2 Application effective states in the HA CBM product



26.2.3 User interfaces

The ‘appctrl’ command that is used by an administrator to change the group and application states is documented in the “User Interface Manager for CBM” feature A00002822.

The “User Interface Manager for CBM” will also group and application management and viewing from the APPL level of the cbmmtc page mode interactive tool.

Commands will also be available to force an HA switch over in order to perform maintenance on a CBM node. These commands are described in the Succession (SSPFS) platform documentation, they do not interface directly into SAM.

26.3 Hardware Requirements or Dependencies

As defined by SSPFS platform documentation

26.4 Software Requirements or Dependencies

SSPFS platform

CBM Fault management (A00002757)

26.5 Limitations and restrictions

In the initial release the software will only support:

- Two nodes per CBM cluster
- One group, the “active side applications” group
- All applications must be contained in the above group; thus, can only run on the active system.

26.6 Interactions

26.7 Applicable customer facing sections

Fault Management

Logs	__N/A_
Alarms	__N/A_

Configuration

Data Schema	__N/A_
User Interface	___1__
Element Management	__N/A_

Security __N/A_

Service Order __N/A_

Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

Note 1: This feature provides new user commands, these are documented in the User Interface section of the “User Interface Manager for CBM”, feature number A00002822.

26.8 Glossary

Term	Description
New term	Definition

27: Functional Description (FN): A00002186

27.1 Feature name

A00002186: IOM DDU Capacity Enhancement

27.2 Description

For more information, please refer to TURKPFN in FMDOC library.

27.2.1 Introduction

In 1999, Nortel committed to Netas to deliver sufficient storage for their switches for 25M billing records.

The feature patch was implemented for SN04/CSP17, and this is the source implementation of the enhanced functionality. The FN for the original feature patch can be found in FMDOC library as TURKPFN.

The IOM DDU disk capacity is currently limited to 1G. This feature provides increase in the capacity to 4G by utilizing the additional capacity supported by the new IOM load, IOMEXXXX.

27.2.2 Functional Overview

This feature increases the IOM DDU capacity from 1G to 4G. The maximum number of volumes per DDU increases from 32 to 63. The maximum volume size remains unchanged at 65,536 KBytes. By allocating 63 volumes at maximum volume size, the entire 4G can be used.

There are no HMI changes introduced in this feature. All the maintenance tools, such as DISKDBG, DSKALLOC, and DSKUT will continue to function with no visible changes to their interface.

27.2.3 Soc BASE0015

The ability to use the additional disk capacity is controlled by SOC BASE0015. The status of this SOC must be set to YES before the additional capacity is visible. If the status is set to IDLE after additional volumes have been allocated, further volume allocation maintenance may not be possible, however all volumes and files will continue to be accessible.

27.3 Hardware Requirements or Dependencies

- The capacity enhancement is applicable only to the IOM DDU

- The IOM disk drive, NTFX32BA must be Release 7 or later

27.4 Software Requirements or Dependencies

- SOC BASE0015 needs to be activated for this functionality.
- The IOM load with version IOMEXXXX must be used in conjuction with this feature

27.5 Limitations and restrictions

- Once the IOM has been upgraded to the new load, do not revert back to the old load, as this may cause the DDU to no longer function correctly and potentially require the disk to be reformatted.
- The IOM disk drive, NTFX32BA must be Release 7 or later.
- Setting the SOC BASE0015 to IDLE may prevent further volume allocation maintenance, however the volumes which have already been allocated will continue to be accessible.

27.6 Interactions

None

27.7 Applicable customer facing sections

Fault Management

Logs	_N/A__
Alarms	_N/A__

Configuration

Data Schema	_N/A__
User Interface	_N/A__
Element Management	_N/A__
Security	_N/A__
Service Order	_N/A__
Office Parameters	_N/A__

Accounting (includes AMA billing)	_N/A__
Performance (includes operational measurements)	_N/A__

27.8 Glossary

DDU	Disk Drive Unit
DIRP	Device Independent Recording Package
HMI	Human Machine Interface
IOM	Input/Output Module
MOP	Method of Procedure

28: Functional Description (FN): A00002196

28.1 Feature name

Enhanced Do Not Disturb

28.2 Description

28.2.1 Background

Do Not Disturb (DND) is an existing DMS feature that makes an MDC station appear busy to incoming calls when the station is idle. DND is scheduled via table DNDSCHED and allows pre-programmed times to be datafilled which specify a begin time to activate DND and an end time to deactivate it. DND is not currently supported on RES lines but will be as a result of this activity.

Selective Call Acceptance (SCA) feature allows a subscriber to selectively accept calls arriving from a limited set of previously identified directory numbers.

There is currently no mechanism to allow a subscriber to create a list of callers that would by-pass DND when it is active. This activity will change the current interaction between SCA and DND so that a subscriber can selectively accept calls while DND is active.

28.2.2 Enhanced Do Not Disturb

Currently there is no combination of features that allows a subscriber to activate a Do Not Disturb feature at a predetermined time each day, for example from 6 p.m. until 7 p.m. each evening (dinner hour), and at the same time maintain a list of DNs that are optionally allowed to bypass DND when it is active.

The Enhanced DND feature will be available to RES & MDC lines and provides the following capabilities:

- Via Table DNDSCHED, calls can be blocked at a predetermined time period each day. Table DNDSCHED allows up to 63 different time periods to be datafilled per customer group.
- A subscriber can dial DND feature access codes to activate or deactivate Do Not Disturb. The DNDACT feature access code will activate Do Not Disturb and the DNDDEACT feature access code will deactivate Do Not Disturb.

- Table DNDSCHED begin and end times will interact with DNDACT and DNDDEACT feature access codes. If a subscriber's line has Do Not Disturb active as a result of a begin time in table DNDSCHED, the subscriber can dial the DNDDEACT feature access code to deactivate DND. Likewise, an end-time deactivation of DND via Table DNDSCHED will turn off Do Not Disturb, whether it was activated via the DND feature access code or a begin time in table DNDSCHED.
- SCA will be enhanced to allow callers on the SCA screening list to bypass DND when it is active. This functionality will be controlled by the new parameter DND_ONLY, which will be visible when provisioning SCA.
- The new field DND_ONLY will default to N during provisioning and is visible during NEW, ADO (Add Option), and CHF (Change Feature) commands.
- Enhanced DND is defined as a line with both the DND and SCA options with SCA field DND_ONLY = Y.
- When Enhanced DND is active (DND and SCA with DND_ONLY=Y are both active), callers not on the SCA screening list will be routed to SCA treatment while callers on the SCA screening list will bypass DND and terminate to the line.
- If DND is active and SCA with DND_ONLY=Y is inactive, then all callers receive DND treatment as defined by Tables DNDSCHED and IBNTREAT.
- If DND is inactive and SCA is active (DND_ONLY=Y) then SCA screening will not be attempted on any termination. With DND_ONLY = Y, SCA screening is only done when DND is active. Under this condition, no SCA OMs will be pegged.
- Enhanced Do Not Disturb will be controlled by SOC RES00102.

28.2.3 New Activation Code for Table IBNXLA

Current implementation of DND does not allow a MDC or RES line to mark its DN busy by dialing an access code that interworks with scheduled Do Not Disturb times. This will be changed by this activity so that an access code can be datafilled in Table IBNXLA that MDC or RES lines can dial to activate and deactivate DND and that interworks with Table DNDSCHED.

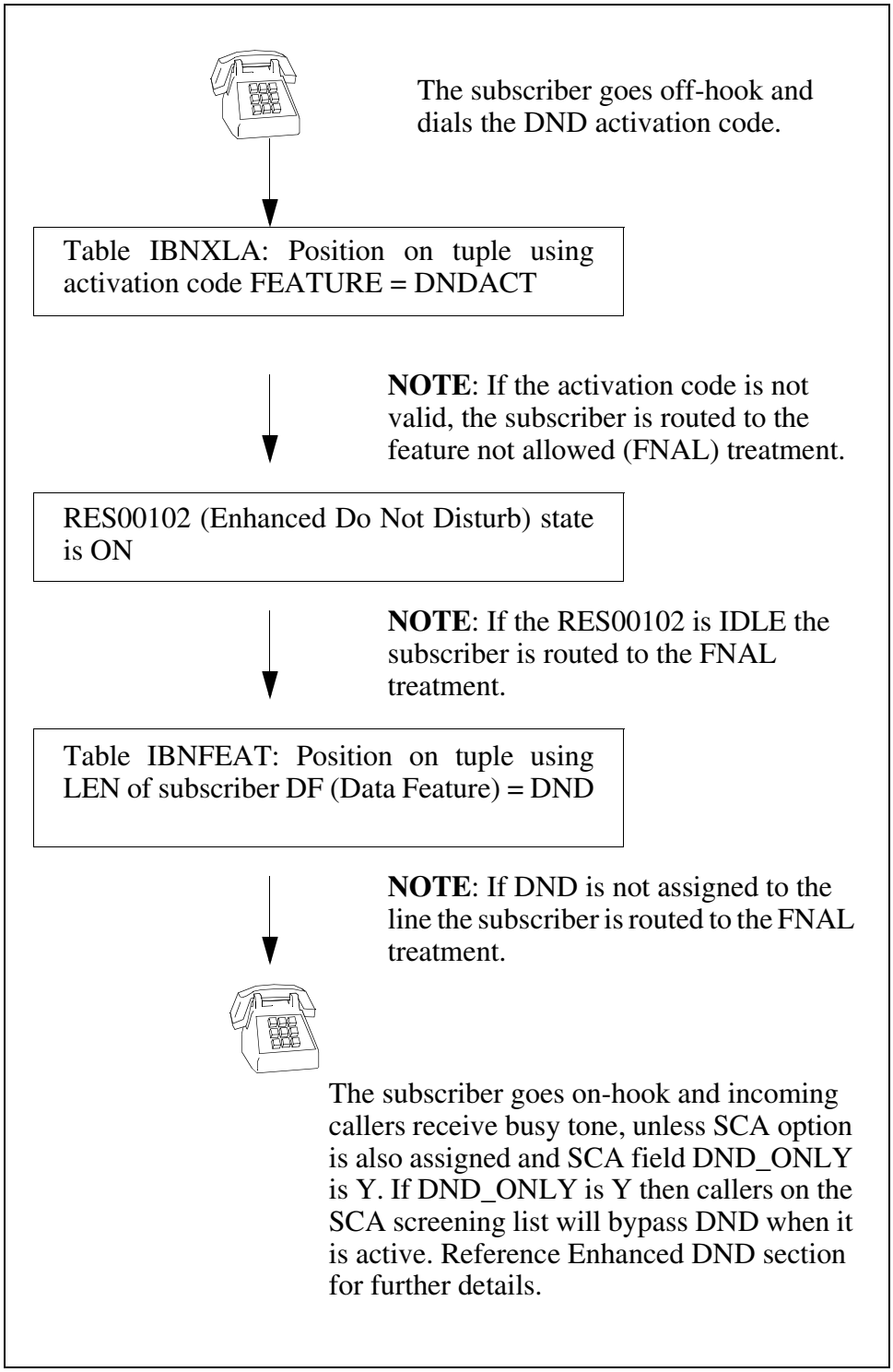
If DND is active on a line as a result of a begin time in table DNDSCHED it is currently not possible to deactivate it by dialling an access code. This activity will enhance DND so a Table DNDSCHED activation of DND can be deactivated by MDC and RES lines by dialing the DND deactivation access code.

The DND Activation and Deactivation access codes will be available when the TRSEL (TRanslation SELector) is set to FEAT in Table IBNXLA. The new

Features added are DNDACT (DND Activate) and DNDDEACT (DND Deactivate).

A Table DNDSCHED activation of DND will create an entry in Table DNDMSB with STATUS set to DNDGA. DNDACT and DNDDEACT will interwork with Table DNDSCHED, therefore a subscriber who dials DNDACT to activate DND will also create an entry in Table DNDMSB of DNDGA.

Figure 1 DND Activation



Refer to the configuration section (section optcn) for further details.

28.2.4 Selective Call Acceptance

28.2.4.1 Background

Currently, the SCA feature allows a subscriber to selectively accept calls arriving from a limited set of previously identified directory numbers.

In its current implementation SCA will not override DND when DND is active. If DND and SCA are active on a subscriber's line, callers on the SCA list will not terminate but will receive busy treatment due to DND. With this activity the interaction between DND & SCA will be modified when the new field DND_ONLY is Y so that callers on the SCA list can bypass DND when DND is active. If DND_ONLY is N then existing behavior remains unchanged.

28.2.4.2 Enhancement

The SCA enhancement being provided by this activity will change the conditions under which SCA screening can be applied so that SCA screening is only considered if DND is active. This functionality will be provided by a new field DND_ONLY (Y/N) that will be included at SCA servord provisioning. Current SCA subscribers will have the new field DND_ONLY initialized to FALSE over an ONP to preserve existing functionality. Refer to the configuration section (section optcn) for further details.

When DND is active and SCA is active with the DND_ONLY field set to Y on a subscriber's line then only callers on the SCA list will be allowed to terminate to the line. All callers not on the SCA list will be routed to SCA treatment.

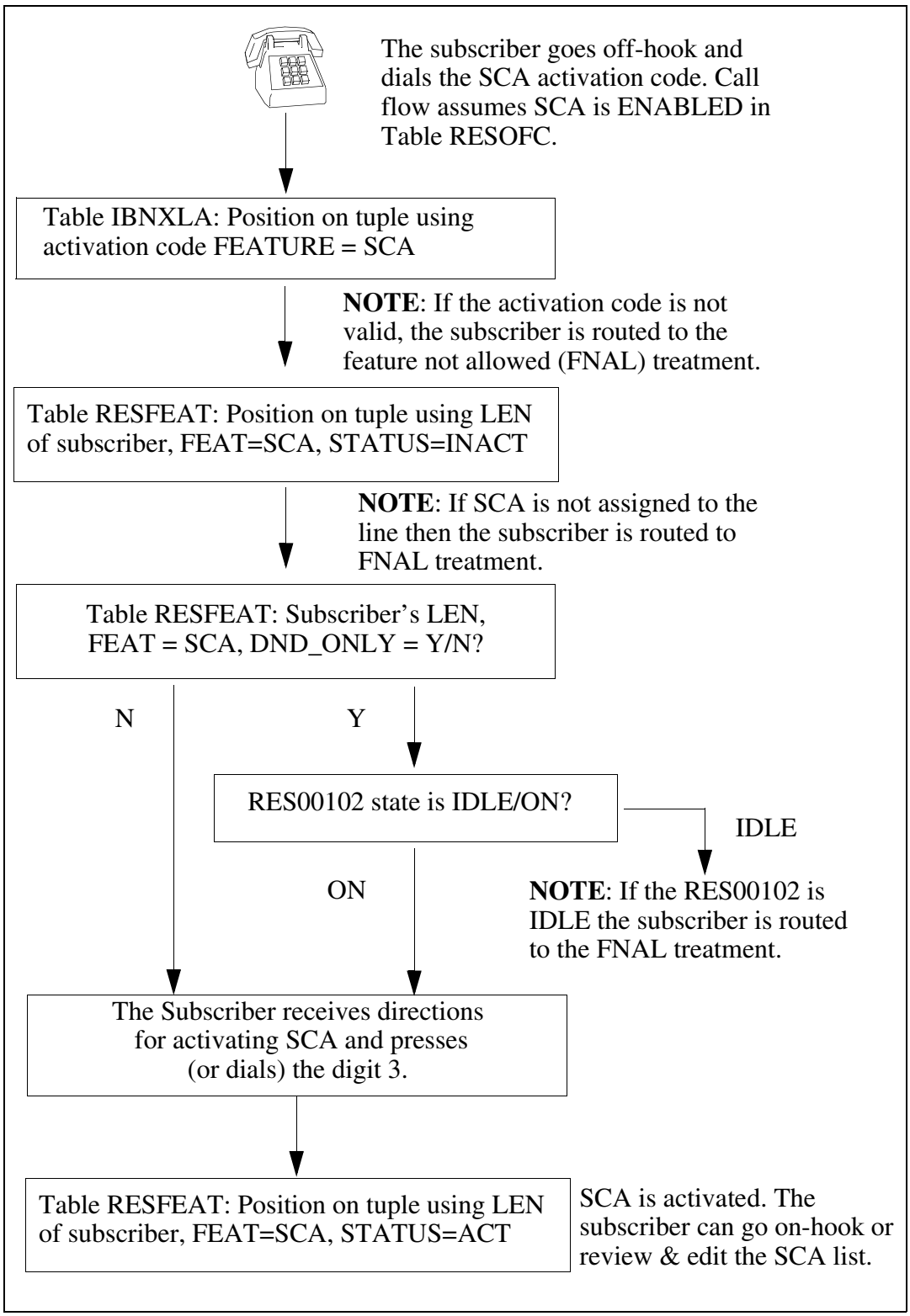
If DND is not active and the SCA field DND_ONLY is set to Y, then SCA screening will not apply to any incoming calls and all callers terminate to the line. The purpose of SCA screening when DND_ONLY is set to Y is to allow a list of callers to bypass the Do Not Disturb feature. If DND is not active then the SCA screening list will not apply to any incoming calls.

If DND_ONLY bool is set to N then the SCA feature (when ACTIVE) will screen callers to the subscriber's line regardless of whether DND is active or not. This preserves existing functionality.

An SCA subscriber with DND_ONLY set to Y can only dial the SCA access code when RES00102 is ON. If RES00102 is IDLE, then the SCA subscriber with DND_ONLY set to Y will receive FNAL (Feature Not Allowed) treatment if the SCA access code is dialed.

The following figure shows the SCA activation call flow:

Figure 2 SCA Activation



28.2.5 Description of Enhanced DND

The following paragraphs and figures show table datafill, servord and a description of call scenarios for Enhanced DND.

Prior to datafilling Table DNDSCHED, Table CUSTSTN should be datafilled to indicate the number of DND groups supported for the customer group. In the example shown, "63" represents the number of Do Not Disturb groups supported by the customer group. Its range is from 1 to 63.

Figure 3 Example datafill for Table CUSTSTN

```
TABLE: CUSTSTN

CUSTNAME OPTNAME OPTION
    RESGRP          DND  DND 63
```

The following figure shows example datafill for Table DNDSCHED.

Figure 4 Example datafill for Table DNDSCHED

```
TABLE: DNDSCHED

DNDSCKEY     DIVERSN          SCHED
RESGRP   1         1              $
RESGRP   2         1      (18 0 19 0)$
```

Using the above datafill as an example, if a RES subscriber who resides in the RESGRP customer group is assigned the DND option and DNDGRP is set to 2, then DND will be active each evening from 6 p.m. until 7 p.m. for this line. If DND is active and the call will not complete due to SCA overriding DND (SCA with DND_ONLY = Y), then the caller will be diverted to IBN treatment number 1 as defined by the DIVERSN field.

The following figure shows an example datafill for Table IBNTREAT. The DIVERSN field in table DNDSCHED should be datafilled in table IBNTREAT so callers who receive DND treatment are routed appropriately.

Figure 5 Example datafill for Table IBNTREAT

```
TABLE: IBNTREAT

CUSTGRP      IBNTRTMT          ITDATA
RESGRP              1    Y TRMT BUSY
```

NOTE: A default tuple should be datafilled in Table IBNTREAT with IBNTRTMT set to 0. This should be done for each customer group. An IBNTRTMT of 0 is used as the default treatment for any line with DND that does not have a corresponding entry in Table DNDSCHED to derive a diversion. An example for the RESGRP customer group is shown in Figure 6.

Figure 6 Example datafill for Table IBNTREAT

```
TABLE: IBNTREAT

CUSTGRP      IBNTRTMT          ITDATA
RESGRP              0     Y TRMT BUSY
```

Referring to Figures 4 & 5, a caller who calls a DND active RESGRP 2 line would be routed to BUSY treatment, provided SCA with DND_ONLY=Y was not active and either allowed the termination or routed the call to SCA treatment.

Figure 7 Example DND ADO with DNDGRP assigned as RESGRP 2

```
ADO $ 6210040
OPTION:
>DND
DNDGRP:
>2
```

If a subscriber in the RESGRP customer group does not want DND to become active at a preset time each day, then they can be assigned to RESGRP 1. This is done by assigning the RESGRP subscriber to DNDGRP 1 at servord time.

Figure 8 Example DND ADO with DNDGRP assigned as RESGRP 1

```
ADO $ 6210042
OPTION:
>DND
DNDGRP:
>1
```

The following ADO example assigns SCA with DND_ONLY set to Y

Figure 9 Example SCA ADO with DND_ONLY = Y

```
ADO $ 6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>
STATUS:
>ACT
DNS:
>6136213500
VBCOUNT:
>7
DNS:
>$
DND_ONLY: N
>Y
```

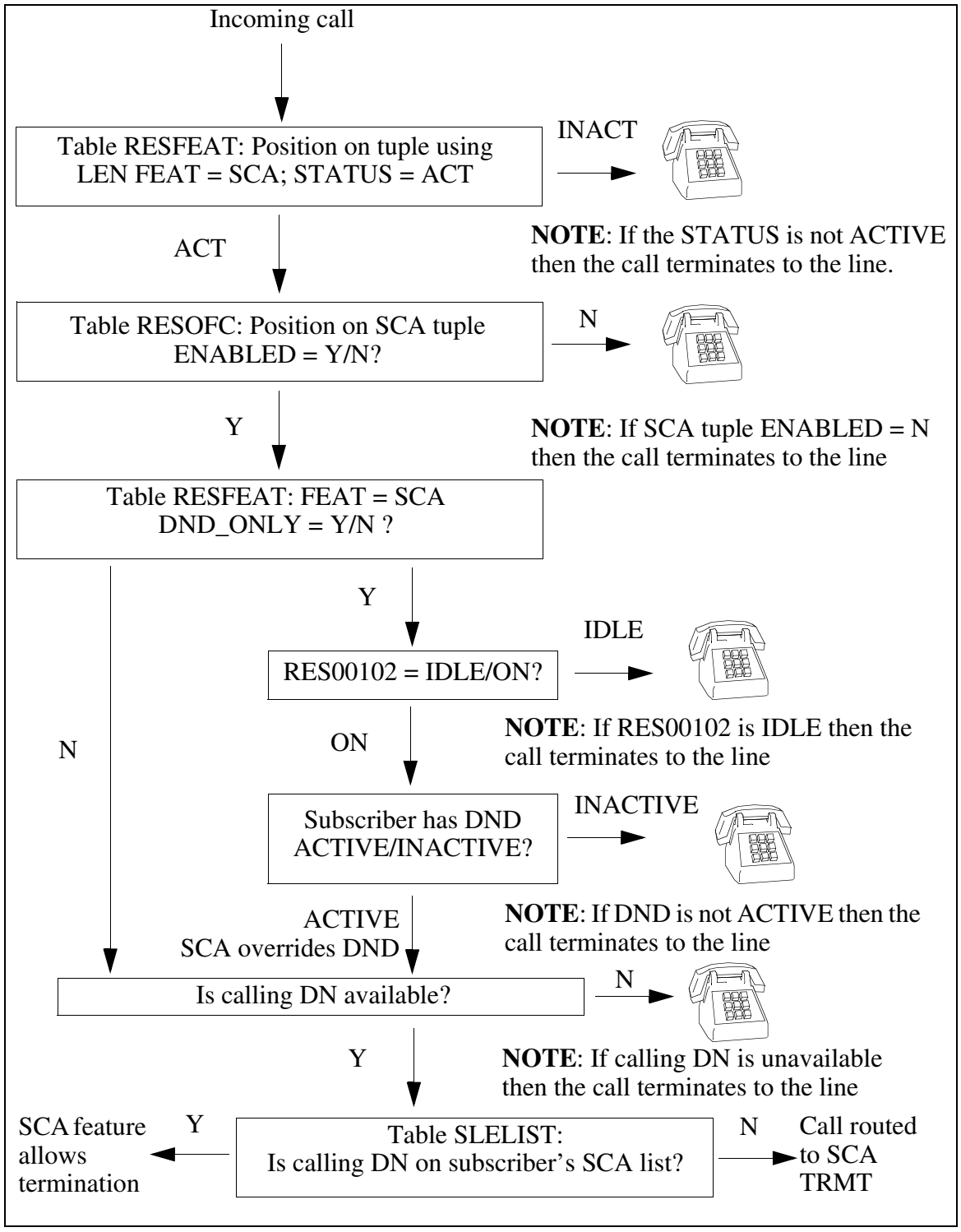
As described in the section 2.2.2, if DND is active on a subscriber's line and it also has subscribed to SCA with DND_ONLY set to "Y" and SCA is active, then callers on the SCA screening list will terminate to a line with DND active, whether DND was activated via Table DNDSCHED or by dialing the DNDACT (DND Activate) access code from Table IBNXLA.

If DND is assigned but not active on a line, and the line has SCA with DND_ONLY bool set to "Y" then SCA screening will not apply to any call termination attempt. Lines with SCA and the DND_Only bool set Y will only apply SCA screening when DND is active.

If the DND subscriber wishes to block all callers when DND is active, then the SCA feature enhancement can be turned off or not subscribed to, or DND_ONLY can be set to "N."

The following diagram shows the Enhanced DND call flow:

Figure 10 Enhanced DND Call Flow



Refer to Table 3 in section 2.6 for a description of DND & SCA interactions provided by this activity.

Refer to Table 4 in section 2.6 for a description of DND and SCA interactions as they existed prior to this activity. This funtionality will be preserved by this activity by setting the SCA DND_ONLY bool to “N” at provisioning time.

No new OMs or billing records are created as a result of this activity. AMA record generation will be not be impacted by Enhanced DND functionality.

28.2.6 Software Optionality Control

Enhanced DND functionality provided by this activity will be under SOC control. The SOC code is RES00102. If SOC is ON then the functionality will be provided:

- MDC & RES subscribers can dial the DNDACT and DNDDEACT access codes.
- MDC & RES SCA subscribers with DND_ONLY set to Y can dial the SCA access code.
- MDC & RES subscribers with DND active and SCA active with DND_ONLY bool set to Y receive Enhanced DND functionality.

If SOC is IDLE then the enhancements just described will not be provided, although datafill will be allowed.

Refer to the Configuration section (optcn) for further details.

If RES00102 is IDLE and the SCA option is added to a line with DND_ONLY set to Y, then DND_ONLY functionality will not be provided. In this scenario a message will be output to the servord user stating that functionality will not be provided until RES00102 is turned ON. An example is provided below:

Figure 11 Assigning DND_ONLY = Y when RES00102 is IDLE

```
>ADO $ 7234500
OPTION:
>SCA
BILLING_OPTION: NOAMA
>
STATUS:
>ACT
DNS:
>$
DND_ONLY: N
>Y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 10 9 PM 7234500 ( SCA NOAMA INACT $ Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
DND_ONLY functionality requires RES00102 to be turned ON
```

28.2.7 QSL changes

Query Screening List (QSL) command will not change as a result of this activity, but the display for SCA out will be changed to reflect the status of the new field DND_ONLY. A new line titled “Do Not Disturb Only” will be displayed and will show the status of DND_ONLY field. Refer to the optcn section for details.

28.3 Hardware Requirements or Dependencies

None

28.4 Software Requirements or Dependencies

RES00035: Selective Call Acceptance

28.5 Limitations and restrictions

Enhanced DND is not available on a pay-per-use (PPU) basis.

Existing limitations and restrictions regarding DND will remain unchanged as a result of this activity.

Existing limitations and restrictions regarding SCA will remain unchanged as a result of this activity.

28.6 Interactions

With this activity there is a new interaction between DND and SCA. The following tables summarizes these interactions:

Note: Enhanced DND subscriber is defined as a subscriber with DND and SCA with DND_ONLY = Y assigned.

Table 1 DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=ON)

IF DND_ONLY = Y	THEN
DND Inactive SCA Inactive	All callers terminate to the Enhanced DND subscriber
DND Inactive SCA Active	All callers terminate to the Enhanced DND subscriber
DND Active SCA Active	Callers on SCA List terminate to the Enhanced DND subscriber Callers not on SCA List receive SCA treatment
DND Active SCA Inactive	No callers terminate to the Enhanced DND subscriber

Table 2 DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=IDLE)

IF DND_ONLY = Y	THEN
DND Inactive SCA Inactive	All callers terminate to the Enhanced DND subscriber
DND Inactive SCA Active	All callers terminate to the Enhanced DND subscriber
DND Active SCA Active	No callers terminate to the Enhanced DND subscriber
DND Active SCA Inactive	No callers terminate to the Enhanced DND subscriber

Table 3 DND & SCA (DND_ONLY = N) Provisioned (RES00102 SOC=IDLE or SOC=ON)

IF DND_ONLY = N	THEN
DND Inactive SCA Inactive	All callers terminate to DND/SCA subscriber
DND Inactive SCA Active	Callers on SCA List terminate to DND/SCA subscriber Callers not on SCA List receive SCA treatment
DND Active SCA Active	Callers on SCA List pass SCA screening but are denied termination by DND Callers not on SCA List receive SCA treatment
DND Active SCA Inactive	Callers denied termination by DND

Note: Inactive assumes that the option is assigned but inactive.

28.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

28.8 Glossary

Term	Description
DND	Do Not Disturb
QSL	Query Screen List
SCA	Selective Call Acceptance

29: Functional Description (FN): A00002251

29.1 Feature name

192M Shared Memory Extension

29.2 Description

This feature increases addressable memory by 192M for selected 10 shared memory card XA-Core systems. This functionality is built into certain loads such as GSM for CSP20. This feature cannot be deactivated.

The 192M feature only has an effect in systems with 10 shared memory cards. This feature is able to entend memory by eliminating triplex memory from the system.

The addressable memory of a 10 shared memory card system without this feature is 1728M and the addressable memory of a 10 card system with this feature is 1920M. The addressable memory of a system sets the maximum load size that a switch can accomodate. Addressable memory can be viewed using the xsmemlim CI. The xsmemlim CI outputs the addressable memory in kilobytes (to convert to megabytes divide by 1024).

Output of xsmemlim for a 10 card system without feature built-in load

```
>xsmemlim

Memory Limits Statistics



Total addressable memory: 1769472 Kbytes

Spare memory:             1146880 Kbytes

 ...

MEMLIM Alarm Status: no alarm

>
```

Therefore the addressable memory for this system is 1769472/1024 = 1728M.

Output of xsmemlim for a 10 card system with feature built-info load

```
>xsmemlim

Memory Limits Statistics


Total addressable memory: 1966080 Kbytes

Spare memory:             1343488 Kbytes

...

MEMLIM Alarm Status: no alarm
```

Therefore the addressable memory for this system is 1966080/1024 = 1920M.

Any configuration with less then 10 cards will behave exactly the same with or without the feature. If a load with the feature built-in is booted with less then 10 cards no change will be noticed until enough cards are provisioned.

29.3 Hardware Requirements or Dependencies

The only hardware requirement is that a system has 10 shared memory cards. This feature will not extend memory by 192M unless there are 10 shared memory cards.

Please Note: This document discusses this feature in the context of 384M shared memory cards (NTLX14CA). This feature is applicable to newer larger shared memory cards. With larger shared memory cards the addressable memory gained by eliminating triplex addresses would be more than 192M.

29.4 Software Requirements or Dependencies

There are no software requirements or dependances. The load that is delivered must have the feature built into it.

29.5 Limitations and restrictions

The feature cannot be deactivated.

29.6 Interactions

Not applicable.

29.7 Applicable customer facing sections

Fault Management

- Logs ___N/A___
- Alarms ___N/A___

Configuration

- Data Schema ___N/A___
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

30: Functional Description (FN): A00002281

30.1 Feature name

Table AMAPRT Expansion

30.2 Description

Table STDPRTCT, subtable AMAPRT is a table that allows customers to add AMA specific options that are triggered by translations. The present limit of 8191 tuples in table AMAPRT limits the customer's ability to assign AMA options based on translations. This feature will expand the maximum value of this table to allow for 32000 entries, thus allowing the customer to datafill many more AMA options.

30.3 Hardware Requirements or Dependencies

N/A

30.4 Software Requirements or Dependencies

N/A

30.5 Limitations and restrictions

N/A

30.6 Interactions

N/A

30.7 Applicable customer facing sections

Fault Management

- Logs ___
- Alarms ___

Configuration

- Data Schema __N/A_
- User Interface ___
- Element Management ___
- Security ___

Service Order ___

Office Parameters ___

Accounting (includes AMA billing) ___

Performance (includes operational measurements) ___

30.8 Glossary

Term	Description
New term	Definition

31: Functional Description (FN): A00002340

31.1 Feature name

Add Extension Registers for Billing OM's

31.2 Description

31.2.1 CDR Oms

Two new OM groups FCDRTM1E and FCDRTM2E will be provided for the overflows from the groups FCDRTMP1 and FCDRTMP2. One new group FCDRALG2 will provided for the overflow from the group FCDRALGR.

The OM groups FCDRTMP1 and FCDRTMP2 each contains 32 registers to peg the usage of up to 32 different CDR templates. The OM group FCDRALGR contains eight registers to count the method used to choose the CDR template. The maximum size of a register is 65535 or #FFFF. The maximum size is controlled by the OM sub-system. With the addition of an extension register, every rollover will be pegged This allows up to a maximum value of 4,294,901,760 before the extension register overflows. This value is calculated by (65535 * 65535) + 65535.

The OM subsystem limits the maximum registers per OM group at 32 so new OM extension groups must be defined for the FCDRTMP1 and RFCDRTMP2 groups.

The new extension functionality will be implemented under SOC control. This will allow for controlled customer implementation and also provide the ability to disable the new extension if required.

The following displays the current OM group FCDRTMP1 along with the new OM extension group FCDRTM1E. The group FCDRTMP2 will be expanded in the same fashion for templates 32-63 using the new group FCDRTM2E.

The FCDRALGR group will have its extension registers in the new group FCDRALG2 as shown below.

```
FCDRTMP1

CLASS: HOLDING
START:2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;
SLOWSAMPLES:          3 ; FASTSAMPLES:          30 ;

          TMPLT_0     TMPLT_1     TMPLT_2     TMPLT_3
          TMPLT_4     TMPLT_5     TMPLT_6     TMPLT_7
```

```
          TMPLT_8    TMPLT_9   TMPLT_10   TMPLT_11
         TMPLT_12   TMPLT_13   TMPLT_14   TMPLT_15
         TMPLT_16   TMPLT_17   TMPLT_18   TMPLT_19
         TMPLT_20   TMPLT_21   TMPLT_22   TMPLT_23
         TMPLT_24   TMPLT_25   TMPLT_26   TMPLT_27
         TMPLT_28   TMPLT_29   TMPLT_30   TMPLT_31

    0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0


FCDRTM1E

CLASS: HOLDING
START:2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;
SLOWSAMPLES:         3 ; FASTSAMPLES:         30 ;

          TMPLT_0    TMPLT_1    TMPLT_2    TMPLT_3
          TMPLT_4    TMPLT_5    TMPLT_6    TMPLT_7
          TMPLT_8    TMPLT_9   TMPLT_10   TMPLT_11
         TMPLT_12   TMPLT_13   TMPLT_14   TMPLT_15
         TMPLT_16   TMPLT_17   TMPLT_18   TMPLT_19
         TMPLT_20   TMPLT_21   TMPLT_22   TMPLT_23
         TMPLT_24   TMPLT_25   TMPLT_26   TMPLT_27
         TMPLT_28   TMPLT_29   TMPLT_30   TMPLT_31

    0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0


FCDRTMP2

CLASS: ACTIVE
START:2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;
SLOWSAMPLES:         5 ; FASTSAMPLES:         50 ;

         TMPLT_32   TMPLT_33   TMPLT_34   TMPLT_35
         TMPLT_36   TMPLT_37   TMPLT_38   TMPLT_39
         TMPLT_40   TMPLT_41   TMPLT_42   TMPLT_43
         TMPLT_44   TMPLT_45   TMPLT_46   TMPLT_47
         TMPLT_48   TMPLT_49   TMPLT_50   TMPLT_51
         TMPLT_52   TMPLT_53   TMPLT_54   TMPLT_55
         TMPLT_56   TMPLT_57   TMPLT_58   TMPLT_59
         TMPLT_60   TMPLT_61   TMPLT_62   TMPLT_63

    0
```

```
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0


FCDRTM2E

CLASS: ACTIVE
START:2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;
SLOWSAMPLES:         5 ; FASTSAMPLES:         50 ;

         TMPLT_32   TMPLT_33   TMPLT_34   TMPLT_35
         TMPLT_36   TMPLT_37   TMPLT_38   TMPLT_39
         TMPLT_40   TMPLT_41   TMPLT_42   TMPLT_43
         TMPLT_44   TMPLT_45   TMPLT_46   TMPLT_47
         TMPLT_48   TMPLT_49   TMPLT_50   TMPLT_51
         TMPLT_52   TMPLT_53   TMPLT_54   TMPLT_55
         TMPLT_56   TMPLT_57   TMPLT_58   TMPLT_59
         TMPLT_60   TMPLT_61   TMPLT_62   TMPLT_63

    0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0


FCDRALGR

CLASS: ACTIVE
START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;
SLOWSAMPLES:         1 ; FASTSAMPLES:          3 ;

         INTERNAL   CALLTYPE    SUBRNUM        TRK
             TCAP      FIXED    BESTFIT    RTEATTR

    0
                0          0          0          0
                0          0          0          0

FCDRALG2

CLASS: ACTIVE
START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;
SLOWSAMPLES:         1 ; FASTSAMPLES:          3 ;

         INTERNAL   CALLTYPE    SUBRNUM        TRK
             TCAP      FIXED    BESTFIT    RTEATTR

    0
                0          0          0          0
                0          0          0          0
```

31.3 Hardware Requirements or Dependencies

None.

31.4 Software Requirements or Dependencies

The capabilities will be under SOC control.

This activity only impacts offices using the UCS software layer.

31.5 Limitations and restrictions

None

31.6 Interactions

The existing OM groups will not be changed. The new groups will contain only new registers. The new OM groups are:

- FCDRTM1E
- FCDRTM2E
- FCDRALG2

31.7 Applicable customer facing sections

Fault Management

Logs	__N/A____
Alarms	__N/A____

Configuration

Data Schema	__N/A____
User Interface	__N/A____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) ___X___

31.8 Glossary

Term	Description

32: Functional Description (FN): A00002380

32.1 Feature name

MG9K ABI ESA

Emergency Stand Alone (ESA) service for lines off the Access Bridge Interface (ABI) cards of an MG9K Media Gateway 9000 (MG9K).

32.2 Description

This activity provides the ability for the Succession Call Server 2000 (CS2000) to support Emergency Stand Alone calling on the following DMS-100 Legacy Extended Peripheral Modules (XPM) subtending a Media Gateway 9000 (MG9K):

- LGC, LGCI
- LTC, LTCI
- SMA2

32.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies for this feature.

32.4 Software Requirements or Dependencies

This ESA activity on the MG9000 is dependent upon the following activity for successful completion.

A00003567: MG 9000 Element Mgr Support for ABI ESA

The primary function of this component is to pull ESA data from the Core, organize this information in the EM in a meaningful way for the MG9K, and put it into the ESA subsystem on the ABI in a usable format.

The following activities support ITP ESA. ABI ESA and ITP ESA have a common design and the ITP documents should be considered as preliminary reading. The ABI ESA documentation supersedes the ITP ESA documentation.

A00002020: ESA Translation Download [ITP - CM]

A00002019: ESA EM Enhancements [ITP - MG9000 EM]

A00001982: ESA Enhancements [ITP - MG9000]

The following activities are related to this activity.

A00003486: Gateway Location Information [CM]

A00003693: ESA for ABI ON SMS

32.5 Limitations and restrictions

32.5.1 ABI VMG Naming convention

In order for the ESA data download to function properly, the VMG name for the ABI must contain the XPM node number of the XPM directly connected to the ABI pair. The typical name of an ABI is “EXPM168” where 168 is the node number of the ABI subtending XPM. The node number of the XPM can be obtained by posting it and the PM MAP level in the CM and using the querypm command. If the node number in the VMG name does not match the node number of the XPM, either no ESA data or incorrect ESA data will be downloaded to the ABI card.

32.5.2 Entering ESA

- Only calls that are in an active state (i.e. talking state) will survive warm entry into ESA mode.
- Calls that are intraswitched on RLCMs, OPMs, or OPACs can survive warm entry (not just network switched calls).
- Calls that won’t survive entry into ESA mode may be released over a period of time (not immediately).
- Only an Active Call on the PDN key of a P-phone is capable of surviving warm entry.
- Active Calls on non-PDN keys of a P-phone are dropped.
- The message waiting lamp is not extinguished during warm entry should an analog or P-phone terminal be so equipped.
- The lamp associated with the members of an SCA MADN group is not extinguished during warm entry should one member be in an active state (i.e. talking state).

32.5.3 During ESA

- Coin loop-start lines will be supported in ESA; however, ESA will supervise coin return upon call completion. The MG9K only supports CDF (Coin Dial First) and Coinless Coin phones.
- ESA between physical MG9000 master shelves (separate MGs) is not allowed.
- All members of a MADN group will be allowed to originate calls.

- Dialing a MADN member will result in a termination to the first idle MADN member and only this member. Not all MADN members will receive ringing.
- ESA is unavailable when DCC packs are out of service.
- ESA call processing is only supported between VMGs (ABIs or ITPs) currently in ESA on the same MG9000. Partial ESA (one VMG in ESA and another VMG not in ESA but on the same MG9000--commonly called *one up, one down*) is not supported.
- Emergency service (i.e. 911) translations are supported, but not emergency service features.
- No maintenance actions (whether from LCI, EMs, card-pulls, etc.) are recommended while in an ESA operational mode.
- Hunting is linear to those DNs physically residing on a VMG. Hunting on a hunt group that is divided across several VMGs does not guarantee true linear hunting for the entire group.
- Dialing directly to a DNH hunt member will cause a termination to that member. If the member is not available, hunting will be done only on the group members local to that VMG.
- If the "H" selector is used in table ESAPXLA then a call dialed with those digits will hunt through all hunt group members on the VMG. The Sequence Number, which normally causes hunting to start from a specific member, is not supported.
- The ESAPXLA table in the Core should be provisioned with the emergency service numbers (i.e. 911) needed while in ESA. Each VMG (as represented by an ABI XPM or LGRP) must be provided with its own emergency service line as well as table ESAPXLA translations terminating to the DN of that line.
- Basic call processing is supported on P-phone lines in ESA only for the primary DN.
- The PDN, Hold, RLS and digit keys are the only recognized keys supported for P-phones while in ESA.
- Hand-set and hands-free operation is supported for P-phones in ESA.
- Basic call processing during ESA is supported for analog and P-phone lines on RLCMs, OPMs, and OPACs. Intraswitching is not supported.

32.5.4 Exiting ESA

- Warm exit from ESA is not supported. Any call attempts or stable calls that coincide with exit from ESA will be torn down by the controlling MGC.

- Service codes are only supported on a limited basis for ESA. Emergency service 911 calls (or any other call using a service code) will not be preserved over ESA exit.

32.6 Interactions

While ABI ESA will be supported for the Legacy XPMs noted in section 32.2, it will not supersede Legacy ESA for Remote Switching Center (RSC) XPMs. RSCs that subtend an ABI XPM will enter existing Legacy ESA when an isolation occurs. They will not be controlled by ABI ESA. All existing RSC ESA functionality will remain intact.

32.7 Applicable customer facing sections

Fault Management

Logs _ x ___

Alarms _____

Configuration

Data Schema _ x ___

User Interface _ x ___

Element Management _____

Security _____

Service Order _____

Office Parameters _ x ___

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

32.8 Glossary

Term	Description
ABI	Access Bridging Interface
AUL	Automatic Lines
CM	Computing Module
DCC	Data Controller Card

Term	Description
DLH	Distributed Line Hunt
DN	Directory Number
DNH	Directory Number Hunt
EM	Element Manager
ESA	Emergency Stand Alone
GW	Gateway
GWC	Gateway Controller
IBN	Integrated Business Network
ITP	Integrated Telephony Processor
LCI	Local Craft Interface
LGC	Line Group Controller
LGRP	Logical Group
LTC	Line/Trunk Controller
MADN	Multiple Appearance Directory Number
MG	Media Gateway
MG9K	Media Gateway 9000
MGC	Media Gateway Controller
MLH	Multi-line Hunt
OPAC	Outside Plant Access Cabinet
OPM	Outside Plant Module
PDN	Primary Directory Number
POTS	Plain Old Telephone Service
RLCM	Remote Line Concentrating Module
RLS	Release Key
RSC	Remote Switching Center
SCA	Single Call Arrangement
SMA2	Subscriber-Carrier Module Access 2
VMG	Virtual Media Gateway
XPM	Extended Peripheral Module

33: Functional Description (FN): A00002431

33.1 Feature name

A00002431 - LX82BA CAPACITY DELIVERY

33.2 Description

This activity provides a mechanism for NORTEL to sell incremental call processing capacity for the NTLX82BA CEM card to its DMSCP SPM customers. The various levels of capacities for DMSCP class of SPMs are

1. Standard capacity - Call processing capacity equal to that of the NTLX82AA CEM card.
2. Enhanced capacity - Call processing capacity approximately equal to that of 2 times that of the NTLX82AA.
3. Premium capacity - Call processing capacity approximately equal to that of 3 times that of the NTLX82AA.

For Non-DMSCP class of SPMs, only two levels of capacities, Standard and Premium are provided based on the CEM PEC (NTLX82BA) that are datafilled in table MNCKTPAK. If both the CEMs are datafilled with NTLX82BA PEC, then the capacity is Premium else the capacity is Standard.

Currently, NTLX82BA CEMs running CST and CEM loads (DMSCP SPM) have their CALLP capacity reduced to that of the NTLX82AA whereas NTLX82BA CEMs running IWS (IW SPM) or MG4 (MG4K SPM) load have their CALLP capacity equivalent to that of NTLX82BA.

33.2.1 DMSCP class of SPMs:

This activity provides the ability to control the call processing capacity at the node level for DMSCP class of SPMs provisioned with NTLX82BA cards, using core SOC options. The customer can provision the desired capacity in table MNNODE if appropriate SOC keys are available.

The various functionalities provided as part of this activity are :

- Two usage SOCs, one for Enhanced and the other for Premium capacity.
- Table control changes in table MNNODE and table MNCKTPAK.

- New CI tool to display the capacity provisioned on the SPMs present in the office

33.2.1.1 Two Usage SOCs to provide Enhanced and Premium Capacity

Two new USAGE SOCs are created under the existing SPMS group for DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity and the SOC option SPMS0028 corresponds to the SPMs with Premium capacity. When the SOC keys are not available, the limit and the usage are zero and no DMSCP class of SPMs are capable of running at Enhanced or Premium capacity. Refer Figure 1 for the format of the two SOCs. Both the SOC options have hard usage limit. RTU is 'Y' for usage limit >0 and RTU is 'N' for usage limit = 0. For each value of the hard limit a separate SOC key is available for the customer. The threshold value for these SOC options are set to 100%.

The hard limit value of SPMS0020 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Enhanced capacity and the hard limit value of SPMS0028 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Premium capacity.

The value of the USAGE of SPMS0020 and SPMS0028 denotes the number of DMSCP class of SPMs currently running with the Enhanced and Premium capacity respectively from Core's perspective.

Please refer to section 13.7 of Configuration Document for more details on the Usage SOCs.

Figure 1 SPMS group options as listed in SOC framework

```
>select option SPMS0020 verbose

GROUP:SPMS
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
SPMS0020  Enhanced Call cap      Y     -       0       0      1SM  03/06/13
          replaces options:      NONE
          threshold:     100%    high water mark:       0

          FEATURE   STATE  USAGE     UNITS
          -------   -----  -----     -----
          00002431      -  0            1SM
             NAME:  SPMS Enhanced Call cap

>select option SPMS0028 verbose

GROUP:SPMS
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
SPMS0028  Premium Call cap       Y     -       0       0      1SM  03/06/13
          replaces options:      NONE
          threshold:     100%    high water mark:       0

          FEATURE   STATE  USAGE     UNITS
          -------   -----  -----     -----
          00002432      -  0            1SM
             NAME:  SPMS Premium Call cap
```

Note: SOC option SPMS0028 uses the feature id 00002432.

33.2.1.2 Table control support to provision the desired capacity in table MNNODE

For DMSCP class of SPMs, table control changes are made to provision the desired capacity per node in table MNNODE. A new field ‘capindx’ is added in table MNNODE, only for DMSCP class of SPMs to provision this capacity. This new field can take the values ‘Standard’, ‘Enhanced’ or ‘Premium’, ‘Standard’ being the default value.

During an ONP from an earlier release where the capindx field is not present to a release where the capindx field is introduced in table MNNODE, this field is set to ‘Standard’. For using ‘Enhanced’ or ‘Premium’ values during tuple addition, the respective SOC options must have its RTU set to Y and Usage count must be less than its Limit. Also for using ‘Enhanced’ capacity, number of DMSCP SPMs provisioned with Enhanced capacity must be less than the limit of SPMS0020 SOC option and for using ‘Premium’ capacity, number of DMSCP SPMs provisioned with Premium capacity must be less than the limit of SPMS0028 SOC option.

SOC 504 is an existing log that gets generated when the RTU is set for any SOC option.

While changing the capindx field to ‘Enhanced’ or ‘Premium’ values, the PEC codes of the CEM units provisioned in table MNCKTPAK for this node are also verified for NTLX82BA, in addition to the SOC check. If all the check passes, the appropriate SOC usage value is incremented. For capindx field changes from ‘Enhanced’ or ‘Premium’ values to ‘Standard’, appropriate SOC usage counts are decremented only if both the CEM tuples are present in table MNCKTPAK. Tuple change without any change to the ‘capindx’ field is not validated. For tuple deletion, there are no restrictions enforced on this field.

In table MNCKTPAK, the CEM tuples of DMSCP variant of SPM are allowed to be provisioned only with the PECs - NTLX82AA, NTLX82AB and NTLX82BA. The provisioning of the PEC is dependent on the capindx field present in table MNNODE. Incase the capindx in table MNNODE is ‘Standard’, the PEC shall be allowed to be datafilled as NTLX82AA, NTLX82AB or NTLX82BA. In case of ‘Enhanced’ or ‘Premium’ capindx, the PEC must be datafilled as NTLX82BA.

The provisioned capacity in table MNNODE, is downloaded to the local using DDM framework. Local throttles the callp capacity based on the capacity index downloaded.

Please refer to section 13.5 of Configuration Document for more details on the error, warning and success messages introduced by this activity during table control operations in table MNNODE and table MNCKTPAK.

33.2.1.3 CI tool to display capacity information

A new CI tool, SPMCPCAP, is introduced to display the capacity information of SPM. This tool enables to list the SPM and their capacities based on the variant type or list the SPMs based on the capacities. There is also a provision to find out capacity for a given SPM number. Remarks field in this tool displays if CEM(s) are not datafilled in table MNCKTPAK.

Please refer to section 13.9 of Configuration Document for more details on the CI tool.

33.2.2 Non-DMSCP class of SPMs

Table MNNODE is not modified for Non-DMSCP class of SPMs. Also in table MNCKTPAK no validations for CEM PEC are introduced by this activity.

The CI tool, SPMCPCAP, is used to display the capacity information of Non-DMSCP class of SPMs also. Only two capacities, ‘Standard’ and ‘Premium’ are displayed in this case. For Non-DMSCP variants, MG4K and IW, the capacity information is derived based on the table MNCKTPAK datafill. If both the CEM are datafilled with NTLX82BA PEC cards, then capacity is set

to ‘Premium’. For other combinations of PEC cards, the capacity is set to ‘Standard’. Remarks field in this tool displays if CEM(s) are not datafilled in table MNCKTPAK.

Please refer to section 13.9 of Configuration Document for more details on the CI tool.

33.3 Hardware Requirements or Dependencies

None.

33.4 Software Requirements or Dependencies

None.

33.5 Limitations and restrictions

- SOC limit can be decremented to a value less than the usage count.
- The CI tool displays the callp capacities for SPMs from core’s perspective only. The capacity will be enforced if there is a PEC mismatch at the local.

33.6 Interactions

None.

33.7 Applicable customer facing sections

Fault Management	
Logs	__N/A__
Alarms	__N/A__
Configuration	
Data Schema	__X__
User Interface	__X__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

33.8 Glossary

Term	Description
CEM	Common Equipment Module
CI	Command Interpreter
PEC	Product Engineering Code
RTU	Right to Use
SOC	Software Optionality Control
SPM	Spectrum Peripheral Module

34: Functional Description (FN): A00002432

34.1 Feature name

ACT.A00002432 - Enhanced Spectrum Overload Operational Measurements (OMs) and Logs

34.2 Description

In the SP20 release, two new software optionality control (SOC) keys will be available that provides enhanced and premium call processing capability on the NTLX82BA CEM card. These keys are being added in feature A00002431. This capacity increase will allow the NTLX82BA card's performance to be approximately 2x that of an NTLX82AA card for 'enhanced' capability and approximately 3x for 'premium'. This additional capacity capability requires improvements to the SPM engineering information available to our customers.

This feature is also being used as a reference for the CAP00002 SOC key. That functionality is documented under feature ID A00002431.

This feature implements new operational measurements (OMs, or 'pegs') that will allow a craftsperson to monitor the performance of SPMs when the SPM is experiencing peak traffic levels that are in excess of the SPM engineering limit. It also augments an existing OM group, SPMACT, to include the capacity level.

There are two components that control the number of calls that can be handled by a given SPM. The first is the System Overload Control subsystem, which is controlled by the core and is dependent on core resources. The second is the SPM flow control system, which is controlled by the SPM and is influenced by SPM resource levels. The OMs and logs that are presented in this section will include data from both components.

34.3 Hardware requirements

None, the OMs and logs described in this section apply to all CEM platforms.

34.4 Limitations and restrictions

Core and local loads must both support the new functionality.

34.5 Interactions

The OMs and logs are driven by call processing on the SPM.

A new OM group will be added (SPMOVLD), and one new OM will be added to an existing group (SPMACT). For logs, a new log type (SPM399) will be introduced that indicates transitions in and out of the SPM overload conditions.

34.6 Logs (LG)

A new log will be introduced (SPM399) for flagging overload conditions in SPMs. This log is generated whenever an SPM enters/leaves an overload condition. The reason and the action for the craft are displayed in the log so that some action can be taken to rectify the condition. In addition, some diagnostic information for the designer is also printed in the log.

34.6.1 New/modified logs

Table 1 New or modified logs

Log name	Log number	NEW/MOD/ DELETED	System (SOS/UNIX)
SPM	399	New	SOS
SPM	313	Mod	SOS

The format/field-details and examples of the new log SPM 399 are given in detail in the ‘Fault Management’ section of this document.

34.7 Data schema (DS)

34.7.1 New/modified tables

Table MNNODE will be modified in a related feature:A00002431. Please refer to that design document for more details.

Table 2 New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)

34.8 Office parameters (OP)

34.8.1 New/modified office parameters

Table 3 New or modified commands

Parm table	Parameter name	NEW/CHANGED/ DELETED/RELOCATED

Not applicable.

34.9 Service orders (SO)

Not applicable.

34.10 Alarms (AL)

Not applicable.

34.10.1 New/modified directories

Table 4 New or modified directories

Directory name	NEW, CHANGED OR DELETED	New name (if renamed)	Target	RES/ NONRES

34.11 Command interface (CI)

34.11.1 New/modified commands

Table 5 New or modified commands

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/MAP level name	MENU/NON-MENU /HIDDEN

34.12 Operational measurements (OM)

34.12.1 New/modified OM groups

Table 6 New or modified OM groups

Group name (acronym)	Group name (expanded)	NEW, CHANGED or DELETED	Reason
SPMACT	Spectrum Activity	Changed	One register added
SPMOVLD	Spectrum Overload	New	

One new register will be added to the SPMACT OM group - CAPLEVEL, which indicates what the SPM's capacity index is. The capacity index is a numeric value, with possible values of 0, 1, or 2, corresponding to regular, enhanced and premium capacity, respectively.

The new SPMOVLD group will have 18 OM registers that give metrics on the SPM flow control system and the system overload control component. All OM registers that apply to the system overload control component start with an 'S', all others apply to the flow control system:

Table 1

Flow Control Peg	SOC Peg	Description
OVLDNUM	SOVLDNUM	Number of times the system entered overload. For SOC (system overload control), this means the CM is in beyond_capacity state.
OVLDPNUM	not applicable	Number of times the SPM entered 'overload pending'.
OVLDUSG	SOVLDUSG	For Flow control, OVLDUSG represents the number of seconds the system was in overload. For SOC, SOVLDUSG represents the number of messages that were processed by SOC while the CM was in a beyond_capacity state.
OVLDPUSG	not applicable	Number of seconds the SPM was in 'overload pending'.
CLSDLYD	SCLSDLYD	The number of calls delayed by the two systems. When flow control and SOC are active, this will be equal to the number of new originations.
CLSDND CLSPTQ	SCLSDND	In flow control, CLSDND represents calls that were denied due to there being too many calls in the flow control system, while CLSPTQ represents calls denied because of too many messages on a PTQ. In SOC, these two registers are combined into a single 'Calls Denied' register that counts calls that were tossed regardless of the reason. This register in SOC includes origination messages that were counted in SMSGPTQ and SHDROVFL (see below).
CLSABDN	SCLSABDN	Calls in either system that were abandoned by the client. Normally the abandon message comes from call processing on the Core.

Table 1

Flow Control Peg	SOC Peg	Description
CLSMSC	not applicable	Calls lost to miscellaneous resource failures.
not applicable	SNUMORIG	Total number of originations passing through SOC (delayed or not).
not applicable	SMSGLOST	Number of messages lost because of SOC system limits (includes SMSGPTQ and SHDROVFL)
not applicable	SMSGPTQ	Number of messages of any type that were lost due to PTQ overflow.
not applicable	SHDROVFL	Number of messages of any type that were lost due to SOC header array overflow.

All of the above OMs will be presented in OMSHOW on a per-node basis. The 'Performance' section of this book gives details about the new and the changed OM groups.

34.13 AMA/Billing information (AM)

34.13.1 New/changed AMA/billing information

Table 7 New or modified AMA/billing information

Billing format	NEW/CHANGED	Application	Standards

34.14 Glossary

Term	Description
PTQ	Per Terminal Queue - in SOC (System Overload Control) and Spectrum flow control, this is a queue that stores messages that are to be delivered to a given terminal ID.
SOC	An overloaded acronym that can mean either System Overload Control or Software Optionality Control, depending on the context.

34.15 References

A00002431 - Core/SPM Software Optionality Control implementation design document in FMDOC.

N00002432 - Fault Management section of ACT.00002432 in FMDOC

Q00002432 - Performance section of ACT.00002432 in FMDOC

35: Functional Description (FN): A00002433

35.1 Feature name

XA-Core Baseline Control

35.2 Description

35.2.1 Purpose

This activity seeks to address reliability issues related to XA-Core Hardware (HW) and Firmware (FW) not being at field baseline.

35.2.2 Baseline Definition

Field baseline implies the minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation. The HW field baseline is updated due to a class 'A' HW change. The FW field baseline is updated due to a severe FW bug.

1. HW baseline compatibility is based on PEC presence in table PECINV and meeting Release constraints.
2. FW baseline compatibility is based on PEC presence in table FWINV and FW/DLL meeting Version constraints.

See *"35.2.5 Activity Behaviour" on page 353* for detailed info.

35.2.3 Activation

The activity is activated by default, in all XA-Core loads.

35.2.4 Baseline Defaults

XA-Core **hardware** baselines are stored in table **PECINV**.
XA-Core **firmware** baselines are stored in **New table FWINV**.
These tables are provisioned in the loadbuild stage of software delivery.

Tables PECINV and FWINV are user modifiable, but caution must be exercised in making any changes, since the changes can impact the system, as further described below. Both tables are NOT restored over an ONP.
CSP20 defaults are shown in: *Table 1, "CSP20 Baseline HW Releases, FW Versions," on page 352*. HW/FW exceptions can be provisioned to indicate a HW release or FW version which **must** not be allowed. Any release/version greater than or equal to the baseline release/version is OK to use, as long as it is NOT listed as an exception. There are currently no exception values.

Table 1 CSP20 Baseline HW Releases, FW Versions

Grp	Type	PEC	PECINV HW Release	FWINV FW Version[a][s]:	
			Baseline	FW Baseline	DLL Baseline
Cards	PE	NTLX02AA	n/a	Not supported	
		NTLX02CA	01	XAPE01AG	Not user modifiable
		NTLX02DA		XAPE02AB	
	IOP	NTLX03AA	28	XAIO01AK	N/A
		NTLX03AB	03		
		NTLX03BA	28		
		NTLX03BB	03		
	HIOP	NTLX04AA	01	XHIO02AA	XHIO02AH
		NTLX04BA			
		NTLX04CA		XHIO02AH	
		NTLX17AA		XHIO03AA	
PkIt	CMIC	NTLX05AA	n/a	Not supported	
		NTLX05AB	01	PK12CE12	N/A
	AMDI	NTLX05BA			
	ETHR	NTLX09AA		EP14D003	
No FW	SM	NTLX14CA		N/A	
		NTLX14FA			
	DISK	NTLX06AA			
		NTLX06AB			
		NTLX06AC			
	TAPE	NTLX07AA			
		NTLX07BA			
	RTIF	NTLX08AA			
		NTLX08AB			

a. There are currently no hardware or firmware exceptions.

35.2.5 Activity Behaviour

HW and FW baseline behaviour is summarized below for Hardware (PECINV) and Firmware (FWINV) respectively.
Details follow in subsequent sections.

Table 2 Baseline Behaviour - PECINV vs. Hardware

Input Conditions		Behaviour		
PEC	**Hardware Rel vs. PECINV Rel**	**RTS**	**Baseln Alarm**	**SREx**
Not in PECINV	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM | IO
IN PECINV	= exception Rel OR < baseline Rel			
	>= baseline Rel	Pass	Lower	OK

Table 3 Baseline Behaviour - FWINV vs. Firmware

Input Conditions		Behaviour		
PEC	**Firmware Ver vs. FWINV Ver**	**RTS**	**Baseln Alarm**	**SREx**
NOT in FWINV: pe, iop, hiop cards cmic, amdi, ethr pklts	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM | IO
IN FWINV pe, iop, hiop[a] card, cmic, amdi, ethr pklts	= exception Ver			
	< baseline Ver	Pass[b]		OK
	>= baseline Ver	Pass	Lower	
NOT in FWINV: sm, disk, tape, rtif	don't care. FRU have no FW			

a. HIOP: Both FW & DLL must pass baseline checks.
b. FW/DLL updated AFTER unsplit, so we must RTS, since later SREx/ManB/Reload would leave a previously working FRU OOS.

35.2.5.1 Baseln Alarm

New Baseln Major alarm is used to indicate that at least one non-baseline (Hardware or Firmware) FRU is present in the system.
Baseln alarm raising or lowering is triggered by:

1. Manual "MAPCI;MTC;XAC;QUERY CARD" of a below baseline FRU
2. Manual "MAPCI;MTC;XAC;QUERY SHELF"
3. System initiated query - occur periodically and after certain events
4. Manual "MAPCI;MTC;XAC;<level>;UNEQ" after FRU BSY, then pull

The alarm is lowered when all FRU have baseline compatible HW and FW[1].

[1]Or any restart occurs. See *"35.5 Limitations and restrictions" on page 356*

To get a list of the non-baseline FRU responsible for the alarm, type, from MAPCI;MTC;XAC level:

1. ALARM Baseln - lists the problem FRU, but no baseline specific info
2. QUERY SHELF - ALL FRU info in the XA-Core shelf.
   Look for "*" in Hardware and Firmware "OK" columns.

35.2.5.2 Related Logs

1. **New XAC337** (FLT) - generated when the Baseln alarm is first raised, and whenever the list of non-baseline items changes, and is non-empty.
   The log lists the non-baseline FRU with related baseline information.
2. **New XAC637** (INFO)- generated when the Baseln alarm is lowered, indicating all FRU are now baseline compatible. The log is NOT generated due to a restart clearing the alarm, as discussed in *"35.5 Limitations and restrictions"*.
3. XAC415 - generated when SREx Baseline precheck determines that a PE or SM card is non-baseline, so no SREx is permitted.
   New reason added: "XACore Hardware or Firmware is not at baseline".

35.2.5.3 SREx Impact

SREx is **bypassed** and an XAC415 log generated if a PE or SM card is not at baseline. Subsequent AutoDump is disallowed, since no image test was run.

OOS IO tests are bypassed if ONLY IO related FRU are non-baseline.

35.2.5.4 Table Control

Table PECINV - **new warning** is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.
Warn that FRU WILL NOT RTS if the tuple is deleted or if the baseline or exception list change is not compatible with existing/newly inserted hardware.

New table FWINV - contains firmware (and DLL) baseline(s) indexed by PEC. Also provides the ability to indicate a FW release which should not be allowed if declared an "exception" version(s).

Table XAFWLOAD - **new warning** is displayed if the user attempts to provision a non-baseline firmware loadname.
Warn that Baseln alarm will be raised after the FRU is RTS'd, if a non-baseline loadname is used.

35.2.5.5 OAM

From MAPCI;MTC;XAC level (or sublevels), QUERY SHELF output **adds** Hardware and Firmware baseline[s] and FRU status indicator ("OK").
Any "*" in the OK column requires investigation.
The OK column entry is of the form "x" where x is:

1. **P*** = PEC not in table **P**ECINV
2. **F*** = PEC not in table **F**WINV, and FRU has FW (and DLL - HIOP only)
3. **N*** = **N**ot baseline compatible. I.e. Below baseline.
4. **X*** = Release/Version is an e**X**ception Rel/Ver in table PECINV/FWINV
5. **I*** = Could not read MIM **I**DPROM, to get PEC/Rel.
   This occurs during some maintenance activities.
   Baseln alarm/log will NOT be generated solely from this info.
6. **Y** = **Y**es, this FRU is baseline compatible.

"HW-SW vintage" column is **removed** from QUERY SHELF output, to allow for new baseline information. Vintage is still visible from the QUERY CARD command.

CI "POLL SHORT <dev1> <dev2>" is **enhanced** to show the output from a "QUERY SHELF" command. On a Supernode, it currently displays the output from MAPCI;MTC;CM;QUERYCM NOEMPTY.
XAC;QUERY SHELF is the XA-Core logical equivalent.

35.2.5.6 ONP Prechecks

The following **ONP precheck steps are enhanced** to detect non-baseline FRU on the active image. The steps fail if the equivalent of a QUERY SHELF displays "P*, F*, X* or N*", as previously described in *"35.2.5.5 OAM"*.

1. "ONPREADY", step "DISPLAY_PEC_INFO"
2. "SWUPGRADE READY; START", step "VERIFY_SN_PECS_INFO"
3. "BCSUPDATE; PRECHECK", step "DISPLAY_PEC_INFO"

35.2.5.7 ONP Pre-SWACT

While split, a **new pre-SWACT check** requests/receives the new-side PECINV (hardware baseline) data, to see if existing HW meets new-side baseline requirements. Alert the user if it does not.

FW checks are NOT done, since FW is currently updated in the first available Mtc window AFTER the unsplit succeeds. The Baseln Major alarm WILL be raised shortly after the unsplit, if the FWINV baselines have changed from one CSP release to another - this is a reminder to do the suggested FW/DLL upgrades.

35.3 Hardware Requirements or Dependencies

This activity applies only to XA-Core.

The XA-Core must be at hardware baseline for new ONP prechecks to pass. Hardware baselines are detailed in "XA-Core Maintenance Manual" (NTP 297-8991-510).

A patch will be developed for each of CSP17-CSP19, in order to determine the switch's current hardware baseline status. The intent is to avoid any ONP baseline issues when upgrading to CSP20-CSP22.

35.4 Software Requirements or Dependencies

No new software dependencies.

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised. Firmware baselines are detailed in the "DMS-100 Family NA100 Peripheral Module Software Release Document" (NTP 297-9081-599).

35.5 Limitations and restrictions

New Baseln alarm is cleared over all restarts. The alarm is re-raised when the non-baseline item is queried manually or by the system (within 10 minutes).

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised.

No incompatibilities with other features.

35.6 Interactions

Table XAFWLOAD - a new warning is displayed if the user attempts to provision a non-baseline firmware loadname.
Warn that Baseln alarm will be raised after the FRU is RTS'd.

Table PECINV - a new warning is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.
Warn that FRU **WILL NOT** RTS if the tuple is deleted.
Warn that FRU **MAY NOT** RTS if the baseline or exception list change is not compatible with existing/newly inserted hardware.

35.7 Applicable customer facing sections

Fault Management

Logs	_X____
Alarms	_X____

Configuration

Data Schema	_X____
User Interface	_X____
Element Management	_n/a___
Security	_n/a___
Service Order	_n/a___

Office Parameters _n/a___

Accounting (includes AMA billing) _n/a___

Performance (includes operational measurements) _n/a___

35.8 Glossary

Term	Description
Baseline	The minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation.
DLL	DownLoadable Loader
Exception	A HW release/FW version greaterthan or equal to the baseline release/version is OK to use, as long as it is NOT listed explicitly as an exception. I.e. an exception indicates HW/FW which must not be used.
FRU	Field Replaceable Unit - card or IOP packlet
FW	FirmWare
HW	HardWare
IOP	Input Output Processor Card
ManB	Manual Busy
MIM	Module Information Memory
ONP	One Night Process
OOS	Out Of Service
PE	Processor Element Card
RTS	Return To Service
SM	Shared Memory Card
SREx	System Routine Exercise

36: Functional Description (FN): A00002499

36.1 Feature name

XA-Core Baseline Control

36.2 Description

36.2.1 Purpose

This activity seeks to address reliability issues related to XA-Core Hardware (HW) and Firmware (FW) not being at field baseline.

36.2.2 Baseline Definition

Field baseline implies the minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation. The HW field baseline is updated due to a class 'A' HW change. The FW field baseline is updated due to a severe FW bug.

1. HW baseline compatibility is based on PEC presence in table PECINV and meeting Release constraints.
2. FW baseline compatibility is based on PEC presence in table FWINV and FW/DLL meeting Version constraints.

See *"35.2.5 Activity Behaviour" on page 353* for detailed info.

36.2.3 Activation

The activity is activated by default, in all XA-Core loads.

36.2.4 Baseline Defaults

XA-Core **hardware** baselines are stored in table **PECINV**.
XA-Core **firmware** baselines are stored in **New table FWINV**.
These tables are provisioned in the loadbuild stage of software delivery.

Tables PECINV and FWINV are user modifiable, but caution must be exercised in making any changes, since the changes can impact the system, as further described below. Both tables are NOT restored over an ONP.
CSP20 defaults are shown in: *Table 1, "CSP20 Baseline HW Releases, FW Versions," on page 352*. HW/FW exceptions can be provisioned to indicate a HW release or FW version which **must** not be allowed. Any release/version greater than or equal to the baseline release/version is OK to use, as long as it is NOT listed as an exception. There are currently no exception values.

Table 1 CSP20 Baseline HW Releases, FW Versions

Grp	Type	PEC	PECINV HW Release	FWINV FW Version[a][s]:	
			Baseline	FW Baseline	DLL Baseline
Cards	PE	NTLX02AA	n/a	Not supported	
		NTLX02CA	01	XAPE01AG	Not user modifiable
		NTLX02DA		XAPE02AB	
	IOP	NTLX03AA	28	XAIO01AK	N/A
		NTLX03AB	03		
		NTLX03BA	28		
		NTLX03BB	03		
	HIOP	NTLX04AA	01	XHIO02AA	XHIO02AH
		NTLX04BA			
		NTLX04CA		XHIO02AH	
		NTLX17AA		XHIO03AA	
PkIt	CMIC	NTLX05AA	n/a	Not supported	
		NTLX05AB	01	PK12CE12	N/A
	AMDI	NTLX05BA			
	ETHR	NTLX09AA		EP14D003	
No FW	SM	NTLX14CA		N/A	
		NTLX14FA			
	DISK	NTLX06AA			
		NTLX06AB			
		NTLX06AC			
	TAPE	NTLX07AA			
		NTLX07BA			
	RTIF	NTLX08AA			
		NTLX08AB			

a. There are currently no hardware or firmware exceptions.

36.2.5 Activity Behaviour

HW and FW baseline behaviour is summarized below for Hardware (PECINV) and Firmware (FWINV) respectively.
Details follow in subsequent sections.

Table 2 Baseline Behaviour - PECINV vs. Hardware

Input Conditions		Behaviour		
PEC	**Hardware Rel vs. PECINV Rel**	**RTS**	**Baseln Alarm**	**SREx**
Not in PECINV	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM | IO
IN PECINV	= exception Rel OR < baseline Rel			
	>= baseline Rel	Pass	Lower	OK

Table 3 Baseline Behaviour - FWINV vs. Firmware

Input Conditions		Behaviour		
PEC	**Firmware Ver vs. FWINV Ver**	**RTS**	**Baseln Alarm**	**SREx**
NOT in FWINV: pe, iop, hiop cards cmic, amdi, ethr pklts	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM | IO
IN FWINV pe, iop, hiop[a] card, cmic, amdi, ethr pklts	= exception Ver			
	< baseline Ver	Pass[b]		OK
	>= baseline Ver	Pass	Lower	
NOT in FWINV: sm, disk, tape, rtif	don't care. FRU have no FW			

a. HIOP: Both FW & DLL must pass baseline checks.
b. FW/DLL updated AFTER unsplit, so we must RTS, since later SREx/ManB/Reload would leave a previously working FRU OOS.

36.2.5.1 Baseln Alarm

New Baseln Major alarm is used to indicate that at least one non-baseline (Hardware or Firmware) FRU is present in the system.
Baseln alarm raising or lowering is triggered by:

1. Manual "MAPCI;MTC;XAC;QUERY CARD" of a below baseline FRU
2. Manual "MAPCI;MTC;XAC;QUERY SHELF"
3. System initiated query - occur periodically and after certain events
4. Manual "MAPCI;MTC;XAC;<level>;UNEQ" after FRU BSY, then pull

The alarm is lowered when all FRU have baseline compatible HW and FW[1].

[1]Or any restart occurs. See *"35.5 Limitations and restrictions" on page 356*

To get a list of the non-baseline FRU responsible for the alarm, type, from MAPCI;MTC;XAC level:

1. ALARM Baseln - lists the problem FRU, but no baseline specific info
2. QUERY SHELF - ALL FRU info in the XA-Core shelf.
   Look for "*" in Hardware and Firmware "OK" columns.

36.2.5.2 Related Logs

1. **New XAC337** (FLT) - generated when the Baseln alarm is first raised, and whenever the list of non-baseline items changes, and is non-empty.
   The log lists the non-baseline FRU with related baseline information.
2. **New XAC637** (INFO)- generated when the Baseln alarm is lowered, indicating all FRU are now baseline compatible. The log is NOT generated due to a restart clearing the alarm, as discussed in *"35.5 Limitations and restrictions"*.
3. XAC415 - generated when SREx Baseline precheck determines that a PE or SM card is non-baseline, so no SREx is permitted.
   New reason added: "XACore Hardware or Firmware is not at baseline".

36.2.5.3 SREx Impact

SREx is **bypassed** and an XAC415 log generated if a PE or SM card is not at baseline. Subsequent AutoDump is disallowed, since no image test was run.

OOS IO tests are bypassed if ONLY IO related FRU are non-baseline.

36.2.5.4 Table Control

Table PECINV - **new warning** is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.
Warn that FRU WILL NOT RTS if the tuple is deleted or if the baseline or exception list change is not compatible with existing/newly inserted hardware.

New table FWINV - contains firmware (and DLL) baseline(s) indexed by PEC. Also provides the ability to indicate a FW release which should not be allowed if declared an "exception" version(s).

Table XAFWLOAD - **new warning** is displayed if the user attempts to provision a non-baseline firmware loadname.
Warn that Baseln alarm will be raised after the FRU is RTS'd, if a non-baseline loadname is used.

36.2.5.5 OAM

From MAPCI;MTC;XAC level (or sublevels), QUERY SHELF output **adds** Hardware and Firmware baseline[s] and FRU status indicator ("OK").
Any "*" in the OK column requires investigation.
The OK column entry is of the form "x" where x is:

1. **P*** = PEC not in table **P**ECINV
2. **F*** = PEC not in table **F**WINV, and FRU has FW (and DLL - HIOP only)
3. **N*** = **N**ot baseline compatible. I.e. Below baseline.
4. **X*** = Release/Version is an e**X**ception Rel/Ver in table PECINV/FWINV
5. **I*** = Could not read MIM **I**DPROM, to get PEC/Rel.
   This occurs during some maintenance activities.
   Baseln alarm/log will NOT be generated solely from this info.
6. **Y** = **Y**es, this FRU is baseline compatible.

"HW-SW vintage" column is **removed** from QUERY SHELF output, to allow for new baseline information. Vintage is still visible from the QUERY CARD command.

CI "POLL SHORT <dev1> <dev2>" is **enhanced** to show the output from a "QUERY SHELF" command. On a Supernode, it currently displays the output from MAPCI;MTC;CM;QUERYCM NOEMPTY.
XAC;QUERY SHELF is the XA-Core logical equivalent.

36.2.5.6 ONP Prechecks

The following **ONP precheck steps are enhanced** to detect non-baseline FRU on the active image. The steps fail if the equivalent of a QUERY SHELF displays "P*, F*, X* or N*", as previously described in *"35.2.5.5 OAM"*.

1. "ONPREADY", step "DISPLAY_PEC_INFO"
2. "SWUPGRADE READY; START", step "VERIFY_SN_PECS_INFO"
3. "BCSUPDATE; PRECHECK", step "DISPLAY_PEC_INFO"

36.2.5.7 ONP Pre-SWACT

While split, a **new pre-SWACT check** requests/receives the new-side PECINV (hardware baseline) data, to see if existing HW meets new-side baseline requirements. Alert the user if it does not.

FW checks are NOT done, since FW is currently updated in the first available Mtc window AFTER the unsplit succeeds. The Baseln Major alarm WILL be raised shortly after the unsplit, if the FWINV baselines have changed from one CSP release to another - this is a reminder to do the suggested FW/DLL upgrades.

36.3 Hardware Requirements or Dependencies

This activity applies only to XA-Core.

The XA-Core must be at hardware baseline for new ONP prechecks to pass. Hardware baselines are detailed in "XA-Core Maintenance Manual" (NTP 297-8991-510).

A patch will be developed for each of CSP17-CSP19, in order to determine the switch's current hardware baseline status. The intent is to avoid any ONP baseline issues when upgrading to CSP20-CSP22.

36.4 Software Requirements or Dependencies

No new software dependencies.

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised. Firmware baselines are detailed in the "DMS-100 Family NA100 Peripheral Module Software Release Document" (NTP 297-9081-599).

36.5 Limitations and restrictions

New Baseln alarm is cleared over all restarts. The alarm is re-raised when the non-baseline item is queried manually or by the system (within 10 minutes).

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised.

No incompatibilities with other features.

36.6 Interactions

Table XAFWLOAD - a new warning is displayed if the user attempts to provision a non-baseline firmware loadname.
Warn that Baseln alarm will be raised after the FRU is RTS'd.

Table PECINV - a new warning is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.
Warn that FRU **WILL NOT** RTS if the tuple is deleted.
Warn that FRU **MAY NOT** RTS if the baseline or exception list change is not compatible with existing/newly inserted hardware.

36.7 Applicable customer facing sections

Fault Management

Logs	_X____
Alarms	_X____

Configuration

Data Schema	_X____
User Interface	_X____
Element Management	_n/a___
Security	_n/a___
Service Order	_n/a___

Office Parameters _n/a___

Accounting (includes AMA billing) _n/a___

Performance (includes operational measurements) _n/a___

36.8 Glossary

Term	Description
Baseline	The minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation.
DLL	DownLoadable Loader
Exception	A HW release/FW version greaterthan or equal to the baseline release/version is OK to use, as long as it is NOT listed explicitly as an exception. I.e. an exception indicates HW/FW which must not be used.
FRU	Field Replaceable Unit - card or IOP packlet
FW	FirmWare
HW	HardWare
IOP	Input Output Processor Card
ManB	Manual Busy
MIM	Module Information Memory
ONP	One Night Process
OOS	Out Of Service
PE	Processor Element Card
RTS	Return To Service
SM	Shared Memory Card
SREx	System Routine Exercise

37: Functional Description (FN): A00002505

37.1 Feature name

Universal Signaling Point Interface Client - GUI

37.2 Description

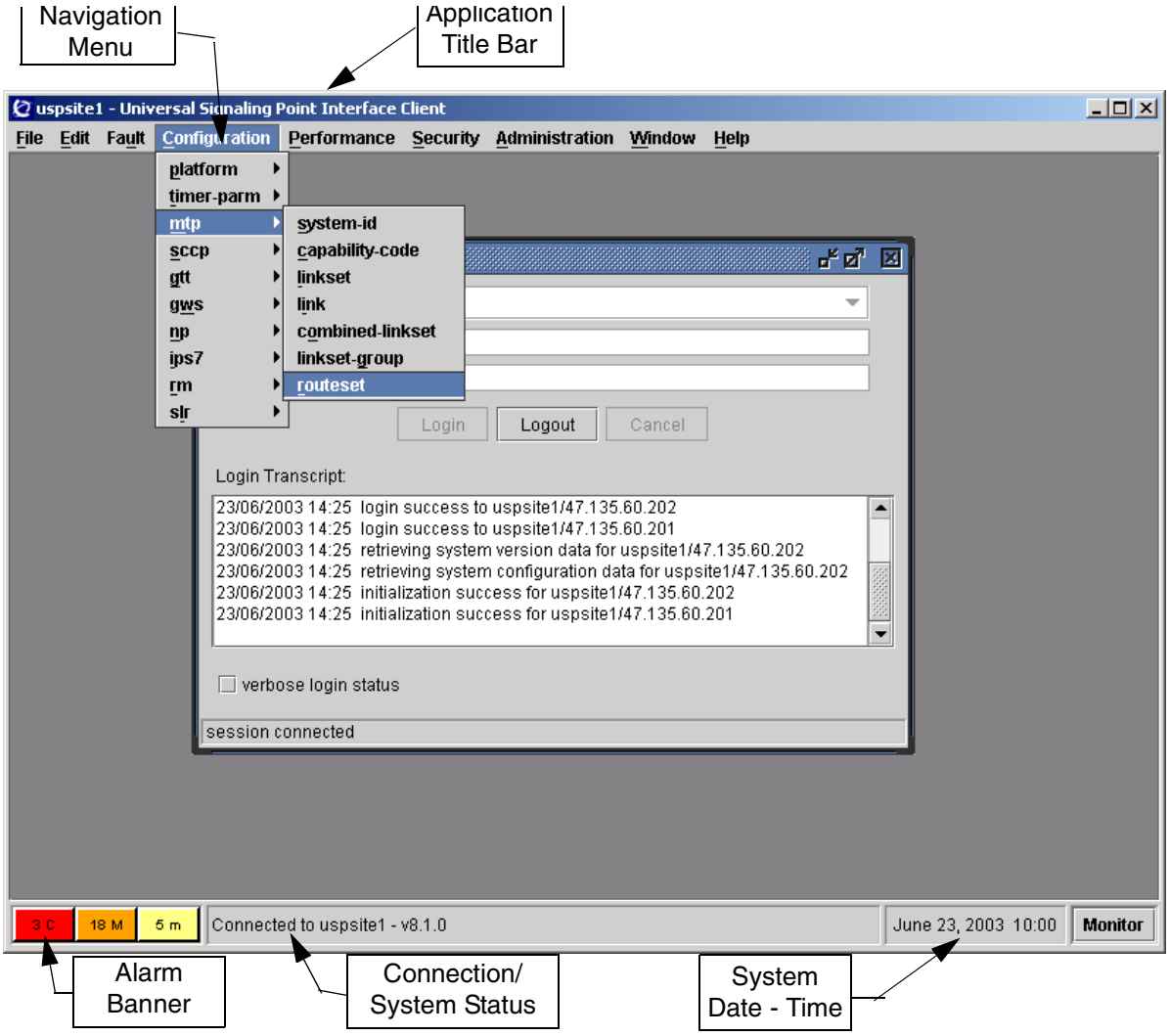
The purpose of this feature is to provide a graphical user interface (GUI) capable of running on multiple operating system platforms in a windows based environment. The GUI will have provisions for administering, monitoring and reporting on the Universal Signaling Point (USP). The GUI delivered by this feature is a replacement for the GUI provided with previous software releases (pre USP8.1.0) and will include and expand upon the functionality and usability provided by the previous GUI version.

The GUI provides a complete multi-platform solution for managing the operation of the USP by providing an intuitive user interface client to perform administration, system monitoring and reporting. The GUI client implements a consistent interface model to present all USP data to ensure ease-of-use and quick navigation of the data retrieved from the USP.

All communication with the USP is accomplished by establishing a standard TELNET connection to the USP Command Line Interface (CLI) and will maintain that connection, reestablishing the connection if necessary. There are no custom protocols or ports to configure which simplifies interoperability and allows for all existing security restrictions and firewalls to be enforced. Local security is also enhanced by initiating idle session lockout and re-authentication if a session is left unattended for an extended period of time. Interoperability is enhanced through context-sensitive launching, using command line arguments, which allows external applications to control the launch sequence of the GUI to have it automatically navigate to the desired table and records using the supplied retrieval criteria.

The GUI is designed as a single encapsulating window manager to help organize and manage the layout of the large number of tables offered by the USP. Access to each table is achieved by a hierarchical menu structure. This structure provides fast and simple navigation to the desired table by simply clicking on the desired table from the pull down menus. See the following figure for an example of the main window of the GUI application.

GUI Main Window



For monitoring purposes, the bottom panel of the main window has connection and status information related to the currently connected site. The alarm banner presents a summary of the current alarmed components of the USP. The status panels provide further overall site information about the current connected site; including, connection information, running software versions and the current system date-time.

The GUI is built on a proven transaction based multi-threaded framework to ensure it will remain responsive even under heavy operation. This permits multiple tasks to be performed simultaneously and assures that progress and status information can always be relayed to the user for the current operation. The cross-platform support of the GUI is accomplished by exploiting the multi-platform support of the Java 2 technology.

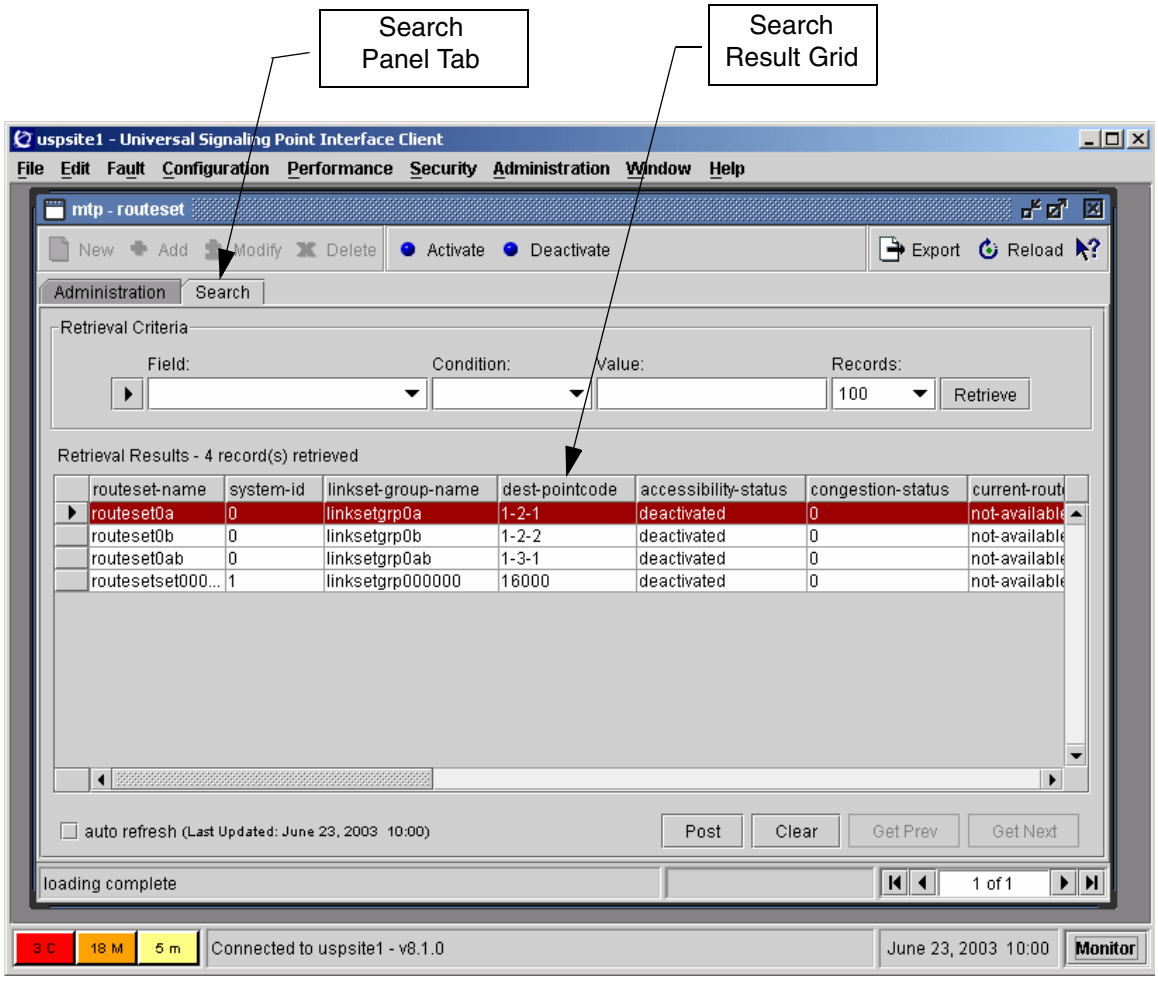
Management of all system operations and provisioning data is achieved through a common table interface. This common interface simplifies usability and reduces learning times by providing consistent presentation formats and navigation controls. The common table interface consists of an Administration and Search panel for each table accessible from the USP.

The Administration panel provides the provisioning and maintenance operations for that table. All record manipulation can be performed by the Administration screen for a particular table, including the addition, modification and deletion of records. To enhance usability, all table fields are linked to context-sensitive help to provide a complete field description; including field type, data type, minimum and maximum values, input restrictions, allowed value lists and optional descriptive text for field explanation or special notes. See the following figure for an example of a table Administration panel.

Table Administration Panel

The Search panel provides record retrieval and navigation, with the added capability of supplying search criteria for most table fields. All tables support both basic and advanced data retrieval and search capabilities to allow for quick navigation to the data of concern. See the following figure for an example of a table Search panel.

Table Search Panel

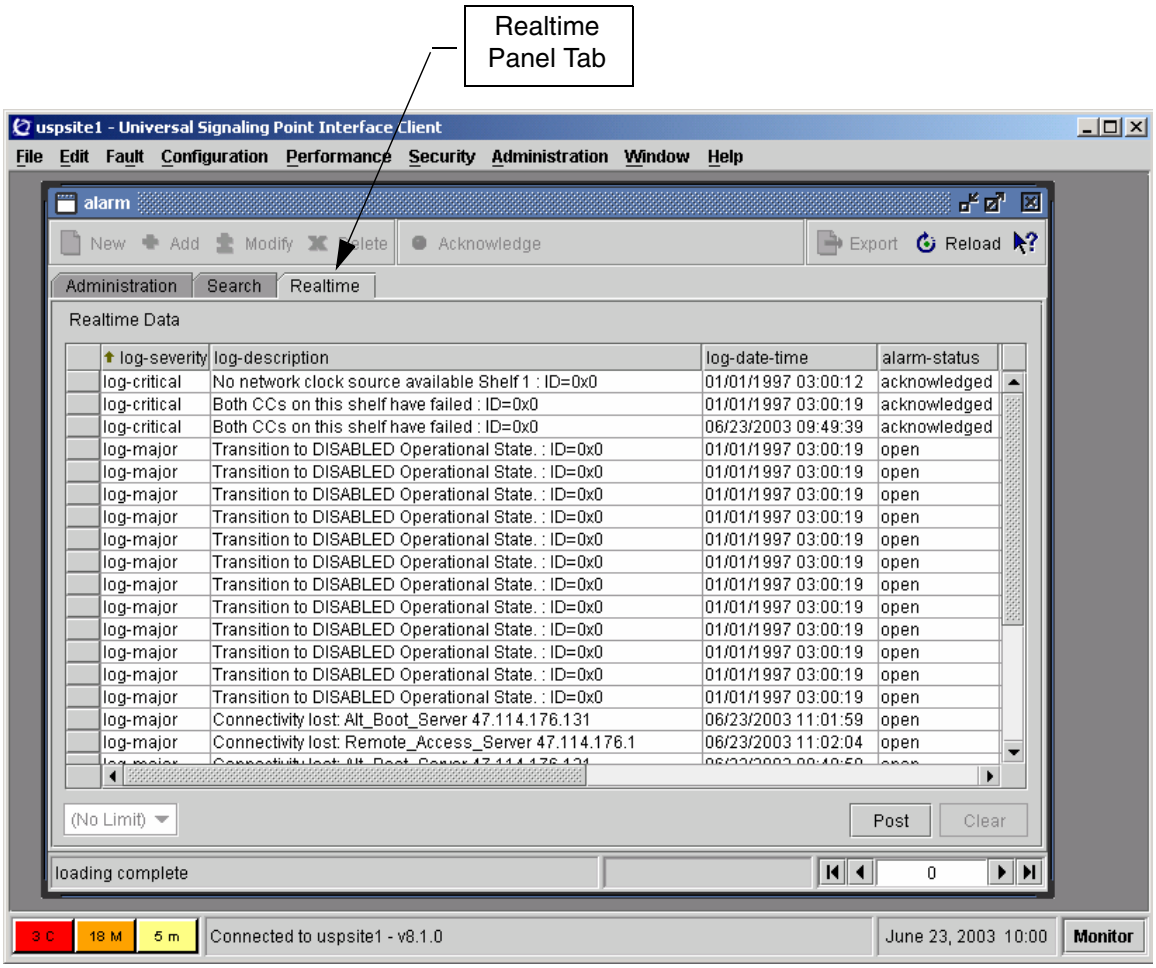


All data retrieved from the USP can be formatted and exported to an external file for the purpose of capturing the data in static form. Data can be exported in HTML, CSV and plain text formats. The Search panel facilitates the data capture and customized reporting through the search result grid containing the retrieved table records. Customization is accomplished by adjusting the appearance, presence and location of table fields of a table grid to help organize and report on the critical data.

Fault monitoring of a specific site can be performed in real-time by viewing the summary information from the status bar of the main window, or by accessing the specific fault information from the alarm and log tables. In addition to Administration and Search panels, the fault management tables have a Realtime panel which allows for real-time monitoring and viewing of USP events (i.e. logs and alarms). Similar to search screens, the data presented

by the Realtime panel can be customized and navigated using the same common interface. See the following figure for an example of a table Realtime panel.

Table Realtime Panel



37.3 Hardware Information

The GUI has been verified on the following platforms running JRE1.4.1_02:

- Windows (NT4.0+SP5/2000 prof+SP2/XP)
- Solaris OS + patches (http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE)

The following system requirements must be met to run the GUI application:

- minimum of 64 megabytes of RAM, recommended 128 megabytes

- minimum of 100 megabytes of disk space to install JRE and to store site configuration, preferences and local logs required by GUI application
- graphical window environment running at least 16-bit color depth

37.3.1.1 GUI/CLI Information

The summary of the changes have been outlined in the "Description" section. For a complete and detailed description of the changes and the usage of the GUI, please refer to the document titled *Universal Signaling Point GUI - User Guide*.

37.3.1.2 CLI changes

All communication (data exchange) with the USP will be performed through a TELNET connection to the USP using the CLI. The GUI will make use of the CLI-API machine interface of the USP and will therefore require no additional functionality.

37.3.2 GUI changes

Refer to the "Description" section for details of GUI changes. The new GUI is a replacement for the GUI distributed with the previous software releases (pre USP8.1.0).

37.3.3 OMs

Not Applicable.

37.3.4 Logs, and Alarms

Not Applicable.

37.4 Interactions

The GUI facilitates administration, monitoring and reporting of all existing functions of the USP. The functionality provided by the USP will continue to operate as normal and will not be affected by the interface changes introduced by the GUI.

37.5 Restrictions and Limitations

None.

37.6 Definitions and Terms

CLI - Command Line Interface

CPU- Central Processing Unit

GUI - Graphical User Interface

J2SE- Java 2 Standard Edition

JRE - Java Runtime Engine

MDI- Multiple Document Interface

USP - Universal Signaling Point

38: Functional Description (FN): A00002510

38.1 Feature name

LANCOMM IP over IRM.

38.2 Description

This document provides the design intent for the feature to provide LANCOMM IP over the IRM on XA-CORE. The purpose of this feature is to provide LANCOMM TCP and UDP availability when communicating over the XACORE Ethernet messaging system. This feature does not address LANCOMM issues of performance or robustness.

At present the IRM IP is used to transmit and receive packets to and from the XACORE IO hardware. The IRM implementation of IP is very minimal with some of the features such as ARP routing being performed by the firmware. The IRM IP implementation does not support TCP or features like IP fragmentation and extra options. The LANCOMM version of IP supports IP more completely. This feature will use the IRM IP to receive packets from the IO cards, however the IRM will then will use callback routines that will be registered with the IRM for packets intended for LANCOMM to pass the packets to LANCOMM UDP or TCP. The LANCOMM IP will be used to process the packets. A TCP or UDP packet coming from the LANCOMM intended for the IRM will be injected in to the IRM IP after it has passed through the LANCOMM IP to be transmitted to Ethernet.

The specific purpose of this feature is to support the Next generation Supernode Data Manager (nSDM) that is being developed on a Solaris platform to replace the existing SDM FX which uses a DS512 to connect to the CORE. The nSDM will not have a DS512. It will connect to the CORE via Ethernet. This feature will also support FTP or TELNET over IRM from another source other than the SDM like for instance an workstation. [1]This will not be a EIU replacement but will exist in the same load as EIU.This Feature will support the following SDM applications with LANCOMM IP over IRM.

- RPC (UDP)
- NTP -Network Time Protocol (UDP)
- FTP (TCP)
- Telnet (TCP)
- SBA -Billing (RFC TCP)

[1]Telnet and FTP over IRM will be enabled for all devices connected to a CORE that is in lab mode. In field mode the only recognised device allowed to access the CORE through the Ethernet will be SDM.

38.3 Hardware Requirements or Dependencies

A nSDM and a SDM FX which are connected to the Core by HIOP are required to fully test the feature. We also need a nSDM system that is connected to a core that has both EIU and HIOPs.

38.4 Software Requirements or Dependencies

There should be no software dependencies as this feature will work with both the existing SDM FX and NSDM.

38.5 Limitations and restrictions

Only one SDM will be connected to the CORE at a time.

Any application that wants to use LANCOMM IP over IRM is required to bind to the NIL IP address. All present SDM applications are compliant.

Any applications that are using the EIU will continue to function.

Under this CSP20 release only, the SDM will be the only application node making use of the LANCOMM IP over IRM feature. The number of SDM nodes are limited to four.

The EIU and the XA-Core Ethernet (IRM) interface subnets should be isolated, and they should not be connected, directly or indirectly.

38.6 Interactions

All applications using LANCOMM IP over IRM on the nSDM will function as they did before on the SDM fx without any impact to the user.

38.7 Applicable customer facing sections

Fault Management	
Logs	X
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A

Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	X

38.8 Glossary

Term	Description
Arp	Address Resolution Protocol
Core	DMS switch computing engine
FTP	File Transfer Protocol
HIOP	High Performance I/O processor packlet
IP	Internet Protocol
IRM	IP routing and Maintenance
LANCOMM	Core network layer for Telnet and FTP
nSDM	next Generation Supernode Data Manager
SDM	Supernode Data Manager
SDM FX	SDM Fault tolerant platform based on IBM AIX UNIX and redundant Motorola hardware.
TCP	Transmission Control Protocol
UDP	internet User Datagram Protocol

39: Functional Description (FN): A00002538

39.1 Feature name

A00002538 - Performance Measurements Tools

39.2 Description

This feature will remove the COMPLEX (call complexity) measurement from the XA-Core platform as this measurement is not valid for XA-Core.

The COMPLEX measurement is currently displayed in:

- the CAPCI CI command
- the CAPACITY level of MAPCI
- the DETAIL level of MAPCI
- the SCHEDMAP level of MAPCI
- CAPLOGS - specifically the CAP100 and CAP101 logs
- XASTAT OM - XASCMPLX measurement

39.3 Hardware Requirements or Dependencies

None

39.4 Software Requirements or Dependencies

None

39.5 Limitations and restrictions

None

39.6 Interactions

None

39.7 Applicable customer facing sections

Fault Management

Logs	__X___
Alarms	_____

Configuration

Data Schema	_____
User Interface	_____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) ___X__

39.8 Glossary

Term	Description

40: Functional Description (FN): A00002549

40.1 Feature name

A00002549: CSP20 Callp Robustness

- ***Design Component 2: OM threshold alarms for call processing resources - table ALARMTAB.***
- ***Design Component 3: Extension Block Format Code expansion.***
- ***Design Component 4: Increase Cpwakeup Accuracy.***

40.1.1 Design Component 2: OM threshold alarms for call processing resources - table ALARMTAB

This feature component adds datafill to the system table ALARMTAB. The table is datafilled prior to the release of the nodata load to the field. This adds an alarm to the existing EXT alarm banner component and the existing log OM2200 to be triggered upon depletion of the base call processing resource ECCB (Extended Call Condense Blocks). This alarm is based on the existing Operational Measurement register defined in CP2 - ECCBOVFL (ECCB Overflow). The table ALARMTAB currently exists for several base call processing resources. This addition is an enhancement to this set of alarms.

All actions and explanations are already documented for the existing base call processing resources and are identical for the ECCB resource depletion. Documentation for the logs and the alarm already exist and can be found in the following NTPs:

- ***297-8991-500 04.02 Maintenance and Operations Manual***
- ***297-2621-851P1 09.02 UCS DMS-250 Data Schema Reference Manual Vol 1 of 5***
- ***297-2621-8141 10.03 DMS-250 Operational Measurements Reference Manual Vol 1 of 2***
- ***297-8101-8141 06.01 Operational Measurements Reference Manual Vol. of 3***
- ***297-2621-8403 09.01 UCS DMS-250 Logs Reference Manual Vol 3 of 6***
- ***297-2621-8405 09.01 UCS DMS-250 Logs Reference Manual Vol 5 of 6***
- ***297-8101-3503 06.01 Base DMS STP Translations Guide Vol. 3 of 6***
- ***297-2621-106 07.02 UCS DMS-250 ISDN Reference Manual***
- ***297-2621-395 08.02 DMS-250 Billing Records Application Guide***
- ***297-2621-851P5 09.02 UCS DMS-250 Data Schema Reference Manual Vol 5 of 5***
- ***297-5051-914 07.02 DDMS and GUIDE Install and Admin Reference Manual***
- ***297-8101-8142 06.01 Operational Measurements Reference Manual Vol. 2 of 3***

40.1.2 Extension Block Format Code expansion

Currently, there are only a total of 256 extension format codes in the system. We are quickly approaching this limit thereby limiting the number of available extension format codes for new users. Design Component 3 of this feature -

EXT Format Code Expansion - addresses this issue. In particular, the total number of extension format codes in the system will be increased from 256 to 511.

Increasing the total number of extension format codes from 256 to 511 causes the size of the extension format codes to increase from 8-bits to 9-bits. The extension format code is a field within the extension block header (the first structure/field in every extension block). This may affect downstream processors if they extract the format code from the extension blocks hex dump. The total size of the extension block header is not being increased; however, two of its fields were re-arranged so that the new size of the format code could be accommadated. Specific details of this change are presented in the FM (Fault Management) section of this feature.

For each extension format code, there is a corresponding (unique) AUD and XAUD log. The XAUD logs are output whenever an extension block is reclaimed by the XA-Core audit process and the AUD logs are used to dump extension block contents for all other processes (ie. non-audit reclaims such as call deaths).

Currently the AUD logs assume the values 400 through 431, and 500 through 723. The XAUD logs assume values 600 through 610 (for standard call processing resources) and 700 through 955 (for extension blocks).

This feature will require that the ranges for the before mentioned AUD logs be extended beyond 723 to accommodate the new extension format codes. The XAUD logs will also be extended and the numbering convention (numeric range) will be changed to match that for the AUD logs for simplicity. That is, each extension format code will now have the same AUD and XAUD number (ie. the associated logs for extfc 109 will be AUD577 and XAUD577).

Please note that as each new extension format code is defined/added in the system, it is the responsiblity of the user to define and document it. Therefore, the only changes visible to the customer will be for the existing XAUD log numbers (those currently defined at the time of this feature). Furthermore, the contents of these logs (apart from the location and number of bits of the extfc in the extension block head) are in no way being changed.

40.1.3 Increase Cpwakeup Accuracy

This component of the feature will affect the real-time of the switch. This real-time increase will be minimal.

40.2 Hardware Requirements or Dependencies

Not applicable.

40.3 Software Requirements or Dependencies

Not applicable.

40.4 Limitations and restrictions

Not applicable.

40.5 Interactions

Not applicable.

40.6 Applicable customer facing sections

Fault Management

Logs	____X____
Alarms	___N/A__

Configuration

Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

40.7 Glossary

Term	Description

41: Functional Description (FN): A00002555

41.1 Feature name

SERVORD MANIPULATION OF THE GND OPTION

41.2 Description

This SN07 activity allows Servord commands ADO, DEO and CLN to manipulation the GND option. The GND option for lines resides in table LNINV. Table LNINV contains the hardware information about the line including the Line Equipment Number (LEN) card code and GND. If GND is set to Y, the line will be a ground start line if the line card is supportive. The list of line cards supported are:

- 3A06BA
- 7A25AA
- RDTCON
- RDTLSG
- SCD271

The GND option appears as a line option when a query is performed on the DN or LEN but it is currently not an option than can be manipulated via Servord. This activity will allow Servord to manipulate the GND option on the above line cards, including

- ADO and DEO of the GND option
- CLN will propagate the GND information of the OLD_LEN to the NEW_LEN

Lines that currently auto populate table LNINV on NEW, EST and ADD such as Succession and lines off of RDT peripherals will continue to function as before.

The redundant feature which is turned on by table OFCVAR parm SO_ALLOW_REDUNDANT_FEATURE is now supported for the GND option for the ADO, DEO and CLN Servord commands.

CLN will set the value of GND to that of the OLD_LEN if the NEW_LEN is one of the supported line cards. A warning message will be output that GND being set to the OLD_LEN value. The below example shows the warning message if GND will be set to TRUE on the NEW_LEN

WARNING: GND will be changed to TRUE in Table LNINV
on the NEW LEN, same setting as the OLD LEN

Also for CLN, if the NEW_LEN is not a supported line card and the value of GND is different

than the OLD_LEN GND value, the below warning message will be output

**WARNING: GND is FALSE in Table LNINV on the NEW LEN
the setting was TRUE on the OLD LEN**

If the value of GND is the same on the OLD_LEN and the NEW_LEN, no warning message is output.

There are additional line cards that support GND but also require some manual intervention such as a strap or a switch to be toggled in order for the GND to take effect. Attempts to manipulate GND on these type line cards will result in an error message as in releases prior to this feature.

It may be necessary to BSY and RTS the line at the MAP in order for the change in GND value to effect.

41.3 Hardware Requirements or Dependencies

There is no new hardware introduced by this feature. It is limited to the servord commands and linecards aforementioned

41.4 Software Requirements or Dependencies

This is a. SN07 deliverable

41.5 Limitations and restrictions

Servord GND manipulation is limited to the ADO, DEO and CLN commands and to the supported line card types

- 3A06BA
- 7A25AA
- RDTCON
- RDTLSG
- SCD271

Currently, GND can be added via NEW, NEWACD, EST, ADD, EXBEST and EXBADD for lines that can be autopopulated into table LNINV This is not changed by this feature.

41.6 Interactions

If the Servord Redundant feature which is activated by table OFCVAR parameter SO_ALLOW_REDUNDANT_FEATURE is turned off, attempts to manipulate GND on commands or line cards not supported will be rejected. If If this office parameter is turned on, then a warning message will be output that GND will be ignored for non-supported commands and line cards.

41.7 Applicable customer facing sections

Fault Management

- Logs _n/a_____
- Alarms _n/a_____

Configuration

- Data Schema __n/a____
- User Interface __n/a____
- Element Management __n/a____
- Security __n/a____
- Service Order ___X___
- Office Parameters ___n/a___

Accounting (includes AMA billing) __n/a____

Performance (includes operational measurements) __n/a____

41.8 Glossary

Term	Description
GND	GROUND as in GROUND START
MAP	Maintenance Administration Position
BSY	BUSY -Refersto maintenance action at MAP
RTS	Return To Service -Refers to maintence action at MAP

42: Functional Description (FN): A00002558

42.1 Feature name

LDI display for Class phone

42.2 Description

42.2.1 Overview

The Long Distance Indicator (LDI) feature identifies long distance calls and provides the LDI indicator information to the subscriber. The feature works with CND, CNAMD, DDN features that use the Multiple Data Message (MDM) format.

Figure 1 Functional Behavior Diagram

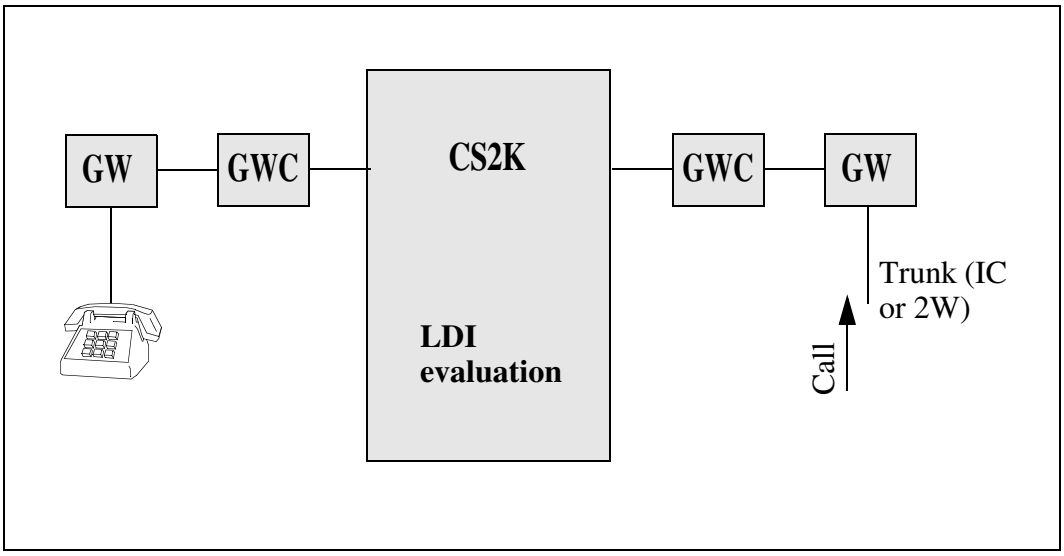


Figure 1 shows an example of an ISN07 office which is a terminating exchange. When a long distance call reaches the subscriber set, LDI evaluates the call. A call is deemed long distance when any of the following condition is satisfied:

- Reverse translation - The dialable DN's first digit is 1 and it has a total of 8 or 11 digits; or
- Table TOLLTRKS - The incoming trunk group CLLI present in table TOLLTRKS.

If a call is deemed long distance, the system delivers the LDI to the line through MGCP. The LDI is delivered as the character L. Following is the message which captured by tool CALLTRAK.

```
OUTGOING  02:07:15.859  NODE TYPE= LCM_NODE
DS512: ENCAP MS_CARD= 6 MS_PORT= 20  NODE= 8216
NN= 0041  TN= 0004  MSGTAG= 00  ROUTE= 2018  ERROR= 00  LENGTH= 30
AGENT= HOST 01 0 00 03    DN 1066020003
80 5F DF 65 00 DE A4 CC 1F 09 39 17 1B 80 19 01 08 30 34 33 30 30 32 30 37 02
0A 31 31 31 31 31 31 31 31 31 31 06 01 4C

00    80  STKI1    5F
02    DF  ASSCH2
03    65  STPIDSCAN
04    00  NOOP
05    DE  SEND
          DST  = TPT_P3
          SRC  = CC
          LEN  = 1F
          FIAT = FIAT_CCCP
               39 17 1B 80 19 01 08 30 34 33 30 30 32 30 37 02 0A 31 31
               31 31 31 31 31 31 31 06 01 4C
```

The LDI is displayed as the example below:

“12345656L Name “ or

“12345656
L Name“

42.2.2 Datafill

42.2.2.1 Reverse translation

The following is an example of how to make a call be deemed as a long distance call through reverse translation:

Table DNREGION

TEST 0 9

Table DNREVXLA

TEST1 0 9 (TEST 0 N N) $

Table CUSTNTWK

GDNTCUST PUBLIC 1 (PUBLIC **TEST1** 11) $ (CLID OFFNET) (RNID OFFNET) $

42.2.2.2 Table TOLLTRKS

If the trunk is datafilled in table TOLLTRKS, the call is deemed as a long distance call too. The following shows an example on how to datafill TOLLTRKS. For more information of this table, please refer to the CN section of this document.

Table TRKGRP
HKISUP IBNT2 0 NPDGP NCRT GDNTCUS2 0 MIDL 0 N
ANSDISC 0 Y N N N N N Y 0 0 N 0 0 0 0 N N N N N N N
N N INTL $

Table TOLLTRKS

HKISUP

42.3 Hardware Requirements or Dependencies

Not applicable

42.4 Software Requirements or Dependencies

Not applicable

42.5 Limitations and restrictions

1. All the limitations and restrictions of feature AG1841CLASS/CMS Long Distance Indicator.

42.6 Interactions

Not applicable.

42.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A

Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

42.8 Glossary

Term	Description
CLASS	Custom Local Area Signaling Services
CLLI	Common Language Location Identifiers
CNA	100 North America
CNAMD	Calling Name Delivery
CND	Calling Number Delivery
DDN	Dialable Number Delivery
LDI	Long Distance Call Indicator
MDM	Multiple Data Message format

43: Functional Description (FN): A00002585

Purpose:This FN described the new feature added to TMM by ACTID00002585 which includes the following new components:

1. Post by Carrier . This component allows TMM to post and perform maintenance actions on trunks based ona specific carriers.
2. Show trunk type. This component enhance the operation "PostByGatewayName" to add trunk type in result.
3. Add online help. This component provide online help for TMM.

Reference: Design Intent DOC (DID) A00002585 (TMM Support PTS Trunk, Post By Carr iers)

43.1 Introduction

This document details the OAM&P functionality being delivered by the feature "TMM Support PTS Trunk, Post By Carrier" (Activity ID is A00002585 and Feature ID is 24651) in SN07. This document will describe the changes being made to the web based GUI and interface via OSSGate.

43.2 Feature name

TMM PTS Trunk Support, Post By Carrier - Activity ID A00002585.

43.3 Description

In SN07, the activity A00002585 will deliver the changes required to extend TMM functionality to support the following:

PTS Trunk maintenance:

1• PTS trunk maintenance will be supported by TMM. All maintenance commands related to ISUP trunk and PRI trunk will be supported for PTS trunk.

Post By Carriers name:

1• In addition to selecting a trunk gateway, user can select a specific carrier name, post trunks and perform all maintenance operations supported by "Maintenance by Gateway Name" today for ISUP, PRI and PTS trunks from GUI and OSSGate.

General TMM Robustness Enhancements:

1• Show trunk types (ISUP, PRI. PTS) in post result sets.

2• Return codes will be kept compliance with OSSGate NTP documents.
3• TMM Help page.

For “PTS Trunk maintenance”, no changes are made on either web based GUI or the interface via OSSGate.

43.4 Web GUI Modifications

This section describes all the changes being made on web based GUI by activity A00002585 in SN07. This section is not meant to be a complete description of the web based GUI. The TMM NTP document will be updated to provide detailes of the changes.

43.4.1 Post By Carrier

A new link “Mtc By Carrer” will be added on TMM main web page. (See Figure 1)

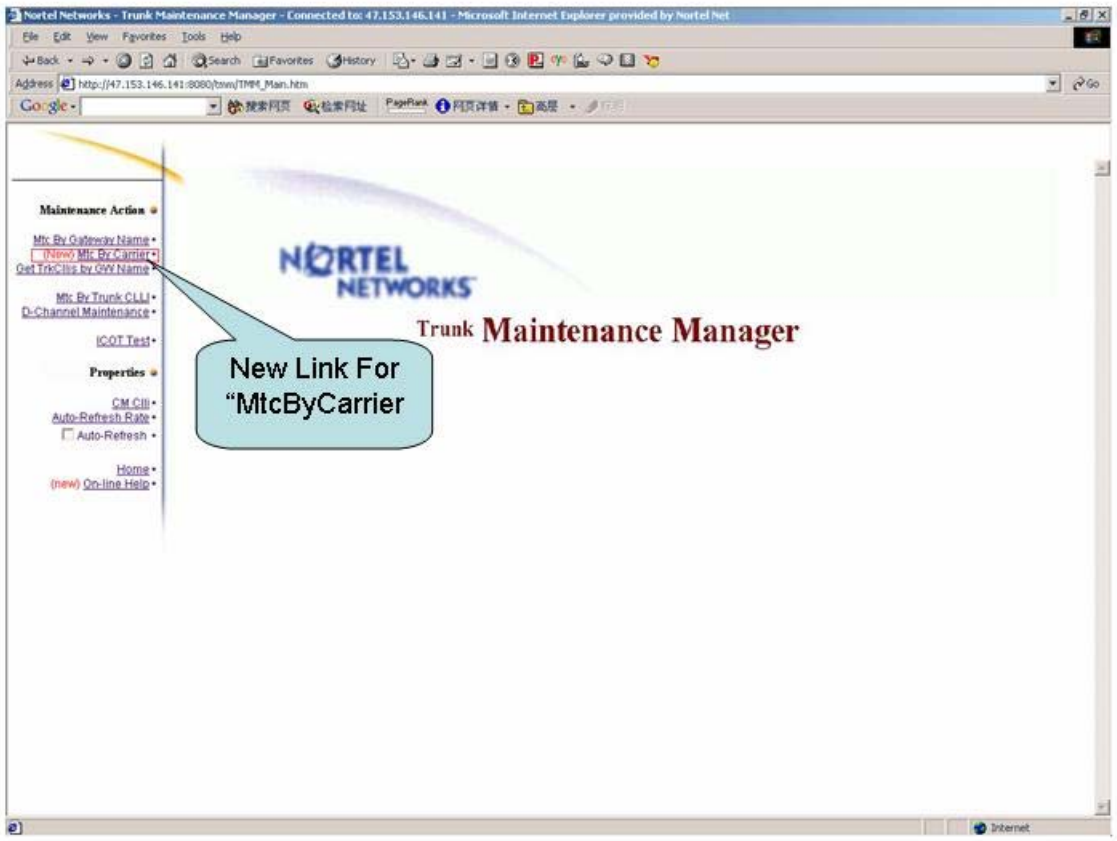


Figure 1

After the link “Mtc By Carrier” is clicked, a web page as Figure 2 will be displayed.

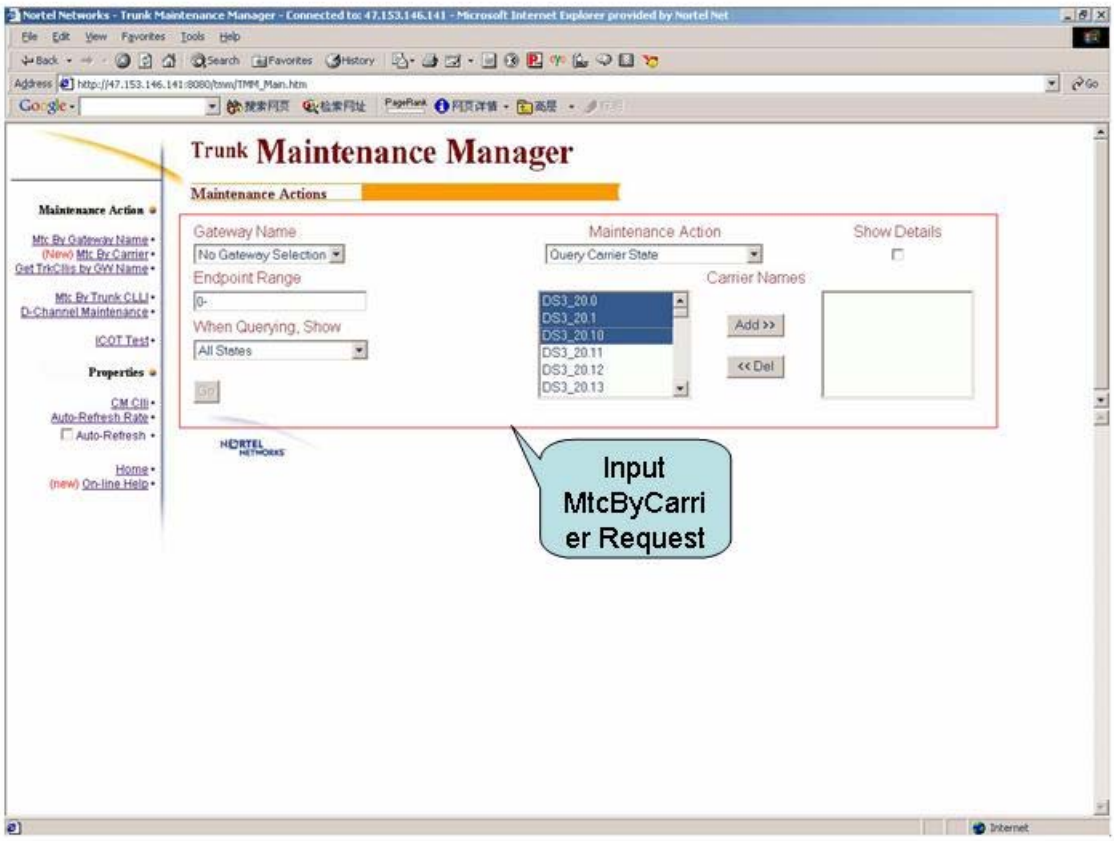


Figure 2

For a valid request “MtcByCarrier”, one and only one gateway should be defined, one and only one action should be defined and at **least** one carrier should be selected.

if no carrier is selected it will post all the carriers.

The gateway will be selected from drop list named “Gateway Names”. the action will be selected from drop list named “Maintenance Action”. The carrier will be selected from list box. After one item in the list box is highlighed, please click button “Add” or “Del” to add or remove carriers from request input. Multiple selection with normal Windowns style is supported. (For example, shift+mouse button, or ctrl+mouse button) (See Figure 3, 4, 5)

There are serveral options for the request “MtcByCarrier”.

- “Endpoint Range”, its default is “0-”.
- “States Filter” which can be selected from the drop list “When Querying, Show”, its default is “All States”.
- “Show Details” which can be set by setting check box “Show Details”, its default is “false”.

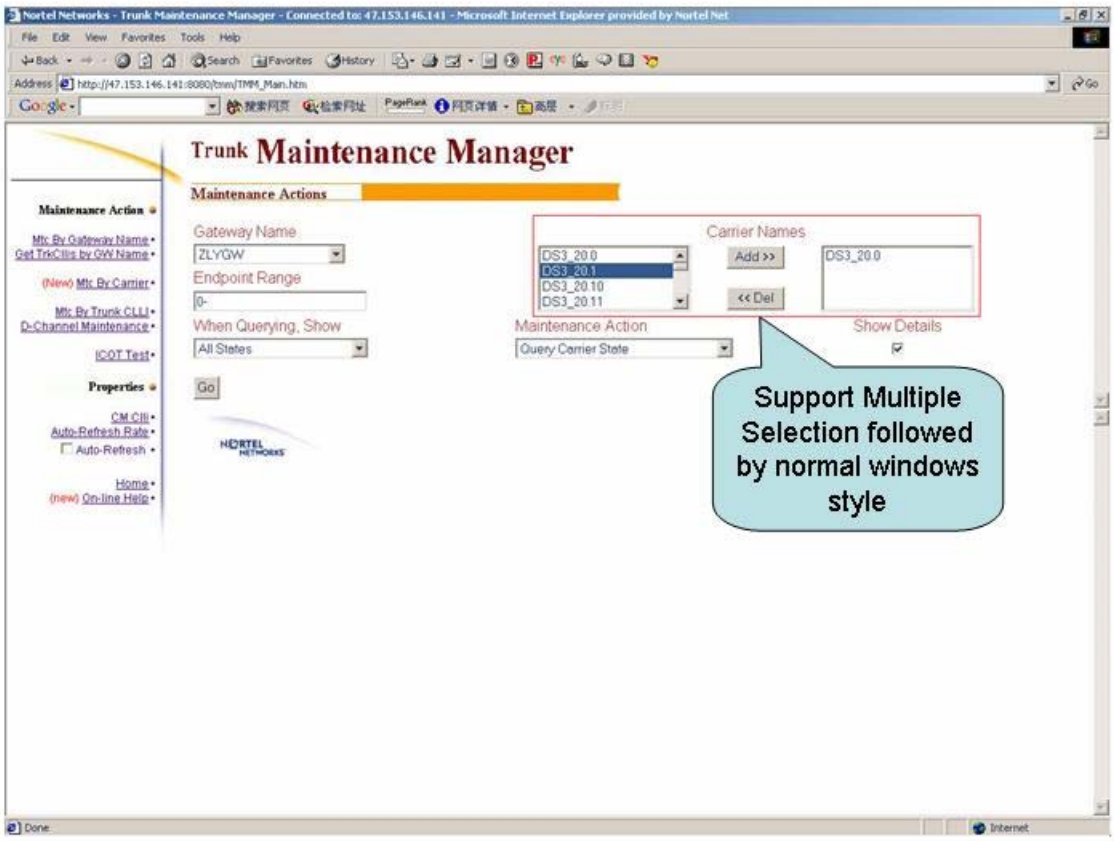

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllls by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Go
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Query Carrier State
Show Details
Support Multiple Selection followed by normal windows style
Done
Internet

Figure 3

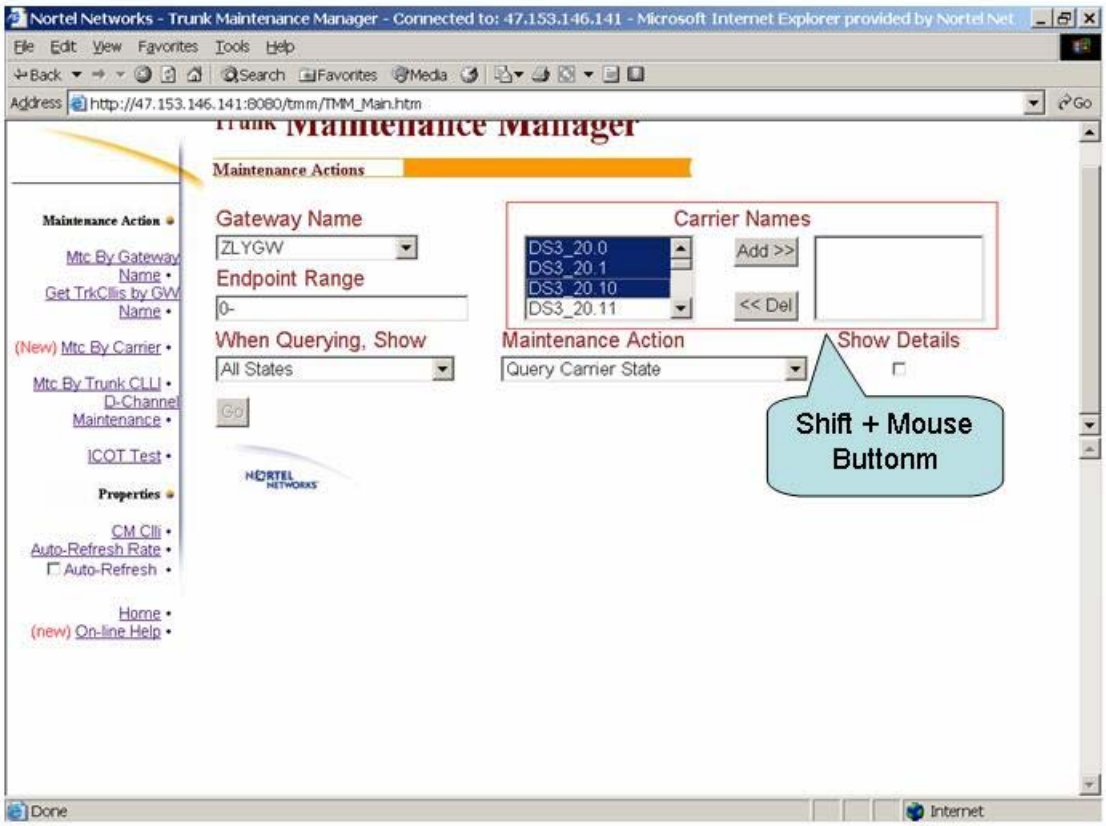

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Go
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllis by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Go
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
Maintenance Action
Query Carrier State
Show Details
Shift + Mouse Buttonm
Done
Internet

Figure 4

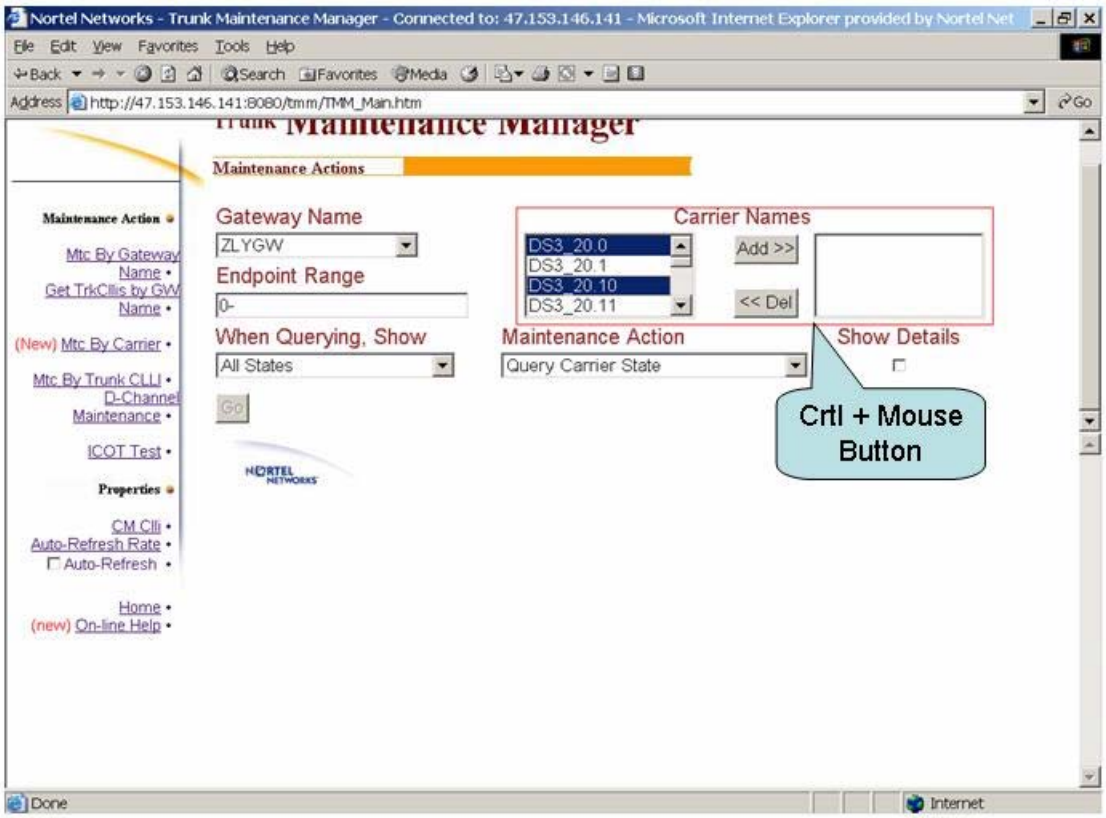


Figure 5

After gateway and carriers are defined, the button “go” will be activated. (See Figure 6). After the button “go” is clicked, the corresponding response will be displayed.

Currently, six commands are supported by “MtcByCarrier”.

- The response for the command “Query Carrier State” is as Figure 7.
- The response for the command “Post Carrier” is as Figure 8.
- The response for the command “Busy Carrier ” is as Figure 9.
- The response for the command “Return Carrier to Services ” is as Figure 10.
- The response for the command “Force Release Carrier” is as Figure 11.
- The response for the command “Installation Busy Carrier” is as Figure 12.

If the command failed, the error messages will be displayed. Please see an example as Figure 13.

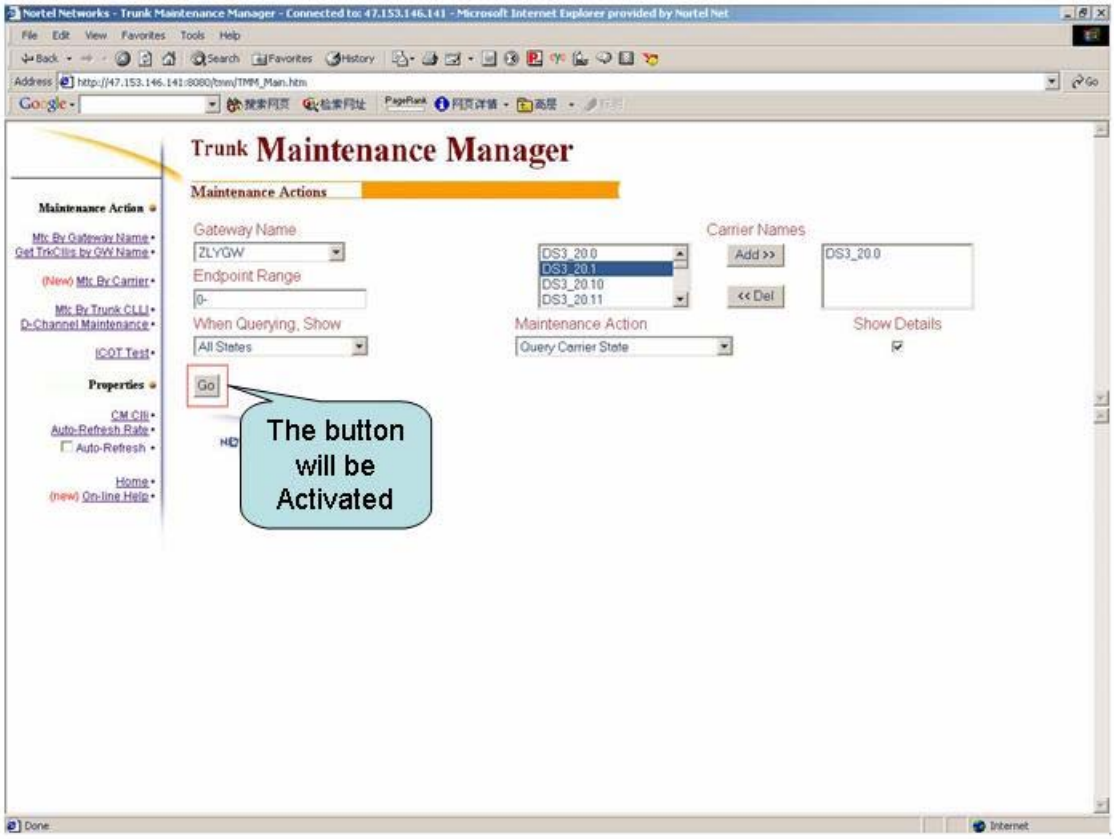

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllls by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Go
Carrier Names
DS3_20 0
DS3_20 1
DS3_20 10
DS3_20 11
Add >>
<< Del
DS3_20 0
Maintenance Action
Query Carrier State
Show Details
The button will be Activated
Done
Internet

Figure 6

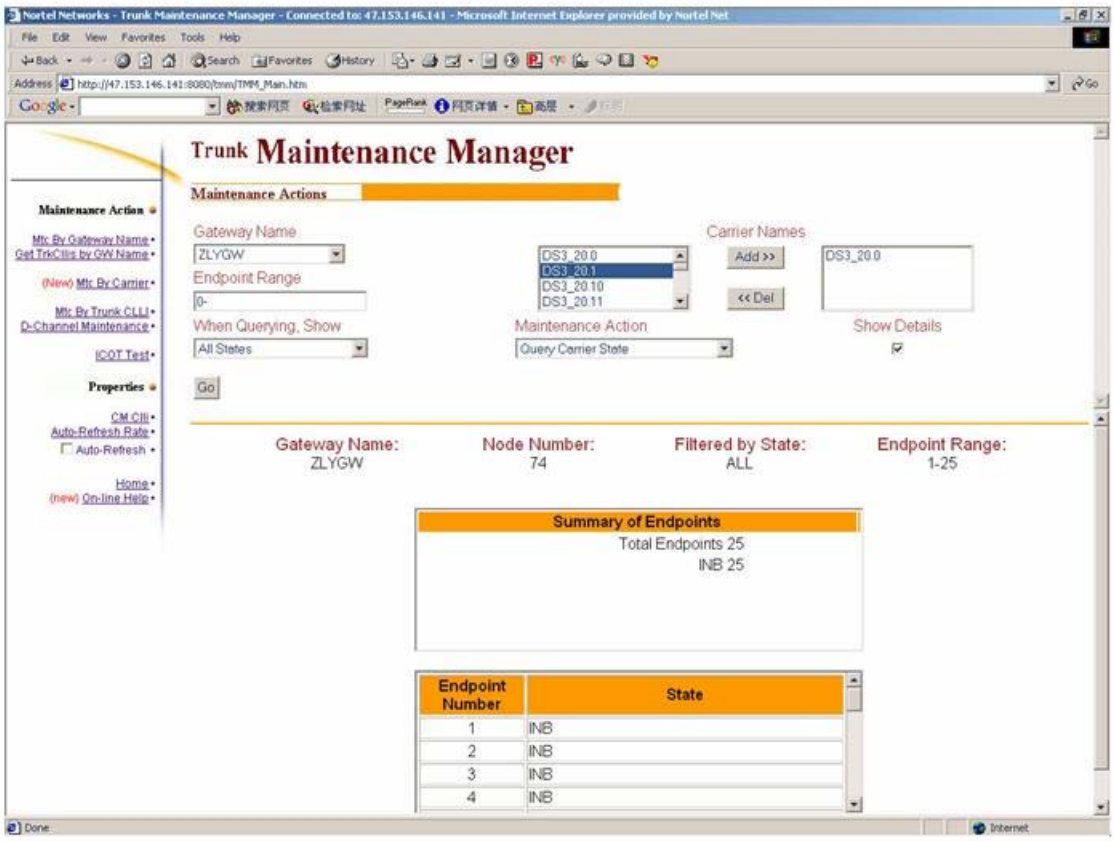

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkClls by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Go
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Query Carrier State
Show Details
Gateway Name: ZLYGW
Node Number: 74
Filtered by State: ALL
Endpoint Range: 1-25
Summary of Endpoints
Total Endpoints 25
INB 25
Endpoint Number
State
1 INB
2 INB
3 INB
4 INB
Done
Internet

Figure 7

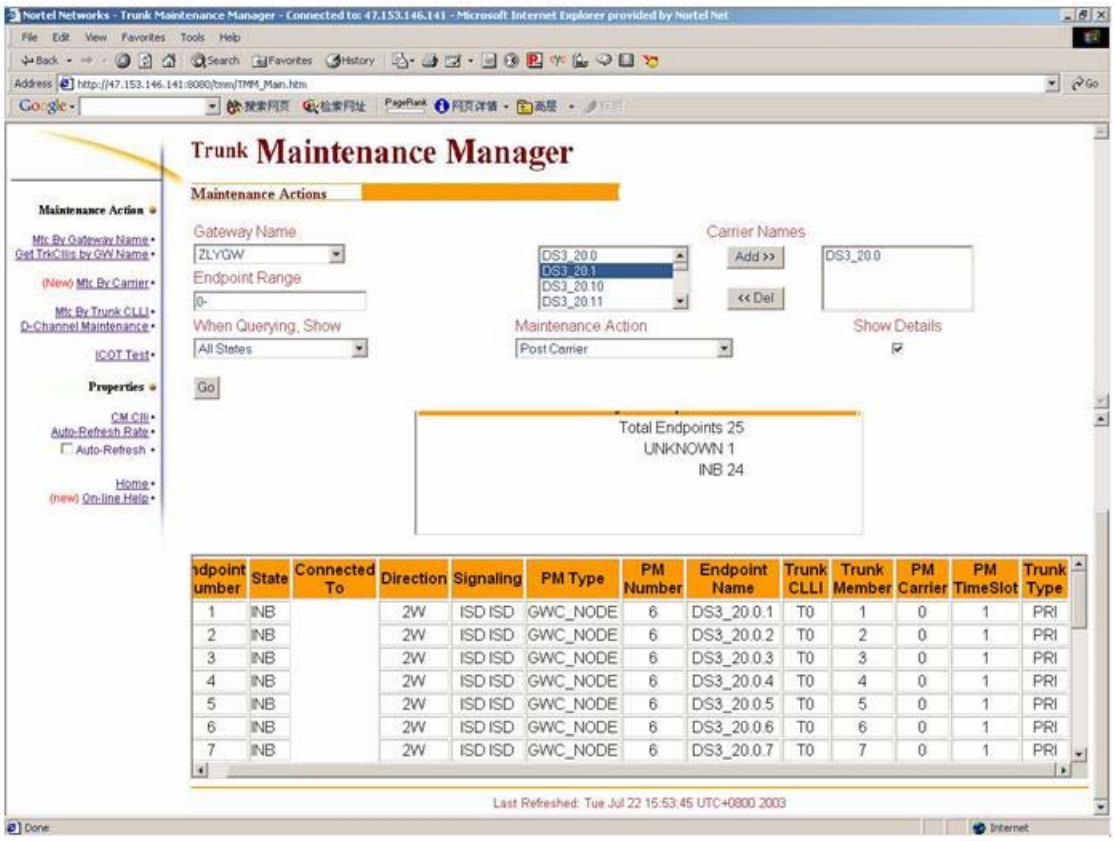

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
Trunk Maintenance Manager
Maintenance Actions
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Post Carrier
Show Details
Go
Total Endpoints 25
UNKNOWN 1
INB 24
Maintenance Action
Mtc By Gateway Name
Get TrkCllis by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Endpoint Number
State
Connected To
Direction
Signaling
PM Type
PM Number
Endpoint Name
Trunk CLLI
Trunk Member
PM Carrier
PM TimeSlot
Trunk Type
1 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.1 T0 1 0 1 PRI
2 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.2 T0 2 0 1 PRI
3 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.3 T0 3 0 1 PRI
4 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.4 T0 4 0 1 PRI
5 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.5 T0 5 0 1 PRI
6 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.6 T0 6 0 1 PRI
7 INB 2W ISD ISD GWC_NODE 6 DS3_20.0.7 T0 7 0 1 PRI
Last Refreshed: Tue Jul 22 15:53:45 UTC+0800 2003
Done
Internet

Figure 8

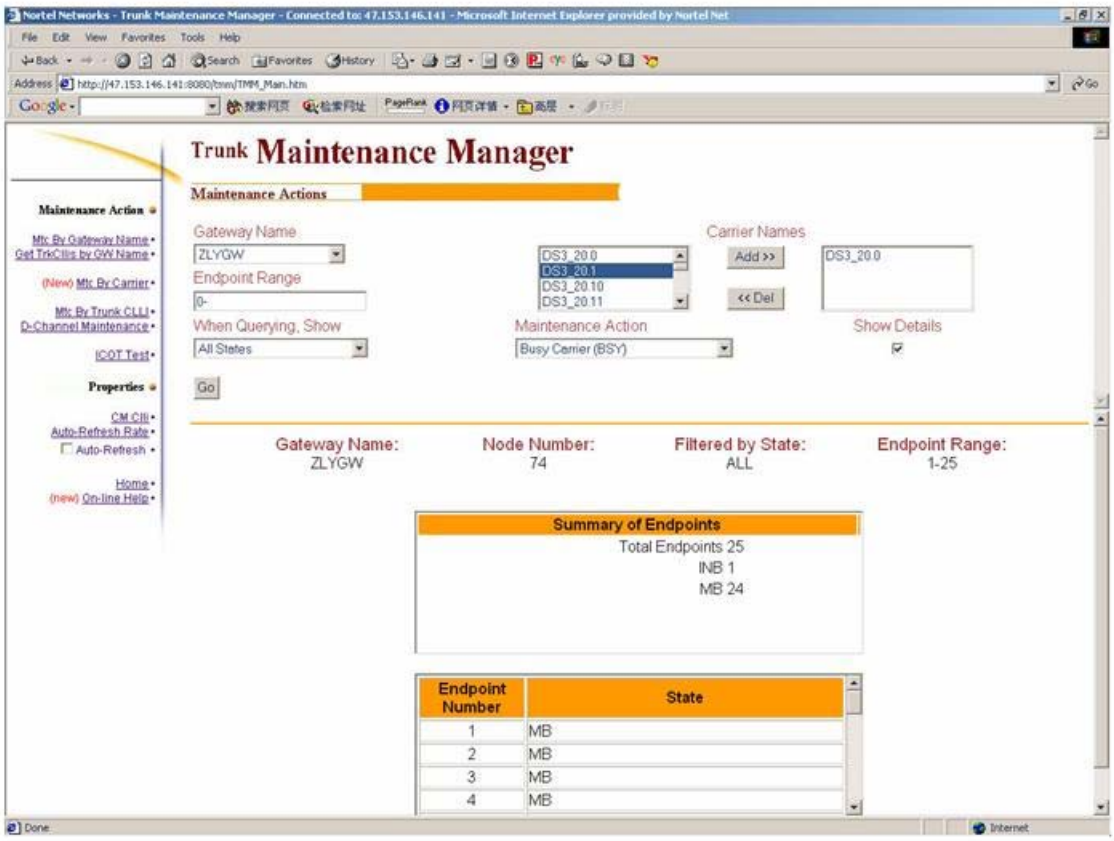

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllis by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Busy Carrier (BSY)
Show Details
Go
Gateway Name: ZLYGW
Node Number: 74
Filtered by State: ALL
Endpoint Range: 1-25
Summary of Endpoints
Total Endpoints 25
INB 1
MB 24
Endpoint Number
State
1 MB
2 MB
3 MB
4 MB
Done
Internet

Figure 9

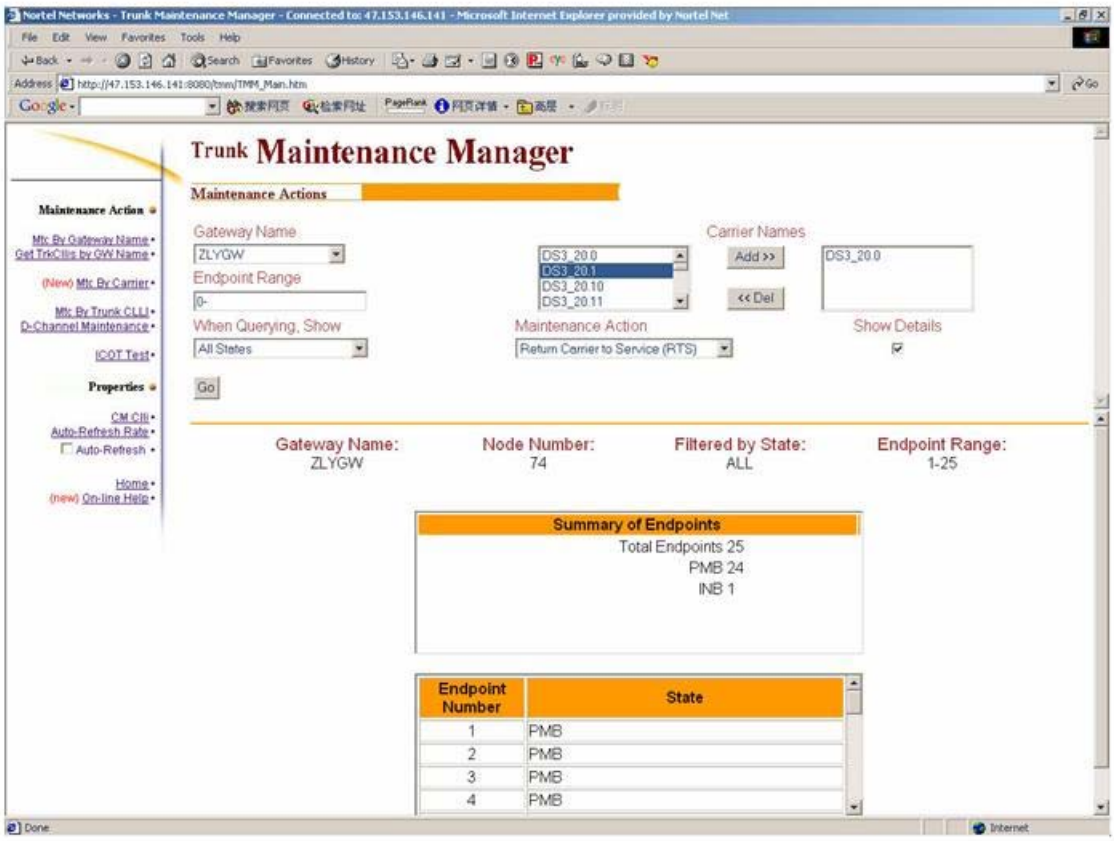

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllls by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Return Carrier to Service (RTS)
Show Details
Go
Gateway Name: ZLYGW
Node Number: 74
Filtered by State: ALL
Endpoint Range: 1-25
Summary of Endpoints
Total Endpoints 25
PMB 24
INB 1
Endpoint Number
State
1 PMB
2 PMB
3 PMB
4 PMB
Done
Internet

Figure 10

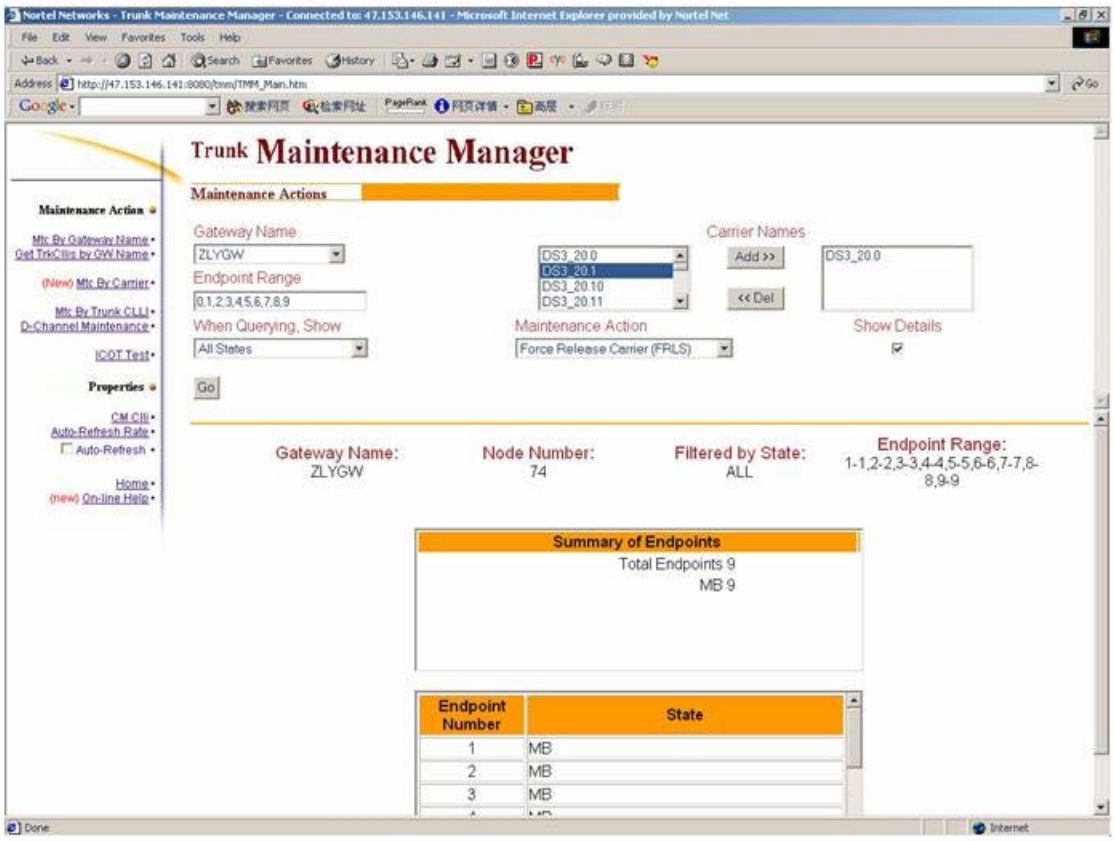

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkClits by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0,1,2,3,4,5,6,7,8,9
When Querying, Show
All States
Go
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Force Release Carrier (FRLS)
Show Details
Gateway Name: ZLYGW
Node Number: 74
Filtered by State: ALL
Endpoint Range: 1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9
Summary of Endpoints
Total Endpoints 9
MB 9
Endpoint Number
State
1 MB
2 MB
3 MB
Done
Internet

Figure 11

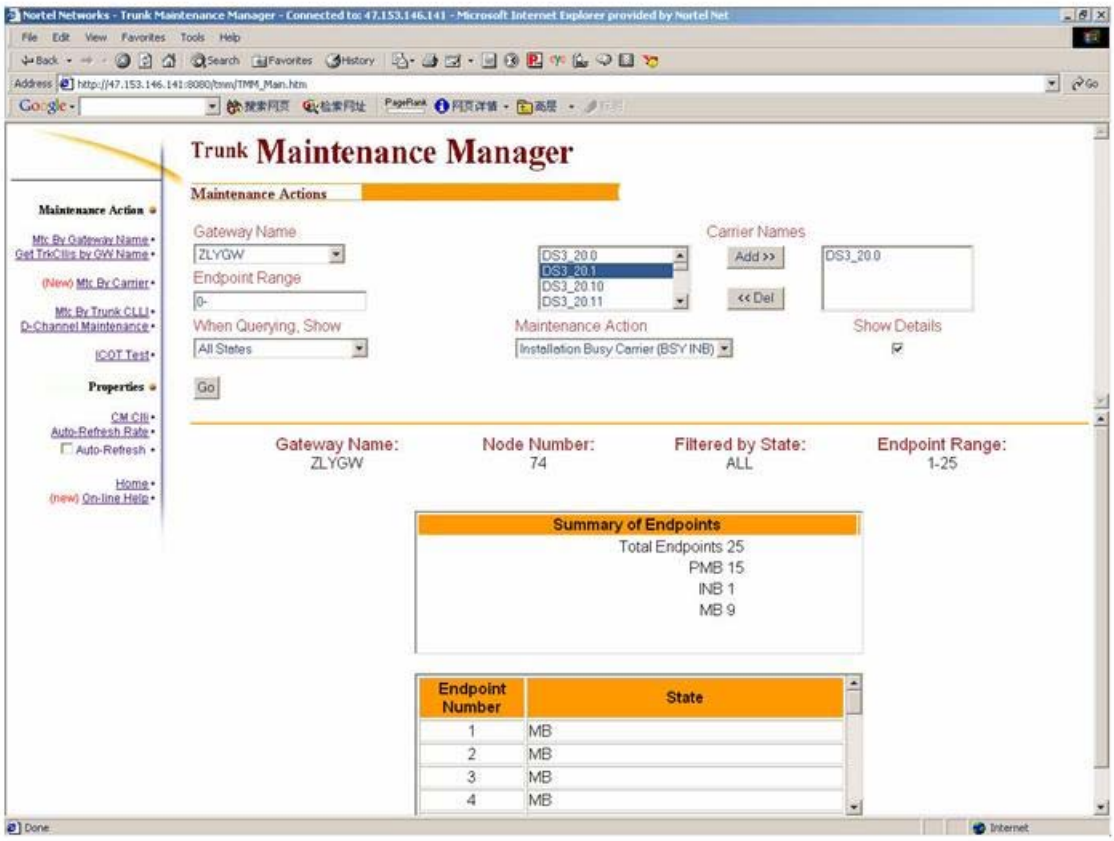

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllls by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
0-
When Querying, Show
All States
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Installation Busy Carrier (BSY INB)
Show Details
Go
Gateway Name: ZLYGW
Node Number: 74
Filtered by State: ALL
Endpoint Range: 1-25
Summary of Endpoints
Total Endpoints 25
PMB 15
INB 1
MB 9
Endpoint Number
State
1 MB
2 MB
3 MB
4 MB
Done
Internet

Figure 12

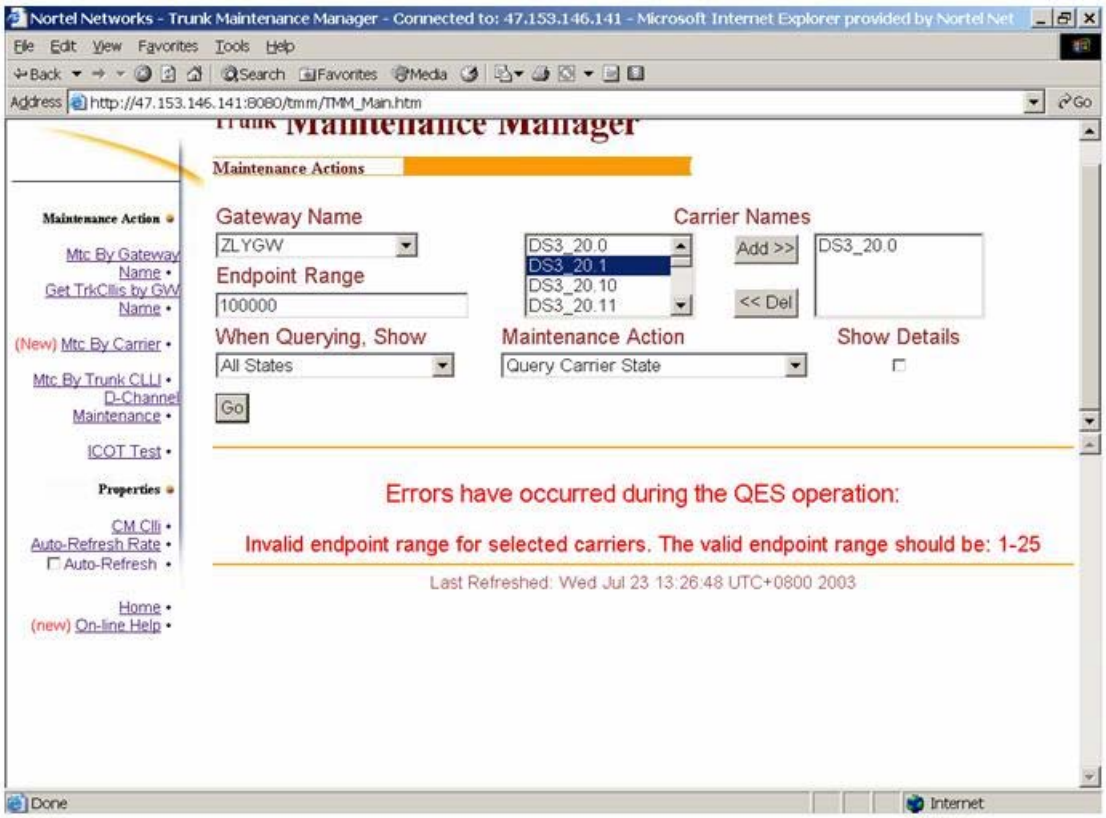

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Go
Trunk Maintenance Manager
Maintenance Actions
Maintenance Action
Mtc By Gateway Name
Get TrkCllis by GW Name
(New) Mtc By Carrier
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
Gateway Name
ZLYGW
Endpoint Range
100000
When Querying, Show
All States
Go
Carrier Names
DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11
Add >>
<< Del
DS3_20.0
Maintenance Action
Query Carrier State
Show Details
Errors have occurred during the QES operation:
Invalid endpoint range for selected carriers. The valid endpoint range should be: 1-25
Last Refreshed: Wed Jul 23 13:26:48 UTC+0800 2003
Done
Internet

Figure 13

43.4.2 Show trunk types in post result set

For the command “Post By Gateway” with the option “Show Details” to be set (See Figure 14), the corresponding response will include trunk type. (See Figure 15).

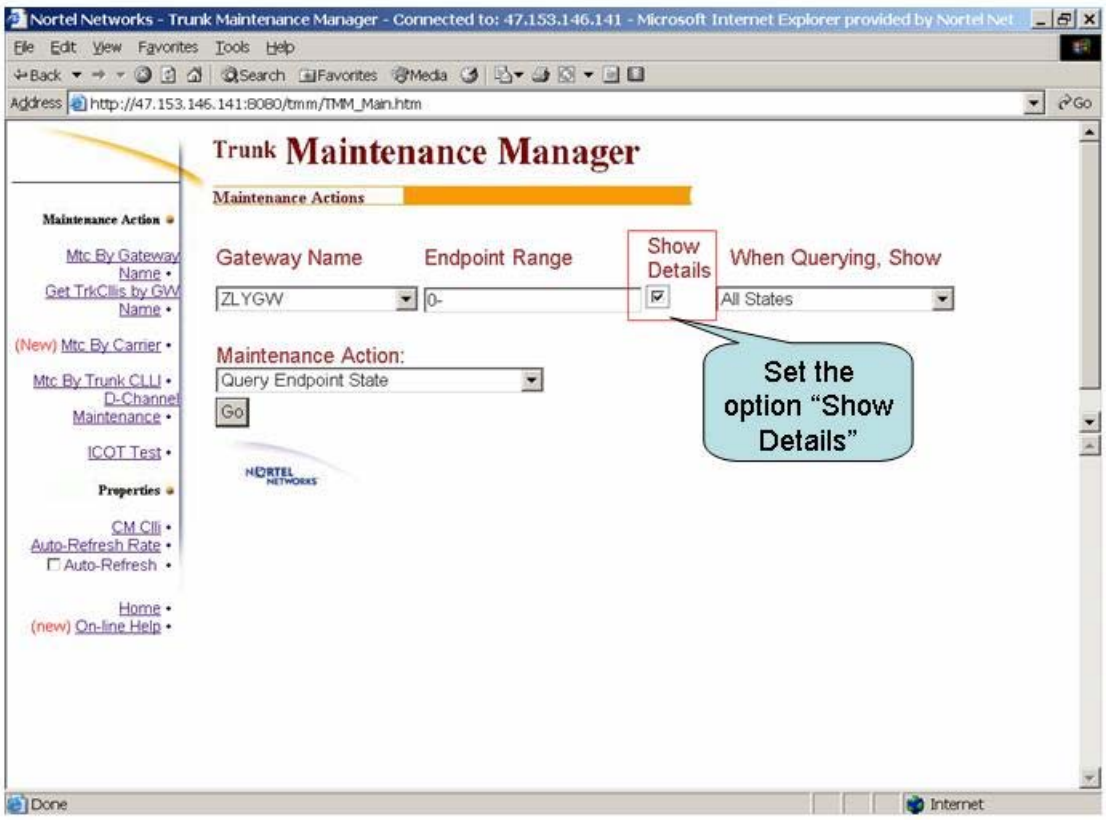
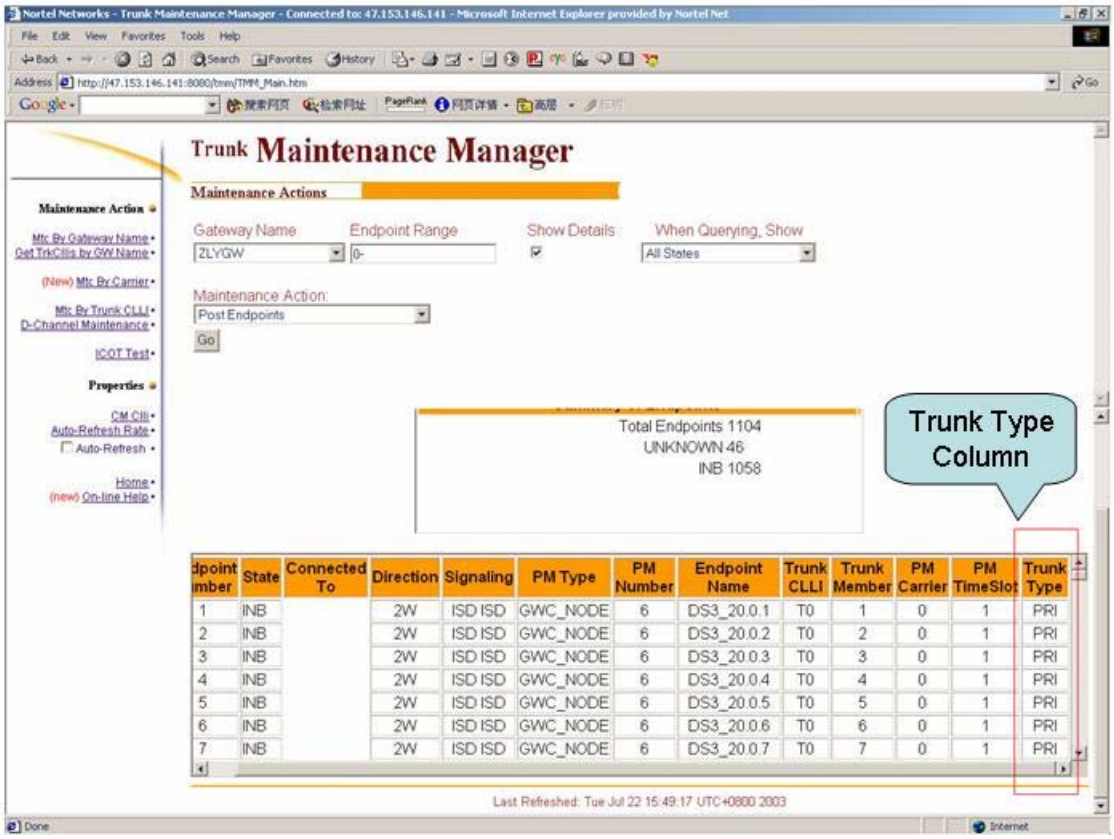


Figure 14



dpoint imber	State	Connected To	Direction	Signaling	PM Type	PM Number	Endpoint Name	Trunk CLLI	Trunk Member	PM Carrier	PM TimeSlot	Trunk Type
1	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.1	T0	1	0	1	PRI
2	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.2	T0	2	0	1	PRI
3	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.3	T0	3	0	1	PRI
4	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.4	T0	4	0	1	PRI
5	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.5	T0	5	0	1	PRI
6	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.6	T0	6	0	1	PRI
7	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.7	T0	7	0	1	PRI

Figure 15

43.4.3 Adding TMM Help

A new link will be added on TMM web page. (See Figure 16). After the link is clicked, a help window including help web page will be popped out. (See Figure 17).

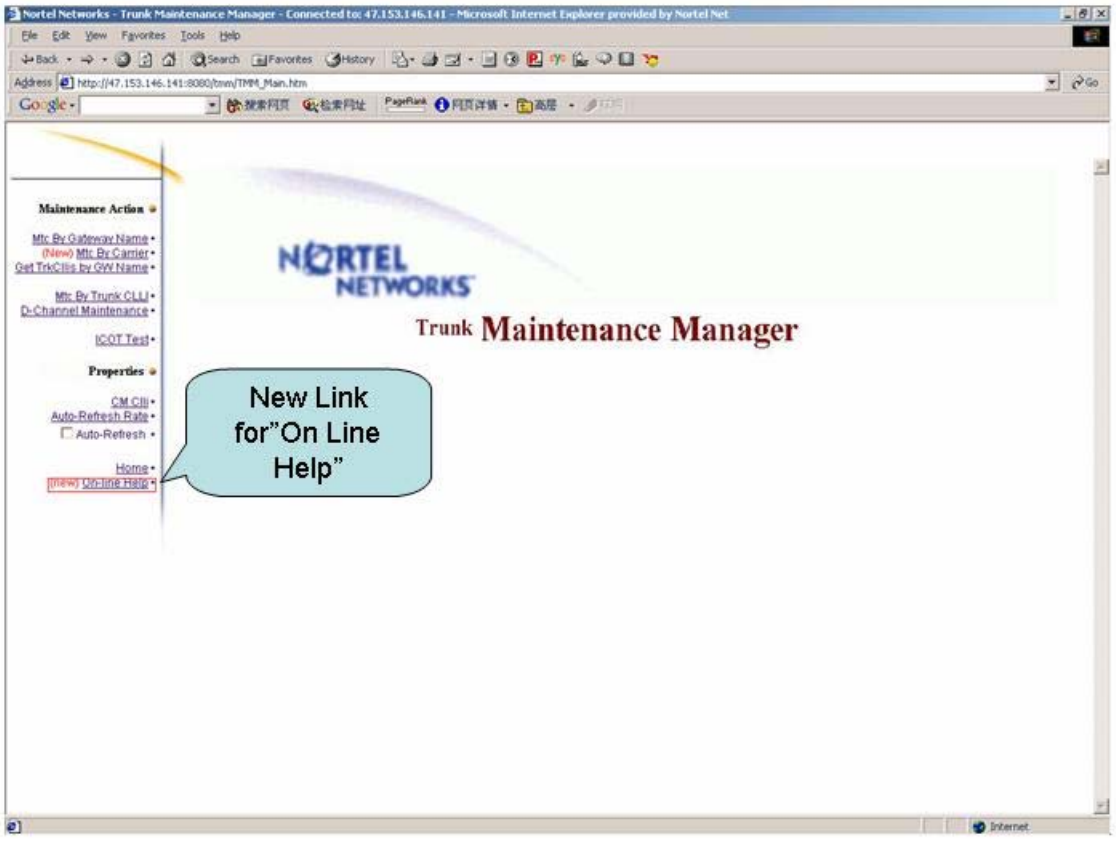

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Address http://47.153.146.141:8080/tmm/TMM_Main.htm
Maintenance Action
Mtc By Gateway Name
(New) Mtc By Carrier
Get TrkClls by GW Name
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Cli
Auto-Refresh Rate
Auto-Refresh
Home
(new) On-line Help
NORTEL NETWORKS
Trunk Maintenance Manager
New Link for"On Line Help"
Internet

Figure 16

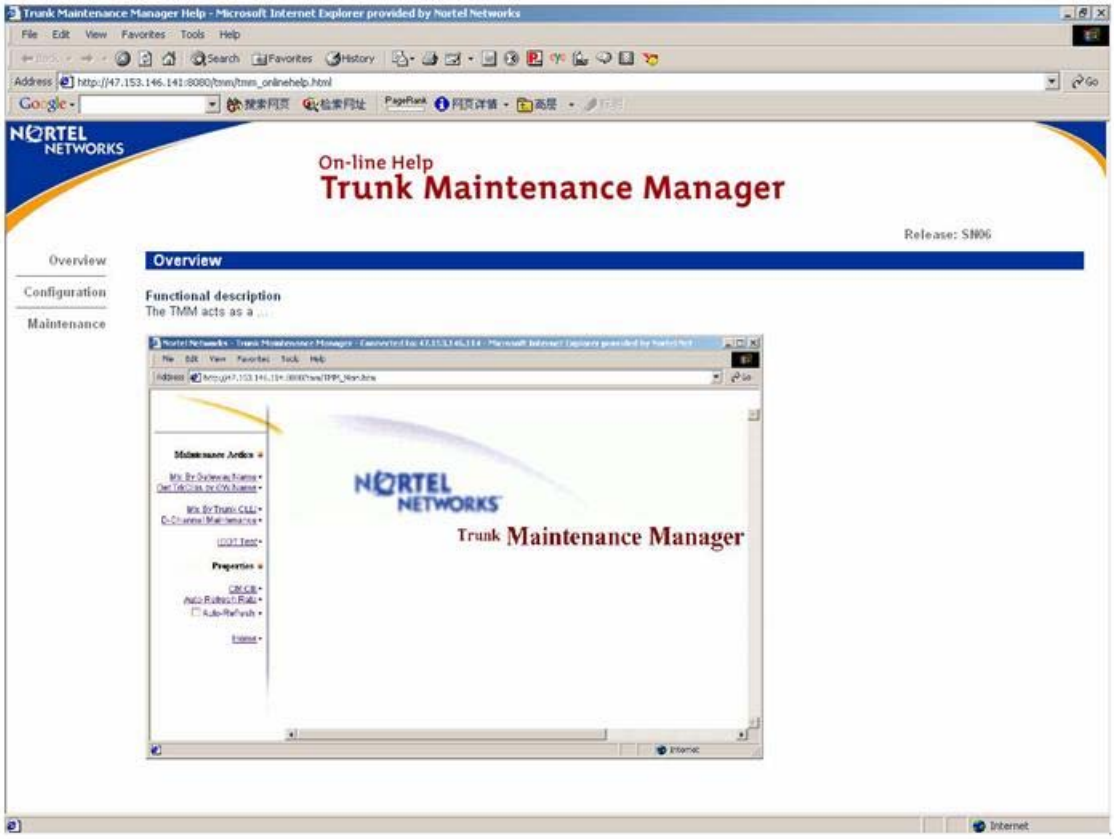


Figure 17

43.5 Hardware Requirements or Dependencies

Not Applicable.

43.6 Software Requirements or Dependencies

Not Applicable.

43.7 Limitation and Restrictions

Not Applicable.

43.8 Interactions

Not Applicable.

43.9 Applicable customer facing sections

Fault Management

Logs	N/A___
Alarms	N/A___

Configuration

Data Schema	N/A___
User Interface	X_____
Element Management	N/A___
Security	X_____
Service Order	N/A___
Office Parameters	N/A___

Accounting (includes AMA billing)	N/A___
Performance (includes operational measurements)	N/A___

43.10 Glossary

Not Applicable.

43.11 References

Please refer to the document on http://ptm.

43.12 Appendix A

This document “TMM_A0002585_Commands_Responses_Errors.fm” on http://ptm describes the changes being made to the interface via OSSGate by activity A00002585 in SN07. Please refer to document “TMM_A0002585_Commands_Responses_Errors.fm” for all examples of changes.

44: Functional Description (FN): A00002607

44.1 Feature name

A00002607 - ABI XPM SITE and MG9K Location support

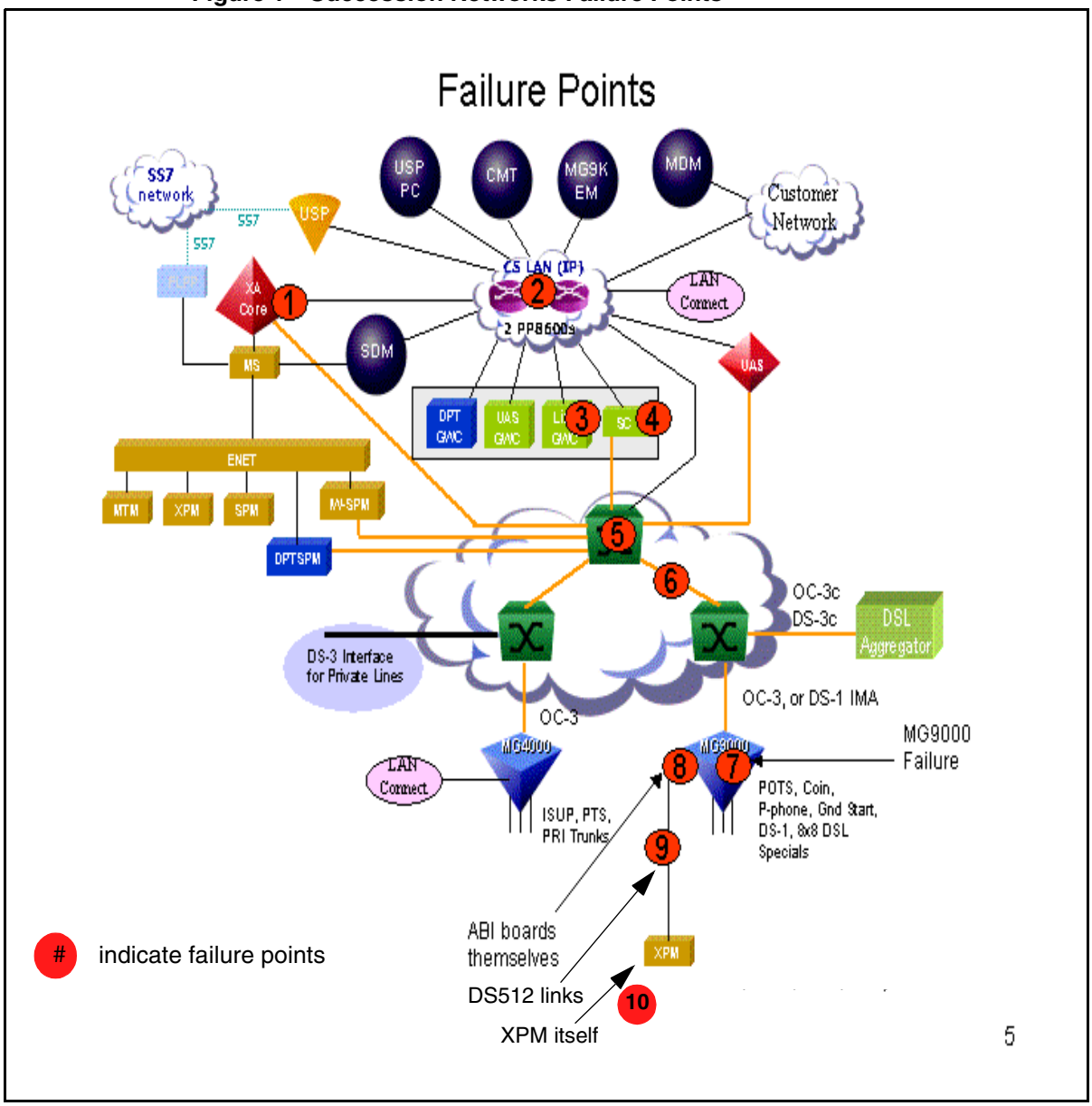
This is a Core feature available in both the SN07 release and in the SN06.2 release via patches.

44.2 Description

The purpose of this feature is to provide physical location data to aid in the determination and ultimately the resolution of ABI XPMs out of service conditions and native MG9K line troubles on the Core where applicable.

Currently, these service impacting failures can occur in many different points in the Succession networks. Please refer to Figure 1 on page 408.

Figure 1 Succession Networks Failure Points



The ability to identify MG9Ks involved in the ABI configurations and MG9K frames hosting native H.248 lines and their physical location was not easily determined.

This feature will aid in identifying the failure points detectable by the Core by providing necessary and accurate location data. Then using this newly provisioned data to correctly report and identify problem areas in the form of Logs, OMs, and Mapci commands.

In order to provide these new functionalities, the customer will see changes in the following areas:

- operation of Table LTCINV
- operation of Table LGRPINV

44.2.1 Table LTCINV Impacts

The identification of MG9K Gateways and ABI cards involved in ABI configurations is accomplished by provisioning this data in the modified ABI optional field in table LTCINV. For details on what/how this is provisioned, refer to Table LTCINV Database Schema information in the configuration section of this feature. No other changes have been made to the table.

44.2.2 Table LGRPINV Impacts

The identification of MG9K Frame and its physical location is accomplished by provisioning this data in the new Location optional field in table LGRPINV. Physical location information is maintained on a SITE/FRAME/SHELF granularity. For details on what/how this is provisioned, refer to Table LGRPINV Database Schema information in the configuration section of this feature. No other changes have been made to the table.

44.3 Hardware Requirements or Dependencies

There is no hardware dependencies required to execute this feature.

44.4 Software Requirements or Dependencies

This feature requires the Core load to be a Succession load. Specifically Succession release SN07 or later. Also, Succession release SN06.2 with this feature patches applied is also a valid configuration.

44.5 Limitations and restrictions

The ABI XPM location data is only be applicable to the XPMs which are datafilled in table LTCINV with the ABI (i.e. EXTDS512) option. Because of this restriction, the ABI XPM location data can only be datafilled after Legacy XPMs have been Upgraded to the ABI configurations.

For MG9K native lines, the SESM provisioning of this MG9K Frame location data will not auto populate the same data in LGRPINV. Therefore manual datafilled of this data in table LGRPINV via the Core is required. There are plans to have this flow through in a future release.

The Gateway Frame location data is optional however, there must be a Logical Group defined on the Core in table LGRPINV to have the possibility to

provision this physical location data. MG9K's which have no native lines, MG9Ks configured with ABI XPMs only, have no Logical Group representation in table LGRPINV and therefore have no physical location data available on the Core. The location data for these MG9K's are available on the MG9K-EM via the Network Element number, part of the newly provided ABI XPM location data, datafilled in table LTCINV. To obtain the location data of the ABI MG9K given the Network Element Number, the craftsperson would take the following steps:

1. Post the peripheral at the PM level of the map and execute the Querypm command. This provides the Network Element number for the MG9000 that host the peripheral.
2. Launch the MG9000 Element Manager.

   The MG9000 Element Manger will open with the Subnet View. This view shows all the MG9000 elements that have been configured for this Call Server. Each MG9000 has a unique Element Number per Call Server. This number is displayed below the Network Element icons in brackets ([ ]).
3. Find the MG9000 with the Network Element number that matches the Network Element number provide by the Querypm command from step 1.
4. Double click on the element to pull up the Element Frame View.
5. From the Element Frame View, under the "Actions" pull-down menu, select "Provision Frame Location Information". This will display the Frame Location View window that contains the desired information.

   Note: The Frame Location information for the MG9K is data that must be entered by the craftsperson manually. It is usually recommended that this information be datafilled when the element is commissioned/discovered in the element manager.

44.6 Interactions

The following are the feature interactions for this feature:

- Features which this feature is dependant on:
  - — none
- Features which are dependent on this feature:
  - — A00002746 - ABI XPM Fault Isolation / QueryPM
    This feature will use the ABI XPM MG9K hosting data provisioned by this feature.
- Features which have an interaction with this feature:
  - — A00002704 - MG9K EM Frame Location (Site and Frame Number)
    This interaction is not functional (i.e. the data is not feed to the Core from the 9K) but takes the form of common location data between the two components.

44.7 Applicable customer facing sections

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with "N/A" if these sections do not apply to this functionality.

Fault Management

- Logs ___X___
- Alarms ___n/a___

Configuration

- Data Schema ___X___
- User Interface ___n/a___
- Element Management ___n/a___
- Security ___n/a___
- Service Order ___n/a___
- Office Parameters ___n/a___

Accounting (includes AMA billing) ___n/a___

Performance (includes operational measurements) ___n/a___

44.8 Glossary

Term	Description
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512. These XPMs are physically connected to MG9K Gateways via a DS512 interface.
Upgraded	A process where existing DMS ENET/JNET based XPMs have been converted to the ABI networks on the same DMS.
Core MG9K Gateways	These MG9K Gateways are represented in Core as Logical Groups with a GRPTYPE of "S". MG9K Logical Groups are auto-datafilled in Table LGRPINV from SESM Gateway provisioning.

45: Functional description (FN): A00002739

45.1 Feature name

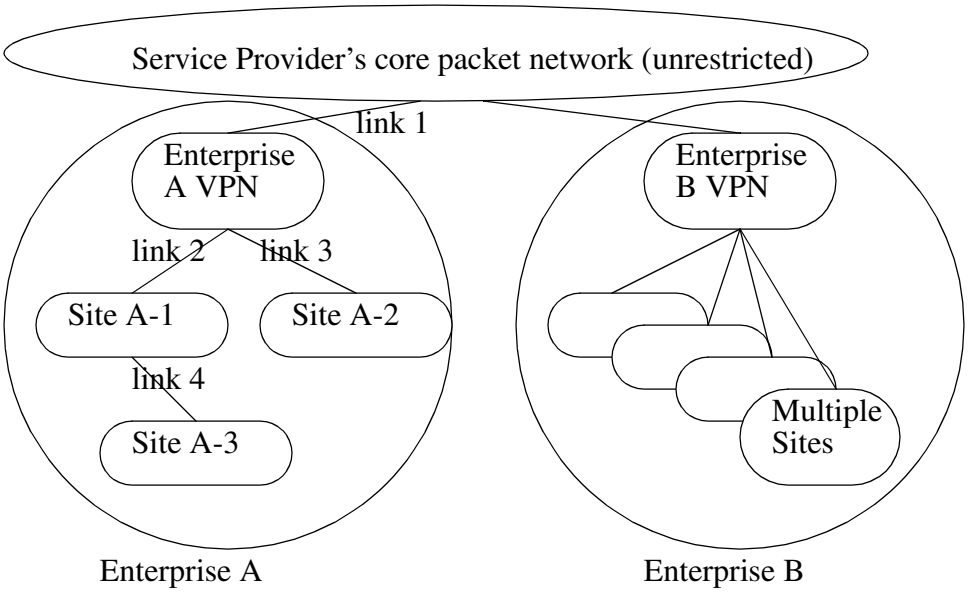
Virtual Call Admissions Control (VCAC) on Communication Server 2000.

45.2 Description

Virtual Call Admissions Control (VCAC) is a Quality of Service (QoS) mechanism that allows the Communication Server 2000 (CS 2000) to cancel post-dial, pre-ringing calls that would overload a segment of the packet network. A very high level description follows:

VCAC depends on a logical model of the packet network. This starts with the Service Provider's core packet network and points of bandwidth concentration. These could, for example, be customer enterprises that are made up of a collection of sites or a regional broadband agreggation point. These sites are connected by a mix of Limited Bandwidth Links (LBLs) and NATs. The VoIP GWs and hence the lines are located within the sites in each enterprise.

Figure 1, High level view of a sample VCAC topology



The logical model that VCAC uses is based on the links between the sites. The GWs are described as being behind or below a particular link. So, in Enterprise A in Figure 1, A GW in Site A-3 is behind link4, which is behind link2, which in turn is behind link 1.

Each of these links will be either a Limited Bandwidth Link (LBL) or a NAT. The LBLs have a provisioned level of resources available and know how many resources each call type consumes. NAT traversal was handled in Feature ACT.89007980 in SN06.

Once a call is made, the CS 2000 identifies the LBLs and NATs along the speech path between the two endpoints, and calculates if there are sufficient resources available on all the LBLs not to exceed the provisioned limits. If all the LBLs can handle the new call, then the call progresses as normal. If one or more LBLs cannot handle the call the originator receives a treatment provisioned by the carrier. The terminator has not reached a ringing stage so is unaware of the call attempt.

An example would be a call between a GW in Site A-3 and Site A-2. This call will use resources on links, 2, 3 and 4, but not on link 1 as the call doesn't leave the enterprise. An insufficient resources failure on any of the links will result in the call going to treatment.

The provisioning of this activity is described in Activity ACT.A00002512, GWC-EM Internet Transparency VCAC Provisioning.

Detailed description

The Logical Network Model
VCAC requires an operator to create a logical model of their network, made up of Limited Bandwidth links (LBL) and NATs. NAT traversal was added in ACT.89007980 in SN06, so the remainder of this description will focus on LBLs.

A LBL can represent a physical part of the network that has a bandwidth restriction (e.g. an ADSL line running at 600kbs) or a logical 'QoS point' (e.g. a customer has purchased a maximum of 1Mb/s of simultaneous VoIP calls). Each LBL has the following set of properties:

- Resource Usage Factor (RU Factor)- This is a provisioned look-up that turns the codec (G711A, G729, etc.) and packetisation rate (ptime) (10/20 ms) into how much resources that call will use on that middlebox.

Note: The term 'resource', rather that bandwidth is used because the value may be normalised, or an engineering factor may be applied to increase/ decrease the value away from the real 'bits on the wire' value. This also allows a customer to simply count calls on a LBL (all codec/ptime pairs use 1 unit of resource).
Note: The resource usage is per LBL not common across the whole network because is can relate to a real network element. E.g. for VoIP, a layer 3 value for a codec/ptime pair will be consistent across the network, but the layer 2 values will vary - i.e. ethernet vs. ADSL (which is ATM based).

- Maximum Count - This is the maximin amount of resources on the LBL in the same units the RU Factor is in.

The logical network model is a tree structure made up of LBLs and NATs according to the following rules (a generic term used to represent a LBL or NAT is middlebox (MB)):

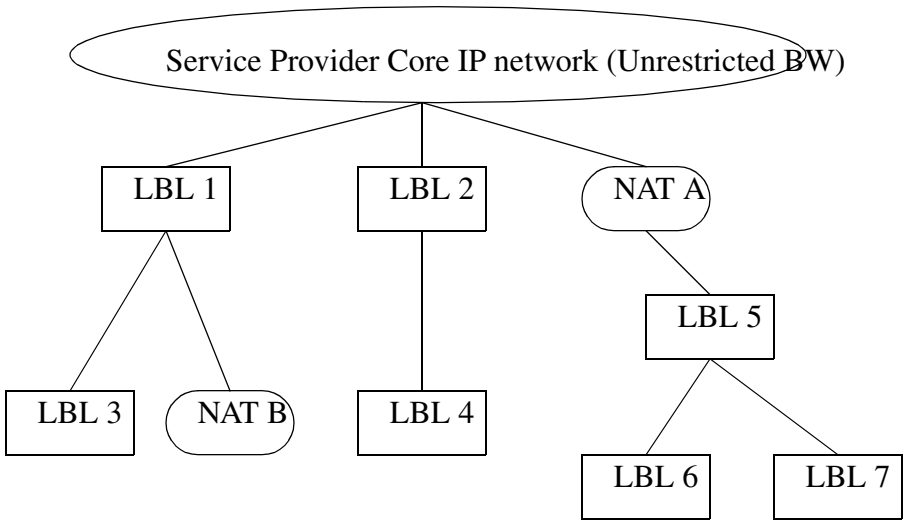
- A MB can be either a LBL or NAT.
- A top level MB must be connected to a non-bandwidth constrained ‘core network’.
- A MB can have only one parent MB (closer to the core network) or the core network.
- A MB can have any number of children (subject to the maximum number of MBs that may be datafilled per GWC).

These rules mean that:

- There can be no circular network paths.
- There can only be one route from a particular MB back to the core network

This logical model of the network must contain the key connectivity routes in the modeled network. E.g. If a set of duplicate routes exist between 2 MBs they must be modelled as one link, not two as otherwise the VCAC capacity counting will not be accurate.

Figure 2, Sample VCAC network model



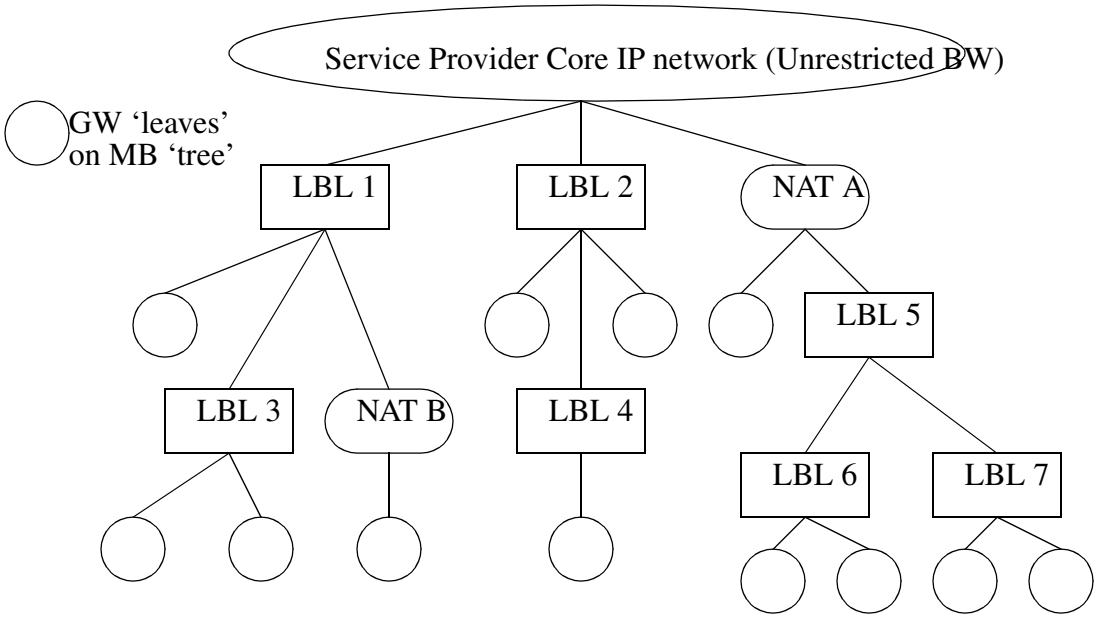
Adding GWs to the Model

GWs can be added to any MB in the logical model. A MB can have any number of GWs hanging off it. This is usually described as having GW 'leaves' on the MB 'tree'.

Note: PVG and UAS/AMS GWs are assumed to be within the core network. Similarly, SIP-T trunks are assumed to start/finish in the core network

This means that any GW will have a single path through the model to the core network, and to any other GW that is within the model.

Figure 3, GWs attached to the MB network model



VCAC

VCAC works by calculating the path between the originating and terminating GWs, looking at the negotiated codec and ptime for the call and checking that each LBL in the path has sufficient resources for the call to be set up. If so, the call proceeds as normal, if not the call is released and a user provisionable treatment (which must be a tone) is applied to the originator. The terminator has not reached a ringing stage.

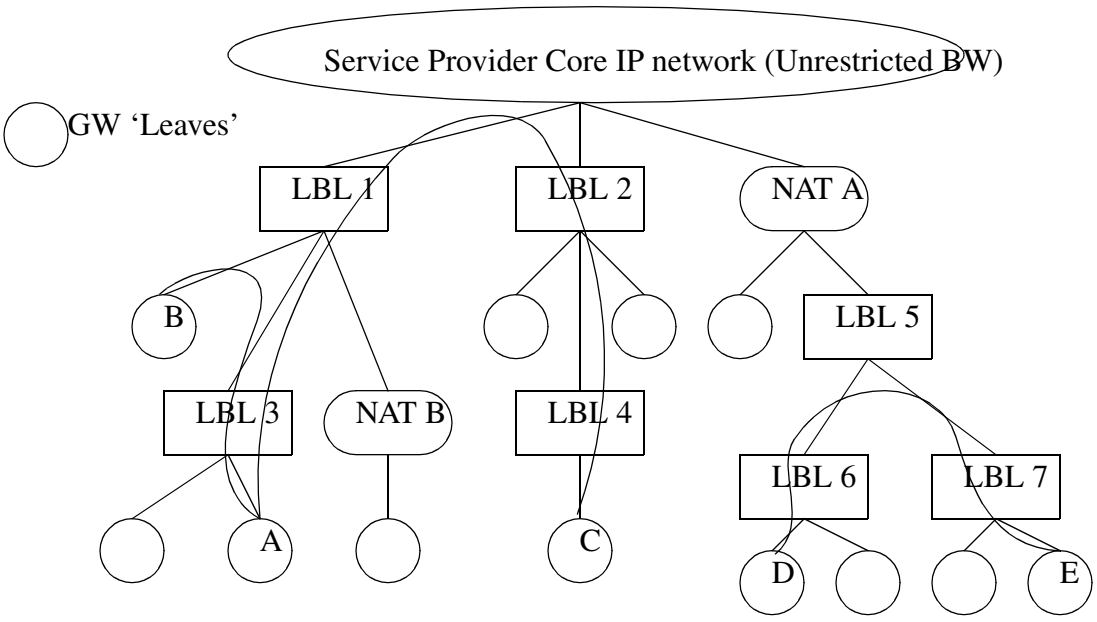
Note: VCAC uses the real, negotiated codec for the call. There are exception for certain call types (e.g. fax, modem) that are detailed below.

Note: Only the MBs on the path are used - resources are not always used all the way to the core network if there is a shorter route through the network.

For example in Figure 4 below:

- An A-to-B call uses resources on LBL 3. LBL 1 is not used event though it a part of the MB chain as the path between the GWs does not use it.
- An A-to-C call uses resources on LBL 3, LBL 1, LBL 2 and LBL 4. All the MBs in the originator and terminator chains are on the GW path.
- A D-to-E call uses resources on LBL 6 and LBL 7. They are both behind the same NAT so no Media proxy is required.

Figure 4, VCAC path finding

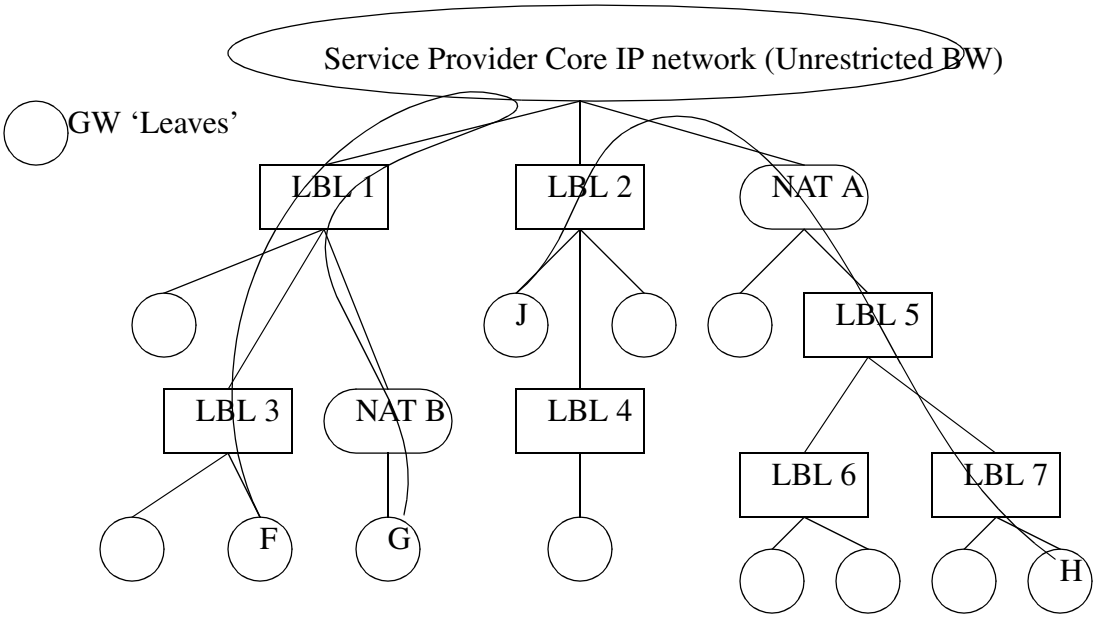


If there is a NAT MB on the call path then the call must extend as far as a Media Proxy (MP) (as described in ACT.89007980). These are located in the core network, so both the originator and terminator must use resources up to the core network, even if there is a shorter path between them.

Figure 5 below has examples of path finding when there is a NAT on the path between the GWs.

- An F-to G call uses resources on LBL 3 and LBL 1. LBL 1 has two call flows on it as both the originator and terminator need to use it to reach the Media Proxy (MP) in the Core network
- A H-to-J call uses resources on LBL 7, LBL 5 and LBL 2. This call will require a MP but the path between the GWs already traverses all the MBs in the chain so there is no need to change this.

Figure 5, VCAC path finding though NATs



This Feature is controlled by state SOC order code CS2Q0002. This has two states:

- ON, which will display ON and have VCAC enabled.
- OFF, which will display IDLE and will disable VCAC.

Further detail on all aspects of this feature can be found in the FNs for the provisioning Features (see dependencies below), and the Performance, Fault management and configuration sections within this book.

45.3 Hardware Requirements or Dependencies

No new hardware requirements.

45.4 Software Requirements or Dependencies

This feature is dependant on:

- A00002512 VCAC provisioning for the GWCEM.
- A00004981 VCAC support for CICM GW
- A00003568 E911 location support for CICM.
- SOC option CS2Q0002 controls the use of this feature

45.5 Limitations and restrictions

The VCAC architecture has some provisioning limits that are enforced by the the provisioning system. These are:

1. A LBL can only be used on one GWC. This means that all the GWs or endpoints behind a single LBL must be on the same GWC.
2. There is a maximum of 2000 LBLs per GWC.
3. There is a maximum of 5 LBLs and NATs between a GW and the Service Provider's core network.
4. VCAC only uses the negotiated values for a call. This means that fax and modem upspeeding to G711 from G729 will not be modelled. Similarly T.38 fax calls will not change the modelled bandwidth for the call.
5. VCAC does not model voice and data traffic on the same LBL. This can be done by careful modeling of the logical network, as a part of the system engineering, or by physical separation of the voice and data traffic (e.g. on different VPNs). There is a requirement that voice traffic is prioritised over the data traffic.

45.6 Interactions

VCAC potentially affects any call. If there is insufficient resources for a call or call leg to complete then the call will be released, and the user directed to a treatment.

VCAC can deny call admission whenever the speech path changes, so the main scenarios are:

1. Call Origination. After the digits have been dialed and the CS 2000 attempts to establish a speech path prior to ringing/ringback VCAC can deny admission to the call. This is the main VCAC scenario.
2. Call Hold. The bearer path is dropped for a call placed on hold, whether as a call hold service or as a step in another service such as 3WC or consultation transfer. If other calls have consumed the available resources then an attempt to retrieve the held call will fail.
3. Call Transfer. The bearer path is changed after it has been set up. This can be caused by services such as call transfer, CFNA, 3WC. IN services use this functionality by connecting a call to announcements before routing to other destinations. This fails if there is a LBL in the new path without resources for the new call leg.

On call denial VCAC will clear down the call that would overload the LBL. **Service handling will be on a best effort basis, i.e. there is no attempt to retry or changes to a less demanding codec**.

45.7 Applicable customer facing sections

Fault Management

- Logs ___X__
- Alarms ___X__

Configuration

- Data Schema ___X__
- User Interface ___X__
- Element Management __NA__
- Security __NA__
- Service Order __NA__
- Office Parameters __NA__

Accounting (includes AMA billing) __NA__

Performance (includes operational measurements) ___X__

45.8 =Glossary

Term	Description
codec	Voice encoding for the call - G711a, G711u, or G729
LBL	Limited Bandwidth Link
MB	Middlebox, either a NAT or LBL
MP	Media Proxy, used for NAT traversal
ptime	Packetisation time, usually 10ms or 20ms
VCAC	Virtual Call Admissions Control

46: Functional Description (FN): A00002740

46.1 Feature name

International Directory Assistance Call Completion (IDACC)

46.2 Description

This feature allows DA calls with an international requested number to be completed using manual DA Call Completion (DACC) or Automated DACC (ADACC).

46.2.1 Overview

TOPS needs an international indicator to process a called number as international/overseas. When a call is signalled with an international called number, there is either a prefix or parameter to indicate international. When an international called number is entered by an operator at position, a functions key is first entered to indicate the number is international. Currently, when TOPS receives a requested number from the DA Service provider (DAS), it is assumed to be domestic (or local). This feature requires the DAS to provide a predetermined international indicator along with an international requested number. Thus, the **DAS must be upgraded** prior to activating this feature.

This feature enhances TOPS to look for the international prefix on requested numbers from the DAS. When found, TOPS will translate the requested number as international for call completion.

Since this feature is dependent upon DAS changes, there are a variety a scenarios which can or cannot be supported based on the level of DAS support. For full IDACC support, ensure the vendor supports the international prefix in all messages which contain the requested number.

The initial release of this feature only supported the ADACC scenario as documented in a00002740.aa01; these limitations have been reproduced in an appendix of this document. A second release (a00002740.aa02) added the ability to restrict overseas ADACC by adding it to table TDBDAOPT. This version captures the full functionality TOPS can provide for IDACC calls.

46.2.2 IDACC Callflow using ADACC

International listing numbers are supported via an international indicator prepended to the listing number. This international prefix indicator is datafillable via a new parameter in TOPSPARM, as described later in this document.

When TOPS receives a listing number from the DAS with the pre-determined international prefix, the listing is treated as an international number. The following callflow illustrates the ADACC scenario, and notes the IDACC specifics below.

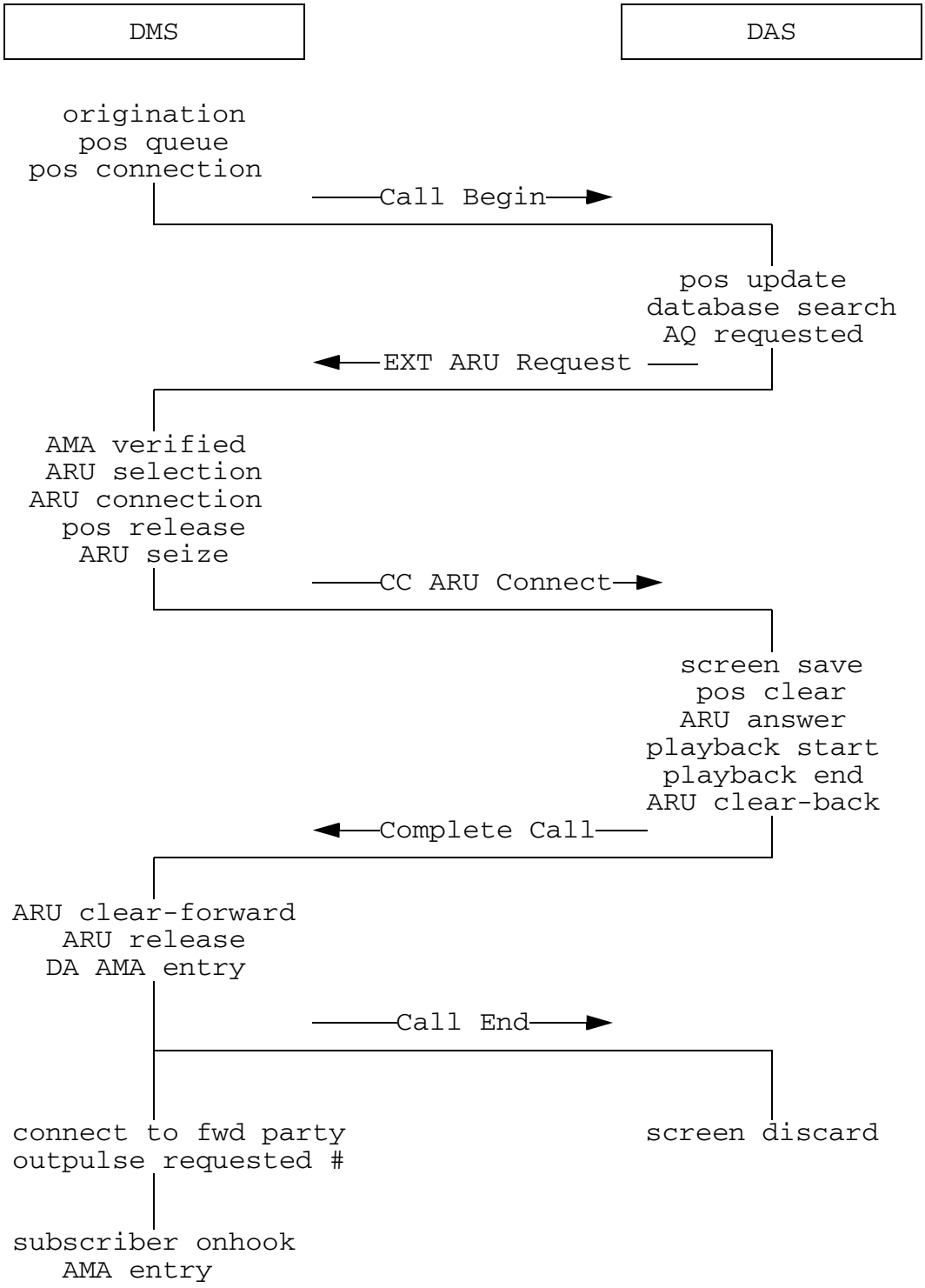


Figure 1 Auto-quote with Call Completion, DA Call

In the EXT ARU Request message, the DAS sends the international indicator, the country code, and the listing number (prefix+CC+listing). TOPS recognizes the international prefix and records the listing number as international. The prefix is then removed from the listing to enable existing translations to be used.

When the Complete Call message is received, TOPS will generate a DA AMA record[1] with the requested number showing the country code and listing number. It will also contain an international indicator.

```
*HEX ID:AA  STRUCTURE CODE:40106C  CALL CODE:194C  SENSOR TYPE:036C
 SENSOR ID:0000000C  REC OFFICE TYPE:036C  REC OFFICE ID:0000000C
 DATE:30410C  TIMING IND:00000C  STUDY IND:0200000C  SERVICE OBSERVED:0C
 SIG DIGITS NEXT FIELD:010C  ORIG OPEN DIGITS 1:01036321005C
 ORIG OPEN DIGITS 2:FFFFFFFFFF  ORIGINATING CHARGE INFO:FFFF
 CONNECT TIME:0854090C  ELAPSED TIME:000000112C  SERVICE FEATURE:000C
 STATION SIGNALING IND:9C  SCREENING CODE:000C  CALLED NUMBER INPUT:1C
 CALLING NUMBER SOURCE:1C  MODULE CODE:042C
 CALL RECORD SEQUENCE NUMBER:0000035C  MODULE CODE:311C  ORIG CALL TYPE:036C
 MODULE CODE:032C  OPERATOR IDS:1050915009999C
 ACC OPERATOR WORK TIME:00060C  MODULE CODE:037C  LINE NUMBER TYPE:001C
 DOMESTIC/INTL INDICATOR:2C  SIG DIGITS NEXT FIELD:011C
 TERM OPEN DIGITS 1:10123444444C  TERM OPEN DIGITS 2:FFFFFFFFFF
 MODULE CODE:310C  KEYING ACTIONS:111111111C  MODULE CODE:055C
 SERVICE ID:001C  MEANS OF INFORMATION INPUT:1C  MEANS OF LSDB ACCESS:1C
 LSDBS BOC ID:12138C  LSDB ACCESSES:FF  LISTING RESPONSE:1C
 LISTING STATUS:999999900C  REQUEST COUNTER:001C  MODULE CODE:104C
 TRUNK FACILITY ID:102950000C  MODULE CODE:000C
```

TOPS can then utilize ADACC to complete the call if all ADACC checks pass.

In addition to existing ADACC checks in tables DABILL, DATRKOPT, ADACCOPT and ICNTRY (for direct routes to country), table TDBDAOPT includes a new option for International/Overseas calls. Thus, for IDACC calls to complete using ADACC, the ADACCSRV field of TDBDAOPT must include the new option, OVERSEAS, or be set to ALL.

> ***Note:*** Please ensure existing datafill for table TDBDAOPT field ADACCSRV which is set to 'ALL' should be completing International/ Overseas calls.

Table DOMBILL still enforces billing restrictions for domestic calls and table OVSBILL is now used for billing restrictions for international calls.

Table VROPT has a parameter, DACC_LOCAL_TOLL_ACTIVATION, in which international/overseas calls are now part of the TOLL and ALL options for this parameter.

[1]This AMA structure is not changed by this feature; however, DA AMA records can now include the international indicator and country code. Although the country code is included with the listing number in the 'TERM OPEN DIGITS' fields, the number of country code digits is not specified for open numbering dialling plans for this 'new' DA record (194) nor for the existing call completion record (192).

Auto-collect as sent from the DAS also includes a TOLL/ALL option in which now include international/overseas calls.

When ADACC processing can be applied to the IDACC call, existing translations are performed using the operator FOREIGN entry in table IOPRTRAN.

If outpulsing to a SS7 ISUP trunk (ANSI or ETSI), the NOA of the IAM will contain ‘international’ as shown below.

```
OUTGOING  10:25:30.038  NODE TYPE= LTC_NODE
S512: ENCAP MS_CARD= 6 MS_PORT= 3  NODE= 4123
N= 001D  TN= 01CC  MSGTAG= 00  ROUTE= 101B  ERROR= 00  LENGTH= 2A
GENT= CKT     T915TO95ETSI    1
F 01 00 01 00 0A 03 0A 10 01 00 01 02 03 00 01 00 06 04 10 01 21 43 45 0A 07
3 10 01 63 23 01 50 00

             CCS7 MESSAGE TYPE:  ISUP_IAM
             DATA BYTES:         00 01 00 0A 03 0A 10 01 00 01
                                 02 03 00 01 00 06 04 10 01 21
                                 43 45 0A 07 03 10 01 63 23 01
                                 50 00

             NATURE OF CONNECTION:    ISUP_NO_SATELLITE,  NO_ISUP_CONT_CHK
                                      ISUP_NO_HALF_ECHO_SUP

           FORWARD CALL INDICATORS: ISUP_Call Type:      ISUP_INTERNATIONAL_CALL
                                   E_to_E_Method:        NO_E_TO_E_METHOD_AVAIL
                                     ISUP_Interworking:    NO_INTERWORKING
                                     E_to_E_Info_Check:    NO_E_TO_E_INFO
                                     ISDN_UP_Ind:          NOT_ISUP_ALL_THE_WAY
                                  ISDN_UP_Pref_Ind:     ISDN_UP_PREF_ALL_THE_WAY
                                     ISDN_Access_Ind:      ACCESS_NON_ISDN
                                   Trans_Called_Num_Ind: NUMBER_NOT_TRANSLATED
                                    Routing_Attempt_Ind:  NO_ROUTING_ATTEMPT

             CALLING PARTY CATEGORY:  #0A - ISUP_CPC_SUBSCRIBER_1

             MAND.VARIABLE PART:      Generic Base USI:
                                        TRANSMISSION MEDIUM REQ:   TMR_NIL
                                      INFORMATION TRANSFER CAP:  GEN_ITC_SPEECH
                                        CODING STANDARD:           STD_CCITT
                                        INFORMATION TRANSFER RATE: ITR_64KB
                                        TRANSFER MODE:             MODE_CIRCUIT
                                     LAYER1 INFORMATION:        LAYER1_G711_ALAW
                                        USER RATE:                 USER_RATE_NIL
                                        SYNCHRONIZATION:           SYNCHRONE
                                     NEGOTIATION:               NEGOT_NOT_INBAND
                                        MESSAGE PRIORITY:          1

                                       CALLED PARTY:
                                     EVEN_ODD_IND  :          EVEN_NUM_NIBBLES
                                        NATURE_OF_ADD : #04 - INTERNAT_NUMBER
                                        NUMBERING_PLAN : ISDN_TELEPHONY_NUM_PLAN
                                        ADDRESS_INFORMATION = 10123444
                                        INTERNAL_NET_NUMBER : ALLOWED

             OPTIONAL PART:           CALLING PARTY:
                                     EVEN_ODD_IND:            EVEN_NUM_NIBBLES
                                      NATURE_OF_ADD : UNIQUE_NATIONAL_SIG_NUMBER
                                  ADDR_PRES_RESTRICTED_IND : PRESENTATION_ALLOWED
```

```
                    NUMBERING_PLAN : ISDN_TELEPHONY_NUM_PLAN
                   SCREENING_IND  : USER_PROVIDED_NOT_SCREEN
                CLG_PTY_INCOMPL_IND : CALLING_PARTY_COMPLETE
                    ADDRESS_INFORMATION = 1036321005
```

When the call ends, the call completion AMA record is generated as shown below. No changes were made to this AMA record.

```
*HEX ID:AA  STRUCTURE CODE:40106C  CALL CODE:192C  SENSOR TYPE:036C
 SENSOR ID:0000000C  REC OFFICE TYPE:036C  REC OFFICE ID:0000000C
 DATE:30410C  TIMING IND:00000C  STUDY IND:0200000C  SERVICE OBSERVED:0C
 SIG DIGITS NEXT FIELD:010C  ORIG OPEN DIGITS 1:01036321005C
 ORIG OPEN DIGITS 2:FFFFFFFFFF  ORIGINATING CHARGE INFO:FFFF
 CONNECT TIME:0854304C  ELAPSED TIME:000000052C  SERVICE FEATURE:000C
 STATION SIGNALING IND:9C  SCREENING CODE:000C  CALLED NUMBER INPUT:4C
 CALLING NUMBER SOURCE:1C  MODULE CODE:042C
 CALL RECORD SEQUENCE NUMBER:0000036C  MODULE CODE:316C  LOCAL INDICATOR:1C
 MODULE CODE:311C  ORIG CALL TYPE:002C  MODULE CODE:032C
 OPERATOR IDS:1050915009999C  ACC OPERATOR WORK TIME:00040C
 MODULE CODE:033C  DOMESTIC/INTL INDICATOR:2C  SIG DIGITS NEXT FIELD:011C
 TERM OPEN DIGITS 1:10123444444C  TERM OPEN DIGITS 2:FFFFFFFFFF
 COMPLETION IND:001C  RATE IND:7C  OSS CALL COMPLETION CONDITIONS:1121710C
 ALTERNATE ROUTE NUMBER:FFFF  MODULE CODE:310C  KEYING ACTIONS:221111111C
 MODULE CODE:104C  TRUNK FACILITY ID:102950000C  MODULE CODE:000C
```

46.2.3 Enabling International DACC

In ISN07 and above loads, this feature is controlled by a SOC option and a TOPSFTR parameter. The intent is to only turn SOC on once and then use TOPSFTR to activate/deactivate the functionality.

Table 1 SOC Option

SOC Option	
ENSV0108	DA Intl Call Compltn

ENSV0108 requires ENSV0101, OSB00101, OSDA0101, and OSDA0102.

Table 2 Table TOPSFTR

FTRNAME	FTRENABL
International_DA_Call_Comp	Y

Table TOPSFTR can be set to Y to activate or N to deactivate.

The SOC option and TOPSFTR parameter can be set regardless of the other; however, a warning message will be generated if the other is not set as needed.

TOPSFTR parameter, cellular_automatic_da_call_comp, must also be set to Y to utilize table TDBDAOPT field ADACCSRV.

46.2.4 Defining the International_DACC_Prefix

The international DACC prefix is datafillable in table TOPSPARM. It contains the actual prefix digits (0-999). It can be 1, 2, or 3 digits.

Table 3 Table TOPSPARM

PARMNAME	PARMVAL
INTERNATIONAL_DACC_PREFIX	00

This example datafill will mark requested numbers arriving with a ‘00’ prefix as international. Thus, a requested number of 123456789 sent from DAS as 00123456789 will be translated as international. The 00 prefix will be removed, the 123 will be checked for a country code and the rest stored as the called number. International translations will be called using the country code and called number; the prefix is not used for translations.

46.2.5 Restricting ADACC Overseas calls

Table TDBDAOPT includes a field, ADACCSRV, which indicates the types of calls that can be completed via ADACC. It includes INTER, INTRATOLL, INTRALCL, ALL, and NONE. A new option, OVERSEAS, is added to the range. Thus, IDACC calls can be eligible for ADACC service if the datafill includes either OVERSEAS or ALL.

Table 4 Table TDBDAOPT

TDBDAIDX	ADACCSRV	BILLOPT	ADASERV
0	ALL	ALL	N
1	INTRALCL	ALL	N
2	NONE	ALL	N
3	OVERSEAS	ALL	N
4	INTER, INTRATOLL, OVERSEAS	ALL	N

In the example, calls which index tuples 0, 3, or 4 are eligible for IADACC service.

Table TDBDAOPT is indexed by table TOPSDB, which can be indexed by tables DNSCRN, TOPEACAR, and COANISCR.

Note: ADACCSRV is only used for carrier calls. Thus, the call must be either an EA call (north american) or GCA call (international).

46.2.6 Manual DA Call Completion and Operator Functions

IDACC is supported for manual DA call completion at an TOPS operator position or OSSAIN Service Node (SN).

The international requested number can be obtained from either a DAS message or the operator/SN entering the requested number. For all cases, the international requested number must arrive to TOPS with the datafilled international prefix indicator.

Thus, the international prefix indicator must be prepended to the international requesting number in all DAS messages, when the operator enters the requested DN at position, or when the SN sends in a DN request. In all cases, TOPS will scan the requested number for the international prefix.

Note: This means TOPS operators and SN applications will need to be able to recoginize an international listing and prepend the prefix for TOPS to treat the number as interational. An operator must enter prefix+cc+number when entering an international requested number. SNs must send prefix+cc+number in the called DN update message.

When the international prefix is found, TOPS will treat the requested number as international/overseas and will utilize overseas tables such as OVSBILL instead of DOMBILL.

Note: The DA forward function available at some operator positions currently only supports domestic numbers. Since this function is intended for emergency calls only, there is currently no need to enhance this function to include international numbers. In addition, the DA forward function uses a called number for outpulsing; the IDACC feature is for requested numbers. If a requested number is entered prior to the DA forward function, then the requested number is overwritten.

46.3 Interactions

The following note the interactions with the existing DA system.

46.3.1 Local-Toll Activation

Table VROPT has a parameter, DACC_LOCAL_TOLL_ACTIVATION, which is used for activating call completion for local and/or toll calls. Currently, the parameter can be set to NONE, LOCAL, TOLL, ALL. NONE

and LOCAL are not affected; however, the TOLL and ALL settings will now included International requested numbers.

46.3.2 Auto-Collect

Auto-collect is for business numbers which allow the subscriber to automatically bill collect. No verification is required for these collect calls. This option can be applied to the requested number in the DAS and sent to TOPS with the requested number. This functionality is currently provided with the following options: none, local, toll, all, and surcharge. All options remain the same except for the toll and all options. International requested numbers are now included in the toll and all auto-collect options.

46.3.3 Billing Restrictions

All existing DA and TA billing restrictions will be maintained with the addition of utilizing table OVSBILL for international requested numbers in comparision to table DOMBILL for domestic calls.

46.3.4 Invalid Country Code

Country codes must be datafilled in table CCTR to be valid. International requested numbers with invalid country codes can still be announced and generate an AMA record but cannot be completed. Calls with invalid country codes are not allowed to utilize ADACC and will be presented to an operator.

46.3.5 Direct and Alternate Routes

ADACC requires a direct route to complete international calls. If a direct route is not available, the call will be presented to an operator to select an alternate route, if available.

46.4 Software Requirements or Dependencies

This feature is dependent upon base TOPS and DA functionality being present and activated. It also requires the ADACC functionality.

ENSV0108 is the SOC option for this functionality. It requires ENSV0101, OSB00101, OSDA0101 and OSDA0102.

46.5 Limitations and restrictions

- Table TDBDAOPT field ADACCSRV is only for carrier calls.
- DA forward key function supports domestic/local numbers only. It has not been enhanced to support international numbers.
- This feature will remove the international prefix from the requested number so that existing translations can be used. It is not outpulsed nor included in any log or AMA record. The prefix is intended to only mark the call as international for translations and thus is removed for all other purposes. External listing announcements controlled by the DAS vendor

may include the prefix in the announcement according to the vendor implementation. Contact DAS vendor for specifics.

- International Requested numbers will be treated as toll (same as Domestic numbers) for activation and auto-collect.
- ADACC requires direct routes to the country. If a direct route is not available, this feature is not supported.
- LNP is not supported in Global loads.

46.6 Glossary

Term	Description
IADACC	International Automated Directory Assistance Call Completion
ADACC	Automated Directory Assistance Call Completion

46.7 Appendix A: International ADACC (IADACC) Limitations

IADACC is described as the functionality and limitations provided by TOPS when the DAS vendor only supports the EXT ARU Request message for International DA Call Completion (IDACC).

For IADACC, TOPS **can** support the following:

- International Indicator recognition
- International DA AMA record generation
- Call completion to the international number based on TDBDAOPT

TOPS **cannot** support the following with IADACC:

- Manual DA call completion (DACC) - DA call which receives an international listing then the operator switches service to Toll to complete the call. This is not supported.
- Multiple Requests - DA call at position with international listing; GEN AMA for first listing; obtain second listing. This is not supported.
- Verbal quotes - Operator verbally quotes listing to subscriber and releases call. This is not supported.
- Recalls / Reconnects - DA call obtains listing and is released to announcement; call recalls back to position; if a GEN AMA, service switch or position release is performed then the call is not supported. (If a

second listing is obtained, without gen ama for first listing, and is then released to announcement, the call can be supported.)

- Transfer with context scenarios are not supported.
- Alternate Routes are not supported since they require manual call completion which is not supported. Automated DA Call Completion (ADACC) requires direct routes.
- IADACC Error handling is limited since manual call completion is not available. Any scenario in which ADACC cannot service the international call is not supported.
- Any scenario utilizing DAS protocol messages - AMA transfer, Service Request, Position Request, and Position Release are not supported.

47: Design Description Excerpts: A00002741

47.1 Feature name

Supernode Billing Application Base Real Time Billing Robustness

47.2 Purpose

This activity robustifies SBA Base RTB to auto recover from downstream and network connectivity problems once the issues are resolved. This functionality will be optionalized. As well, the activity addresses many other deficiencies tracked by CRs and other means.

47.3 Problem Symptoms

Each item of functionality to be considered by this activity is grouped below, along with a summary explanation for the item.

1. Deletion/modification of underlying schedule tuple:

Problem Description: The billing stream Schedule tuple configuration is shared by both Outbound file transfer and the RTB Destination configuration. If the schedule tuple is removed or certain fields are modified while the corresponding RTB Destination is InSv, the RTB Destination would fail ungracefully.

Solution Description:

i. This activity displays a message to the user asking him to OffL and delete the any possible corresponding RTB Destination before modifying/deleting the associated Schedule tuple if the protocol of the tuple is RFTPW.

ii. Also, RTB will now check for the current schedule tuple every transfer event irrespective of whether failure has occured or not. If an active file is being transferred by RTB, and the schedule tuple is deleted or the protocol changed, the current active file will continue to transfer until it is closed as is the case currently. If another active file is opened, RTB will move to SYSB state as is the behaviour now.

2. Auto Recovery: “Test File transfer” and “Temp File renaming on DPMS”:

Problem Description: In order for RTB to recover from a user defined maximum number of consecutive outages in connectivity between the SDM and the DPMS, manual intervention was required (i.e. have to BSY/RTS RTB Destination in billmtc) in order to resume real time transfer of future open billing files to the DPMS.

Also, a Temporary open file (with suffix .tmp) exists on the DPMS to collect the billing data sent by RTB. Whenever there was a LAN failure or when SDM/ Downstream processor reboots, this open file was not complete nor properly named. Its corresponding file on the SDM is moved from Open to ClosedNotSent (CNS) directory, and renamed. Thus, when RTB resumed service, a new open file was transferred and thus a new .tmp file was created on the DPMS. Thus there would be two .tmp files at the DPMS.

Solution Description:

i. Enhancements are made to RTB such that after the maximum consecutive number of failures for a Destination, it will move to ISTB state to denote that RTB will initiate an autorecovery process.

When the above is encountered, it then starts a monitoring operation consisting of FTPing a test file (of size 10MB, named as NetworkTest) to the DPMS test file directory, and analysing the response to figure out if the test transfer was successful, or in case of error, if it was due to a network issue or a non-network issue. . Below are the 2 resulting scenarios:

–If it is a non-network issue, RTB will sleep until a new file is open on the the SDM and then resume its INSV state.

–If it is a network issue, RTB will try the operation again until it succeeds 3 consecutive times or until a non-network issue is detected, in which case the previous stated behaviour above for this case is followed.

The location of the test files on the downstream can be configured through RMI (BILLMTC).

ii. Enhancements are made such that whenever RTB resumes operation after an outage, the <filename>.tmp file on the downstream (for the associated stream/destination configuration) will be renamed to <filename>.partial before opening a new .tmp file. The location of this partial file is configurable through RMI (BILLMTC).

Both the test file transfer and partial file renaming functionality are one combined auto-recovery option (which applies to any/all configured RTB Destinations), which can be turned ON of OFF.

If the user sets the option to OFF,-manual intervention will be required to return to service the RTB Destination after the configured maximum # of consecutive network failures occurs**.** In this case, RTB will go to SYSB state, and manual intervention is required to ever get out of this state, as is the behaviour now.

3. Interoperability between RTB and base SBA status:

Problem Description: RTB behaviour is heavily dependant on the status of base SBA resources such as the stream state, and the application status of SBA. RTB fails ungracefully when base SBA stream or application states change.

Solution Description:

i. The RTB Destination will check the underlying stream status before executing the transfer event. If it is not INSV, a designlog and custlog will be raised, and the transfer will not be executed.

ii. Whenever SBA is restarted, RTB will check the previous state for each RTB Destination and will bring the Destination INSV if it was previously INSV or ISTB or SYSB at the time of SBA application shutdown.

47.4 Limitations and restrictions

- There already exists a limitation on SBA, which is the following: Multiple schedule tuples must not be configured (across OR within SDMs) sharing the same 'remote destination IP', 'remote directory', 'file format' (DIRP), and 'File_Extension.' If this is not respected, collisions between billing filenames may result. This feature adds more of a limitiation based on the above, which is the following: Multiple schedule tuples must not be configured (across OR within SDMs) sharing the same 'remote destination IP' and 'remote directory', and where there exists at least 1 RTB Destination configuration (on any SDM) based upon one of these underlying schedule tuple configurations. If this is not respected, and the Auto-recovery option is turned ON, then one transfer may remove files owned by another transfer.
- A new limitation exists if the Auto-recovery option is turned ON. Multiple RTB Destinations must not be configured (across OR within SDMs) with the same 'partial file location' OR the same 'test file location' on the DPMS. If this is not respected, collisions between files may result.

Definitions & Abbreviations

Acronym	Expansion
CNS	Closed Not Sent
FTP	File Transfer Protocol
MIB	Management Information Base
RMI	Remote Maintenance Interface
RTB	Real Time Billing
SBA	SuperNode Billing Application
DPMS	Data Processing and ManagementSystem
CM	Computing Module
SDM	SuperNode Data Manager

47: Functional Description (FN): A00002744

47.1 Feature name

SBA: Automatic Recovery File Closure.

47.2 Description

If the core SBA application is unable to send billing data to the SDM SBA applications, core SBA changes its state to backup mode. In backup mode, the core stores billing data in backup storage. Once communication resumes between the core SBA and SDM SBA, the core SBA will transition from backup mode to recovery mode. During recovery, the core SBA will send the current billing data and the stored backup billing data to the SDM SBA. SDM SBA will open separate files to store the current data and the billing data recovered from backup storage. Once all billing data has been recovered from backup storage, core SBA will transition from recovery mode to normal mode.

For each billing stream configured in SBA, its corresponding billing files can be configured to be rotated based on elapsed time since the file was opened. The crafts person must specify a maximum file size and a maximum number of records for each billing file. In addition to these facilities for file closure, this feature brings in a mechanism to close the recovery file as soon as the SBA core transitions from recovery mode to normal mode, irrespective of the file closure criteria.

47.3 Hardware Requirements or Dependencies

None.

47.4 Software Requirements or Dependencies

- SuperNode Billing Application (SBA) is installed and InSv.
- Billing configured on the CM.

47.5 Limitations and restrictions

None

47.6 Interactions

None

47.7 Applicable customer facing sections

Existing logs will be retained. No new logs are introduced as part of the feature.

Fault Management

- Logs ___N/A___
- Alarms ___N/A___

Configuration

- Data Schema ___N/A___
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

47.8 Glossary

Term	Description
Automatic Message Accounting	Telcordia specification for accounting records.
Automatic Message Accounting Data Networking System (AMADNS).	System for transferring accounting records from a generating system to application systems. Comprises a Data Server component and a Data Processing and Management System (DPMS) component.
CDR	Call Detail Record
Data Processing and Management System (DPMS)	System for receiving accounting records from Data Servers and processing the records as required for transfer to application systems.
data server	Component that collects accounting records from a generating system.
Digital Multiplex System (DMS)	DMS core Digital telephone switch
Device-Independent Recording Package (DIRP)	file format file format used by SBA to store billing records, based on the DIRP billing file format on the DMS core

Term	Description
File Transfer Protocol (FTP)	application protocol for transferring files via Internet Protocol (IP)
generating system	Component that generates accounting records, such as the DMS core.
Generic Requirements (GR)	Telcordia specification document
Management Information Base (MIB).	In the context of this document, refers to the persistent data repository where SBA configuration information is kept. Individual values stored within the MIB are referred to as MIB values
Non-Computing module Load (NCL)	software load for components other than the DMS core; in the context of this document, software load for the SDM
outbound file transfer	SBA file transfer mode where SBA initiates the transfer of billing files to a downstream FTP server.
recovery file	A file on the SDM in which the SDM SBA saves the billing data recovered from the core SBA backup storage.
Supernode Billing Application (SBA)	Accounting collection data server that resides on the SDM. Implements the Data Server function of an AMADNS environment.
Supernode Data Manager (SDM)	Motorola FX computing node upon which resides Operations, Administration, Maintenance, and Provisioning applications / Fault, Configuration, Accounting, Performance, and Security management applications. SDM xxrefers to a given SDM NCL release, where xx is a two-digit number.
Reset EOS	Message from CM Indicating the end of a session.

48: Functional Description (FN): A00002746

48.1 Feature name

A00002746 - ABI XPM FAULT ISOLATION / QUERYPM

This is a Call Server CM feature which is being released in SN07 and in SN06.2 via patches.

48.2 Description

This feature provides new functionality which will assist the craftsperson with maintaining XPMs which subtend the MG9K. This new functionality consists of changes to the existing QUERYPM command which is part of the PM level of the MAP.

The QUERYPM command changes consist of:

- Provide SITE name and ABI location information.
- Provide an interface to assist in isolating communication issues between the CM and the ABI XPM over the Succession network.

48.3 Hardware Requirements or Dependencies

There are no hardware dependancies for this feature.

48.4 Software Requirements or Dependencies

This feature is dependant upon the following features:

- A00002607 - ABI XPM SITE and MG9K Location support.
- A00002146 - MAPCI ABI Link Test & Legacy Comparison.

This feature is not subject to any requirements other than the requirements of the features listed above.

48.5 Limitations and restrictions

There are no known limitations nor restrictions as of this writing.

48.6 Interactions

This feature directly interacts with the following features:

- A00002607 - ABI XPM SITE and MG9K Location support.
- A00002146 - MAPCI ABI Link Test & Legacy Comparison.

48.7 Applicable customer facing sections

Fault Management

- Logs __N/A____
- Alarms __N/A____

Configuration

- Data Schema __N/A____
- User Interface __X____
- Element Management __N/A____
- Security __N/A____
- Service Order __N/A____
- Office Parameters __N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) __N/A____

48.8 Glossary

Term	Description
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512. These XPMs are physically connected to MG9K Gateways via a DS512 interface.

49: Functional Description (FN): A00002756

49.1 Feature name

A00002756 JAPAN TRUNK SERVICES

49.2 Description

49.2.1 Introduction

This activity migrates Japan trunk services “Notification of Time and Charge” (NTC), “Carrier Name Notification” (CNN) and “Account Code” (ACCT) from the legacy MMP product to CS2K Hybrid product IP side in ISN07. It transparently ports the functionality implemented under these MMP features onto the CS2K Hybrid IP side. “Hybrid” always means “CS2K Hybrid” within this document.

If these services are triggered by incoming IP side in hybrid, they are provided by IP side directly. On the contrary, if triggered by incoming TDM side, they are provided by legacy MMP features.

About the services provided by TDM side in hybrid, it is not the scope of this activity and please read the original MMP activities listed below.

The existing MMP NTC service was implemented by following activities:

- AR0480 Notification Of Time & Charge
- AR1344 NTC
- AR1599 Enhancement to NTC
- AR1816 Multilingual NTC
- A59017299 Japan Interconnect ISUP

The service of “Carrier Name Notification for Japan” has been provided on MMP under following activities:

- A59027517 Equal Access Carrier Name Notification
- A59034248 Carrier Name Notification for Carrier Designation Service

The “Account Code” service on MMP was originally done under following activities:

- AR2028 Account Code
- A59017299 Japan Interconnect ISUP

49.2.2 Notification of Time and Charge (NTC)

49.2.2.1 Functional Overview

Notification of Time and Charge is a service provided over JI-ISUP trunks to the Japanese domestic market.

The subscriber activates this service by using the NTC service code prior to the destination address digits. A call is registered as requesting NTC service when traversing a tuple in universal translation that has the NTC feature assigned to it. The NTC service contains two calls: original NTC call and NTC callback.

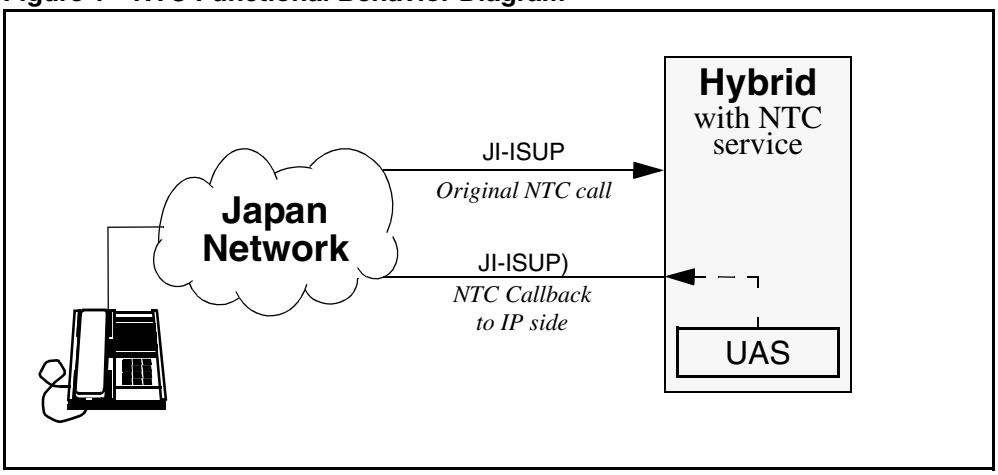
The original NTC call proceeds normally. After a successful call is answered, released and an AMA billing record is produced, NTC service calls the subscriber back using the Calling Line IDentifier (CLID) and provides an announcement indicating such information as the destination address digits, the duration of the original call and the charge amount for this service. The NTC announcement is delivered from EDRAM hardware on Hybrid TDM side. As a Hybrid switch IP side is unlikely to use EDRAM hardware, this activity will rework the feature to use the newer UAS hardware in IP side.

The NTC announcement is a custom announcement that consists of a number of simple and compound phrases. Each simple phrase has a corresponding recording on UAS. Each compound phrase is composed of 1 or simpler phrases.

NTC service is not affected by the out going agent of the original NTC call. The service works providing the interworking from JI-ISUP to the outgoing agent is available and AMA record is used for the call.

Please refer to Figure 1 ”NTC Functional Behavior Diagram”.

Figure 1 NTC Functional Behavior Diagram



49.2.2.2 Linguistic Logic

In this feature, the linguistic logic supports all of the nine languages, Japanese, English, Tagalog, Portuguese, Chinese, Korean, Thai, Spanish and Malay, supported by legacy MMP features.

Following shows the English version NTC announcement.

*This is IDC. The international call you have just made to **A** the number **B** was **C** hours **D** minutes **E** seconds long and cost **F** yen. Repeat, **C** hours, **D** minutes, **E** seconds long and cost **F** yen. Thank you for using IDC. This is a recording.*

Here:

A = Area Name

B = the number recorded by hybrid during the original call.

C = Hours quantity, range is from 1 to 277.

D = Minutes quantity, range is from 0 to 59.

E = Seconds quantity, range is from 0 to 59.

F = Yen quantity, range is from 1 to 10 065 533 yen.

49.2.2.3 Repeating/Skipping a Language during Cyclic Announcement

NTC service provides announcement in a cyclic fashion. In order to provide the subscriber with some control over NTC announcement playing, this feature

supports ‘*’ key for repeating a language in the same cycle and ‘#’ key for skipping to the next language.

— *skipping:* the received ‘#’ keys are used for skipping.

Skipping does not change the playing sequence of the selected languages. This means that a ‘#’ key stops the language currently being played immediately and starts the *next language* right after. The next language here may be the next one on the current cycle, or the first language of the next cycle if the stopped language is the last one of this cycle.

If a ‘#’ key is received while the last language is being played during the last cycle, skipping is ignored. This is so for providing an explicit ending of the NTC service, i.e. either by a complete announcement in the last language or by subscriber disconnect.

— *repeating:* the received ‘*’ keys are used for repeating.

A received ‘*’ key stops the language currently being played immediately and starts to repeat the *same* language on the current cycle.

The maximal number of repeats allowed per cycle of NTC announcement is datafillable via an office parameter. If ‘*’ keys are received beyond the maximum datafilled, the ‘*’ keys are ignored.

Office parameter NTC_ANNC_CONTROL in table OFCVAR has two fields.

1. The first field sets the total number of cycles for NTC service. This field has a range from 1 to 8 with a default value of 2.
2. The second field sets the maximal number of repeats (i.e. ‘*’ keys) allowed per cycle of the announcement. This field has a range from 0 to 7 with a default value of 2.

Let’s say there are three languages: A, B and C. One cycle is defined as (A B C) and NTC_ANNC_CONTROL is set to (4 2), i.e. four cycles and maximum of two repeats per cycle. The entire announcement without repeating (note, skipping may be happening) is:

```
(A B C) (A B C) (A B C) (A B C)
```

If skipping occurs during the above announcement, the language sequence would still be the same. The only difference is the skipped language would be stopped (except for *C* in the last cycle above) once the ‘#’ key is received by hybrid and the next language, which may be the next language on the current cycle or the first language on the next cycle, starts playing right after. Without skipping, each language would be played completely.

With repeating, the actual announcement may be:

```
(A A A B C) (A B B C C) (A B C) (A B B C)
```

Note that during the first cycle above, language B or C cannot be repeated any more since the only two repeats allowed per cycle is used up for language A. This means that all the '*' keys received during the playing time of B and C in this cycle are ignored.

49.2.3 Carrier Name Notification (CNN)

49.2.3.1 Functional Overview

When a JI-ISUP IAM reaches hybrid IP side, the IAM is analyzed for a number of parameters as to whether the announcement is to be played. Once hybrid decides to provide Carrier Name Notification announcement (The conditions please refer to A59034248 FN section 3.2.2 "Conditions for Feature activation"), an early ACM is sent to the calling party that serves to open a backward speech path and then the announcement is played.

Please refer to Figure 2 "CNN Call Flow for Interworking with ISUP" and Figure 3 "CNN Call Flow for interworking with SIP-T".

This service is supported in the following interworking scenarios by this activity:

- JI-ISUP -> JI-ISUP
- JI-ISUP -> IBN7 ISUP
- JI-ISUP -> ETSI ISUP V1
- JI-ISUP -> ETSI ISUP V2
- JI-ISUP -> SIP-T (JI-ISUP)
- JI-ISUP -> SIP-T (No ISUP to IMS)

Figure 2 CNN Call Flow for Interworking with ISUP

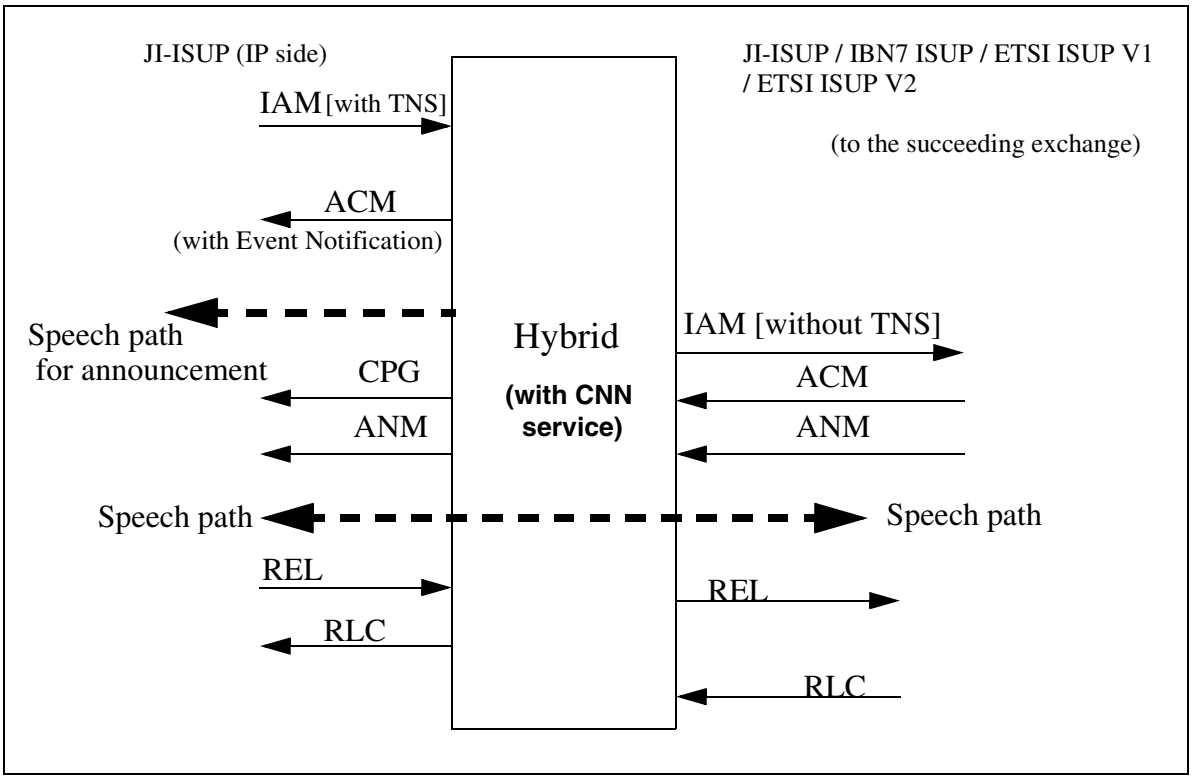
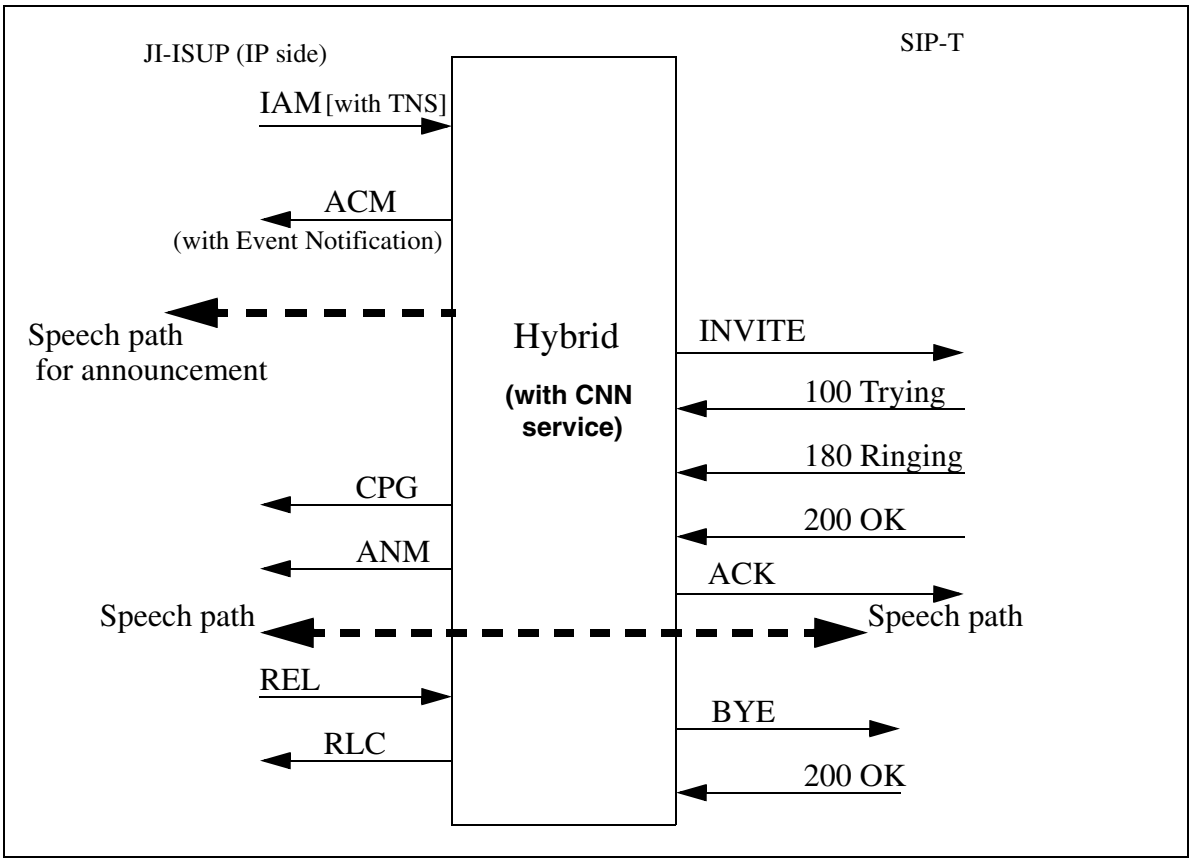


Figure 3 CNN Call Flow for interworking with SIP-T



49.2.3.2 Announcement Handling

If all conditions for feature activation are satisfied and the Network Identification Code in the TNS parameter matches with the CARRID datafill in table CARRNAME, then the announcement recorded corresponding to the announcement CLLI is played. Samples for CNN announcement datafill in ANNS & CARRNAME are shown in Figure 4 "Example datafill in table ANNS" and Figure 5 "Example datafill in table CARRNAME". In this sample, the announcement CLLI is “ANNCLLI1” and CARRID is “111111”.

Figure 4 Example datafill in table ANNS

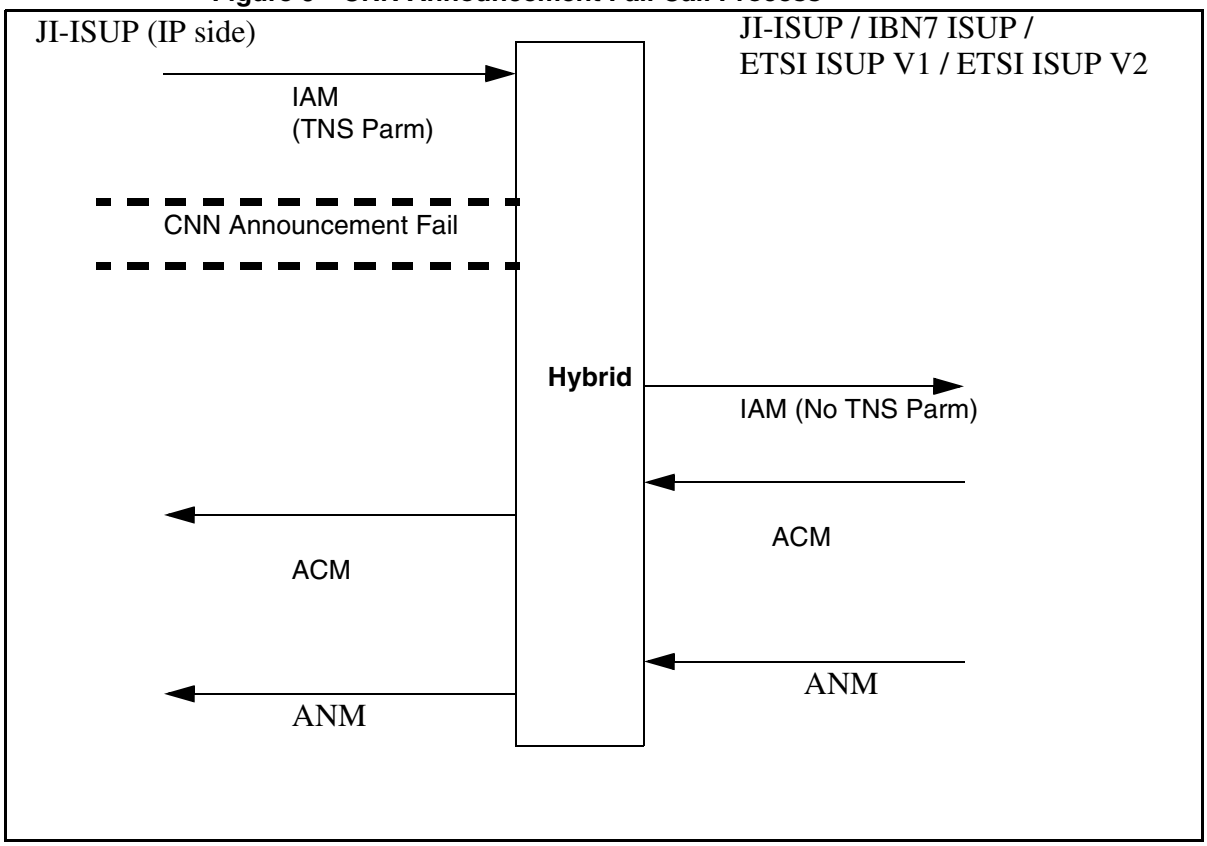
```
ANNCLLI1 NETWK 0 0 1 STND Y 10
```

Figure 5 Example datafill in table CARRNAME

```
111111 ANNCLLLI1
```

If CNN announces fail, e.g. all ANNCLLI1 trunks are busy, the call is tandemed as a normal tandem call and the outgoing IAM doesn't contain TNS parameter. At the same time, CNN101 log is generated. For more information about CNN log, please refer to activity A59034248 FN section 3.7 "Logs". The call process of this case please refer to Figure 6 "CNN Announcement Fail Call Process".

Figure 6 CNN Announcement Fail Call Process



49.2.3.3 Handling of Charge Indicator in BCI of CPG

When CNN feature is triggered, the charge indicator in the CPG is modified according to the CHGIND datafill or the CPGCGIND datafill in table XXCODE / XXHEAD.

The rule of it is shown in Table 1 ”Handling of CPGCGIND in CPG”

Table 1 Handling of CPGCGIND in CPG

CHGIND datafilled	Freedial (NOCHARGE) datafilled	CPGCGIND datafilled	Charge Indicator in CPG
Y / N	N	Y	datafilled value of CPGCGIND
Y	N	N	Datafilled value of CHGIND

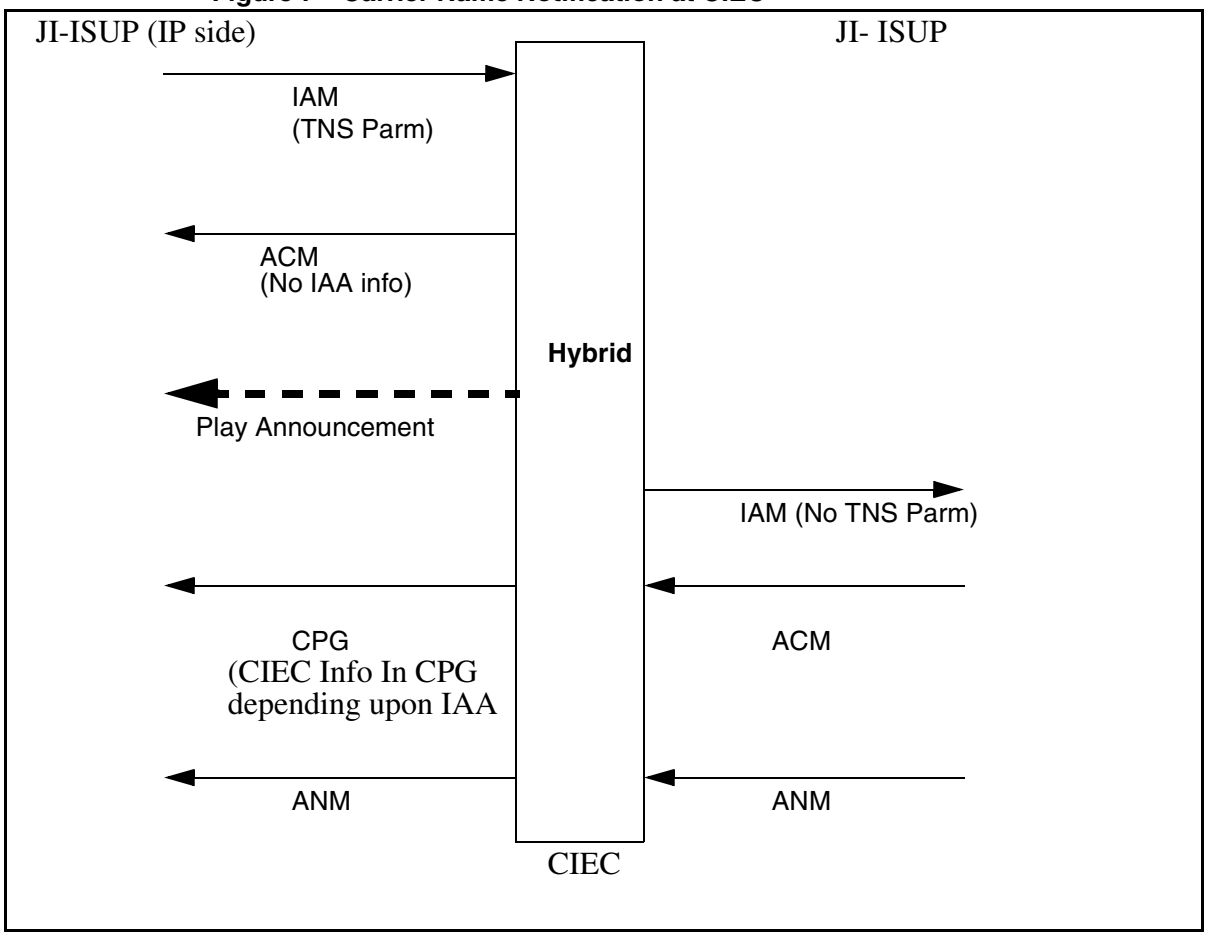
CHGIND datafilled	Freedial (NOCHARGE) datafilled	CPGCGIND datafilled	Charge Indicator in CPG
Y/N	N/Y	Y	Datafilled value of CPGCGIND
Y	N/Y	N	Datafilled value of CHGIND

49.2.3.4 Handling of IAA parameters

IAA is the abbreviation of Inter-Administration Accounting. For more information about IAA, please refer to AU2343 FN section APPENDIX A.

49.2.3.4.1 Carrier Name Notification at CIEC

Figure 7 Carrier Name Notification at CIEC



Please refer to Figure 7 ”Carrier Name Notification at CIEC”.

At hybrid that behaves as a CIEC, if an early ACM for the feature is generated, it will not contain the IAA parameters.

The IAA parameters in the incoming ACM are mapped to the CPG. The IAA parameters of the CIEC are appended to the CPG depending on the IAA logic.

The hybrid will append the CIEC info to the CPG only if all the following conditions are met: -

- the interworking is JI-ISUP to JI-ISUP,
- CIEC datafill in table IAACTRL is encountered during translation;
- all conditions for generating CIEC in IAM are met;
- the incoming ACM must contain the Carrier Info parm (#F1).
- the received TCIT indicator in the incoming IAM must be Backwards (10) or Bothways (11)

If all the above conditions are met, then the behavior depends on which of the following two conditions are met:

(1) if the last sub-block inside the received Carrier Info Parameter in the ACM is CIEC, and the received CIEC Carrier ID is NOT the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then CIEC is not updated by hybrid. On the contrary, if it is the same as TELCO_ID or SUB_TELCO_ID, then the behavior is like: -

Table 2

CarrierID sub-parm	no change
POI-CA sub-parm	no change (even if EXIT_POI_CA is datafilled)
POI-CAT sub-parm	if received, the ENTRY_POI_CAT overwrites the received one when EXIT_POI_CAT is datafilled. And the received EXIT_POI_CAT is not changed; if not received, this sub-parm is added if EXIT_POI_CAT is datafilled;

(2) if the last sub-block inside the received Carrier Info parameter in the ACM is not CIEC, then the Carrier ID in it is not be the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then the behavior is like: -

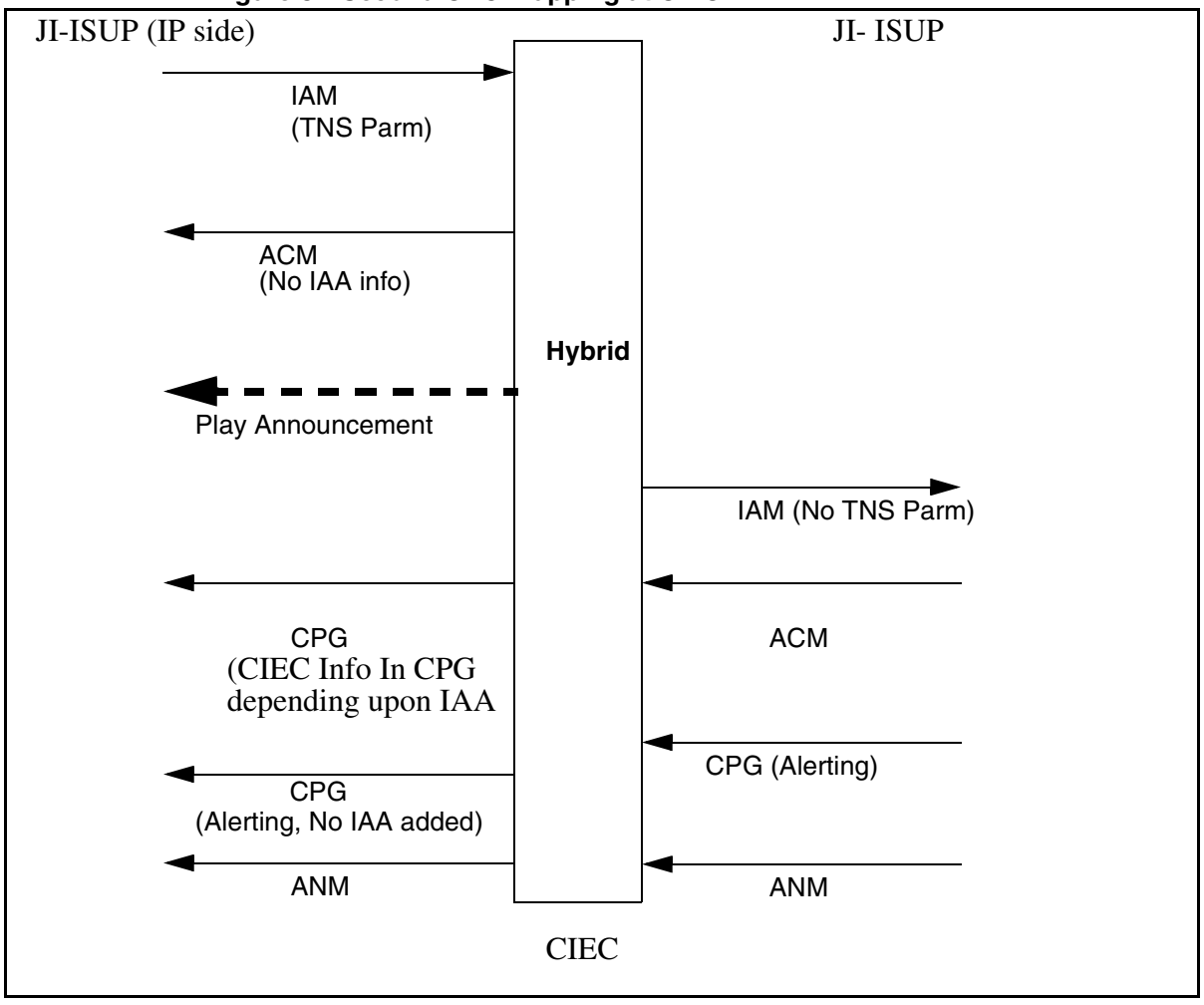
Table 3

CarrierID sub-parm	taken from ofcparm TELCO_ID or SUB_TELCO_ID datafill in table IAACTRL

POI-CA sub-parm	added only if EXIT_POI_CA is datafilled
POI-CAT sub-parm	added if (EXIT_POI_CAT) OR (EXIT_POI_CAT and ENTRY_POI_CAT) is datafilled

After the CPG with IAA is sent out, if there is an alerting CPG coming from outgoing JI-ISUP side, it is just tandemed out to incoming JI-ISUP side and no IAA is added. Please refer to Figure 8 "Second CPG mapping at CIEC".

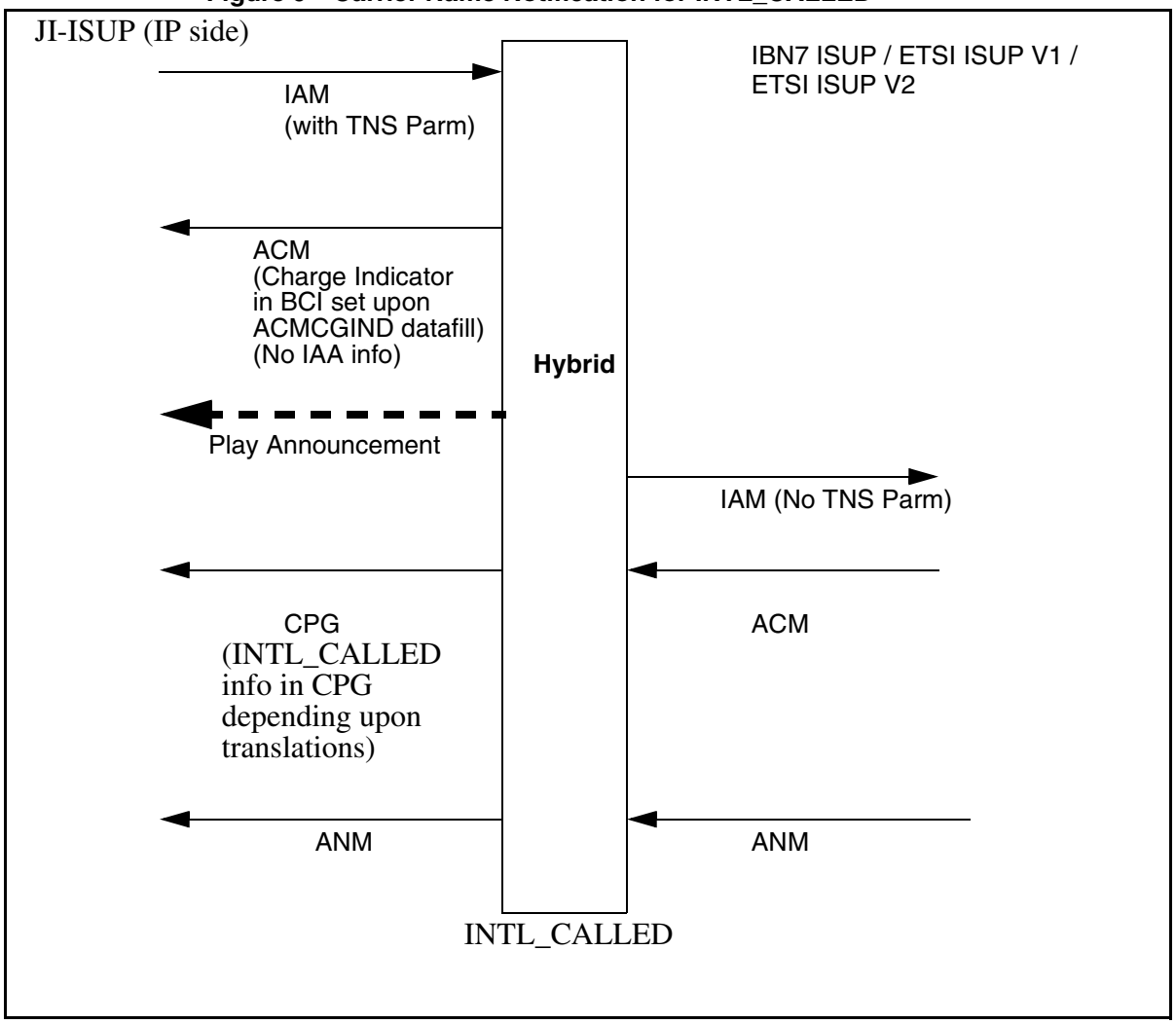
Figure 8 Second CPG mapping at CIEC



49.2.3.4.2 Carrier Name Notification at INTL_CALLED (Outbound International Calls)

Please refer to Figure 9 ”Carrier Name Notification for INTL_CALLED”.

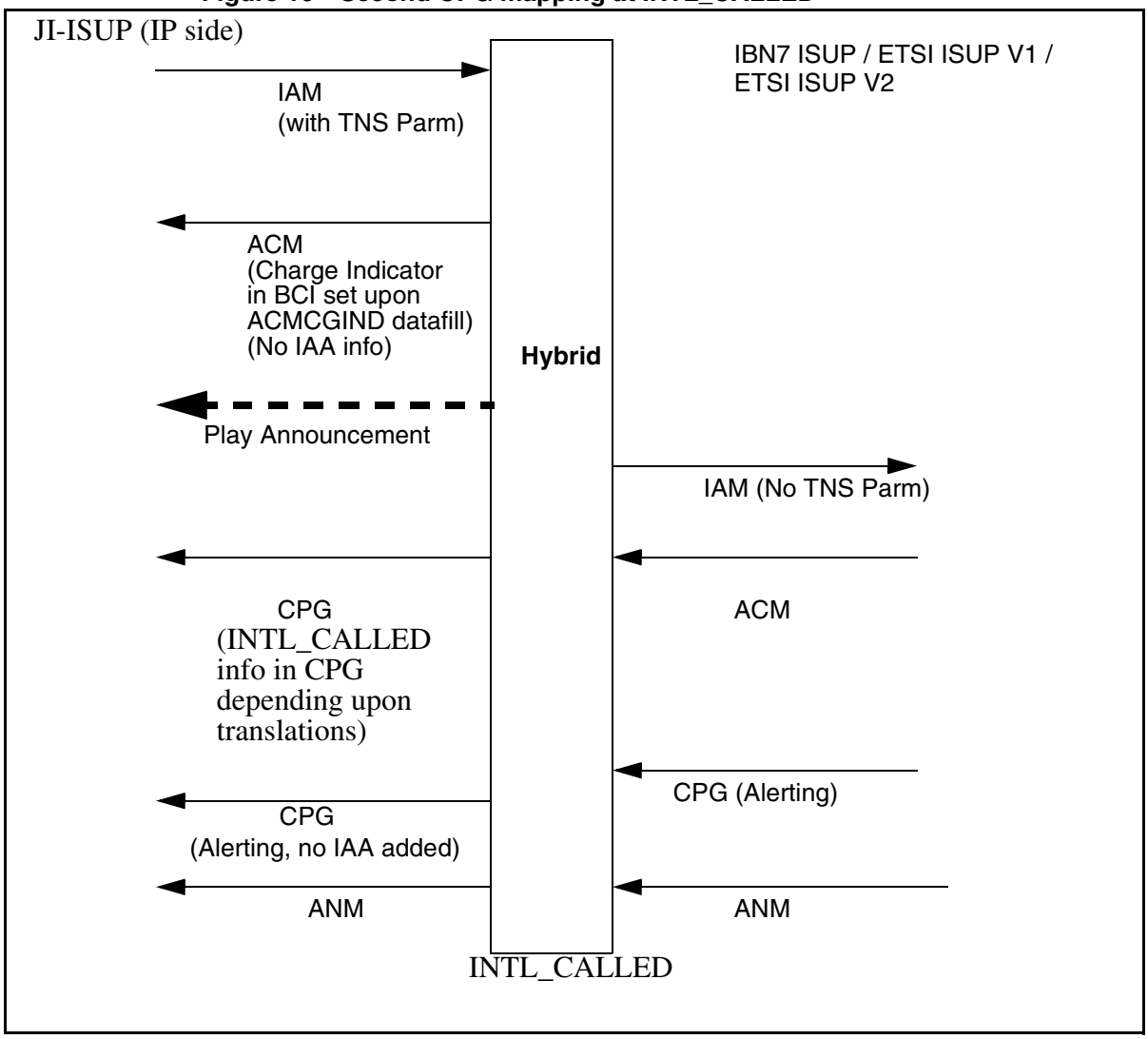
Figure 9 Carrier Name Notification for INTL_CALLED



At hybrid that behaves as an INTL_CALLED (for an international outbound call), if an early ACM for the feature is generated, it will not contain the IAA parameters. So the IAA parameters of the INTL_CALLED will be added to the CPG, i.e. the Carrier Information Parameter containing the Carrier ID.

After the CPG with IAA is sent out, if there is an alerting CPG coming from outgoing IBN7 ISUP side, it is just tandemed out to incoming JI-ISUP side and no IAA is added. Please refer to Figure 10 "Second CPG mapping at INTL_CALLED".

Figure 10 Second CPG mapping at INTL_CALLED



49.2.3.4.3 Carrier Name Notification at IEC

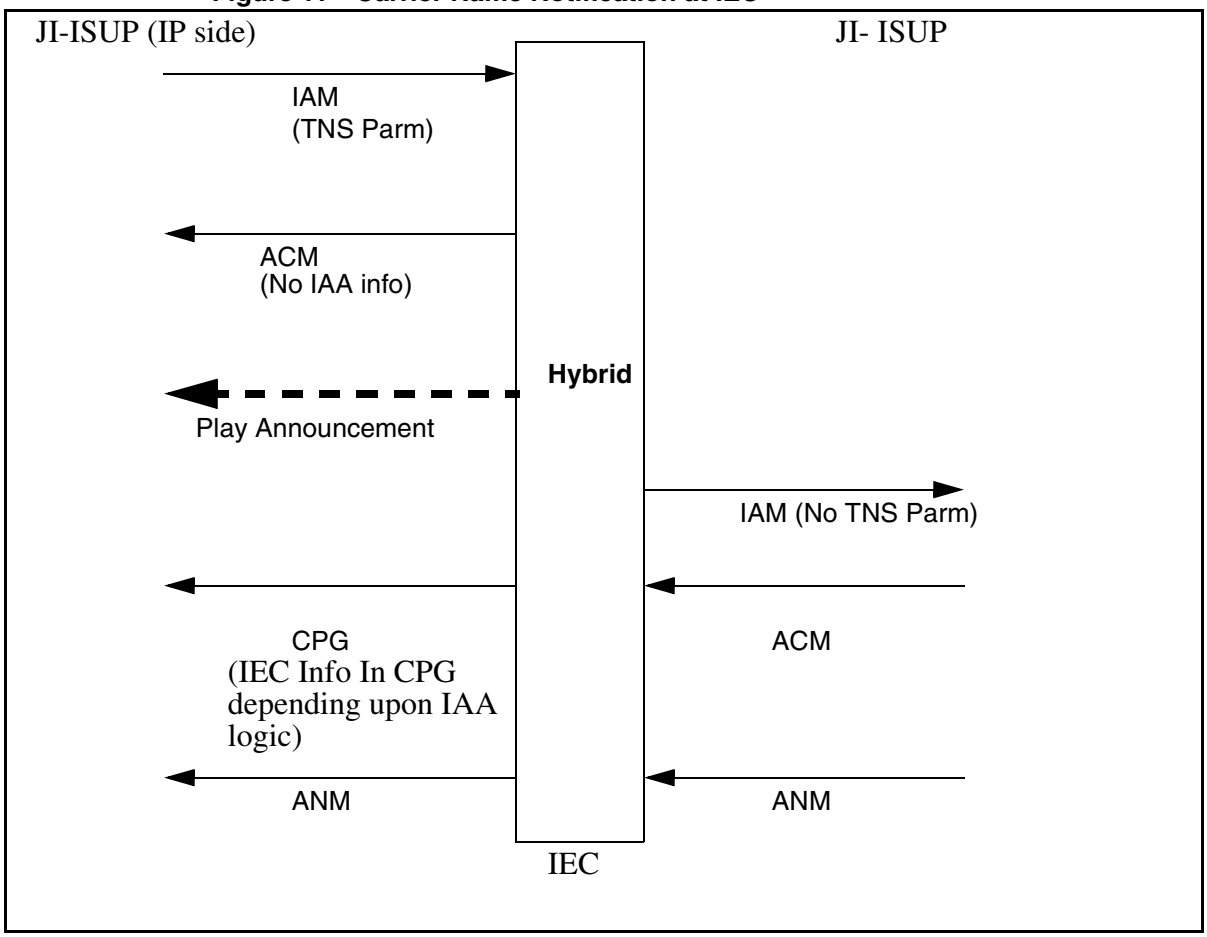
The activation of Carrier Name Notification announcement doesn't differentiate between IEC, CIEC or INTL_CALLED.

If the announcement is played at an IEC, the early ACM generated will not contain the IAA parameters.

The IAA parameters in the incoming ACM are mapped to the CPG. The IAA parameters of the IEC are appended to the CPG depending on the IAA logic.

Please refer to Figure 11 "Carrier Name Notification at IEC".

Figure 11 Carrier Name Notification at IEC



The hybrid updates the IEC carrier info parm to the CPG only if all the following conditions are met:

- the interworking is JI-ISUP to JI-ISUP;
- IEC datafill in table IAACTRL is encountered during translation;
- all conditions for generating IEC in IAM, except the condition regarding the received TCIT value, are met;
- the incoming ACM must contain the Carrier Info parm (#F1);
- the received TCIT indicator in the incoming IAM must be Backward (10) or Bothways (11);

If all the above conditions are met, then the behavior depends on which of the following two conditions are met: -

(1) if the last sub-block of the received #F1 parm is IEC, and this received IEC Carrier ID is NOT the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then IEC is not updated by hybrid. On the contrary, if it is the same as TELCO_ID or SUB_TELCO_ID, then the behavior is like:

Table 4

CarrierID sub-parm	No Change
POI-CA sub-parm	no change (even if EXIT_POI_CA is datafilled)
POI-CAT sub-parm	if received, the ENTRY_POI_CAT overwrites the received one when EXIT_POI_CAT is datafilled. And the received EXIT_POI_CAT is not changed; if not received, this sub-parm is added if EXIT_POI_CAT is datafilled;

(2) if the Carrier ID in the last sub-block of the received #F1 parm is not the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then the behavior is like: -

Table 5

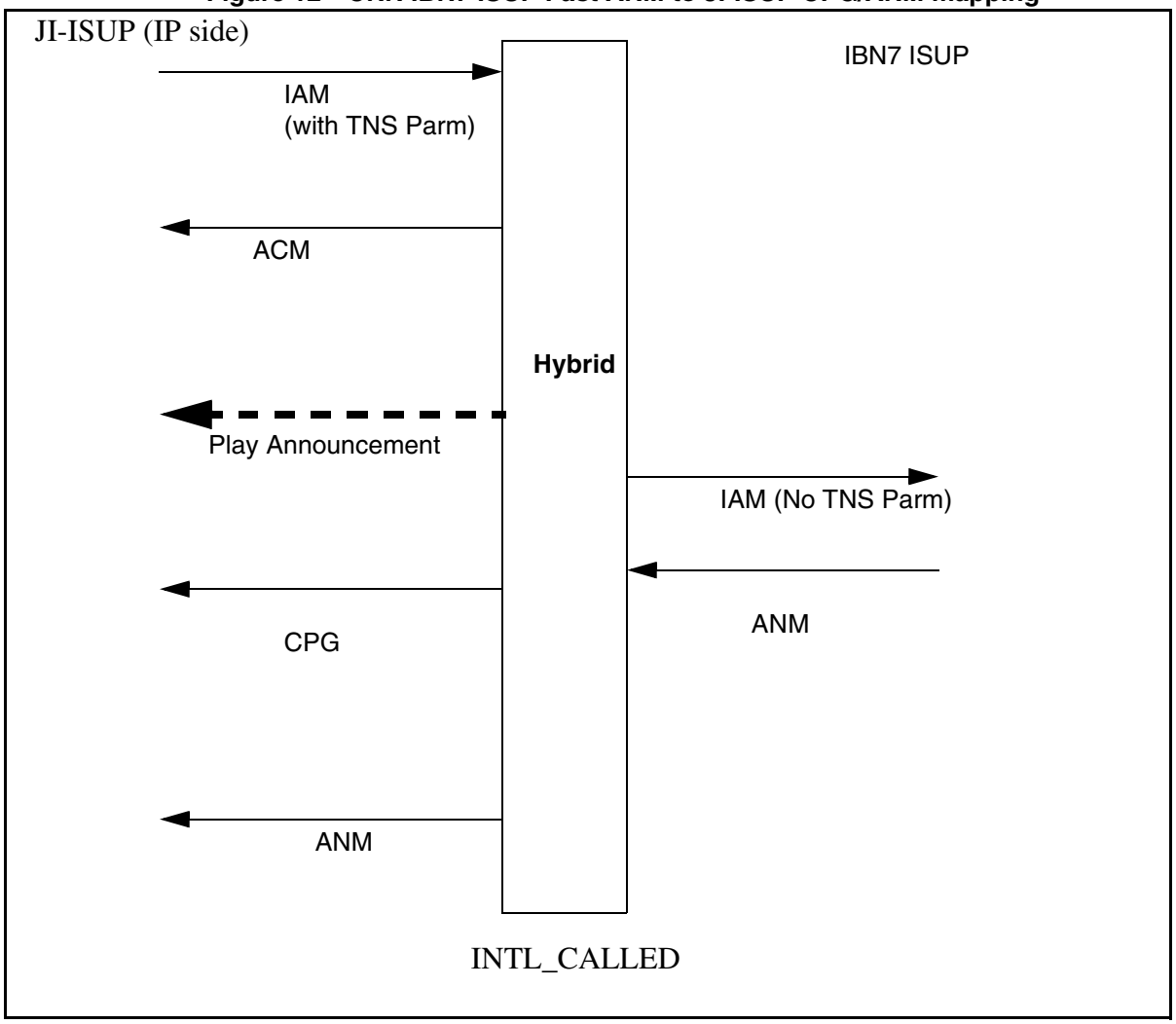
CarrierID sub-parm	taken from ofcparm TELCO_ID or SUB_TELCO_ID datafill in table IAACTRL
POI-CA sub-parm	added only if EXIT_POI_CA is datafilled
POI-CAT sub-parm	added if (EXIT_POI_CAT) OR (EXIT_POI_CAT and ENTRY_POI_CAT) is datafilled

49.2.3.5 Handling IBN7 ISUP Fast ANM

IBN7 ISUP fast ANM to JI-ISUP ACM/ANM mapping is enhanced to JI-ISUP CPG/ANM mapping. The call flow please refers to Figure 12 ”CNN IBN7 ISUP Fast ANM to JI-ISUP CPG/ANM mapping” .

If the fast ANM with no charge and ANM (NOCHG) mapping feature is turned off, ANM is just mapped to CPG and no ANM is sent out. The IAA parameters of the INTL_CALLED exchange will be added to CPG. Except this, the mapping is not impacted.

Figure 12 CNN IBN7 ISUP Fast ANM to JI-ISUP CPG/ANM mapping

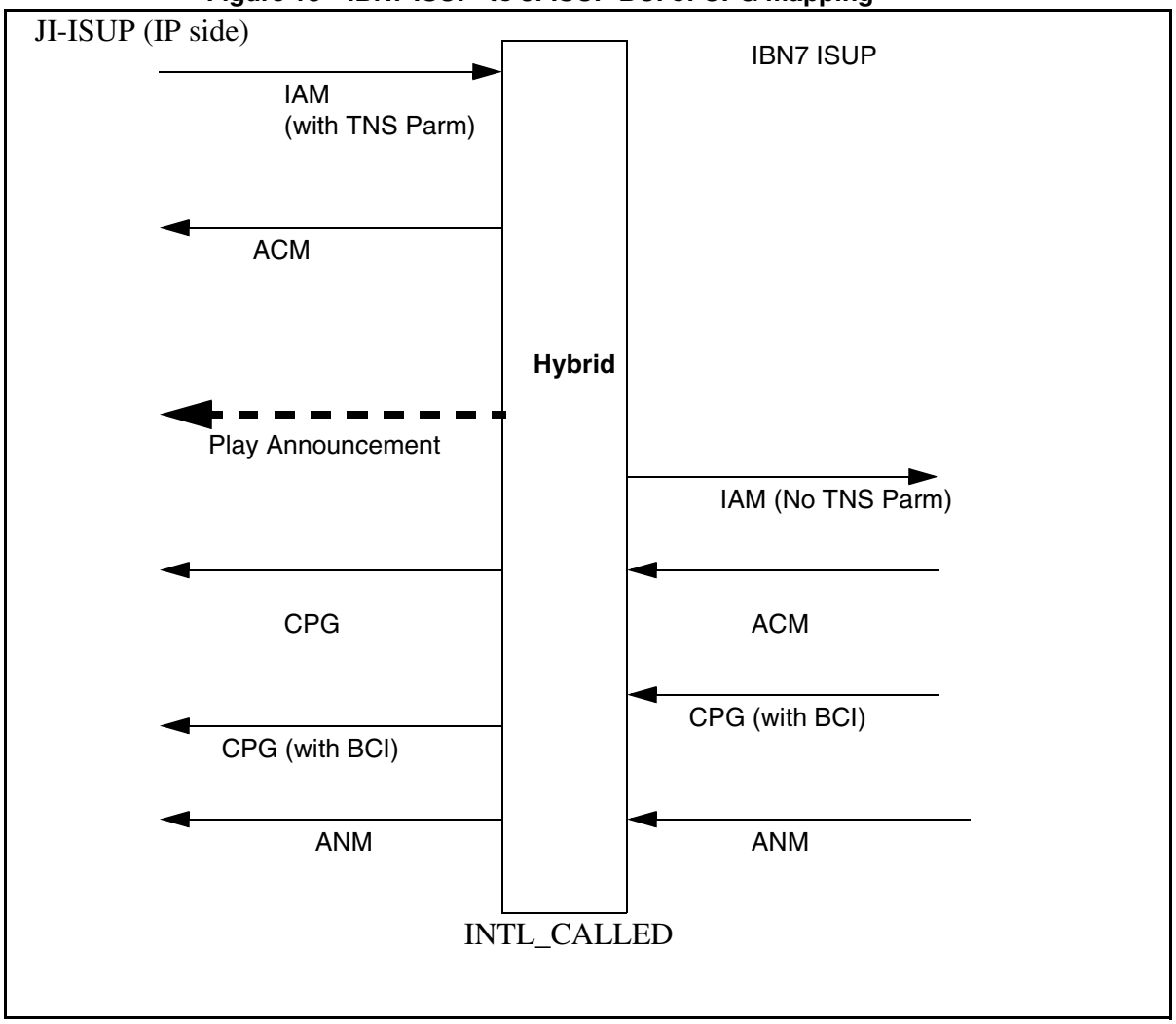


49.2.3.6 IBN7 ISUP to JI-ISUP BCI of CPG Mapping

After the first CPG is sent back to JI-ISUP side, if there is a CPG with BCI is received from IBN7 ISUP side, it is mapped to CPG which has BCI in JI-ISUP side. The BCI mapping rule is the same as BCI of ACM to BCI of CPG mapping. The rule please refers to RS section of A59017299 table 52 “Parameter Mapping - ANSI7+ ISUP ACM to JI-ISUP ACM”.

Please refer to Figure 13 "IBN7 ISUP to JI-ISUP BCI of CPG mapping".

Figure 13 IBN7 ISUP to JI-ISUP BCI of CPG mapping



49.2.4 Account Code (ACCT)

49.2.4.1 Functional Overview

"Account Code" service enables the subscriber to enter an account code during the call setup in order to classify the call on the customer's bill.

The hybrid checks the customer group (CUSTGRP) and the network class of service (NCOS) to see if an account code is required on this call. If it is, the hybrid sends back second dial tone or announcement to prompt the subscriber to enter an account code. The hybrid receives the account code digits as DTMF tones over the voice path.

When entering the account code, the subscriber has the option to enter the reset digit (*). This causes all account code digits entered by the subscriber during the present stage of dialing to be ignored. Accompanying the '*' is a reset tone, ~~of datafillable duration,~~ to prompt the subscriber to begin re-entering the required digits where the first digit dialed breaks the reset tone.

Once the account code digits are entered, the hybrid checks to see if the required number of digits has been entered and the call continues. The entered account code digits will be contained in the AMA billing record.

If the subscriber enters the hash (#) during the dialing phase it is treated as end of dialing. At this point, if the minimum required number of digits has been collected, the call proceeds to the next phase of call processing.

ACCT is supported in following interworking scenarios on hybrid by this activity:

- JI-ISUP -> JI-ISUP
- JI-ISUP -> IBN7 ISUP
- JI-ISUP -> ETSI ISUP V1
- JI-ISUP -> ETSI ISUP V2
- JI-ISUP -> SIP-T (JI-ISUP)
- JI-ISUP -> SIP-T (No ISUP to IMS)

Please refers to Figure 14 "ACCT Interworking with ISUP Functional Behavior Diagram" and Figure 15 "ACCT Interworking with SIP-T Functional Behavior Diagram".

Figure 14 ACCT Interworking with ISUP Functional Behavior Diagram

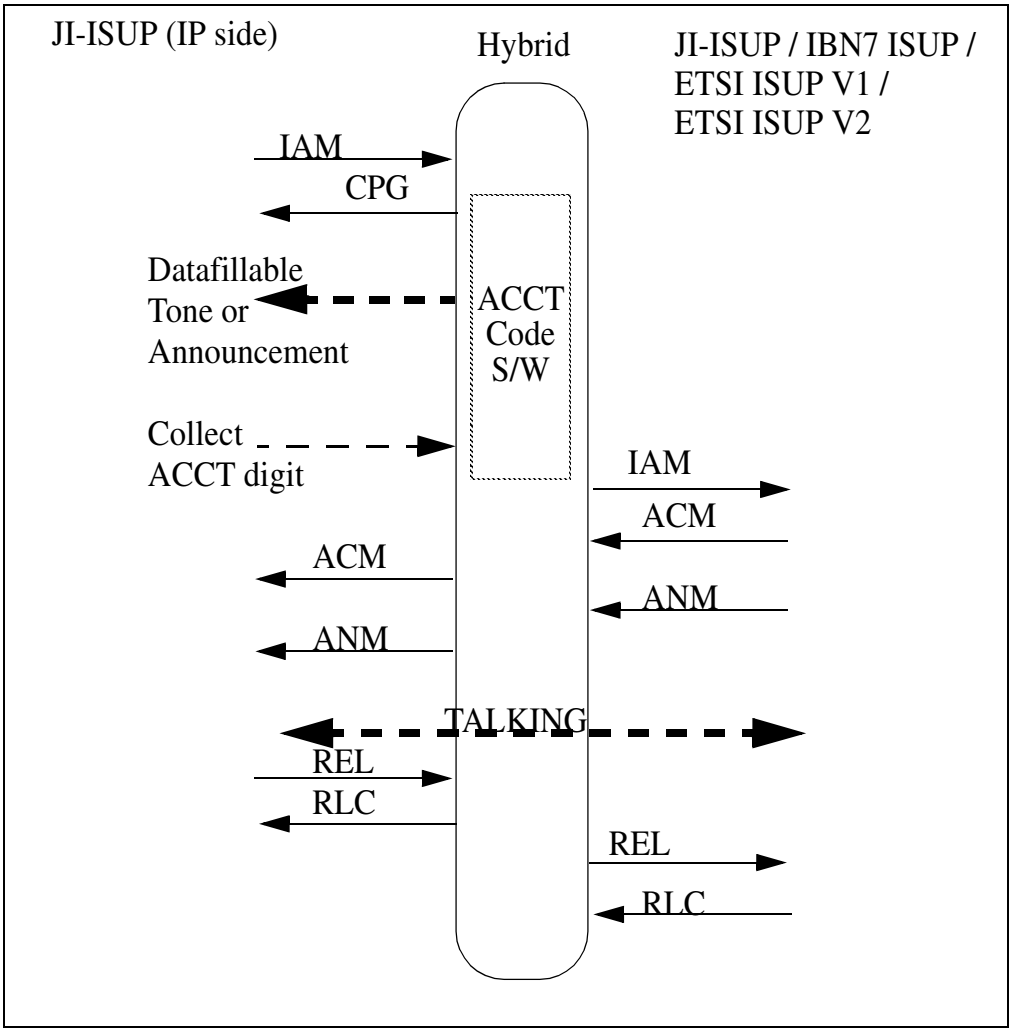
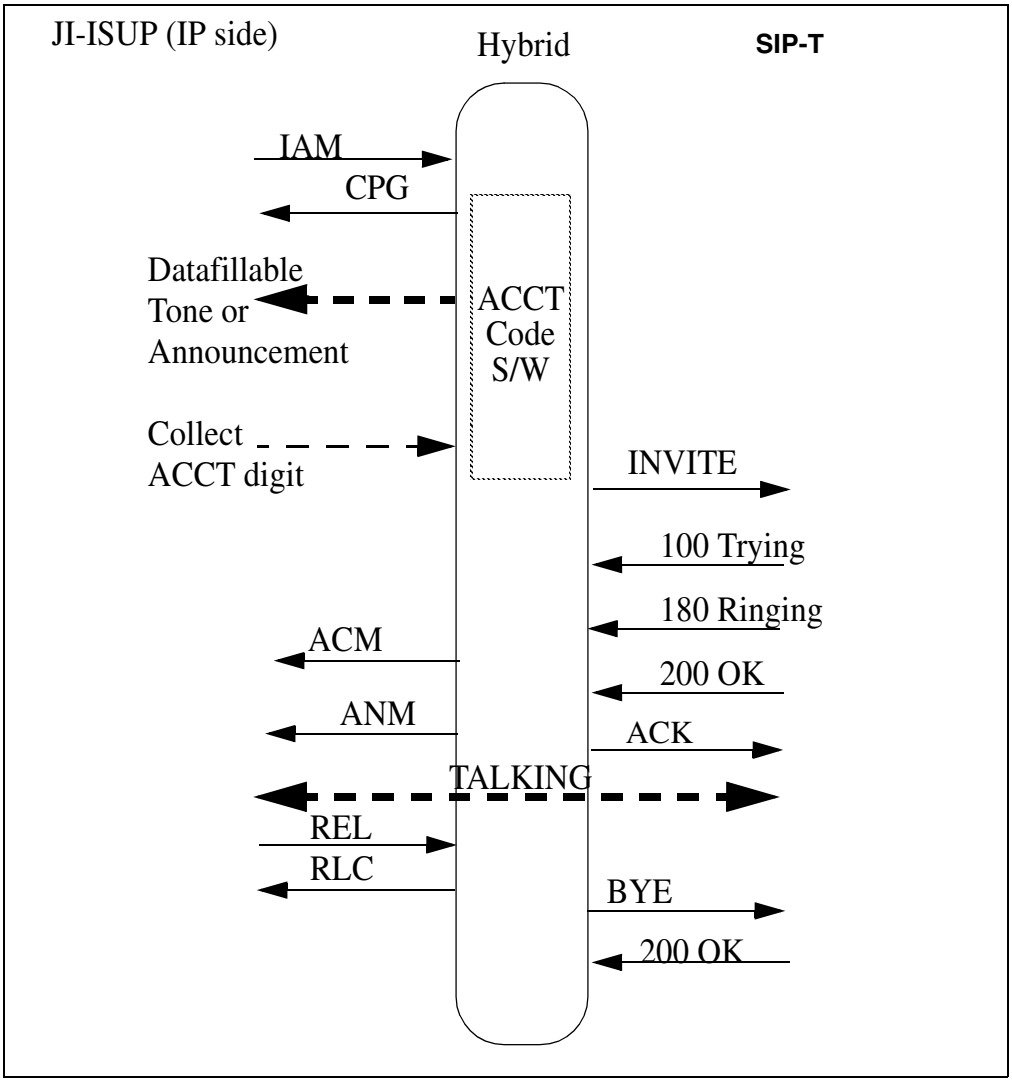


Figure 15 ACCT Interworking with SIP-T Functional Behavior Diagram



49.2.4.2 Reset Tone

When entering the account code, the subscriber has the option to enter the reset digit (*). This causes all account code digits entered by the subscriber during the present stage of dialing to be ignored and “Reset tone” is played. This tone is stopped when first digit is received or reset tone duration is time out.

~~The reset tone duration is controlled by the office parameter RESET_TONE_DURATION_160MS in table OFCVAR.~~

~~For JI-ISUP or IBN7 ISUP to account code calls, the maximum reset tone duration is 24 seconds, even if datafill represents a larger value.~~

The specification of reset tone is shown in Table 6 ”Specification of Reset tone”.

Table 6 Specification of Reset tone

Tone	Single Frequency	Cadence	Duration	Level
Reset Tone (for reset of the digit collection)	400 Hz	Constant	~~Datafillable~~ (0.5 second)	-16 dBmO +/-0.5 dB

49.2.4.3 Tone/Announcement Handling

The JI-ISUP agent, on receipt of the first digit, handles the tone/announcement in the following fashion:

- 0 - 9, ‘*’ - Tone/Announcement stopped
- ‘#’ - Tone stopped/Announcement continues

49.2.4.4 Effect On Permanent Signal Timer

If digit 0 through 9 is entered as a first digit then the permanent signal timer is stopped, and the interdigit timer is used to collect the remaining digits.

If `*' or `#' is entered as the first digit the handling of the permanent signal timer is shown in Table 7 ”Account Code Handling of First Digit” .

Table 7 Account Code Handling of First Digit

Digit Entered	Perm Signal Timer
* (asterisk)	restarted
#(octothorpe)	restarted

49.3 Hardware Requirements or Dependencies

Announcement hardware UAS needs to be present in Hybrid.

49.4 Software Requirements or Dependencies

. N/A

49.5 Limitations and restrictions

. N/A

49.6 Interactions

Due to this activity is a migration, we don't change any code about interaction. So all the interactions are the same as the legacy MMP features.

For more information about NTC, please refer to original documents in AR0480, AR1344, AR1599, AR1816 and A59017299.

For more information about CNN, please refer to original documents in A59027517 and A59034248.

For a detailed description about ACCT, please refer to activities AR2028 and A59017299.

49.7 Applicable customer facing sections

Fault Management

- Logs N/A
- Alarms N/A

Configuration

- Data Schema N/A
- User Interface N/A
- Element Management N/A
- Security N/A
- Service Order N/A
- Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

49.8 Glossary

Term	Description
ACCT	Account Code
ACM	Address Complete Message
ANM	Answer Message
BLO	Blocking Message

Term	Description
BLA	Blocking Acknowledgement Message
CIEC	Chosen Intermediate Exchange Carrier
CNN	Carrier Name Notification
CPG	Call Progress Message
CSM	Channel Supervision Message (CallP)
DMS	Digital Multiplex System
DT	Dial Tone
ENTRY_POI_CA	Entry Point of Interconnect - Charge Area
ENTRY_POI_CAT	Entry Point of Interconnect - Category
EXIT_POI_CA	Exit Point of Interconnect - Charge Area
EXIT_POI_CAT	Exit Point of Interconnect - Category
IAA	Inter Administration Accounting
IAM	Initial Address Message
IEC	Intermediate Exchange Carrier
INTL_CALLED	International Called Carrier
JI-ISUP	Japan Interconnect ISUP
MCMP	Media Controller Messaging Protocol
MGCP	Media Gateway Controller Protocol
MMP	Multiple Market Platform
MTM	Maintenance Trunk Module
NCCI ISUP	New Common Carrier Interface ISUP
NTC	Notification of Time and Charge
OLEC	Originating Local Exchange Carrier
POI	Point of Interconnect
PVG	Passport Voice Gateway
RBT	Ring Back Tone

Term	Description
REL	Release Message
RLC	Release Complete
TCIT	Transit Carrier Indicator
TLEC	Terminating Local Exchange Carrier
TLC	Test Line Call
TMR	Transmission Medium Requirement
TNS	Transit Network Selection
TPT	Terminal Processing Task (CallP)
UAS	Universal Audio Server
UBL	Unblocking Message
UBA	Unblocking Acknowledgement Message
UUI	User to User Information
UUInd	User to User Indicator

49.9 Reference

[1] AR0480 Notification Of Time & Charge

[2] AR1344 NTC

[3] AR1599 Enhancement to NTC

[4] AR1816 Multilingual NTC

[5] A19013546 Announcement Provisioning

[6] A59017299 Japan Interconnect ISUP

[7] Simcoe, Chris. International Succession Japan NTC. Nov 2001. http://snarch.us.nortel.com/files/Architecture%20Areas/Solutions/VToIP/Solution%20Checklist/SN05/International/Information/Japan%20NTC%20on%20CS2000%20v0.1.zip

[8] A59027517 Equal Access Carrier Name Notification

[9] A59034248 Japan Interconnect ISUP Carrier Name Notification Feature for Carrier Designation

[10] A59040192 Carrier Name Notification for Japan

[11] AR2028 original account code feature documentation.

[12] A59017299 Japan Interconnect ISUP

[13] A59040239 Japan Account Code service.

[14] AU2343 Inter-Administration Accounting for International Carriers

49.10 Appendix A: Datafill Sample

```
%% Notification of Time and Charge (NTC)
%% For detail datafill of NTC, firstly please refer to features AR1344, AR1599,
%% AR1816, A59017299 and A19013564.

%% UAS must be provisioned to support variable announcements for 9 languages used
%% by NTC service

%% For AMA billing

TABLE OFCENG
CDR_FORMAT                CDR_NIL_FORMAT
CDR_ENABLE_LOG_ALL        N
UNIVERSAL_AMA_BILLING     Y
ALLOC_UNIV_EXT_BLK        Y


TABLE OFCOPT
LAMA_OFFICE               Y
SMDR_OFFICE               N


TABLE AMAOPTS
LOGAMA   ON


TABLE CRSFMT
AMA     BCFMT         N   NIL_FM      N        N        0
SMDR   SMDRFMT        N   NIL_FM      N        N        0


SOC -> select group rbil
    -> assign state idle to RBIL0014
    -> quit



%% For announcement

TABLE CLLI
NTCCHN   195       10                      NTC_CHINESE


TABLE ANNS
NTCCHN    ALL      25        0      1        NTC    10  NTC_CHN
```

```
TABLE ANNMEMS
NTCCHN    0      UAS AUD 0 AUD 11


TABLE ANNPHLST
NTCCHN 5 NTCCHMAN1 $


TABLE ANNAUDID
NTCCHMAN1 6000



%% For Japan Market
TABLE OFCENG
MARKET_OF_OFFICE JAPAN



%% For NTC feature triggering

TABLE OFCVAR
NTC_XLATIONS FA NTCFTR
NTC_REATTEMPTS   0
NTC_ANNC_CONTROL 2 2


TABLE PXCODE
GDNTLXLA  062 062 FEATINFO NTC DUR_ADJ 1 $ 3 7 17 PX GDNTLXLA


TABLE NTCLANGS
DFLT1       5          CHINESE_NTC_ANNOUCEMENT


TABLE DNSCRN


TABLE AREANAME


TABLE FAHEAD
NTCFTR SDFLT NODFOP NOCON F
NTCRTE SDFLT NODFOP NOCON F


TABLE FACODE
NTCFTR 0 9 DMOD INSRT 062 XLT FA NTCRTE $
NTCRTE 062 062 RTE PF 3 DEST 2 $


TABLE FARTE
NTCRTE 2 S JIISUP2K


TABLE CCGROUPS
CHN


TABLE CC2GROUP
602 CHN
9 CHN
```

```
8 CHN
7 CHN
6 CHN


TABLE DAYOFWK
MON WD
TUE WD
WED WD
THU WD
FRI WD
SAT WD
SUN WD


TABLE TODCHG
CHN WD D D D
```

```
GDNTXLA2 DFLT FEATINFO CALLCHAR (CPGCGIND CI_CHARGE)$ 0 6 22 PX GDNTXLA2 NODFOP
NOCON STD


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% Account Code (ACCT)

TABLE CUSTHEAD
PRADEFAULT PRAXLA NDGT NIL (VACTRMT 0) (EXTNCOS 0) (ACCT 4 N N N N) (SUPERCNF )
(ACR ACCT 1) (ACRANN ACCTANNC) $


TABLE NCOS
PRADEFAULT 0 PRAD 0 0 (ACR N) $


TABLE IBNXLA
PRAXLA 441 NET Y Y 0 N CSDIG N Y DOD N CSIDXA CSGRPA CS_NIL NONE $


TABLE ISERVOPT
ACCTCODE ACCTCODE Y


TABLE OFCVAR
DIG_COL_MAX_RESETS 3
RESET_TONE_DURATION_160MS 3


TABLE: OFCENG
LN_PERM_SIG_TIME 125
LN_SHORT_PARTIAL_DIAL_TIME 25


TABLE IBNTREAT
PRADEFAULT 1 N S FAILACCT


TABLE AMAOPTS
CDAR ON
TRMTID_CAPTURE ON
```

49.11 Appendix B: Mappings between JI-ISUP and ETSI ISUP V1

49.11.1 JI-ISUP to ETSI ISUP V1 Interworking

Table 8 JI-ISUP to ETSI ISUP V1 Message Mappings

JI-ISUP Messages	Trigger Direction (Table reference)	ETSI ISUP V1 Messages
IAM	=> (Table 9)	IAM
ACM	<= (Table 11)	ACM
ANM	<= (Table 13)	ANM
ACM ANM	<= (Table 13)	CON
REL	=> (Table 14)	REL
RLC	<=	No trigger
SUS/RES	<=	SUS/RES
REL	<= (Table 15)	REL
No trigger	=>	RLC
CPG	<= (Table 16)	CPG

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Nature of Connection	**Satellite Indicator**	0 0: No satellite cct. in connection	=>	0 0: No Satellite cct.	**Satellite Indicator[a]**	**Nature of Connection**
		0 1: One satellite cct. in connection.		0 1: One satellite cct.		
		1 0: Two satellite cct. in connection.		1 0: Two satellite cct.		
		1 1: Spare				
	Continuity Check Indicator	00 - continuity check not required	=>	00 - continuity check not required	**Continuity Check Indicator[a]**	
		01 - continuity check required		10 - continuity check performed on a previous circuit		
		10 - continuity check performed on a previous circuit				
		11 - spare		00 - continuity check not required		
	Echo Control Device Indicator	0 - outgoing half echo control device not included	=>	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**Echo Control Device Indicator**	
		1 - outgoing half echo control device included	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Forward Call Indicator	**National/ International Call Indicator**	0 - call to be treated as a national call	=>	Value based on the settings of CLASS field in translations	**National/ International Call Indicator**	**Forward Call Indicator**
		1 - call to be treated as an international call	=>	1 - call to be treated as an international call		
	End-to-End Method Indicator	00 - no end-to-end method available	=>	00 - no end-to-end method available	**End-to-End Method Indicator**	
		01-11 spare	=>			
	Interworking Indicator	0 - no interworking encountered	=>	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	=>	1 - interworking encountered		
	End-to-End Information Indicator	0 - no end-to-end information available	=>	0 - no end-to-end information available	**End-to-End Information Indicator**	
		1 - spare	=>			
	ISDN User Part Indicator	0 - ISDN user part not used all the way	=>	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	
		1 - ISDN user part used all the way	=>	1 - ISDN user part used all the way		
	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	=>	Please refer to "Table 10 ISUP Preference Indicator Parameter Coding" on page 479.	**ISDN User Part Preference Indicator**[a]	
		01 - ISDN user part not required all the way	=>			
		10 - ISDN user part required all the way	=>			
		11 - spare	=>	Release the call.		
	ISDN Access Indicator	0 - origination access non-ISDN	=>	0 - origination access non-ISDN	**ISDN Access Indicator**	
		1 - origination access ISDN	=>	1 - origination access ISDN		
	SCCP Method Indicator	00 - no indication	=>	00 - no indication	**SCCP Method Indicator**	
		01-11 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party category		00000000 - CPC unknown		00001010 - ordinary calling subscriber	**Calling Party category**	
		00000001 - spare 00000010 - spare 00000011 - spare 00000100 - spare 00000101 - spare	=>	00000000 - CPC unknown		
		0000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement	=>	00001010 - ordinary calling subscriber		
		00001001 - national operator desk	=>	00001010 - ordinary calling subscriber		
		00001010 - ordinary calling subscriber	=>	00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority	=>	00000000 - CPC unknown		
		00001100 - data call	=>	00000000 - CPC unknown		
		00001101 - test call	=>	00001101 - test call		
		00001111 - payphone	=>	00001111 - payphone		
		00010000-11110000 spare	=>	00001010 - ordinary calling subscriber		
		11110001-11111110 reserved for national use 11111111 - spare	=>	00001010 - ordinary calling subscriber		

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Transmission Medium Requirement		00000000 - Speech	=>	00000000 - speech	**User Services Information**	
		00000001 - spare	=>	Call is released.		
		00000010 - 64kbit/s Unrestricted	=>	00000010 - 64kbit/s Unrestricted		
		00000011 - 3.1 kHz Audio	=>	00000011 - 3.1 kHz Audio		
		00000100 - Alt speech	=>	Call is released.		
		00000101 - Alt 64K	=>			
		00000110 - 64K pref	=>			
		00000111 - spare	=>			
		00001000 - 384kbit/s unrestricted	=>			
		00001001-11111111 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	Set as required	**Odd/Even Indicator**	**Called Party Number**[b]
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000000 - spare	=>	Release the call	**Nature of Address Indicator**	
		0000001 - subscriber's number	=>			
		0000010 - reserved for national use	=>			
		0000011 - National number	=>	0000011 - National number		
		0000100 - International number	=>	Release the call		
		0000101-1101111 spare	=>			
		1110000-1111101 reserved for national use	=>			
		1111110 - peculiar number of network	=>	0000011 - National number		
		1111111 - spare	=>	Release the call		
	Internal Network Number Indicator	0 - routing to an internal network number allowed	=>	0 - routing to an internal network number allowed	**Internal Network Number Indicator**	
		1 - routing to an internal network number not allowed	=>			
	Numbering Plan Indicator	000 - spare	=>	001 - ISDN numbering plan (If ALL_NPI is datafilled in table TRKSGRP of both trks, then all values map to 001; If not, the call will release except for value 001)	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>			
		010-111 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Called Party Number**
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1111 - ST	=>	Treatment is set and call is released if these values are received.		
		1010 - spare	=>			
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	Set as required	**Odd/Even Indicator**	**Calling Party Number**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000000 - spare	=>	0000011 - National number	**Nature of Address Indicator**	
		0000001 - subscriber's number	=>			
		0000010 - reserved for national use	=>			
		0000011 - National number	=>			
		0000100 - International number	=>			
		0000101-1101111 spare	=>			
		1110000-1111101 reserved for national use	=>			
		1111110 - peculiar number of network	=>			
		1111111 - spare	=>			
	Calling Party Number Incomplete Indicator	0 - complete	=>	0 - complete	**Calling Party Number Incomplete Indicator**	
		1 - incomplete	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Numbering Plan Indicator**	000 - spare	=>	CGPN is discarded	**Numbering Plan Indicator**	**Calling Party Number**
		001 - ISDN numbering plan	=>	001 - ISDN numbering plan		
		010-111 spare	=>	CGPN is discarded		
	Address Presentation Restricted Indicator	00 - presentation allowed	=>	00 - presentation allowed	**Address Presentation Restricted Indicator**	
		01 - presentation restricted	=>	01 - presentation restricted		
		10 - address not available	=>	00 - presentation allowed		
		11 - spare	=>			
	Screening Indicator	00 - spare	=>	01 - user provided, verified and passed	**Screening Indicator**	
		01 - user provided, verified and passed	=>			
		10 - reserved	=>			
		11 - network provided	=>	11 - network provided		

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Calling Party Number**[b]
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1010 - spare	=>	Treatment is set and call is released if these values are received.		
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
		1111 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	
Access Transport			=>	**Access Transport**		
Generic Number			=>	**Discarded**		
All other parameters			=>	Discarded		

a. This value is encoded based on incoming information and existing datafill. Datafill may result in values other than those shown.
b. Fields within this parameter will be set based on translations unless there is only one possible value for that field.

Table 10 ISUP Preference Indicator Parameter Coding

Information Field	**JI-ISUP -->**	**ETSI ISUP V1**	**JI-ISUP -->**	**ETSI ISUP V1**
Supplementary Service	**None (No UUI, ATP or CLIP present in the IAM)**		**Any (UUI, ATP and/or CLIP present in the IAM)**	
(Applies to messages: IAM)	**Bits**	**Bits**	**Bits**	**Bits**
ISUP Preferred	HG	HG	HG	HG
For Bearer Service = Speech	00	01	00	00
For Bearer Service = 3.1 kHz Aud.	00	01	00	00
For Bearer Service = 64k Unres.	00	00	00	00
ISUP Not Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	01	01	01	00
For Bearer Service = 3.1 kHz Aud.	01	01	01	00
For Bearer Service = 64k Unres.	01	00	01	00
ISUP Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	10	01	10	00
For Bearer Service = 3.1 kHz Aud.	10	01	10	00
For Bearer Service = 64k Unres.	10	00	10	00

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	00 - No Indication	**<=**	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	**<=**	01 - No Charge		
		10 - Charge	**<=**	10 - Charge		
		10 - Charge	**<=**	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	**<=**	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	**<=**	01 - subscriber free		
		00 - no indication	**<=**	10 - connect when free		
		00 - no indication (default)	**<=**	11 - spare		
	Called Party's Category Indicator	00 - no indication	**<=**	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	**<=**	01 - ordinary subscriber		
		10 - payphone	**<=**	10 - payphone		
		00 - no indication (default)	**<=**	11 - spare		
	End-to-End Method Indicator	00 - no end-to-end method available	**<=**	00 - no end-to-end method available	**End-to-End Method Indicator**	
				01 - pass along method available		
				10 - SCCP method available		
				11 - SCCP and Pass along methods available		
	Interworking Indicator	0 - no interworking encountered	**<=**	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	**<=**	1 - interworking encountered		
	End-to-End Info Indicator	0 - no end-to-end information available	**<=**	0 - no end-to-end information available	**End-to-End Info Indicator**	
			<=	1 - end-to-end information available		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**ISDN User Part Indicator**	0 - ISDN user part not used all the way	**<=**	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	**Backward Call Indicators**
		1 - ISDN user part used all the way	**<=**	1 - ISDN user part used all the way		
	Holding Indicator	0 - holding not requested	**<=**	0 - holding not required	**Holding Indicator**	
				1 - holding required		
	SCCP Method Indicator	00 - no indication	**<=**	00 to 11 - any value	**SCCP Method Indicator**	
	ISDN Access Indicator	0 - terminating access non-ISDN	**<=**	0 - terminating access non-ISDN	**ISDN Access Indicator**	
		1 - terminating access ISDN	**<=**	1 - terminating access ISDN		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**<=**	0 - incoming half echo control device not included	**Echo Control Device Indicator**	
			<=	1 - incoming half echo control device included		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	00 - CCITT	**Coding Standard**	**Cause Indicators**
			<=	All other values		
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0100 - public network serving the remote user	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		1010 - network beyond interworking point	**<=**	1010 - network beyond interworking point		
		0111 - international network	**<=**	All other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 484.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	0 - octet continues thru the next octet	**Extension Indicator**	
			<=	1 - Last Octet		
	Recommendation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommendation(Octet 1a)**	
Access Transport		transit without alteration	**<=**	**Access Transport**		
discarded			**<=**	**User to User Information**		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Optional Backward Call Indicators	**In-band Information indicator**	1 - in band information or an appropriate pattern is now available	**<=**	0 - no indication	**In-band Information indicator**	**Optional Backward Call Indicators**
			<=	1 - in band information or an appropriate pattern is now available		
	Call Forwarding May Occur indicator	0 - no indication	**<=**	0 - no indication	**Call Forwarding May Occur indicator**	
			<=	1 - call diversion may occur		
	Simple Segmentation Indicator	0 - No Additional Information will be sent	**<=**	0 - No Additional Information will be sent	**Simple Segmentation Indicator**	
			<=	1 - Additional Information will be sent in the segmentation message		
discarded			**<=**	**Call Reference**		
discarded			**<=**	**Connection Request**		
discarded			**<=**	**Information Indicator**		
discarded			**<=**	**Redirection Information**		

Table 12 Cause Value Parameter Coding

Information Field	**JI-ISUP -> ETSI V1**		**ETSI V1 -> JI-ISUP**	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Normal Event	**00X XXXX**	**00X XXXX**	**00X XXXX**	**00X XXXX**
Unallocated Number	000 0001	000 0001	000 0001	000 0001
No route to destination	000 0011	000 0011	000 0011	000 0011
Send Special Information Tone	000 0100	000 0100	000 0100	000 0100
Qor ported	000 1110	0001110	000 1110	000 1110
Normal Call Clearing	001 0000	001 0000	001 0000	001 0000
User Busy	001 0001	001 0001	001 0001	001 0001
No Response From Called User	001 0010	001 0010	001 0010	001 0010
No ans. from user (user alerted)	001 0011	001 0011	001 0011	001 0011
Subscriber Absent	001 0100	001 0100	0010100	001 0100
Call Rejected	001 0101	001 0101	001 0101	001 0101
Number changed	001 0110	001 0110	001 0110	001 0110
Destination out of order	001 1011	001 1011	001 1011	001 1011
Address Incomplete	001 1100	001 1100	001 1100	001 1100
Facility Reject	001 1101	001 1101	001 1101	001 1101
Apply locally			001 1110	001 1111
Normal, Unspecified	001 1111	001 1111	001 1111	001 1111
All other values in this category	Other values	001 1111	Other Values	Tandem

Table 12 Cause Value Parameter Coding

Information Field	**JI-ISUP -> ETSI V1**		**ETSI V1 -> JI-ISUP**	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Resource unavailable	**010 XXXX**	**010 XXXX**	**010 XXXX**	**010 XXXX**
Circuit Congestion	010 0010	010 0010	010 0010	010 0010
Network out of order	010 0110	010 0110	010 0110	010 0110
Temporary Failure	010 1001	010 1001	010 1001	010 1001
Switching Equipment Failure	010 1010	010 1010	010 1010	010 1010
Requested channel not avail.	010 1100	010 1100	010 1100	010 1100
Preemption			010 1101	111 1111
No preemption ckt avail			010 1110	111 1111
Resource unavailable	010 1111	010 1111	010 1111	010 1111
All Other values in this category	Other Values	010 1111	Other values	Tandem
Service or option not available	**011 XXXX**	**011 XXXX**	**011 XXXX**	**011 XXXX**
Req'sted facility, not subscribed	011 0010	011 1111		
Bearer capability not authorized	011 1001	011 1001	011 1001	011 1001
Bearer Cap. not presently avail.	011 1010	011 1010	011 1010	011 1010
Serv./opt. not avail - unspec	011 1111	011 1111	011 1111	011 1111
All Other values in this category	Other Values	011 1111	Other Values	Tandem
Service option not implemented	**100 XXXX**	**100 XXXX**	**100 XXXX**	**100 XXXX**
Bearer Capability Not Implmtd	100 0001	100 0001	100 0001	100 0001
Chnl type not impl			100 0010	100 1111
Svc./opt. not avail - unspec'd	100 1111	100 1111	100 1111	100 1111
All Other values in this category	Other Values	100 1111	Other Values	Tandem

Table 12 Cause Value Parameter Coding

Information Field	JI-ISUP -> ETSI V1		ETSI V1 -> JI-ISUP	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Invalid message	**101 XXXX**	**101 XXXX**	**101 XXXX**	**101 XXXX**
Inv call ref value			101 0001	101 1111
Bearer capability not authorized	101 0111	101 0111		
Incompatible destination	101 1000	101 1000	101 1000	101 1000
Invalid message - unspecified	101 1111	101 1111	101 1111	101 1111
All Other values in this category	Other Values	101 1111	Other Values	Tandem
Protocol error	**110 XXXX**	**110 XXXX**	**110 XXXX**	**110 XXXX**
Inv parm contents			110 0100	110 1111
Recovery on Timer Expiry	110 0110	110 0110	110 0110	110 0110
Protocol error - unspecified	110 1111	110 1111	110 1111	110 1111
All Other values in this category	Other Values	110 1111	Other Values	Tandem
Interworking	**111 XXXX**	**111 XXXX**	**111 XXXX**	**111 XXXX**
Interworking Unspecified	111 1111	111 1111	111 1111	111 1111
All Other values in this category	Other Values	111 1111	Other Values	Tandem

Table 13 Parameter Mapping - ETSI ISUP V1 ANM/CON[a] to JI-ISUP ANM

		JI-ISUP ANM	dir	ETSI ISUP V1 ANM/CON		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	10 - Charge	**<=**	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	**<=**	01 - No Charge		
		10 - Charge	**<=**	10 - Charge		
		10 - Charge	**<=**	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	**<=**	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	**<=**	01 - subscriber free		
		00 - no indication	**<=**	other values		
	Called Party's Category Indicator	01 - ordinary subscriber	**<=**	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	**<=**	01 - ordinary subscriber		
		10 - payphone	**<=**	10 - payphone		
		01 - ordinary subscriber	**<=**	11 - spare		
	End-to-End Method Indicator	00 - no end-to-end method available	**<=**	00 - no end-to-end method available	**End-to-End Method Indicator**	
				01 - pass along method available		
				10 - SCCP method available		
				11 - SCCP and Pass along methods available		
	Interworking Indicator	0 - no interworking encountered	**<=**	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	**<=**	1 - interworking encountered		
	End-to-End Info Indicator	0 - no end-to-end information available	**<=**	0 - no end-to-end information available	**End-to-End Info Indicator**	
			<=	1 - end-to-end information available		

Table 13 Parameter Mapping - ETSI ISUP V1 ANM/CON[a] to JI-ISUP ANM

		JI-ISUP ANM	dir	ETSI ISUP V1 ANM/CON		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**ISDN User Part Indicator**	0 - ISDN user part not used all the way	**<=**	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	**Backward Call Indicators**
		1 - ISDN user part used all the way	**<=**	1 - ISDN user part used all the way		
	Holding Indicator	0 - holding not requested	**<=**	0 - holding not required	**Holding Indicator**	
				1 - holding required		
	SCCP Method Indicator	00 - no indication	**<=**	00 to 11 - any value	**SCCP Method Indicator**	
	ISDN Access Indicator	0 - terminating access non-ISDN	**<=**	0 - terminating access non-ISDN	**ISDN Access Indicator**	
		1 - terminating access ISDN	**<=**	1 - terminating access ISDN		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**<=**	0 - incoming half echo control device not included	**Echo Control Device Indicator**	
			<=	1 - incoming half echo control device included		
Access Transport		transit without alteration	**<=**	**Access Transport**		
discarded			**<=**	**User to User Information**		
discarded			**<=**	**Call Reference**		
discarded			**<=**	**Connection Request**		
discarded			**<=**	**Information Indicator**		
discarded			**<=**	**all other parameters**		

a. CON is mapped to a ACM and a ANM message. The ACM has the same BCI parameter as ANM.

Table 14 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	All values	=>	00 - CCITT	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	=>	0000 - user	**Location**	
		0001 - private network serving the local user	=>	0101 - private network serving the remote user		
		0010 - public network serving the local user	=>	0111 - international network		
		0011 - transit network	=>	0011 - transit network		
		0100 - public network serving the remote user	=>	0100 - public network serving the remote user		
		0101 - private network serving the remote user	=>	0101 - private network serving the remote user		
		0111 - international network	=>	0111 - international network		
		1010 - network beyond interworking point	=>	1010 - network beyond interworking point		
		All other values	=>	1010 - network beyond interworking point		
	Cause Value	value	=>	Please refer to “Table 12 Cause Value Parameter Coding” on page 484.	**Cause Value**	
	Extension Indicator	All Values	=>	1 - Last Octet	**Extension Indicator**	
	Recommendation(Octet 1a)	All Values	=>	Octet Discarded	**Recommendation(Octet 1a)**	
	Extension Indicator(Octet 1a)	All Values	=>	Octet Discarded	**Extension Indicator(Octet 1a)**	
User to User Information			=>	No mapping		
Redirection Number			=>	No mapping		

Table 14 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Para meter	Field	Field Value	=>	Field Value	Field	Para meter
Domestic Redirection Reason			=>	No mapping		

Table 15 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	All Values	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0100 - public network serving the remote user	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		0111 - international network	**<=**	all other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 484.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	All Values	**Extension Indicator**	
	Recommendation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommendation(Octet 1a)**	
	Extension Indicator(Octet 1a)	Octet Discarded	**<=**	All Values	**Extension Indicator(Octet 1a)**	
Discarded			**<=**	**Access Transport**		
no mapping			**<=**	**User to User Information**		
no mapping			**<=**	**Automatic congestion level**		
no mapping			**<=**	**All other parameters**		

Table 16 Parameter Mapping - ETSI ISUP V1 CPG to JI-ISUP CPG

		JI-ISUP CPG	dir	ETSI ISUP V1 CPG		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Event Information	**Event Indication**	0000010 - PROGress		0000000 - spare	**Event Indication**	**Event Information**
		0000001 - ALERTing		0000001 - ALERTing		
		0000010 - PROGress		0000010 - PROGress		
		0000011 - In-band information or appropriate pattern is now available		0000011 - In-band information or appropriate pattern is now available		
		0000100 - call forwarded on busy	**<=**	0000100 - call forwarded on busy		
		0000101 - call forwarded on no reply		0000101 - call forwarded on no reply		
		0000110 - call forwarded unconditional		0000110 - call forwarded unconditional		
		0000010 - PROGress		0000111 to 1111111 - spare		
	Event presentation restricted indicator	0 - no indication		0 - no indication	**Event presentation restricted indicator**	
			<=	1 - presentation restricted		
Access Transport			**<=**	**Access Transport**		
User to User Information			**<=**	**User to User Information**		

49.11.2 ETSI ISUP V1 to JI-ISUP Interworking

Table 17 ETSI ISUP V1 to JI-ISUP Message Mappings

ETSI ISUP V1 Messages	Trigger Direction (Ref Table)	JI-ISUP Messages
IAM	=> (Table 18)	IAM
ACM	<= (Table 19)	ACM
ANM	<= (Table 20)	ANM
REL	=> (Table 19)	REL
RLC	<=	No trigger
REL	<= (Table 20)	REL
No trigger	=>	RLC
SUS/RES	<= (Table 21)	SUS/RES
CPG	<= (Table 22)	CPG

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Nature of Connection	**Satellite Indicator**	0 0: No satellite cct. in connection	=>	0 0: No Satellite cct.	**Satellite Indicator[a]**	**Nature of Connection**
		0 1: One satellite cct. in connection.	=>	0 1: One satellite cct.		
		1 0: Two satellite cct. in connection.	=>	0 1: One satellite cct.		
		1 1: Spare	=>	0 1: One satellite cct.		
	Continuity Check Indicator	00 - continuity check not required	=>	00 - continuity check not required	**Continuity Check Indicator[a]**	
		01 - continuity check required	=>			
		10 - continuity check performed on a previous circuit	=>			
		11 - spare	=>			
	Echo Control Device Indicator	0 outgoing half echo control device not included	=>	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**Echo Control Device Indicator**	
		1 outgoing half echo control device included	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Forward Call Indicator	**National/ International Call Indicator**	0 - call to be treated as a national call	=>	change based on the settings of CLASS field in translations	**National/ International Call Indicator**	**Forward Call Indicator**
		1 - call to be treated as an international call	=>			
	End-to-End Method Indicator	00 - no end-to-end method available	=>	00 - no end-to-end method available	**End-to-End Method Indicator**	
		01-11 spare	=>			
	Interworking Indicator	0 - no interworking encountered	=>	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	=>	1 - interworking encountered		
	End-to-End Information Indicator	0 - no end-to-end information available	=>	0 - no end-to-end information available	**End-to-End Information Indicator**	
		1 - spare	=>			
	ISDN User Part Indicator	0 - ISDN user part not used all the way	=>	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	
		1 - ISDN user part used all the way	=>	1 - ISDN user part used all the way		
	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	=>	00 - ISDN user part preferred all the way	**ISDN User Part Preference Indicator**	
		01 - ISDN user part not required all the way	=>	01 - ISDN user part not required all the way		
		10 - ISDN user part required all the way	=>	10 - ISDN user part required all the way		
		11 - spare	=>	Release the call		
	ISDN Access Indicator	0 - origination access non-ISDN	=>	0 - origination access non-ISDN	**ISDN Access Indicator**	
		1 - origination access ISDN	=>	1 - origination access ISDN		
	SCCP Method Indicator	00 - no indication	=>	00 - no indication	**SCCP Method Indicator**	
		01-11 spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Para meter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Para meter**
Calling Party category		00001010 - ordinary calling subscriber	=>	00001010 - ordinary calling subscriber	**Calling Party category**	
		00001011 - calling subscriber with priority	=>	00001010 - ordinary calling subscriber		
		00001101 - test call	=>	00001101 - test call		
		00001111 - payphone	=>	00001111 - payphone		
		All other values	=>	00001010 - ordinary calling subscriber		
Transmission Medium Requirement		00000000 - Speech	=>	00000 - speech	**Transmission Medium Requirement**	
		00000010 - 64kbit/s Unrestricted	=>	00000010 - 64kbit/s Unrestricted		
		00000011 - 3.1 kHz Audio	=>	00000011 - 3.1 kHz Audio		
		00000100 - Alt speech	=>	Release the call		
		00000101 - Alt 64K	=>			
		00000110 - 64K pref	=>			
		All other values	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	set as required	**Odd/Even Indicator**	**Called Party Number (set according to table CDN CHAR datafill)**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000011 - National number	=>	0000011 - National number	**Nature of Address Indicator**	
		1111110 - peculiar number of network	=>			
		all other values	=>			
	Internal Network Number Indicator	0 - routing to an internal network number allowed	=>	0 - routing to an internal network number allowed	**Internal Network Number Indicator**	
		1 - routing to an internal network number not allowed	=>			
	Numbering Plan Indicator	000 - spare	=>	001 - ISDN numbering plan (default)	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>			
		010-111 spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Called Party Number**
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1111 - ST	=>	Treatment is set and call is released if these values are received.		
		1010 - spare	=>			
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	Set as required	**Odd/Even Indicator**	**Calling Party Number**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000011 - national number	=>	Set by hard-coded default logic (if CLASS selector during translation is set to INTL, then NOA is set to Peculiar; otherwise, NOA is set to National. This setting can be overwritten by table TRKCGPN datafill)	**Nature of Address Indicator**	
		1111110 - peculiar number of network	=>			
		any other value	=>			
	Calling Party Number Incomplete Indicator	0 - complete	=>	0 - complete	**Calling Party Number Incomplete Indicator**	
		1 - incomplete	=>			
	Numbering Plan Indicator	000 - spare	=>	CGPN is discarded	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>	001 - ISDN numbering plan		
		010-111 spare	=>	CGPN is discarded		
	Address Presentation Restricted Indicator	00 - presentation allowed	=>	00 - presentation allowed	**Address Presentation Restricted Indicator**	
		01 - presentation restricted	=>	01 - presentation restricted		
		10 - address not available	=>	01 - presentation restricted		
		11 - spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Screening Indicator**	00 - spare	=>	Discard CGPN	**Screening Indicator**	**Calling Party Number**
		01 - user provided, verified and passed	=>	01 - user provided, verified and passed		
		10 - reserved	=>	Discard CGPN		
		11 - network provided	=>	11 - network provided		
	Address Signals	0000 - digit 0	=>	map as it is	**Address Signals**	
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1010 - spare	=>	Discard CGPN		
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
		1111 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	
Access Transport			=>	**Access Transport**		
User Service Information			=>	**User Service Information**		
All other parameters			=>	discarded		

a. This value is encoded based on incoming information and existing datafill. Datafill may result in values other than those shown.

Table 19 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	All values	=>	00 - CCITT	**Coding Standard**	**Cause Indicators**
			=>			
	Location	0000 - user	=>	0000 - user	**Location**	
		0001 - private network serving the local user	=>	0101 - private network serving the remote user		
		0010 - public network serving the local user	=>	0100 - public network serving the remote user		
		0011 - transit network	=>	0011 - transit network		
		0100 - public network serving the remote user	=>	0100 - public network serving the remote user		
		0101 - private network serving the remote user	=>	0101 - private network serving the remote user		
		0111 - international network	=>	0111 - international network		
		1010 - network beyond interworking point	=>	1010 - network beyond interworking point		
		All other values	=>	0111 - international network		
	Cause Value	value	=>	Please refer to “Table 12 Cause Value Parameter Coding” on page 484.	**Cause Value**	
	Extension Indicator	All Values	=>	1 - Last Octet	**Extension Indicator**	
	Recommendation(Octet 1a)	All Values	=>	Octet Discarded	**Recommendation(Octet 1a)**	
	Extension Indicator(Octet 1a)	All Values	=>	Octet Discarded	**Extension Indicator(Octet 1a)**	
Access Transport			=>	discarded		
User to User Information			=>	discarded		

Table 19 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Para meter	Field	Field Value	=>	Field Value	Field	Para meter
Automatic congestion level			=>	discarded		

Table 20 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	All Values	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0111 - international network	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		1010 - Beyond an interworking point	**<=**	1010 - Beyond an interworking point		
		1010 - Beyond an interworking point	**<=**	all other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 484.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	All Values	**Extension Indicator**	
	Recommendation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommendation(Octet 1a)**	
	Extension Indicator(Octet 1a)	Octet Discarded	**<=**	All Values	**Extension Indicator(Octet 1a)**	
discarded			**<=**	**User to User Information**		
discarded			**<=**	**Redirection Number**		
discarded			**<=**	**Domestic Redirecting Reason**		

Table 21 Parameter Mapping - JI-ISUP SUS/RES to ETSI ISUP V1 SUS/RES

		ETSI ISUP V1 SUS/RES	dir	JI-ISUP SUS/RES		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Suspend/ Resume Indicators	**Suspend/ Resume Indicator**	0 - subscriber initiated	**<=**	0 - subscriber initiated	**Suspend/ Resume Indicator**	**Suspend/ Resume Indicators**
		1 - network initiated	**<=**	1 - network initiated		
	spare	0000000 - Hard code	**<=**	0000000 - Hard code	**spare**	

Table 22 Parameter Mapping - JI-ISUP CPG to ETSI ISUP V1 CPG

		ETSI ISUP V1 CPG	dir	JI-ISUP CPG		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Event Information	**Event Indication**	Discard CPG	**<=**	0000000 - spare	**Event Indication**	**Event Information**
		0000001 - ALERTing		0000001 - ALERTing		
		0000010 - PROGress		0000010 - PROGress		
		0000011 - In-band information or appropriate pattern is now available		0000011 - In-band information or appropriate pattern is now available		
		Discard CPG		0000100 - call forwarded on busy		
				0000101 - call forwarded on reply		
				0000110 - call forwarded unconditional		
				0000111 - generic notification to terminating user		
				0001000 to 1111111 - spare		
	Event presentation restricted indicator	0 - no indication	**<=**	0 - no indication	**Event presentation restricted indicator**	
				1 - presentation restricted		
Discarded			**<=**	**Cause Indicator**		
Access Transport			**<=**	**Access Transport**		
Discarded			**<=**	**User to User Information**		

50: Functional Description (FN): A00002757

50.1 Feature name

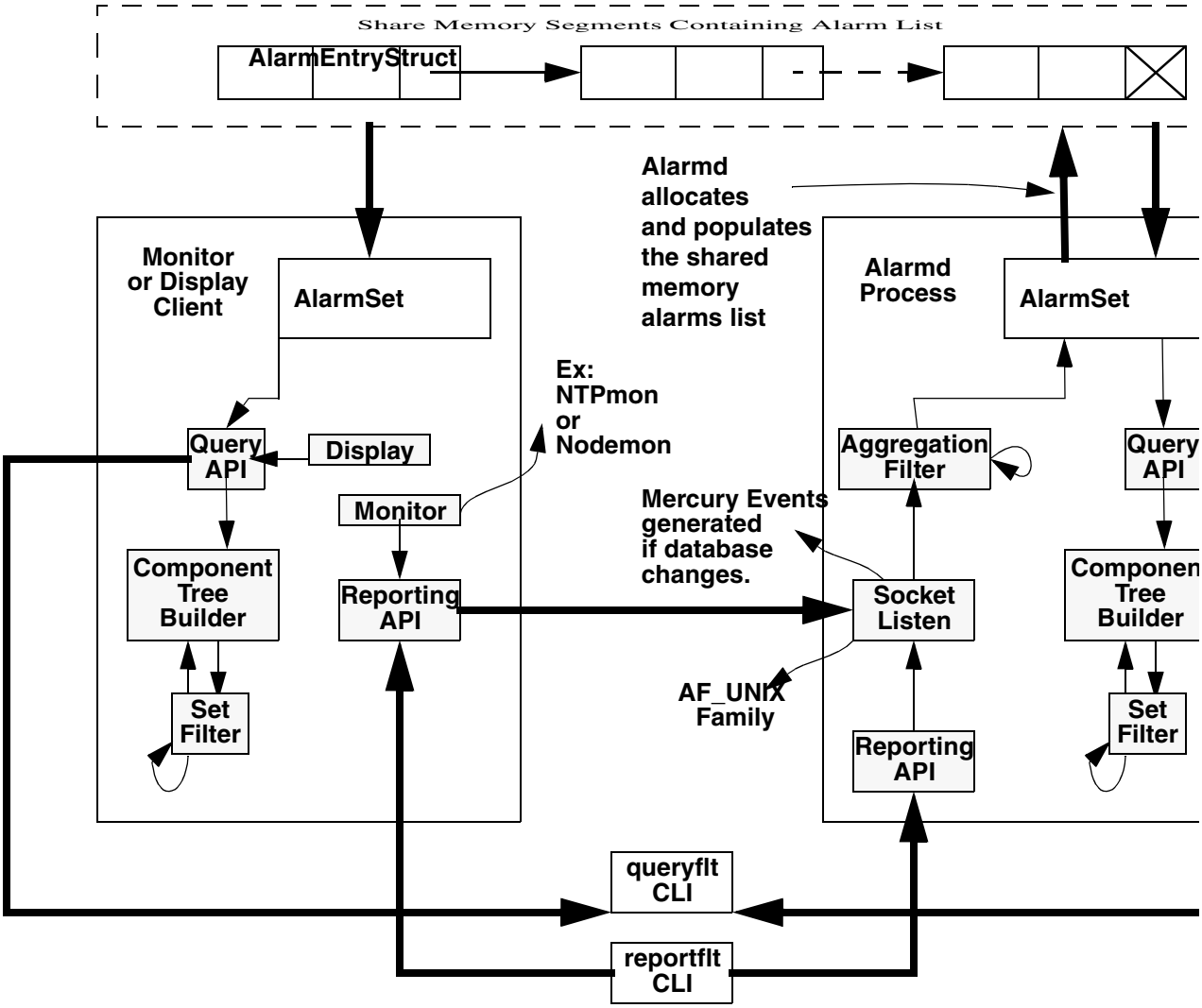
A00002757 CBM FAULT MANAGEMENT (HA)

50.2 Description

This feature provides a generic framework for centralizing fault information for the Next Generation SDM (CBM) product and for the SSPFS platform.

The mandate is to collect detailed fault information about components in the CBM cluster, maintain a list of current alarms, summarize the list in a hierarchical fashion, and report this information to clients in the desired fashion.

Figure 1 Alarmd Server/Client Process and Data Flow



50.2.1 User Interfaces

This feature will require changes to the QueryCBM command in the CBMMTC maintenance tool, as well as various Logs commands for respective CBMMTC levels.

50.3 Hardware Requirements or Dependencies

SSPFS defined platform.

50.4 Software Requirements or Dependencies

A00003617 SSPFS Alarmd Integration will provide the light control API, and component monitors for this feature.

50.5 Limitations and restrictions

N/A

50.6 Interactions

A00003617 SSPFS Alarmd Integration will provide system level monitors that will use the ReportingAPI part of this feature to record any alarms. It will also make use of the Query API in this feature to retrieve alarms stored in the Alarms Databsae.

A00002164 The Application Manager(SAM) for HA will use the Reporting API part of this feature to record any alarms. It will also make use of the Query API in this feature to retrieve alarms stored in the Alarms Databsae.

50.7 Applicable customer facing sections

Fault Management

Logs	__x___
Alarms	_____

Configuration

Data Schema	_n/a__
User Interface	__x__
Element Management	_n/a__
Security	_n/a__
Service Order	_n/a__
Office Parameters	_n/a__

Accounting (includes AMA billing) _n/a__

Performance (includes operational measurements) _n/a__

50.8 Glossary

Term	Description
New term	Definition

51: Functional Description (FN): A00002765

51.1 Feature name

XLAGRP Refinements for Coin Station-Paid Routing

51.2 Description

This feature enhances the Unbundling Translations and Routing functionality by adding the ability to refine the XLAGRP based upon the calling service class and the billing method. With this feature, outgoing translations can now be applied specifically to a coin station-paid call.

The implementation of this feature allows the full range of calling service class and billing methods to be utilized in XLAGRP refinements. New table XLACLASS allows XLAGRP refinements based on a range including coin, station, hotel, and restricted. New table XLABILL allows XLAGRP refinements based on a range including paid, collect, third, cards, special calling, special called.

51.2.1 Background

In TOP09, AF7159 introduced the XLAGRP refinement mechanism for unbundling translations and routing. It created tables XLAGRP, XLASPID, XLAODIGS, and TOPSDP to setup the refinement structure including SPID[1] and originating digits.

Translations Group (XLAGRP) names are datafilled in table XLAGRP, which allows the operating company the ability to datafill various names to represent groupings for translation purposes as needed. These XLAGRP names are then used in the refinement tables to arrive at a final XLAGRP to be used in table TOPSDP (TOPS Dial Plan).

Table TOPSDP centralizes translation and screening attributes. The index into table TOPSDP is chosen in a flexible manner, giving the operating company the ability to fit their individual network needs. Obtaining an XLAGRP and indexing into table TOPSDP is referred to as the ***XLAGRP*** method of performing translations and screening for TOPS calls.

AF7159 provided an initial XLAGRP to be defined in table TOPSTOPT, which is indexed based on a trunk group. It also provided XLAGRP refinements for SPID and originating digits.

[1]Serivice Provider Identification

In TOP12, A59006822 enhanced the XLAGRP method with additional definitions for the initial XLAGRP and additional refinements. It allowed the initial XLAGRP to be defined in table TOPEATRK for EA calls and in table OPRINFO for operator calls. It also provided XLAGRP refinements for Carrier Identification Code (CIC) and EA region, which is based on either a LATA or a ZONE as defined by feature 59006827.

This feature supports all existing XLAGRP methods and enhances the refinement characteristics by adding calling service class and billing methods.

51.2.2 New XLAGRP Refinement Order

To preserve the existing XLAGRP refinement datafill, the new refinements are added at the end of the existing order list for non-EA calls. Thus XLACLASS then XLABILL will refine after XLAODIGS. For EA calls, XLACLASS and XLABILL will refine after XLAODIGS as well. Although this inserts the new refinement tables in the middle of refinement for EA calls, it saves the extra datafill needed in XLACLASS and XLABILL to accomodate those XLACIC and XLAEAREG XLAGRPs.

The following diagrams illustrate the existing XLAGRP refinement order with the new tables, XLACLASS and XLABILL, included.

The figures below outline the refinement order for both EA and NON-EA calls:

Figure 1 XLAGRP Refinement Order NON Equal Access

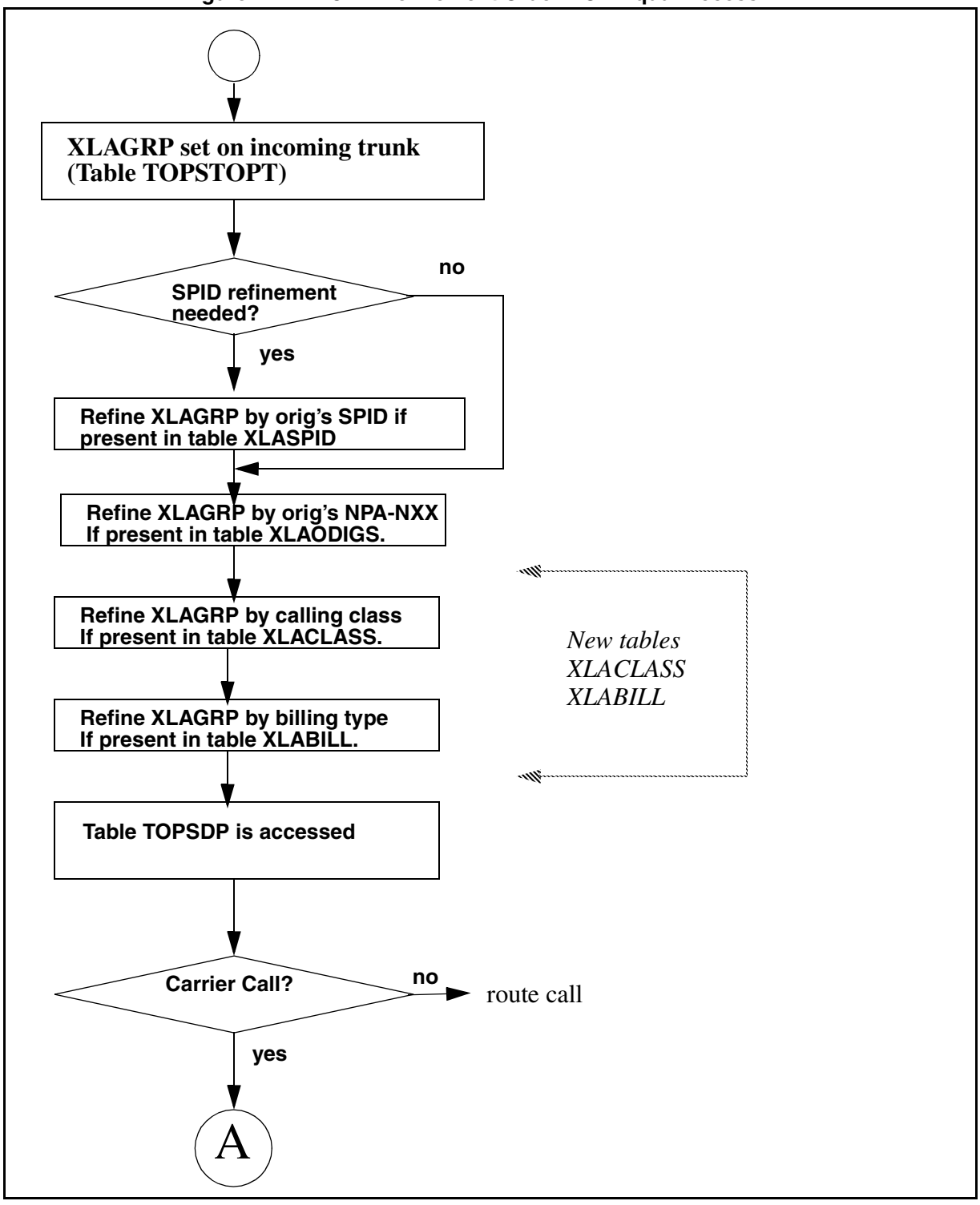


Figure 2 XLAGRP Refinement Order For Equal Acess Calls

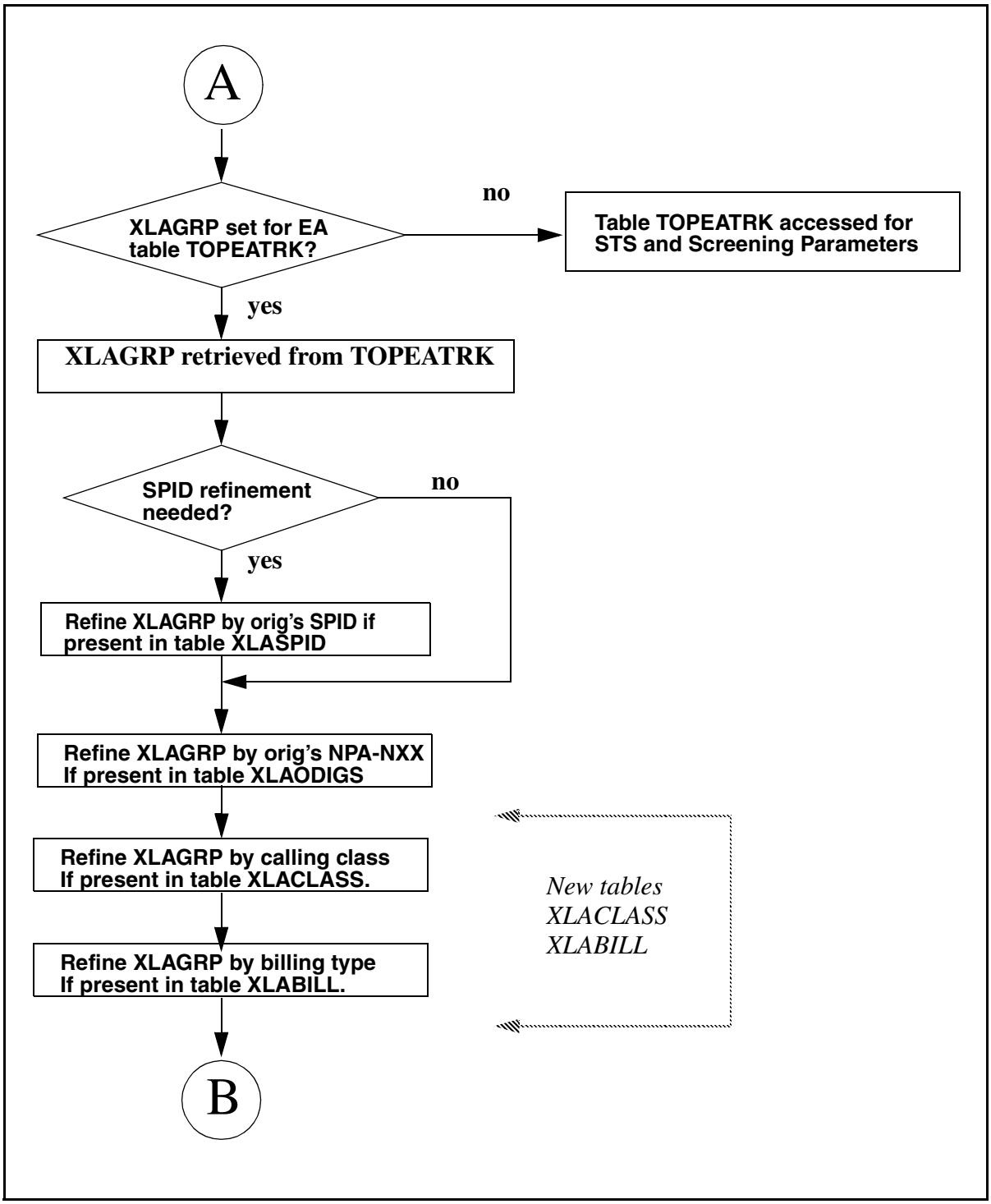
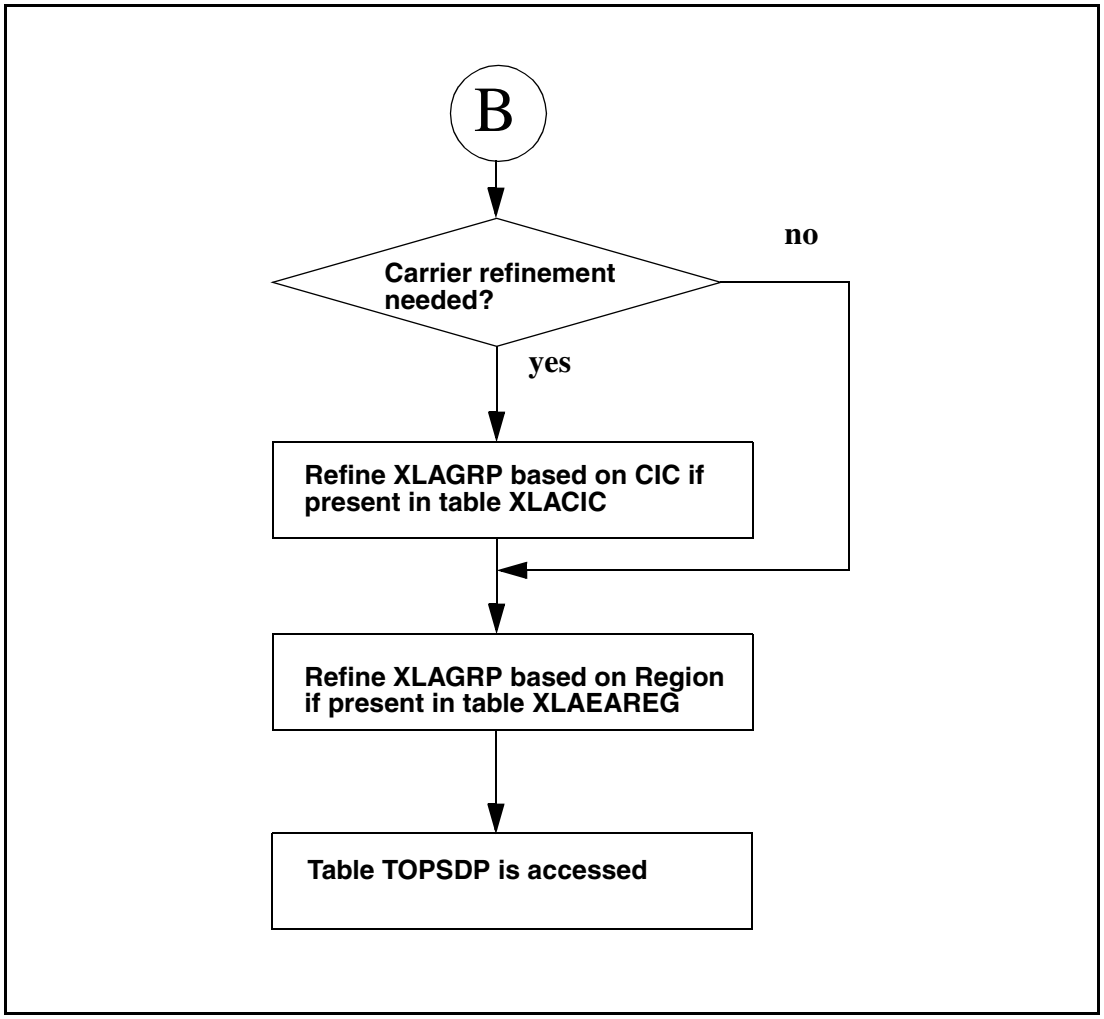


Figure 3 XLAGRP Refinement Order For Equal Acess Calls



51.2.3 Table XLACLASS

Table XLACLASS allows the XLAGRP to be refined based upon the calling service class. The index of the table is the existing XLAGRP and the calling service class. It then provides a new XLAGRP if a match is found.

Table 1 Example of Table XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field CLGCLASS supports a range of {UNKNOWN, STATION, COIN, HOTEL, RESTRICTED}.

51.2.4 Table XLABILL

Table XLABILL allows the XLAGRP to be refined based upon the billing type. The index of the table is the existing XLAGRP and the bill type. It then provides a new XLAGRP if a match is found.

Table 2 Example of Table XLABILL

XLAGRP	BILLTYPE	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field BILLTYPE supports a range of {UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD}.

Note: Station paid and person paid are both handled by the PAID criteria. Both are PAID calls but may have a different rate applied. Since this refinement is to capture the billing method not the rate, station and person ratings are treated the same. This applies to all billing types.

51.2.5 Table Flow Example

This example section illustrates the new refinement tables and how they achieve special routing for coin station paid calls. It is simplified by using an incoming trunk group with non-EA calls. A59006822 fully details XLAGRP methods for EA and operator calls. It is further simplified by not having SPID or originating digit refinements. These are fully documented in AF7159.

Table 1 TOPSTOPT

GRPKEY	ACDDATA	DISPCLG	ADASERV	ADASANS	ANITOCLI	OLNSQRY	DCIBIDX	LNPCLGAM	XLA SCHEM		SPIDPRC	TRKSPID	
									NEWXLA	XLAGRP		DFLTSPID	SPID
TRK1	QMSCAM	N	NONE	NA	N	NONE	0	N	Y	**TRK1**	N	N	

Table 2 XLASPID does not have a match

Table 3 XLAODIGS does not have a match

Table 4 XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

Table 5 XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

Table 6 TOPSDP

XLAGRP	STS	OPERPRTN	ORIGSCRN	OPERSCRN	MCCSPRTN	MCCSSCRN	LCANAME
TRK1	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COINPAID_ROUTE	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COIN_NOROUTE	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA
TRK1COIN	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA

- STS - This is the service translations scheme which is also the index into code translations (i.e., Table HNPACONT).
- OPERPRTN - This is the operator pretranslator name that is used for performing pretranslations from the operator position. It is used to index into Table STDPRTCT.
- ORIGSCRN - This is the class of service screening name that is used for screening based upon the location of the originator. It is used to index into Table CLSVSCRC.
- OPERSCRN - This is the class of service screening name that is used for screening when an operator or service node is associated with the call. It is also used to index into Table CLSVSCRC.
- MCCSPRTN - This is the pretranslator name that is used for performing pretranslations for the Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table STDPRTCT.
- MCCSSCRN - This is the class of service screening name that is used for screening when performing the call screening for Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table CLSVSCRC.
- LCANAME - This is the local call area screening name which is used to determine if the call is local. It is used to index into table LCASCRCN or LCAINFO.

For non-EA COIN PAID calls arriving on TRK1, the initial XLAGRP is determined from table TOPSTOPT and refinements are performed as follows. The current XLAGRP is noted after the arrow.

1. Table TOPSTOPT provides the initial XLAGRP name

----> TRK1

2. SPID refinements are not needed, no change

3. Originating digits are not found in XLAODIGS, no change

4. Table XLACLASS finds TRK1 COIN, changes XLAGRP

---> TRK1COIN

5. Table XLABILL finds TRK1COIN PAID, changes XLAGRP

----> TRK1COINPAID_ROUTE

The final XLAGRP for this non-EA COIN PAID call is TRK1COINPAID_ROUTE. This XLAGRP is indexed in table TOPSDP to find the screening and translations indices.

Note: In this example, if the coin call was billed collect then the final XLAGRP would have been TRK1COIN_NOROUTE which can be setup in table TOPSDP to have screening and translations indices which do not route or route to treatment. Also note that the XLAGRP, TRK1COIN, can be added to TOPSDP and be setup for indices which do not route. This ability limits the amount of datafill needed to only allow coin paid calls to complete. Thus, the refinement TRK1COIN COLLECT in XLABILL is not needed nor the TRK1COIN_NOROUTE XLAGRP. These were only included here to illustrate the options.

51.2.6 Activation

When activating feature A00002765 in a site where XLAGRPs are already in use, the following is recommended.

- For a new trunk group to begin using the XLAGRP translations and is not dependent on existing translations, a new XLAGRP name should be assigned to the trunk group and the new XLAGRP used in the refinement tables as needed. This has no interaction with existing translations since existing XLAGRPs will not find matches in the new tables.
- For an existing trunk group with XLAGRP translations (or a new trunk group which will use existing XLAGRP translations), it is recommended to work backwards in the refinement order. By adding the final XLAGRP first, no matches will be found until the first refinement using the existing XLAGRP is datafilled. For example, if TRK1 has XLA1 defined in TOPSTOPT and has existing translations for SPID where (XLA1 SPID XLA1SPID) is datafilled in table XLASPID, then to create a coin station_paid route for these calls, first add new XLAGRPs (XLA1SPIDCOIN and XLA1SPIDCOINPAID) to table XLAGRP then add to table XLABILL (XLA1SPIDCOIN PAID XLA1SPIDCOINPAID) [so far no changes will occur]. Then add to table XLACLASS (XLA1SPID COIN XLA1SPIDCOIN) - [once this is added coin station_paid calls will route using XLA1SPIDCOINPAID].

  Note: Ensure all XLAGRPs have datafill in table TOPSDP; be sure that XLA1SPIDCOIN can still route correctly. These are the calls which are coin but not paid for that trunk group with that SPID. TOPSDP will need to point to something that goes to treatment (if desired) otherwise they will route to the last route found in standard translations.

51.3 Hardware Requirements or Dependencies

NA

51.4 Software Requirements or Dependencies

UNBN0101, OSB00101

51.5 Limitations and restrictions

- XLACLASS is limited to a range containing UNKNOWN, STATION, COIN, HOTEL, RESTRICTED.
- XLABILL is limited to a range including UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD.
- Station billing and person billing may have different rates but are both treated the same in table XLABILL. For example, station paid and person paid will both refine under the PAID criteria.
- This feature is intended to be used with the dollar pre-pay coin functionality. Limitations for this function include:
  - — External rater not support with OSSAIN
  - — External rater, Coin signalling, ACTS not supported in Global loads

51.6 Interactions

This feature can alter the translations and route selected for calls using the XLAGRP method.

51.7 Glossary

Term	Description
XLAGRP	Translations Group

51.8 References

REF #	Description of Reference
AF7159	AF7159.aa11, January 23, 1998 Unbundling: SPID Processing, Translations, and Routing
59006822	OPRTRANS and EA Unbundling
59006827	LATA Screening Replacement
297-8403-903	TOPS Unbundling User's Guide

52: Functional Description (FN): A00002760

52.1 Feature name

A00002760 - Panther Enhancements For Hybrid Office Support

52.2 Description

Panther tool provides automatic software load upgradation facility for peripherals like DTC, DMSCP SPMs, SMG4 etc.

While upgrading a particular variant of SPM using panther(eg. DMSCP) in a hybrid office which has more than one variant of SPMs(eg. both DMSCP and SMG4), the following problems occur.

- In addition to creating a plan for the desired variant(DMSCP) of SPM, panther has a limitation of creating an upgrade plan for other variants also(eg. SMG4).
- While executing the plan, craft is unable to retain the loads that were existing in the other variant, since the PLAN forces a change in the load for other variants as well. As a result, the RMs and CEMs of other variants of SPMs in a Hybrid office are loaded with the wrong load which may lead to the outages.

This SN07 activity **A00002760**: 'PANTHER ENHANCEMENTS FOR HYBRID OFFICE SUPPORT'ensures upgrading of different variants of SPMs with their corresponding loads. This activity is supported only for the offices that has SPMs provisioned in it.

The various functionalities provided as part of this activity are:

- Eight new EXT files, one for each variant of SPM are available for the crafts.
- Blocking of panther upgrade for SPMs in case of no EXT file on the distribution volume. This blocking is done only in the customer site.

  Note: *However in labs, if there is no EXT file present in the distribution volume, a new prompt is introduced either to continue the upgrade of SPMs or blocking the upgrade for SPMs.*
- Modification of the table SPMLDVAL to support SN releases and creation of a new field to determine the variant of SPM. The size of the table SPMLDVAL is also increased from 256 to 2048.
- ONP support to the table SPMLDVAL.

- Modification of FILECOPY command and filecopy report in Panther to copy appropriate loads to the destination volume based on the load information available in the EXT files.
- Modification of filecopy reports to display the variant of SPM.
- Modification of FILECOPY command to support multiple FILECOPY in an upgrade cycle.
- Modification of PMUPGRADE PLAN command to create tasks based on the load information available in the EXT files.
- Enhancement of the CI tool, SPMLDINFO to support all the variants of SPM.
- Modification of the 'QUERYPM FILES' mapci command to display load release information for all variants of SPMs.
- Introduction of additional warning message during manual loading(loadmod and bulkload) of devices of all variants of SPMs.

  Note: *Refer to the activity ACT.89007535 - SPM MR Loadname Decoder for more information.*

52.2.1 Modification of table SPMLDVAL to support all the product lines of SPM

The table SPMLDVAL is enhanced to support the load lineup for all the following product lines of SPMs.

- DMSCP - NA
- DMSCP - INTL
- SMG4 - ATM
- SMG4 - IP
- IW - ATM
- IW - IP
- DPT - ATM and
- DPT - IP

52.2.1.1 Modification of the key of the table

In SN06, this table supports the load lineup for DMSCP class of SPMs only and the tuple format is as shown below.

SP 17 1 0 (CEM71BA) (COH0071) (DL271AZ) (DLC71AZ) (DSP71BA) (OC371AZ) (SYN71AZ) $

In SN07, the key of the table is modified to support all the product lines of SPMs by introducing a new field. The tuple format is given below with the new field in bold.

SP 17 0 0 **SPMNA** (CEM17BU) (DLC17BV) (DL217BT) (DSP17BU) $
SP 17 0 0 **SPMIN** (CST17BS) (DLC17BV) (DL217BT) (DSP17BU) $
SN 06 0 0 **MG4AT** (MG419BR) (ATC19BO) (IED19BO) (OC419BN) $
SN 06 0 0 **MG4IP** (MG419BR) (GEM19BN) $
SN 06 0 0 **IWSAT** (IWS19BP) (ATC19BO) (SYN19BN) $
SN 06 0 0 **IWSIP** (IWS19BP) (GEM19BN) $
SN 06 0 1 **DPTAT** (IWS19BP) (ATC19BO) (DSP19BN (COH0019) $
SN 07 0 1 **DPTIP** (IWS20BA) $

52.2.1.2 Introduction of ERROR messages during table control operations

During tuple addition, table control checks for the valid combination of load type and product type that are added. The valid combination of the load type and the product type for any tuple are as follows:

- load type: SP and product type: SPMNA and SPMIN.
- load type: SN and product type: MG4AT, MG4IP, IWSAT, IWSIP, DPTAT and DPTIP.

When a tuple with invalid combination of load type and product type is added in table SPMLDVAL, the following error messages are displayed.

```
ERROR: Cannot datafill MG4AT product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill MG4IP product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill IWSAT product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill IWSIP product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill DPTAT product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill DPTIP product type for SP loadtype.
       Only SPMNA or SPMIN are valid for the SP loadtype.
```

```
ERROR: Cannot datafill SPMNA product type for SN loadtype.
       Only MG4AT or MG4IP or IWSAT or IWSIP or DPTAT
       or DPTIP are valid for the SN loadtype.
```

```
ERROR: Cannot datafill SPMIN product type for SN loadtype.
       Only MG4AT or MG4IP or IWSAT or IWSIP or DPTAT
       or DPTIP are valid for the SN loadtype.
```

52.2.1.3 Increasing the size of the table

The size of this table is also increased from 256 to 2048 tuples to support all the product lines of SPMs.

52.2.1.4 ONP support to the table

In SN06, table SPMLDVAL contains both the INTL and NA DMSCP loads in the same tuple. i.e. One tuple contains CST, CEM, STM and OC3 loads. CEM and OC3 loads are specific to DMSCP NA product whereas CST and STM loads are specific to DMSCP INTL product of SPM.

In SN07, since a new field is introduced to identify the product type of each tuple, such a combination of loads becomes invalid. So, during the transfer of the table SPMLDVAL from release SN06 to SN07, a single tuple with both DMSCP NA and INTL loads is splitted up into two tuples. The product type of the first tuple is written as SPMNA and contains CEM and OC3 loads. On the other hand, the product type of the second tuple is written as SPMIN and contains CST and STM loads.

52.2.2 EXT File in load tape to datafill SPMLDVAL

With the implementation of this feature, every spectrum (both succession and TDM) load release tape shall contain an EXT file with the load lineup information for different spectrum load releases and this EXT file will be used to datafill table SPMLDVAL during Panther execution. As a result of this, table SPMLDVAL contain tuples with the loadtype and the device load lineup of various spectrum load releases. In case of offices with no SPMs, there is no impact to the existing panther upgrade behavior.

The EXT file which contains the device load lineup of all the spectrum load releases shall be available through load tape or ESD at the customer site.

The EXT file for DMSCP class of SPMs, **SPMLDEXT** is already in place. Eight new EXT files for different products of SPMs are introduced. The existing SPMLDEXT file will also be used during an upgrade from SN06 to SN07.

- **SPMNAEXT** for DMSCP - NA
- **SPMINEXT** for DMSCP - INTL
- **MG4ATEXT** for SMG4 - ATM
- **MG4IPEXT** for SMG4 - IP
- **IWSATEXT** for IW - ATM
- **IWSIPEXT** for IW - IP
- **DPTATEXT** for DPT - ATM
- **DPTIPEXT** for DPT - IP

These files have details of spectrum load-lineups of all Nortel supported releases. The sample tuples in table SPMLDVAL for the above eight EXT files respectively are shown below:

SP 17 0 0 **SPMNA** CEM17BU DLC17BV DL217BT DSP17BU $
SP 17 0 0 **SPMIN** CST17BS DLC17BV DL217BT DSP17BU $
SN 06 0 0 **MG4AT** MG419BR ATC19BO IED19BO OC419BN $
SN 06 0 0 **MG4IP** MG420BR GEM20BN $
SN 06 0 0 **IWSAT** IWS19BP ATC19BO SYN19BN $
SN 06 0 0 **IWSIP** IWS19BP GEM19BN $
SN 06 0 1 **DPTAT** IWS19BP ATC19BO DSP19BN COH0019 $
SN 07 0 1 **DPTIP** IWS20AB $

The SPMNAEXT and SPMINEXT files shall contain the data starting from load release **SP14.8.1.** The MG4ATEXT, IWSATEXT, IWSIPEXT, DPTATEXT files shall contain the data starting from load release **SN03.1.0** onwards. The MG4IPEXT and DPTIPEXT files shall be empty because these

two products are currently not available. A maximum of 292 tuples are available in each of these EXT files.

52.2.3 Modification in filecopy stage

The filecopy command checks the availability of the EXT file in the distribution volume and first executes the EXT file to datafill table SPMLDVAL and then copies the EXT file from the tape (or any other distribution volume) to the destination volume.

1. In case of customer site, the following warning is displayed if the EXT file is not present.

****** WARNING: EXT file to datafill table SPMLDVAL is not available in the distribution volume. SPMs will not be considered for upgrade. If SPMs are required to be upgraded, quit and start pmupgrade again with the EXT file in the distribution volume. If SPMs are not required to be upgraded, continue filecopy.***

- If SPMs are also required to be upgraded, then the craft can quit filecopy at a later stage and start the filecopy again with the proper EXT file in the distribution volume.
- If the SPMs are not required to be upgraded, then the craft can just continue with the upgrade and no loadmapping shall be done for any of the SPM loads.

Note 1: When the above mentioned warning message is displayed,

- no prompt shall be displayed for any of the SPM current loads,
- the SPM current loads shall not be included in the filecopy report and as a result
- SPMs shall not be included in the plan.

Note 2: *In case of designer Lab, the following prompt is displayed if the EXT file is not present.*

****** WARNING : EXT file to datafill table SPMLDVAL is not available in the distribution volume. Do you want to still consider SPMs for upgrade?***
Please confirm ("YES", "Y", "NO", or "N"):

— *In case the craft enters "Yes" or "Y", SPMs will be upgraded without the EXT file. The same customer site behavior is maintained but the crafts shall have the flexibility of running panther upgrade without checking for the EXT file. This can result in upgradation of SPM*

devices with incorrect loads in a hybrid lab with different product lines of SPM.

— *In case of "No" or "N", SPMs will not be considered for upgrade and the behavior mentioned above in Note 1 shall occur.*

2. If more than one EXT file of the same type is present in the distribution volume, then the following warning message is displayed.

WARNING: Multiple possible replacements found on load distribution volume for <extfile> file: <extfile_ver> <extfile_ver> Any replacement EXT file name may be chosen from the distribution volume. If necessary, consult the PM release documentation or contact the next level of support.

Please enter the replacement file name, Or "Q" (Quit FILECOPY)

If this message is received, the craft needs to enter the correct EXT file name. In case of incorrect file name the following message is displayed.

Response is not one of the allowable options.
Please enter the replacement file name, Or "Q" (Quit FILECOPY)

The above message will be repeated whenever the user enters a wrong response. If the user enters Q, then it will come out of filecopy phase of Panther.

Note: *The extfile in the above WARNING message can be any one of the following: SPMNAEXT, SPMINEXT, MG4ATEXT, MG4IPEXT, IWSATEXT, IWSIPEXT, DPTATEXT and DPTIPEXT.*

3. If the EXT file to be processed is already present in the destination volume, then the following message is displayed.

***** WARNING: <extfile_ver> file already exists in the destination volume.**

Note 1: The extfile in the above WARNING message can be any one of the following: *SPMNAEXT, SPMINEXT, MG4ATEXT, MG4IPEXT, IWSATEXT, IWSIPEXT, DPTATEXT and DPTIPEXT.*

Note 2: All the other existing WARNING messages specific to SPMLDEXT file are applicable for the new EXT files also.

4. During filecopy stage when there is no replacement load in the distribution volume for a particular current load, in SN06, panther prompts the user to enter a new load as follows:

```
*** No replacement found on load distribution volume for DSP17AH load.
Any replsacement load name may be chosen from the load distribution
volume. If necessary, consult the PM release documentation or
contact the next level of support.
Please enter the replacement load name, or "S" (Same), or "Q" (Quit FILECOPY)
>
```

In SN07, the "**replacement load name**" option is removed from the above prompt for all current loads (XPM, SPM, ENET...). This is because panther had already checked for any replacement loadname in the distribution volume and found none and so there is no significance of this option. This prompt shall be modified as follows:

```
*** No replacement found on load distribution volume for DSP17AH load.
If necessary, consult the PM release documentation or contact the next level of support.
Please enter "S" (Same), or "Q" (Quit FILECOPY)
>
```

Note: The loadmapping can also be made using 'SET LOADSELECT' command as follows:

>SET LOADSELECT DSP16AH_010007 DSP17AR_010017

No new restrictions or verifications are done during "SET LOADSELECT" command so that the craft has the flexibility of mapping different loads.

5. Whenever the same current load is present in different product lines of SPMs(NA DMSCP and MG4K ATM) and if there is one EXT file(SPMNAEXT) on the distribution volume, panther shall display, at the most only one prompt for that current load. This prompt is only for the current load for which the EXT file is present. Panther shall not prompt for other product lines of SPMs.

   Also in the filecopy report, the loadmapping is not displayed for all the product lines of SPMs but displayed only for the product for which the EXT file is present. On the other hand, if there were two EXT files (SPMNAEXT and MG4ATEXT) on the distribution volume, panther shall display the prompt twice for the same current load as shown in figure 1 below. If the craft enters DSP17XX for DMSCP NA current load and DSP17YY for MG4K ATM load, then the load file selection report shall be displayed as shown in figure 1 below.

Figure 1 Multiple possible replacement prompt and load file selection report

```
*** Multiple possible replacements found on load distribution
volume for DSP16XX_010025 DMSCP NA load: DSP17XX_010025 DSP17YY_010025

Any replacement load name may be chosen from the load distribution
volume. If necessary, consult the PM release documentation or
contact the next level of support.
Please enter the replacement load name, or "S" (Same), or "Q" (Quit FILECOPY)

*** Multiple possible replacements found on load distribution
volume for DSP16XX_010025 MG4K ATM load: DSP17XX_010025 DSP17YY_010025

Any replacement load name may be chosen from the load distribution
volume. If necessary, consult the PM release documentation or
contact the next level of support.
Please enter the replacement load name, or "S" (Same), or "Q" (Quit FILECOPY)
```

```
                    LOAD FILE SELECTION REPORT
CURRENT LOAD        PM TYPE     FW TYPE     AUTO-SELECTED FILES     EXCLUDED
------------        -------     ------    ----------------------    --------
DSP16XX_010025       SPMNA                   DSP17XX_010025
DSP16XX_010025       MG4AT                   DSP17YY_010025
```

6. At the end of filecopy stage, two reports are generated to display the loadmapping of the current load and the new loads. The format of the two reports are as shown below.

```
                        LOAD FILE SELECTION REPORT
CURRENT LOAD      FW TYPE        AUTO-SELECTED FILES                EXCLUDED
------------      -------        -------------------                --------
DLC17AQ_010016                   Same Load
DSP17AQ_010016                   DSP17AN_010013
```

```
                        LOAD FILE COPY REPORT
CURRENT LOAD      FW TYPE        FILE STATUS   AUTO-SELECTED FILES
------------      -------       -------------  -------------------
DLC17AQ_010016                          S      Same Load
DSP17AQ_010016                        C        DSP17AN_010013
```

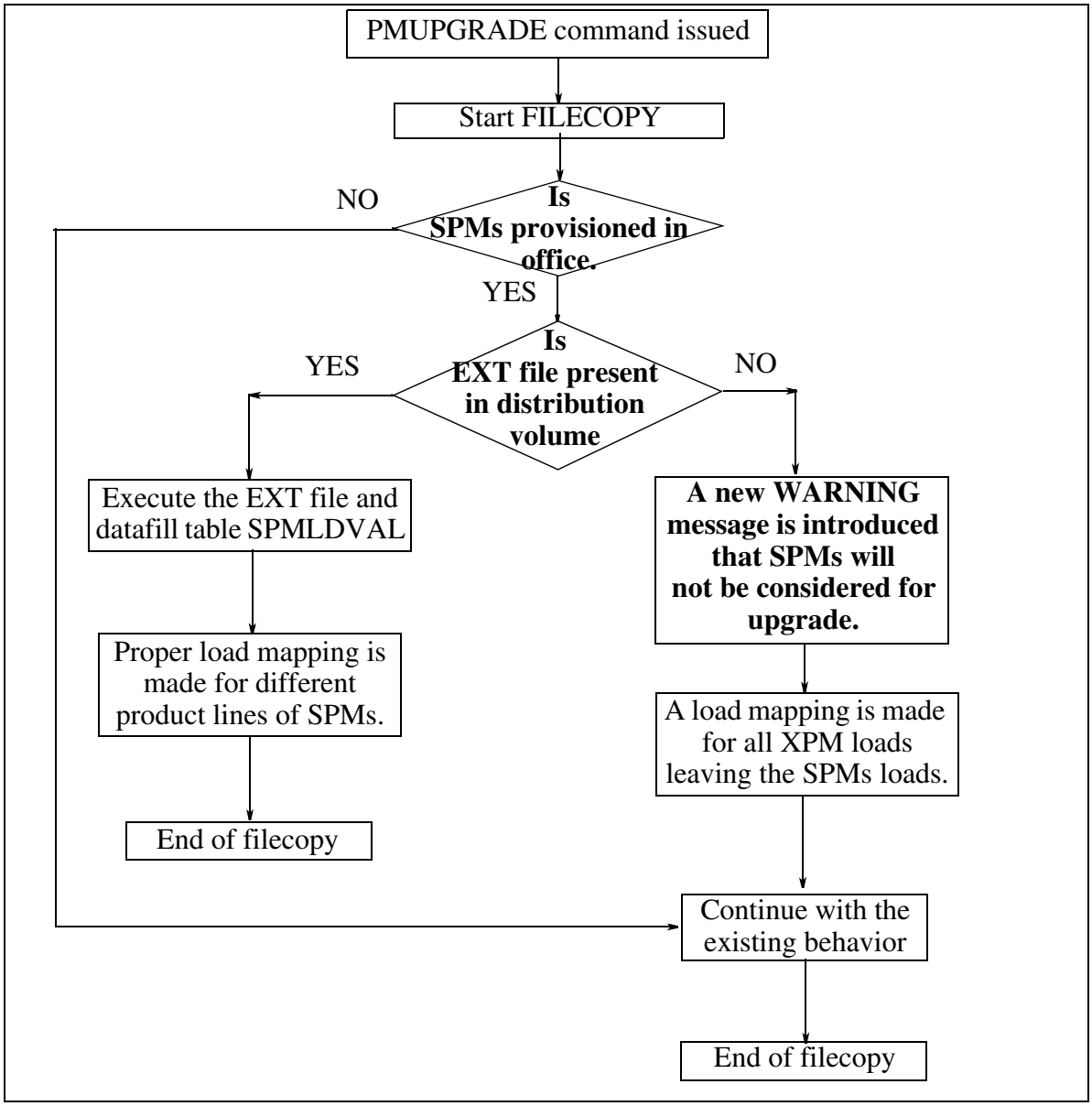
The format of the two reports is changed to display the product type of the corresponding loadmapping as shown below. For SPM loads, this column

shows the SPM variant to which the current load belongs to, whereas for other peripheral loads this column shows None.

```
                    LOAD FILE SELECTION REPORT
CURRENT LOAD       PM TYPE  FW TYPE    AUTO-SELECTED FILES          EXCLUDED
------------       -------  -------    ------------------           --------
DLC17AQ_010016      SPMNA                  Same Load
DSP17AQ_010016      SPMNA                 DSP17AN_010013
DSP17AQ_010016       MG4AT                 Same Load
```

```
                    LOAD FILE COPY REPORT
CURRENT LOAD       PM TYPE  FW TYPE    FILE STATUS      AUTO-SELECTED FILES
------------       -------  -------    -----------      ------------------
DLC17AQ_010016      SPMNA                    S               Same Load
DSP17AQ_010016     SPMNA                     C             DSP17AN_010013
DSP17AQ_010016      MG4AT                    S               Same Load
```

Figure 2 FILECOPY command behavior in customer site



52.2.4 Modification of Planning stage

The planning stage is modified to create tasks based on the SPM product type information of the load mapping. Figure 3 explains the modified panther upgrade planning stage assuming only one load mapping is present during the filecopy stage. A new field called PM TYPE is added in the task to identify the product type of the task. The modification of planning stage is explained below.

Figure 3 Desired behavior of upgrade plan

Suppose there are 8 SPMs in the office as follows.
SPM 1 - DMSCP NA,
SPM 2 - DMSCP INTL,
SPM 3 - SMG4 ATM,
SPM 4 - SMG4 IP,
SPM 5 - IW ATM
SPM 6 - IW IP
SPM 7 - DPT ATM
SPM 8 - DPT IP

Initial Conditions:
The current load of all the DSP RMs(DMSCP+SMG4+IW) is DSP16XX.
The DMSCP NA load tape has DSP71XX load and SPMNAEXT file which is specific to DMSCP NA product line of SPMs.

Action:
DMSCP NA load tape is inserted, which has DSP71XX load and FILECOPY is executed. START PLAN is executed followed by DISPLAY PLAN step.

Filecopy report:

CURRENT LOAD	**PM TYPE**	FW TYPE	FILE STATUS	AUTO-SELECTED FILES
DSP16XX_010032	**SPMNA**		**C**	**DSP71XX_010036**

Plan:

PMUPGRADE PLAN REPORT
Upgrade Layer: 1

TASK 1:
SITE:
LOADS: FROM **DSP16XX_010032** TO **DSP71XX_010036**
NODES: **SPM 1**
PM TYPE: **SPMNA**
REQUIRES: none
LOADED FROM FLASH: NO
AUTOMATED: YES

Result:
The plan is not created for other SPMs though the current load is present in other product lines of SPMs also.

52.2.5 Enhancement of the CI tool - SPMLDINFO

The CI tool SPMLDINFO is used to query the following for the DMSCP class of SPMs only.

- list of device loads for a particular load release,
- spectrum load release name for a given device load and
- list of spectrum load releases running in individual SPMs.

This activity enhances the tool, **'SPMLDINFO'** to support the loads of SMG4 and IW class of SPMs also. There are 3 subcommands for this CI tool which are explained below.

- **Listload:** Displays the device load lineup information for a given spectrum load release name.
- **Listrelease**: Displays the spectrum load release name for a given device loadname.
- **ListspmLoad**: Display the running release load name for the SPMs in the office. Listspmload command has 3 sub-options.
  - — Option '**all**' can be used to list the load release names for all SPMs in the office. If no SPMs are datafilled in the office, then it displays the following warning message and stops execution.
    No SPMs are datafilled in the office.
  - — In the second option, the user can specify a range, say SPM 1 4, in which case, the load release names of all SPMs in the given range is displayed. If an SPM within the specified range is not datafilled, then the following warning message is displayed.
    SPM <spm no> is not datafilled.
  - — If only 1 SPM number is specified, then the command will display the running release load for that SPM. If SPM is datafilled in the office, it displays the datafilled SPM number and relevant data against it. When the entered SPM number is not provisioned, then it displays the following warning message and stops execution.
    SPM No Load Release Name
    ------ ----------------
    SPM <spmno> is not datafilled.

Please refer to Section 13.9 of Configuration Document for more information about the CI tool.

52.2.6 Enhancement of ‘Querypm files’ command

The ‘**Querypm files**’ command displays the running release load name for a DMSCP SPM if the load name is datafilled in table SPMLDVAL. This activity enhances the command ‘Querypm files’ to display the running release load name for SMG4 and IW class of SPMs also. With this enhancement, querypm files displays the name of the running release load of any variant of SPM towards the end of the command output.

In case the running RM loads in an SMG4 or an IW SPM do not match with any of the load release lineups datafilled in table **SPMLDVAL**, then a warning will be displayed to the craftsperson.

Running MG4K ATM Load Release : Load lineup of this SPM does not match with any of the load releases datafilled in table SPMLDVAL.

If the CEMs/RMs of an SPM are out of service such that the running loads in each of the devices cannot be determined, then it will display the following warning message.

Running IWS ATM Load Release : Unable to contact the devices. The requested data cannot be retrieved.

Please refer to section 13.9.6 of Configuration Document for more information about QueryPM files enhancement.

52.2.7 Modification of manual upgrade

52.2.7.1 Loadmod command:

The following WARNING message is displayed in the loadmod command for DMSCP class of SPMs only.

WARNING : Table SPMLDVAL is not datafilled for this loadname. Please add the data in table SPMLDVAL. Do you want to continue without datafilling the table? Please confirm ("YES", "Y", "NO", or "N"):

This activity introduces the above WARNING message in the loadmod and bulkload command for SMG4 & IW/DPT class of SPMs also. The above warning message is displayed when the load file name used for loading is not available in table SPMLDVAL against the product type of the posted SPM.

If the craft enters YES, loadmod shall continue. But the data for this loadname will not be available in table SPMLDVAL for later reference. Entering the data

in table SPMLDVAL is mandatory for information retrieval because SPMLDINFO tool gets the required data from this table. The consequences of going ahead without datafilling the table SPMLDVAL are given below:

- The SPMLDINFO tool will not be able to display the load release information for that particular load.
- The Querypm files command will not be able to display the running release load name for that SPM.

However, there would not be any service impact or impact on the loading process even if the user decides to go ahead with the loading process without datafilling table SPMLDVAL.

If the craft enters NO, loadmod command will be aborted and the craft can issue loadmod command after updating table SPMLDVAL.

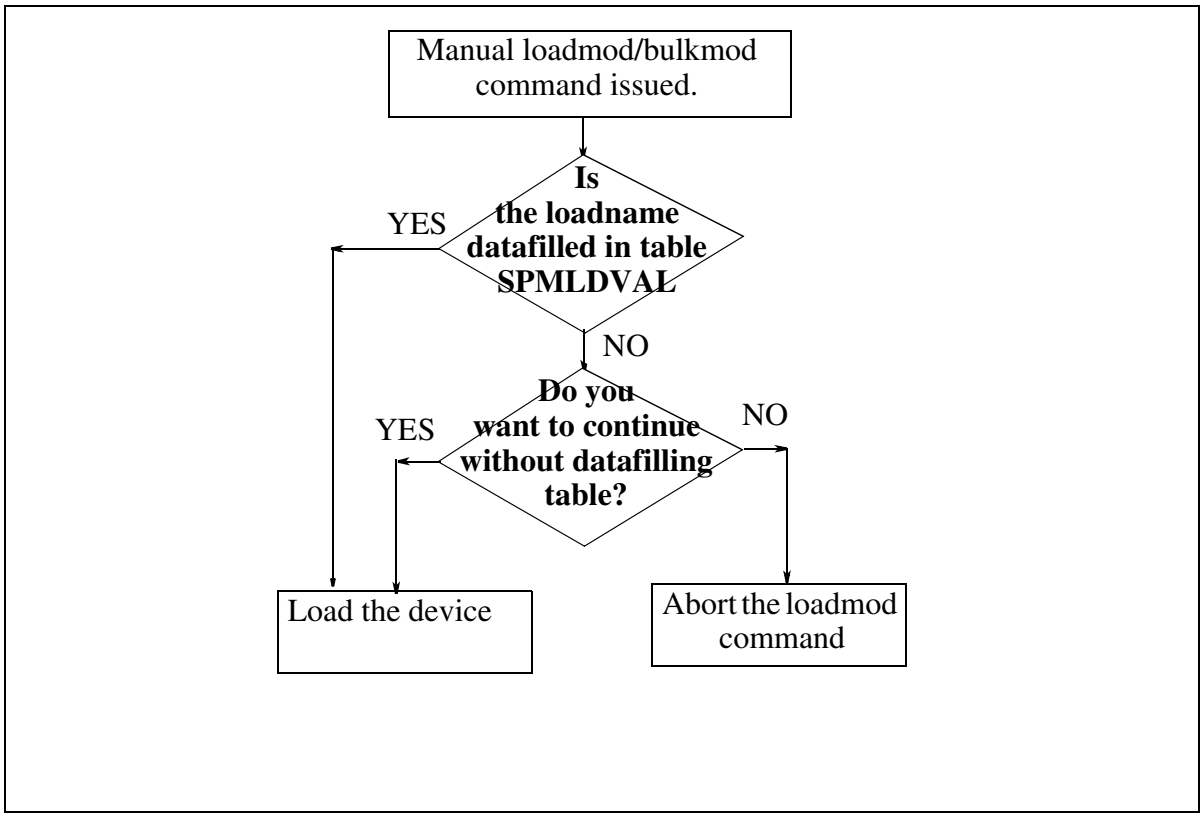
52.2.7.2 BULKLOAD command:

When a number of SPMs of different product types are posted and the bulkload command is performed, the load file name used for loading is checked in table SPMLDVAL against the product types of the posted SPMs. Incase the load file is present for some products of SPMs and not present for some other products, then the following warning message is displayed with a prompt:

WARNING : The specified loadname is not datafilled in table SPMLDVAL for the following SPMs:
SPM 1 2 3 4
Contact your next level of support before proceeding with upgrade. Do you want to continue without datafilling the table?
Please confirm ("YES", "Y", "NO", or "N"):

Figure 4 gives the changes in Manual Upgrade procedure for SPM peripheral with the implementation of this feature.

Figure 4 Manual upgrade of DMSCP, SMG4 and IW class of SPMs



52.3 Hardware Requirements or Dependencies

None.

52.4 Software Requirements or Dependencies

None.

52.5 Limitations and restrictions

None.

52.6 Interactions

None.

52.7 Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms	__N/A__
Configuration	
Data Schema	__N/A__
User Interface	___X___
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

52.8 Glossary

Term	Description
DMS	Digital Multiplexing Switch
DTC	Digital Trunk Controller
SPM	Spectrum Peripheral Module
RM	Resource Module
CEM	Common Equipment Module
IW	Interworking
SN	Succession Network
CI	Command Interpreter
XPM	Extended Peripheral Module
ESD	Electronic Software Delivery
TDM	Time Division Multiplexing

53: Functional Description (FN): A00002765

53.1 Feature name

XLAGRP Refinements for Coin Station-Paid Routing

53.2 Description

This feature enhances the Unbundling Translations and Routing functionality by adding the ability to refine the XLAGRP based upon the calling service class and the billing method. With this feature, outgoing translations can now be applied specifically to a coin station-paid call.

The implementation of this feature allows the full range of calling service class and billing methods to be utilized in XLAGRP refinements. New table XLACLASS allows XLAGRP refinements based on a range including coin, station, hotel, and restricted. New table XLABILL allows XLAGRP refinements based on a range including paid, collect, third, cards, special calling, special called.

53.2.1 Background

In TOP09, AF7159 introduced the XLAGRP refinement mechanism for unbundling translations and routing. It created tables XLAGRP, XLASPID, XLAODIGS, and TOPSDP to setup the refinement structure including SPID[1] and originating digits.

Translations Group (XLAGRP) names are datafilled in table XLAGRP, which allows the operating company the ability to datafill various names to represent groupings for translation purposes as needed. These XLAGRP names are then used in the refinement tables to arrive at a final XLAGRP to be used in table TOPSDP (TOPS Dial Plan).

Table TOPSDP centralizes translation and screening attributes. The index into table TOPSDP is chosen in a flexible manner, giving the operating company the ability to fit their individual network needs. Obtaining an XLAGRP and indexing into table TOPSDP is referred to as the ***XLAGRP*** method of performing translations and screening for TOPS calls.

AF7159 provided an initial XLAGRP to be defined in table TOPSTOPT, which is indexed based on a trunk group. It also provided XLAGRP refinements for SPID and originating digits.

[1]Serivice Provider Identification

In TOP12, A59006822 enhanced the XLAGRP method with additional definitions for the initial XLAGRP and additional refinements. It allowed the initial XLAGRP to be defined in table TOPEATRK for EA calls and in table OPRINFO for operator calls. It also provided XLAGRP refinements for Carrier Identification Code (CIC) and EA region, which is based on either a LATA or a ZONE as defined by feature 59006827.

This feature supports all existing XLAGRP methods and enhances the refinement characteristics by adding calling service class and billing methods.

53.2.2 New XLAGRP Refinement Order

To preserve the existing XLAGRP refinement datafill, the new refinements are added at the end of the existing order list for non-EA calls. Thus XLACLASS then XLABILL will refine after XLAODIGS. For EA calls, XLACLASS and XLABILL will refine after XLAODIGS as well. Although this inserts the new refinement tables in the middle of refinement for EA calls, it saves the extra datafill needed in XLACLASS and XLABILL to accomodate those XLACIC and XLAEAREG XLAGRPs.

The following diagrams illustrate the existing XLAGRP refinement order with the new tables, XLACLASS and XLABILL, included.

The figures below outline the refinement order for both EA and NON-EA calls:

Figure 1 XLAGRP Refinement Order NON Equal Access

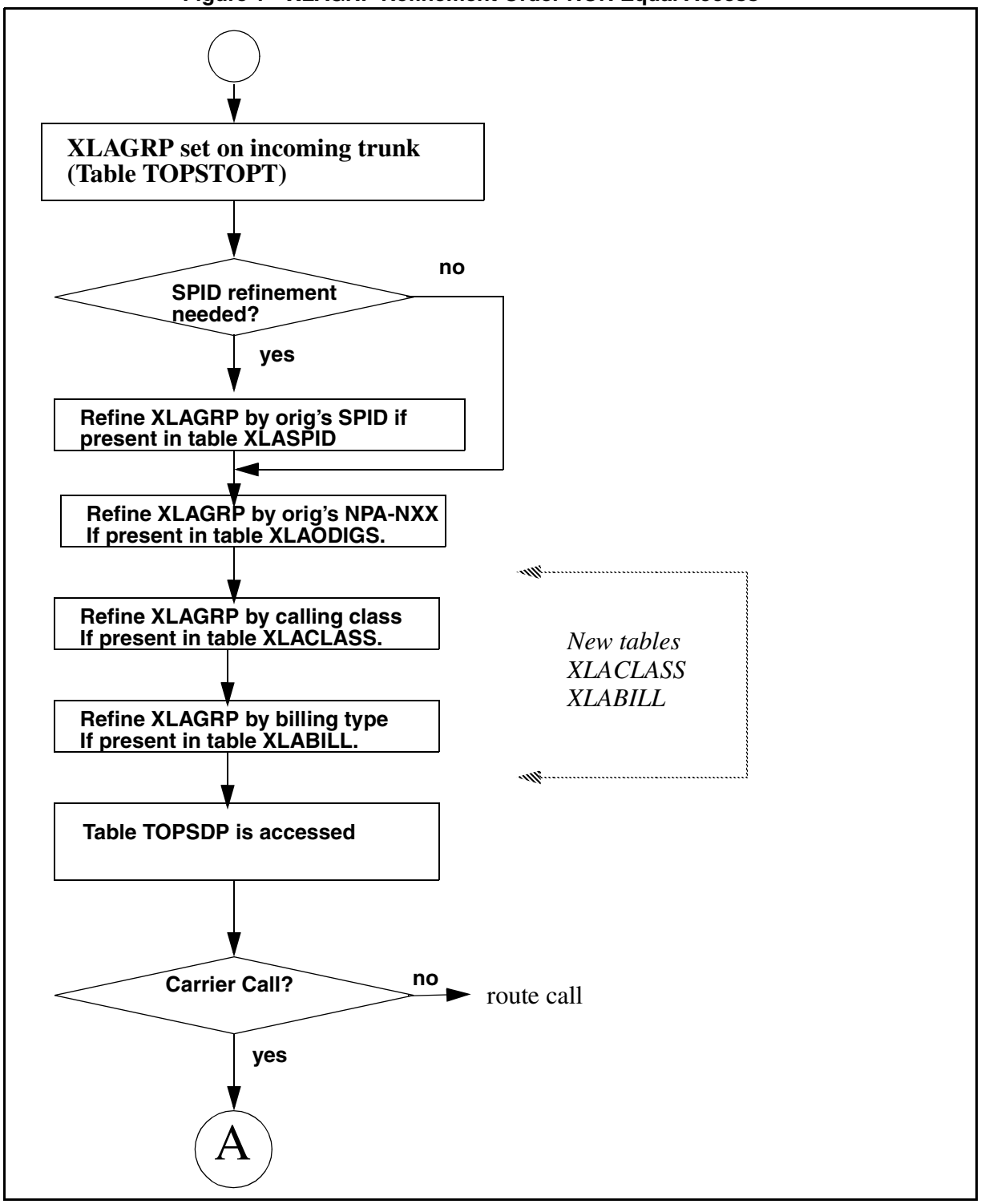


Figure 2 XLAGRP Refinement Order For Equal Acess Calls

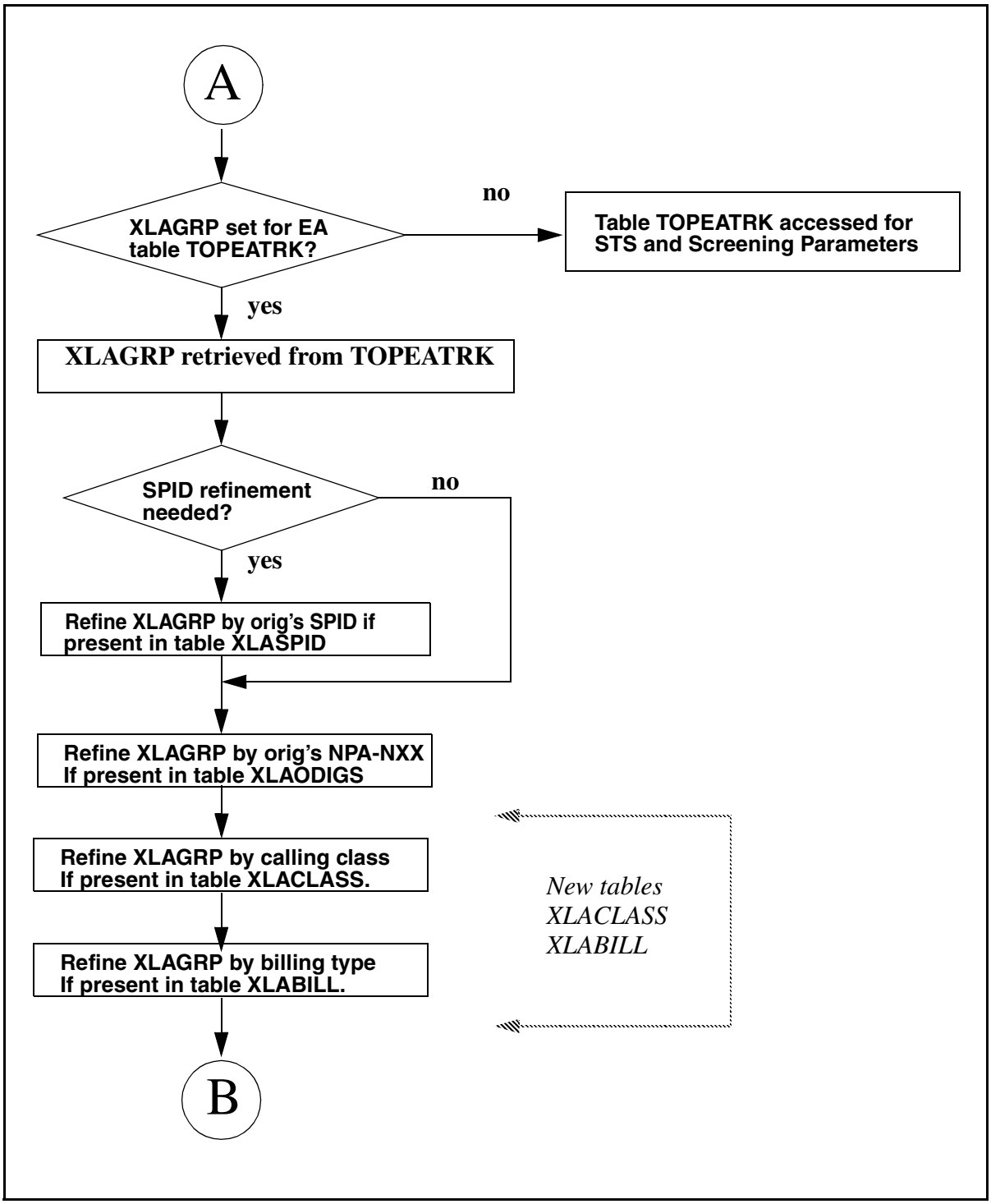
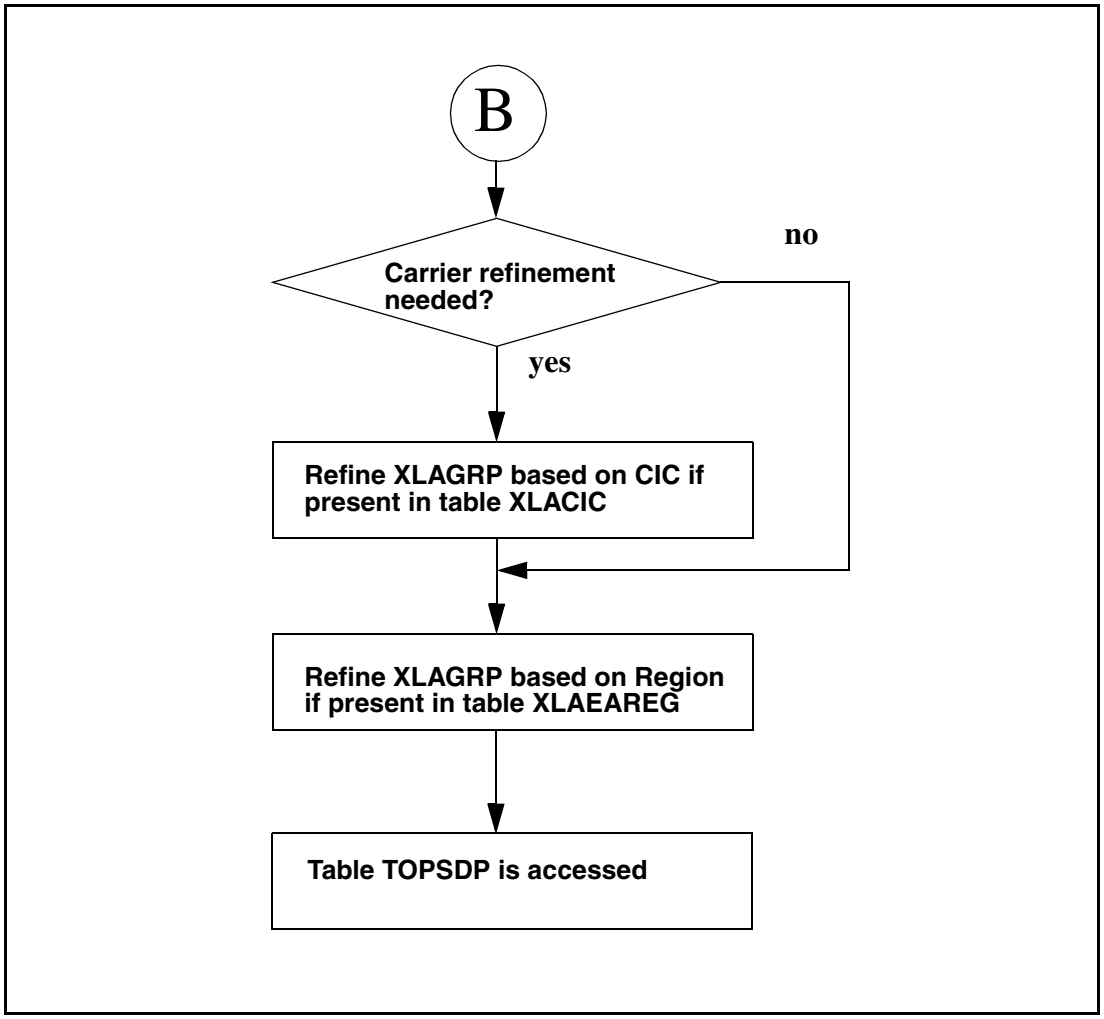


Figure 3 XLAGRP Refinement Order For Equal Acess Calls



53.2.3 Table XLACLASS

Table XLACLASS allows the XLAGRP to be refined based upon the calling service class. The index of the table is the existing XLAGRP and the calling service class. It then provides a new XLAGRP if a match is found.

Table 3 Example of Table XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field CLGCLASS supports a range of {UNKNOWN, STATION, COIN, HOTEL, RESTRICTED}.

53.2.4 Table XLABILL

Table XLABILL allows the XLAGRP to be refined based upon the billing type. The index of the table is the existing XLAGRP and the bill type. It then provides a new XLAGRP if a match is found.

Table 4 Example of Table XLABILL

XLAGRP	BILLTYPE	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field BILLTYPE supports a range of {UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD}.

Note: Station paid and person paid are both handled by the PAID criteria. Both are PAID calls but may have a different rate applied. Since this refinement is to capture the billing method not the rate, station and person ratings are treated the same. This applies to all billing types.

53.2.5 Table Flow Example

This example section illustrates the new refinement tables and how they achieve special routing for coin station paid calls. It is simplified by using an incoming trunk group with non-EA calls. A59006822 fully details XLAGRP methods for EA and operator calls. It is further simplified by not having SPID or originating digit refinements. These are fully documented in AF7159.

Table 1 TOPSTOPT

GRPKEY	ACDDATA	DISPCLG	ADASERV	ADASANS	ANITOCLI	OLNSQRY	DCIBIDX	LNPCLGAM	XLA SCHEM		SPIDPRC	TRKSPID	
									NEWXLA	XLAGRP		DFLTSPID	SPID
TRK1	QMSCAM	N	NONE	NA	N	NONE	0	N	Y	**TRK1**	N	N	

Table 2 XLASPID does not have a match

Table 3 XLAODIGS does not have a match

Table 4 XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

Table 5 XLACLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

Table 6 TOPSDP

XLAGRP	STS	OPERPRTN	ORIGSCRN	OPERSCRN	MCCSPRTN	MCCSSCRN	LCANAME
TRK1	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COINPAID_ROUTE	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COIN_NOROUTE	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA
TRK1COIN	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA

- STS - This is the service translations scheme which is also the index into code translations (i.e., Table HNPACONT).
- OPERPRTN - This is the operator pretranslator name that is used for performing pretranslations from the operator position. It is used to index into Table STDPRTCT.
- ORIGSCRN - This is the class of service screening name that is used for screening based upon the location of the originator. It is used to index into Table CLSVSCRC.
- OPERSCRN - This is the class of service screening name that is used for screening when an operator or service node is associated with the call. It is also used to index into Table CLSVSCRC.
- MCCSPRTN - This is the pretranslator name that is used for performing pretranslations for the Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table STDPRTCT.
- MCCSSCRN - This is the class of service screening name that is used for screening when performing the call screening for Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table CLSVSCRC.
- LCANAME - This is the local call area screening name which is used to determine if the call is local. It is used to index into table LCASCRCN or LCAINFO.

For non-EA COIN PAID calls arriving on TRK1, the initial XLAGRP is determined from table TOPSTOPT and refinements are performed as follows. The current XLAGRP is noted after the arrow.

1. Table TOPSTOPT provides the initial XLAGRP name

----> TRK1

2. SPID refinements are not needed, no change

3. Originating digits are not found in XLAODIGS, no change

4. Table XLACLASS finds TRK1 COIN, changes XLAGRP

---> TRK1COIN

5. Table XLABILL finds TRK1COIN PAID, changes XLAGRP

----> TRK1COINPAID_ROUTE

The final XLAGRP for this non-EA COIN PAID call is TRK1COINPAID_ROUTE. This XLAGRP is indexed in table TOPSDP to find the screening and translations indices.

Note: In this example, if the coin call was billed collect then the final XLAGRP would have been TRK1COIN_NOROUTE which can be setup in table TOPSDP to have screening and translations indices which do not route or route to treatment. Also note that the XLAGRP, TRK1COIN, can be added to TOPSDP and be setup for indices which do not route. This ability limits the amount of datafill needed to only allow coin paid calls to complete. Thus, the refinement TRK1COIN COLLECT in XLABILL is not needed nor the TRK1COIN_NOROUTE XLAGRP. These were only included here to illustrate the options.

53.2.6 Activation

When activating feature A00002765 in a site where XLAGRPs are already in use, the following is recommended.

- For a new trunk group to begin using the XLAGRP translations and is not dependent on existing translations, a new XLAGRP name should be assigned to the trunk group and the new XLAGRP used in the refinement tables as needed. This has no interaction with existing translations since existing XLAGRPs will not find matches in the new tables.
- For an existing trunk group with XLAGRP translations (or a new trunk group which will use existing XLAGRP translations), it is recommended to work backwards in the refinement order. By adding the final XLAGRP first, no matches will be found until the first refinement using the existing XLAGRP is datafilled. For example, if TRK1 has XLA1 defined in TOPSTOPT and has existing translations for SPID where (XLA1 SPID XLA1SPID) is datafilled in table XLASPID, then to create a coin station_paid route for these calls, first add new XLAGRPs (XLA1SPIDCOIN and XLA1SPIDCOINPAID) to table XLAGRP then add to table XLABILL (XLA1SPIDCOIN PAID XLA1SPIDCOINPAID) [so far no changes will occur]. Then add to table XLACLASS (XLA1SPID COIN XLA1SPIDCOIN) - [once this is added coin station_paid calls will route using XLA1SPIDCOINPAID].

  Note: Ensure all XLAGRPs have datafill in table TOPSDP; be sure that XLA1SPIDCOIN can still route correctly. These are the calls which are coin but not paid for that trunk group with that SPID. TOPSDP will need

to point to something that goes to treatment (if desired) otherwise they will route to the last route found in standard translations.

53.3 Hardware Requirements or Dependencies

NA

53.4 Software Requirements or Dependencies

UNBN0101, OSB00101

53.5 Limitations and restrictions

- XLACLASS is limited to a range containing UNKNOWN, STATION, COIN, HOTEL, RESTRICTED.
- XLABILL is limited to a range including UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD.
- Station billing and person billing may have different rates but are both treated the same in table XLABILL. For example, station paid and person paid will both refine under the PAID criteria.
- This feature is intended to be used with the dollar pre-pay coin functionality. Limitations for this function include:
  - — External rater not support with OSSAIN
  - — External rater, Coin signalling, ACTS not supported in Global loads

53.6 Interactions

This feature can alter the translations and route selected for calls using the XLAGRP method.

53.7 Glossary

Term	Description
XLAGRP	Translations Group

53.8 References

REF #	Description of Reference
AF7159	AF7159.aa11, January 23, 1998 Unbundling: SPID Processing, Translations, and Routing

59006822	OPRTRANS and EA Unbundling
59006827	LATA Screening Replacement
297-8403-903	TOPS Unbundling User's Guide

54: Functional Description (FN): A00002766

54.1 Feature name

Add Extension Registers for Billing OM's

54.2 Description

54.2.1 AMA OMs

The ATTAMA OM group now has the maximum limit of 32 registers. Another group will be created to contain the extra extension registers. Only the extension registers for AMANS and AMUNANS will reside in the new ATTAMA2 OM group. The maximum register value for this group is now 32767 before it resets to 0. The extension register will allow capturing the number counter rollovers.

The new extension functionality will be implemented under SOC control. This will allow for controlled customer implementation and also provide the ability to disable the new extension if required.

The following shows the existing ATTAMA group along with the new ATTAMA2 group.

```
ATTAMA
CLASS:   ACTIVE
START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;
SLOWSAMPLES:          7 ; FASTSAMPLES:          69 ;
          AMORIGS   AMORIGS2     AMTRMT    AMTRMT2
         AMNOTRMT      AMANS   AMRCSTPD   AMRCSTP2
         AMLTSTPD   AMEDSTPD   AMNASTPD    AMRC411
          AMLT411    AMED411    AMNA411    AMRC555
          AMLT555    AMED555    AMNA555   AMRCTRCR
         AMLTTRCR   AMRCOTHR   AMLTOTHR   AMEDOTHR
         AMNAOTHR   AMRCLONG   AMLTLONG    AMUNANS
          AMRCSST      AMSST    AMDA555    AMDA411


    0            0          0          0          0
                 0          0          0          0
                 0          0          0          0
                 0          0          0          0
                 0          0          0          0
                 0          0          0          0
                 0          0          0          0
                 0          0          0          0
```

```
ATTAMA2
CLASS:   ACTIVE
START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;
SLOWSAMPLES:          7 ; FASTSAMPLES:          69 ;
             AMANS2 AMUNANS2

    0           0          0
```

54.3 Hardware Requirements or Dependencies

None

54.4 Software Requirements or Dependencies

The capabilities will be under SOC control.

This activity only impacts offices using the Bell Core AMA billing format.

54.5 Limitations and restrictions

None

54.6 Interactions

The existing OM groups will not be changed. The new groups will contain only new registers. The new OM groups are:

- ATTAMA2

54.7 Applicable customer facing sections

Fault Management

Logs	__N/A____
Alarms	__N/A____

Configuration

Data Schema	__N/A____
User Interface	__N/A____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) ___X___

54.8 Glossary

Term	Description

55: Functional Description (FN): A00002822

55.1 Feature name

User Interface Manager for CBM

55.2 Description

The User Interface Manager provides a user interface for local CBM maintenance, administration and system monitoring. The UI consolidate all of the primary maintenance operations under a single unified program which resembles the CM MAP interface.

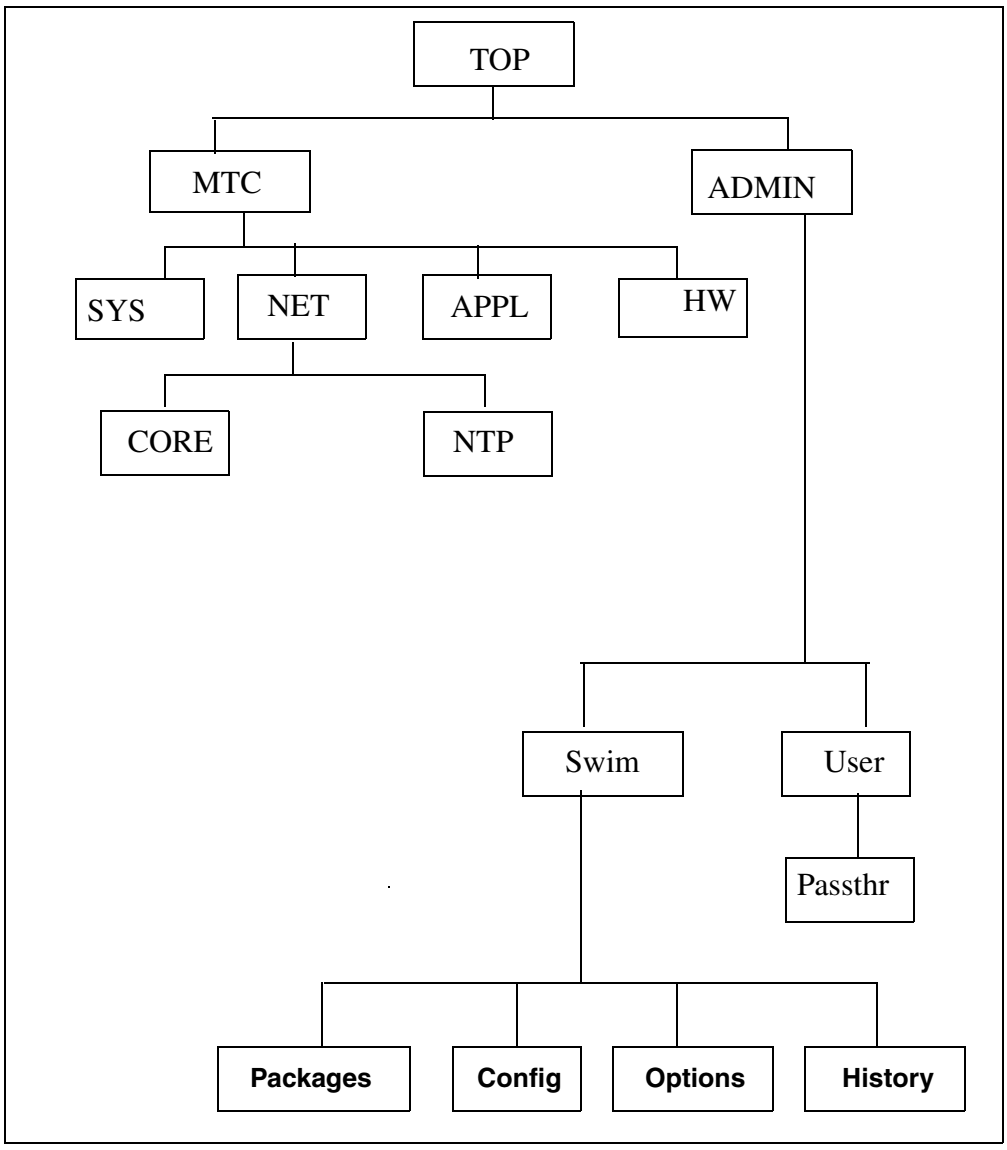
The operations that can be accessed through the UI are divided into two categories; maintenance and system administration. Maintenance provides access and control over the CBM application software. System administration functions include CBM configuration, package installation/removal.

The UI provides input and output to a human operator. When a user selects an operation in the UI, a function contained in the appropriate maintenance subsystem is invoked.

The UI is organized into a system of screens. The screens are organized in a hierarchy, and each screen represents a functional area.

The UI functional structure is shown in Figure 1 below. This is the intended view for CSEN07 (CBM) and is subject to changes as the product evolves.

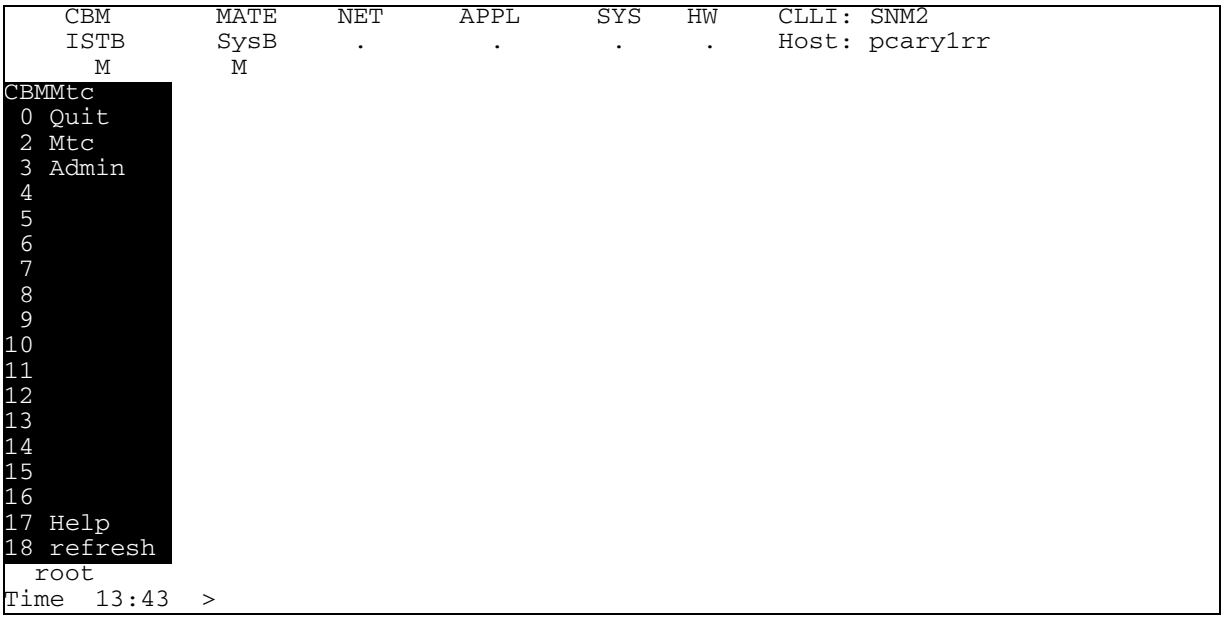
Figure 1 UI functional structure.



55.3 Functionality

The CBM screens are not identical to the MAP screens, but they retain the basic structure and input/output mechanisms as the MAP. Each CBM screen is divided into five areas: alarm banner, command list, output, clock, and input. A typical CBM screen is shown in figure 2.

Figure 2 CBM Main Level Display



55.3.1 Alarm Banner

The top area (referred as I in fig. 2)contains the current screen title and the CBM alarm banner. The alarm banner indicates the node state for the CBM and the state of the major CBM components.This area is updated dynamically, and appears on every CBM screen.

55.3.2 Command List

The area on the left is the CBM command menu(referred as II in fig. 2). Commands available at the current level are listed in MAP style and the current level is displayed at the top of the list.

55.3.3 Output

The area on the right is the RMI output window(referred as III in fig. 2). The information in this window can be either static or dynamic.

55.3.4 Clock

The CBM clock and current userid are displayed at the bottom left of the screen(referred as IV in fig. 2). The clock is updated dynamically.

55.3.5 Input

The single line at the bottom right of the screen is used for CBM input(referred as V in fig. 2).

55.3.6 Commands Available at ‘All’ Levels

The following commands are generally available at each level. The use of and output from these commands is essentially the same. They are:

1. Quit: Quits the current level and moves back to the previous one. You may specify the option ALL in order to exit the CBM from any level.
2. Help: Obtains help specific to the current level. If information on a specific command is desired you may type the command name as an option to get information pertaining to that specific command.
3. Refresh: If the screen display is corrupted, use refresh to force a redraw of the screen.

These commands will not be listed in the screen command descriptions later in this document.

55.3.7 CBM Main Level

The main menu breaks all functions into either the maintenance category, or the system administration category. Additional categories may be added in the future as needed.

There is no default output for this level other than the main banner.

Commands:

1. Mtc: Displays the SDM Maintenance Level.(position 2 in fig. 3)
2. Admin: Displays the SDM System Administration Level.(position 3 in fig. 3)

Figure 3 CBM Main Level Display

```
    CBM         MATE    NET      APPL     SYS     HW CLLI: SNM2
    IsTb        SysB     .        .        .      .          Host :pcary1rr
     M           M
CBMMtc
 0 Quit
 2 Mtc
 3 Admin
 4
 5
 6
 7
 8
 9
10
11
12
13
14
15
16 LogQuery
17 Help
18 refresh
  root
Time  13:43  >
```

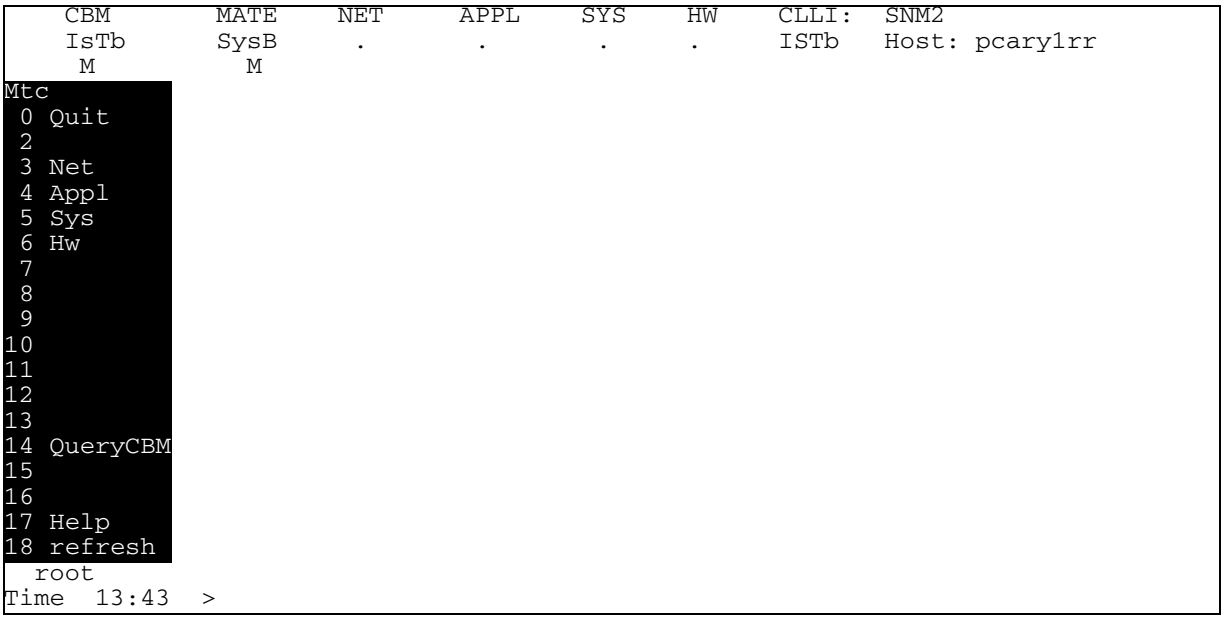
55.3.8 CBM Maintenance Level:

The maintenance level is the highest level for maintenance related commands.

Commands:

1. Net: Displays the LAN Connectivity Level.(position 3 in fig. 4)
2. Appl: Displays the Software Application Status Level.(position 4 in fig.4)
3. Sys: Displays the operating system s/w status level.(position 5 in fig.4)
4. Hw: Displays the Hardware Status Level.(position 6 in fig. 4)

Figure 4 CBM Maintenance Level Display



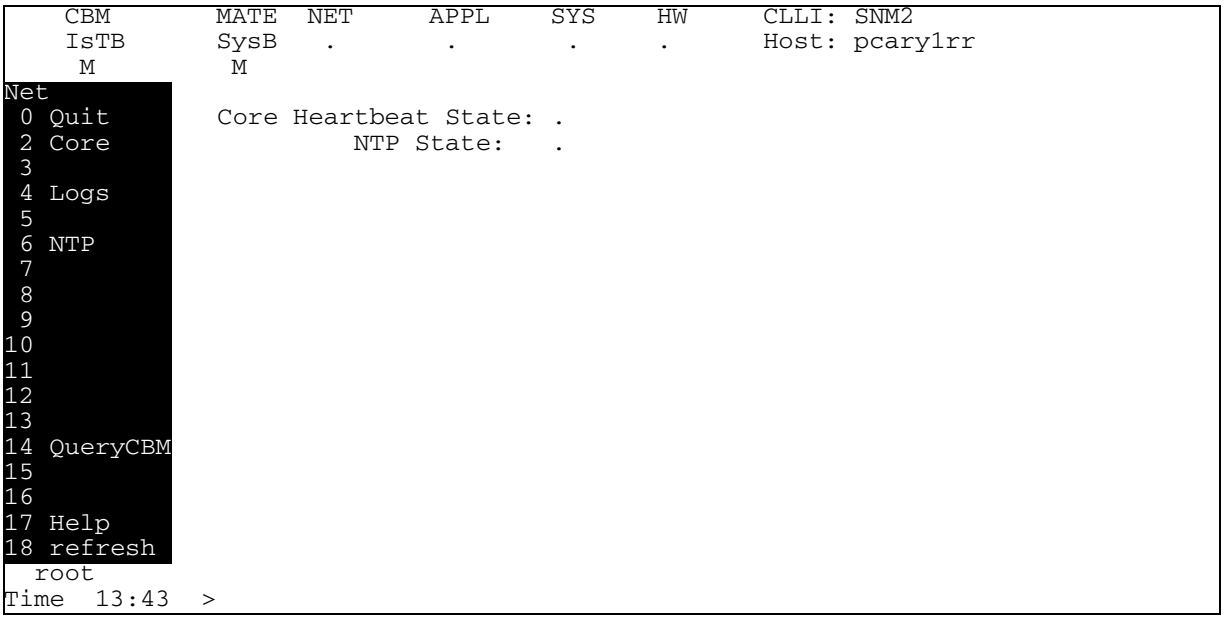
55.3.8.1 Net Connectivity Level

The net level shows the status indicator for the core heartbeat and NTP state.The status indicators displayed at this level are updated dynamically.

Commands:

1. Core: Go to core level (position 2 in fig. 7)
2. NTP: Go to the NTP level.(position 5 in fig. 7)

Figure 5 CBM Net Connectivity Level



55.3.8.1.1 Core Level

The Core level shows the communication paths to the Core and it also monitors the state of that communication. Figure 6 and 7 shows the display for the Ethernet connected cbm's and the OC3 connected cbm's respectively. The command line equivalents of the command are shown in Table 1

Commands:

1. Add: Add a communication path to the Core.
2. Change: Change the values for the given communication path to the Core.
3. Delete: Delete the given communication path to the Core.

Table 1 Core screen command line equivalents

UI Command	Command line equivalents
Add	No command line equivalents
Change	No command line equivalents
Delete	No command line equivalents

Figure 6 CBM Core Level(Ethernet Connected)

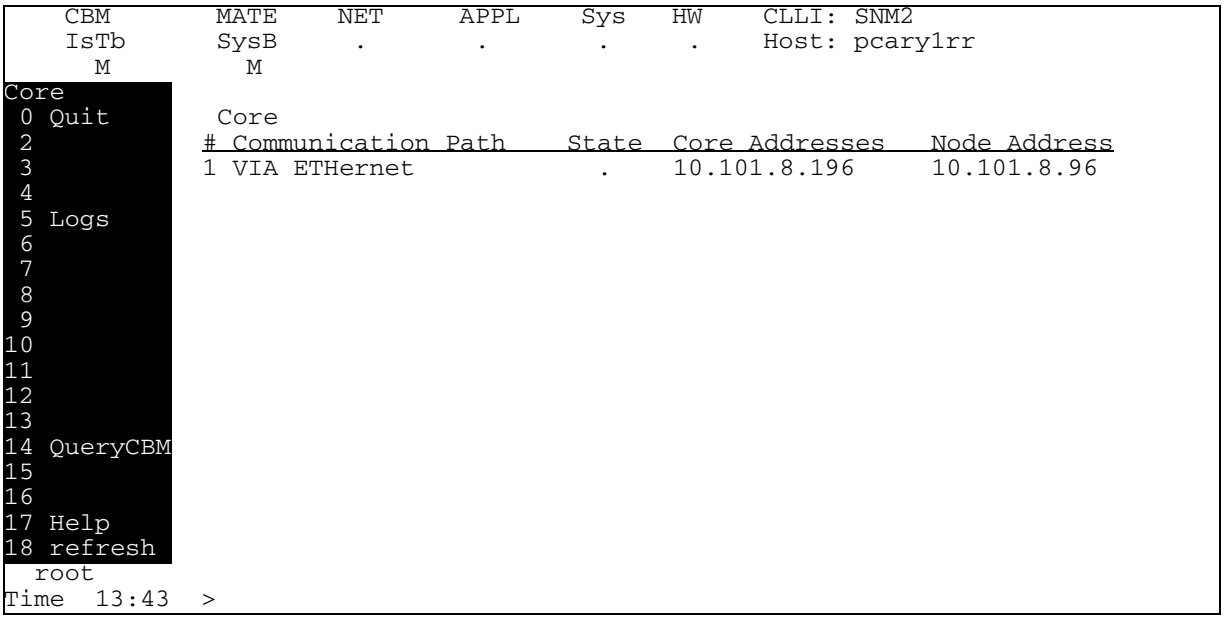
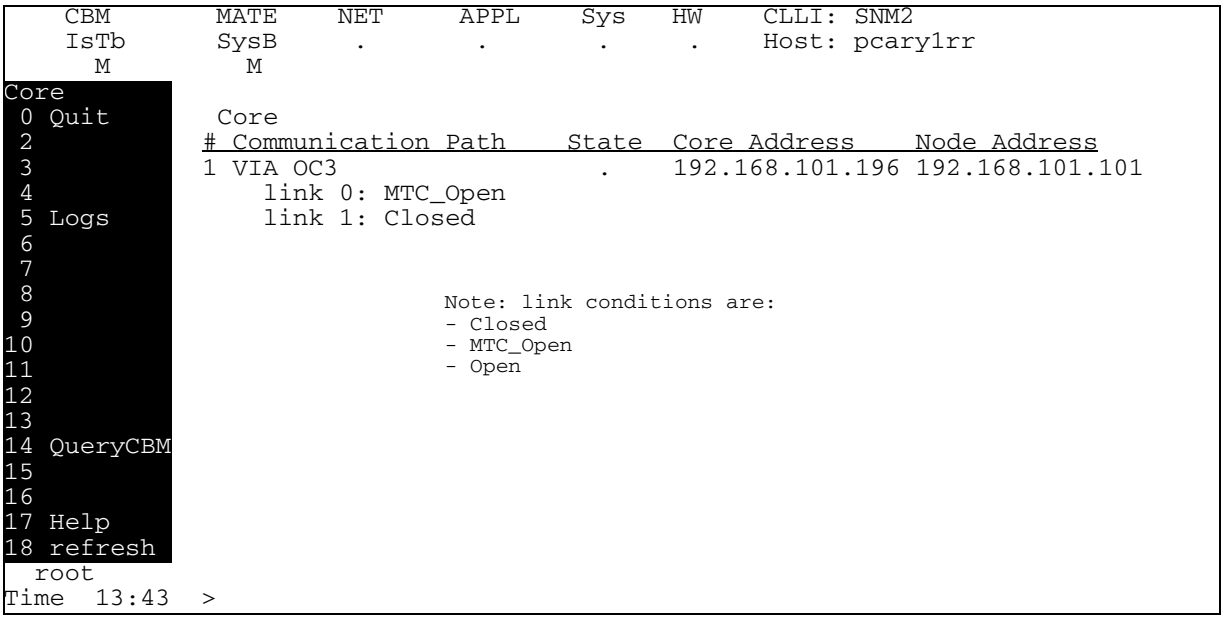


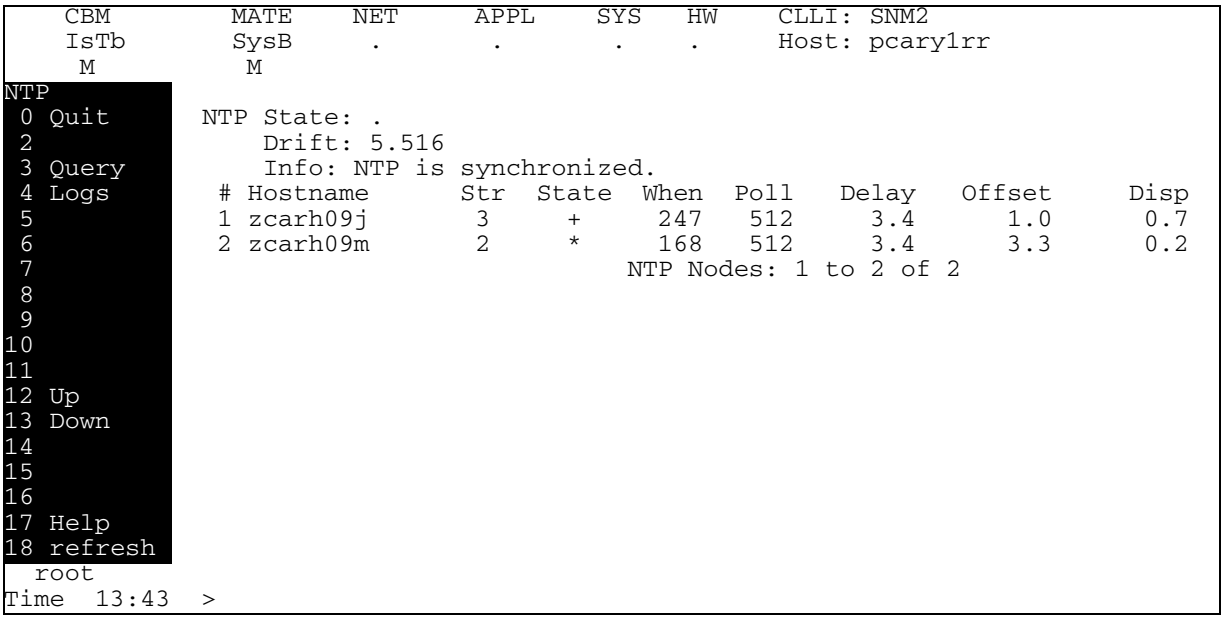
Figure 7 CBM Core Level (OC3 Connected)



55.3.8.1.2 NTP Level

The NTP level will synchronize the system clock. This level allows you to configure NTP daemon to synchronize the system clock with the NTP server(s)/peer(s). There are no command line equivalents commands for the NTP level.

Figure 8 CBM NTP Level



55.3.8.2 CBM Software Application Status Level

The Software Application Status Level shows the application status indicators.For each installed application, this level shows the application description and the current state. Application control is available on each of the installed application.

The status indicators displayed at this level are updated dynamically.

Commands:

1. Logs: Display application status logs.(postion 4 in fig. 9)
2. Bsy: Issues a busy command to the application. Busying an application will run the stop script for that application, and will shutdown all associated processes(position 7 in fig. 9).The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to ManB. Application that are Offline remain offline. The output for this command is displayed beneath the dynamic information. (e.g. bsy 2)

3. RTS: Issues a Return To Service command to the application. Returning an application to service will run the data reformat script for that application, and will initiate all processes associated with that application.(position 8 in fig. 9).The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to InSv(In Service).The InSv state is represented by a dot ".". The output for this command is displayed beneath the dynamic information.
4. OffL: Issues an Offline command to the application.(postion 9 in fig 9)The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to Offline. The applications themselves become ManB, and applications that are Offline remain Offline.The output for this command is displayed beneath the dynamic information in fig. 9).

Figure 9 CBM APPL Level

```
    CBM       MATE    NET     APPL    SYS    HW    CLLI: SNM2
    ISTB       .       .       .       .     .    Host: pcary1rr
     M         M
Appl
 0 Quit        # Application                                    State
 2             1 Table Access Service                            .
 3             2 OM Delivery                                    OffL
 4 Logs        3 OM Access Service                              ISTb
 5             4 Log Delivery Service                           ManB
 6
 7 Bsy
 8 RTS
 9 OffL
10
11
12 Up
13 Down
14 QueryCBM
15
16
17 Help
18 refresh
  root
Time  13:43  >
```

The command line equivalents of the commands under the appl level are shown in Table 2 below:

Table 2 APPL screen command line equivalent commands

UI Command	Command line equivalents
Bsy	appctrl --bsy| -b <appname> | groupname>
Rts	appctrl --rts | -r <appname> | groupname>
Offl	appctrl --offl | -o <appname | groupname>

UI Command	Command line equivalents
QueryCBM flt	queryflt
QueryCBM status	queryflt -s
Query flt mate	queryflt -m

55.3.8.3 CBM System Level

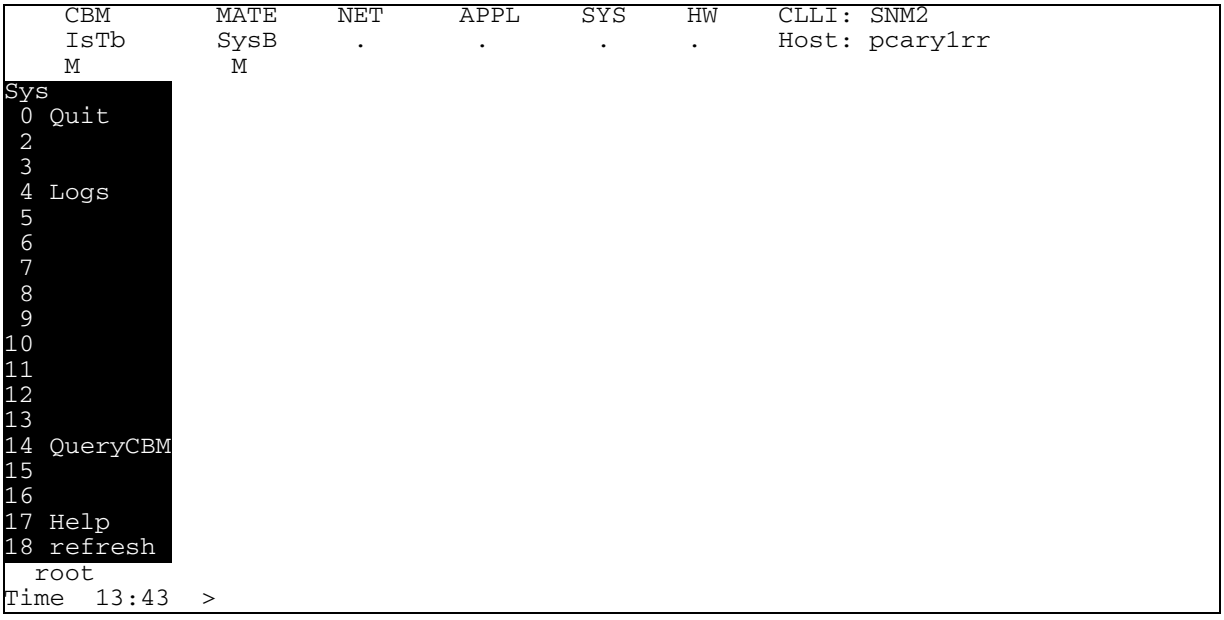
The CBM system level shows the status of operation system software parameters.

Commands:

Logs : Display the last events reported

QUERYCBM <flt, flt mate , status > : Commands are invoked as shown in Table 2.

Figure 10 CBM SYS Level



55.3.8.4 CBM Hardware Status Level.

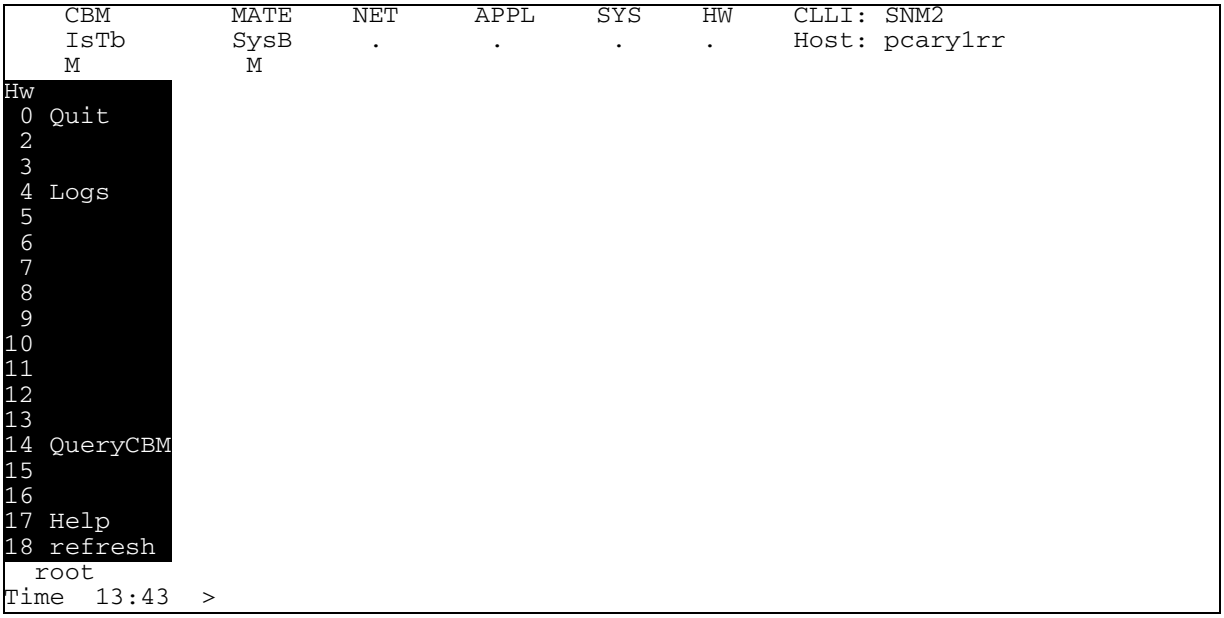
The CBM hardware status level shows the hardware status indicators.The status indicators displayed at this level are updated dynamically.

Commands:

Logs: Displays the last event reported .

QueryCBM < flt, flt mate, status >: Commands are invoked as shown in Table 1

Figure 11 CBM Hardware Level



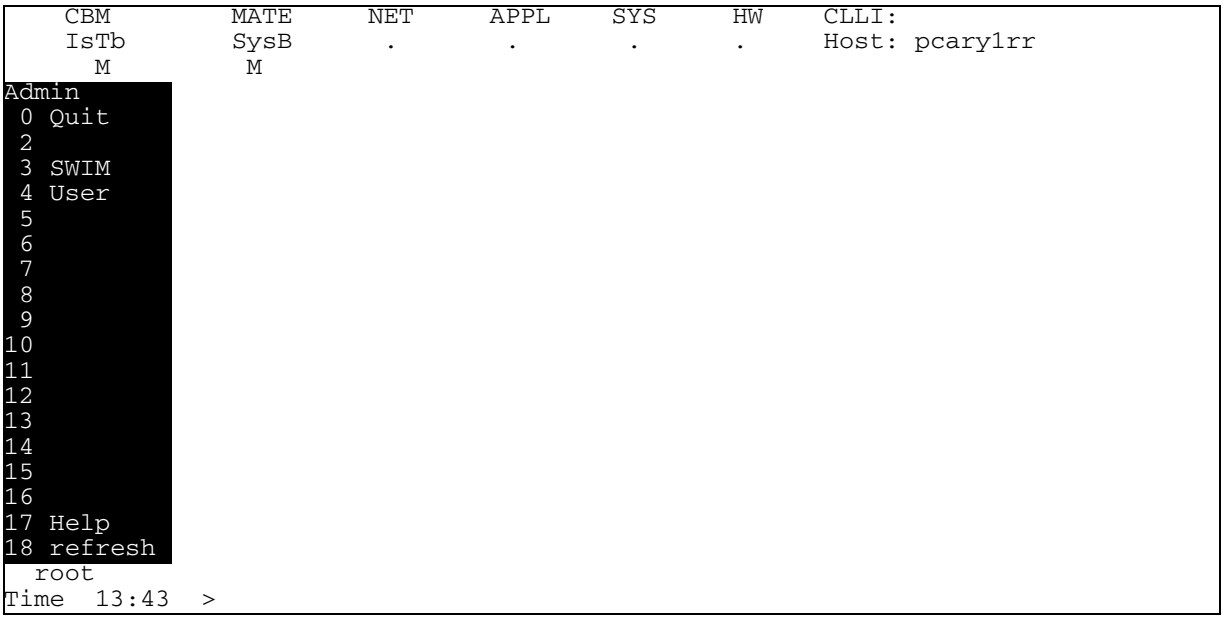
55.3.9 CBM Administration Level

The Admin level is the highest level for system administration commands. The commands available under system administration are dependent on the user id. The root user has full access to all commands. The maint class users are given only a subset of the system administration commands.

Commands:

1. Users: Enter the user administration level.(postion 4 in fig. 10)
2. SWIM: Enter the software inventory management level.(postion 3 in fig. 10)

Figure 12 CBM Admin Level



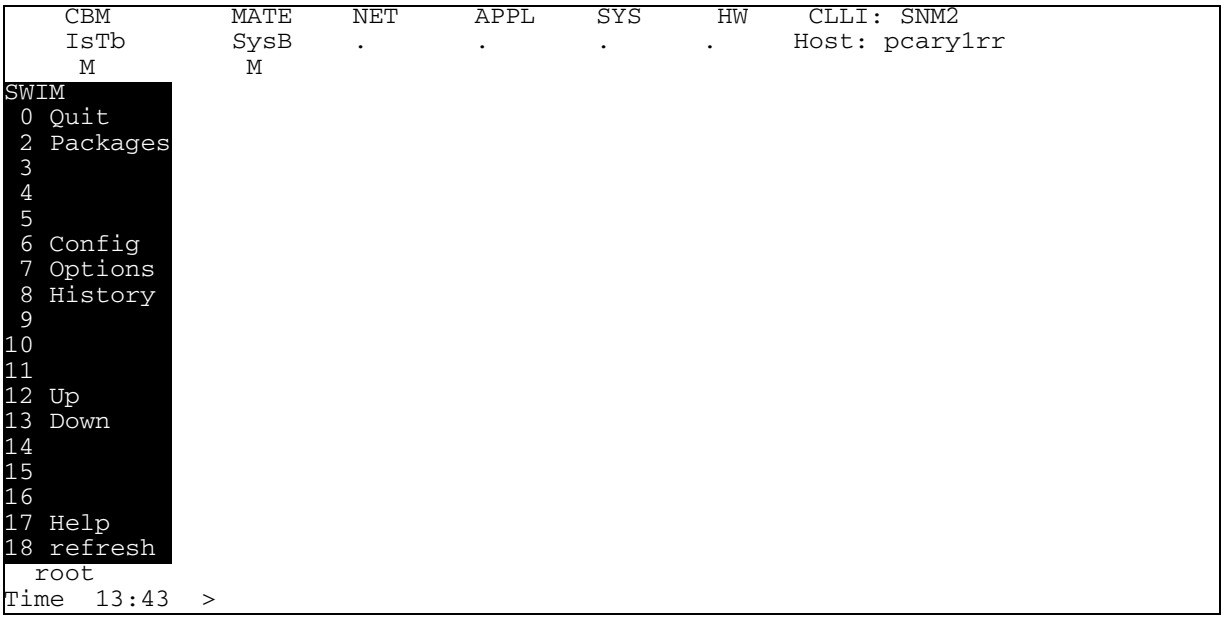
55.3.9.1 SWIM

The swim level of the CBM provides software inventory management.The SWIM level interface will show the product level information and the application status information.

Commands:

1. Packages: Enter the software packages level(position 2 in fig. 13).
2. Config: Enter the software configuration level(position 6 in fig. 13).
3. Options: Enter the options level(position 7 in fig. 13).
4. History: Enter the software history level(postion 8 in fig. 13).

Figure 13 CBM SWIM Level



55.3.9.1.1 SWIM Packages Level

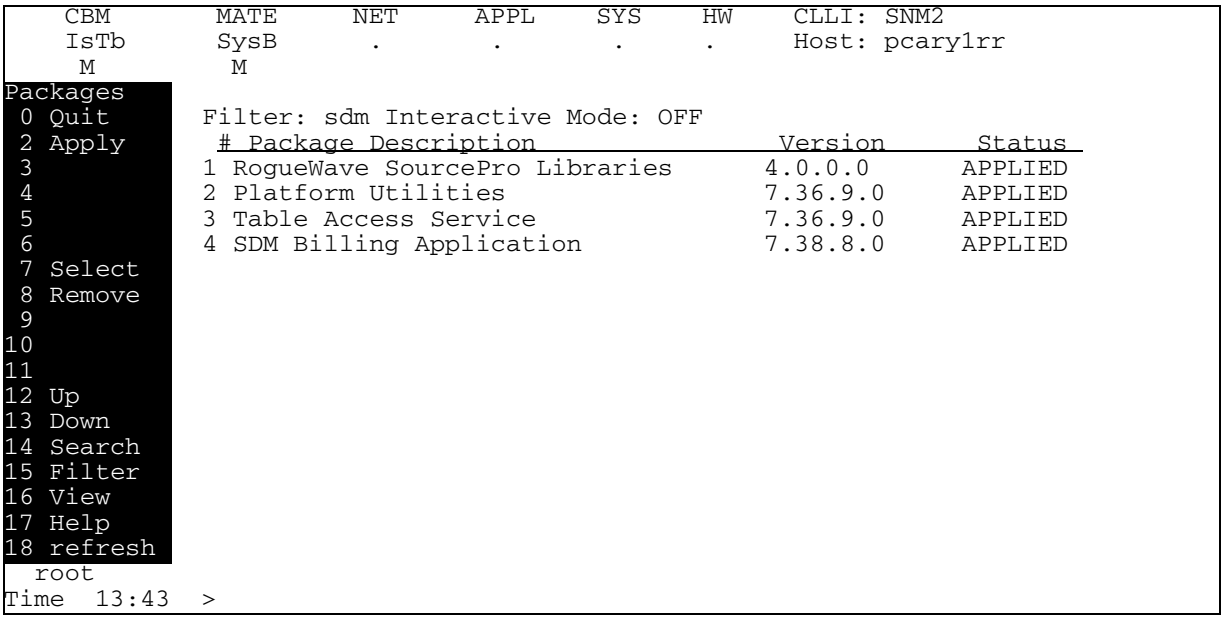
This level contains commands to list and remove installed software. It shows the list of packages which exist on the system. The software can be applied or removed from this level for maintenance purposes. The list columns include: a list index number representing the package in each row, the package name,instance or description , the version number which is currently installed, and the package status (APPLIED, PARTIAL or FAILED).The Status column was added to identify if the package has been APPLIED, if there is a NEWer instance (SDM/Nortel software only and mostly for lab environment) or if the package has NOT been APPLIED, no instance on the system. APPLIED packages versions are currently in use. PARTIAL packages are packages that had an error during installation and are only partially installed. PARTIAL and FAILED packages should be removed from the system. The Packages level is updated every 20 seconds or when you use the Refresh command. The Packages level is shown in Figure 14.

Commands:

1. Apply : Install the selected packages(postion 2 infig. 14).
2. Select : Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again(position 7 in fig. 14).
3. Remove: Remove software. This command can be used to remove software that is in any of the APPLIED, PARTIAL,or FAILED states(postion 8 in figure 14).

4. Search: Search the list for the given text, and reposition the list when a match entry is found(postion 14 in fig. 14).
5. Filter: Filter the list of software(position 15 in fig. 14)
6. View: Toggle between showing the software description, the software package instance and the software package name(position 16 in fig. 14).

Figure 14 CBM Packages Level



55.3.9.1.2 CBM Apply Level

The Packages Apply level shows a list of packages which exist on the source. The default source is automatically listed when entering the Apply level for the first time. The default source can be changed within the Options level. The list columns include: a list index number representing the package in each row, the package description, instance name or package name The current version listed beside every package is updated every 20 seconds or when you use the Refresh command. The command line equivalents are shown in table 3.

Commands :

1. Source: Choose a source directory from which to load packages.
2. Reload: Reload the list of packages from the current source.
3. Select: Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again.
4. Apply: Apply packages on this CBM

5. Upgrade: Upgrade all packages to the latest versions available on the source .
6. Search: Search the list for the given text, and reposition the list when a match entry is found.
7. Filter: Filter the list of software.
8. View: Toggle between showing the software description, the software package instance and the software package name

Figure 15 CBM Apply Level

```
    CBM       MATE     NET      APPL     SYS     HW     CLLI: SNM2
    IsTb      SysB      .        .        .      .     Host: pcary1rr
     M         M
Apply
 0 Quit      Source: the directory /data/swd/sdm.
 2           Filter: OFF Interactive Mode: OFF
 3           # Package Name                    Version          Status
 4 Source    1 Table Access Service              7.36.9.0     APPLIED
 5 Reload    2 GNU Debugger                      7.0.1.0       NOT APPLIED
 6                          Packages on the source: 2 to 2 of 2
 7 Select
 8 Apply
 9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 refresh
  root
Time  13:43  >
```

Table 3 SWIM screen command line equivalents

UI Command	Command line equivalents
Apply	pkgadd -d <full path to the package>
Remove	pkgrm <Package name >
Search	pkginfo -c <any matching string >

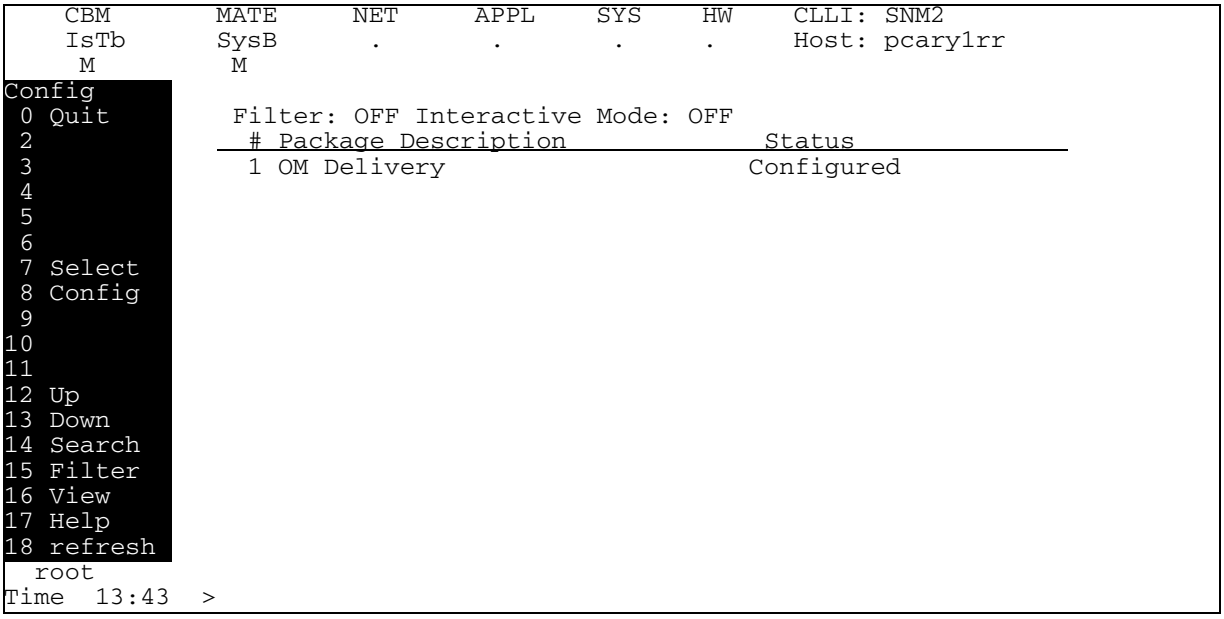
55.3.9.1.3 CBM Config Level

The Config level shows the list of applications which have configuration programs associated with them. Each configuration program can be executed by using the Config command. The Config level is updated every 20 seconds or when you use the Refresh command. The config level is shown in Figure 15.

Commands:

1. Select: Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again.
2. Config: Configure packages
3. Search: Search the list for the given text, and reposition the list when a match entry is found.
4. Filter: Filter the list of software
5. View: Toggle between showing the software description, the software package instance and the software package name.

Figure 16 CBM Config Level



55.3.9.2 User

The User level of the CBM provides administration of the CBM maint userid.The command line equivalents of Passthru level are shown in Table 4.

Figure 17 CBM User Level

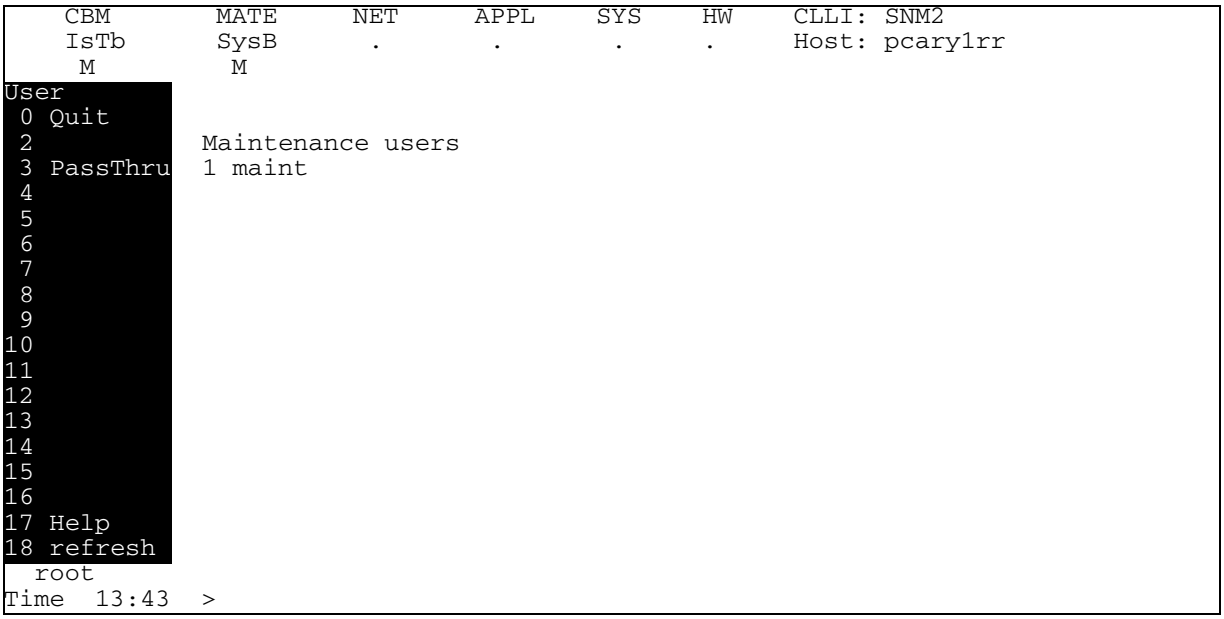


Figure 18 CBM PassThru Level

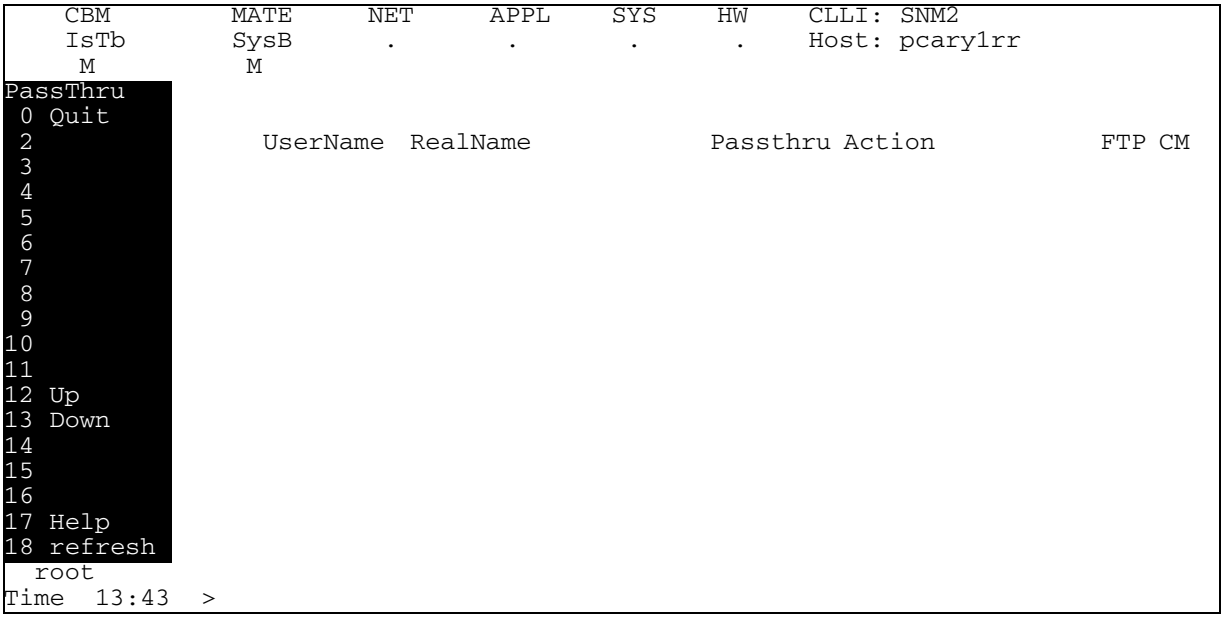


Table 4 PassThru screen command line equivalents

UI Command	Command line equivalents
Add	passthru -m <username> -a realname=<real name> -a args=<telnet target> -a passwd=no
Change	passthru -l <username> -a realname=<new realname> -a args=<new target>
Delete	passthru -d <username>

55.4 Hardware Requirements or Dependencies

None

55.5 Software Requirements or Dependencies

SDM base software is installed

55.6 Limitations and restrictions

None

55.7 Interactions

None

55.8 Applicable customer facing sections

This activity introduces, new logs/ alarms

Fault Management

Logs	__Y____
Alarms	___Y___

Configuration

Data Schema	_____
User Interface	___Y___
Element Management	____NA__
Security	____NA__
Service Order	____NA__
Office Parameters	____NA__

Accounting (includes AMA billing) ____NA__

Performance (includes operational measurements) ____NA_

55.9 Glossary

Term	Description
CBM	Core(sucession) and Billing Manager
CM	Computing Module
MAP	Maintenance and Administration Position
UI	User Interface

56: Functional Description (FN): A00002823

56.1 Feature name

SDM CORE HA MAINTENANCE (HA OAMMTCE)

56.2 Description

This activity adds support for connecting an SDM/CBM to an XA-core using Ethernet on the IRM stack. Support for connecting an SDM to 3PC will be maintained.

From Figure 1 on page 572, one can see that the new connectivity model of CBM goes from:

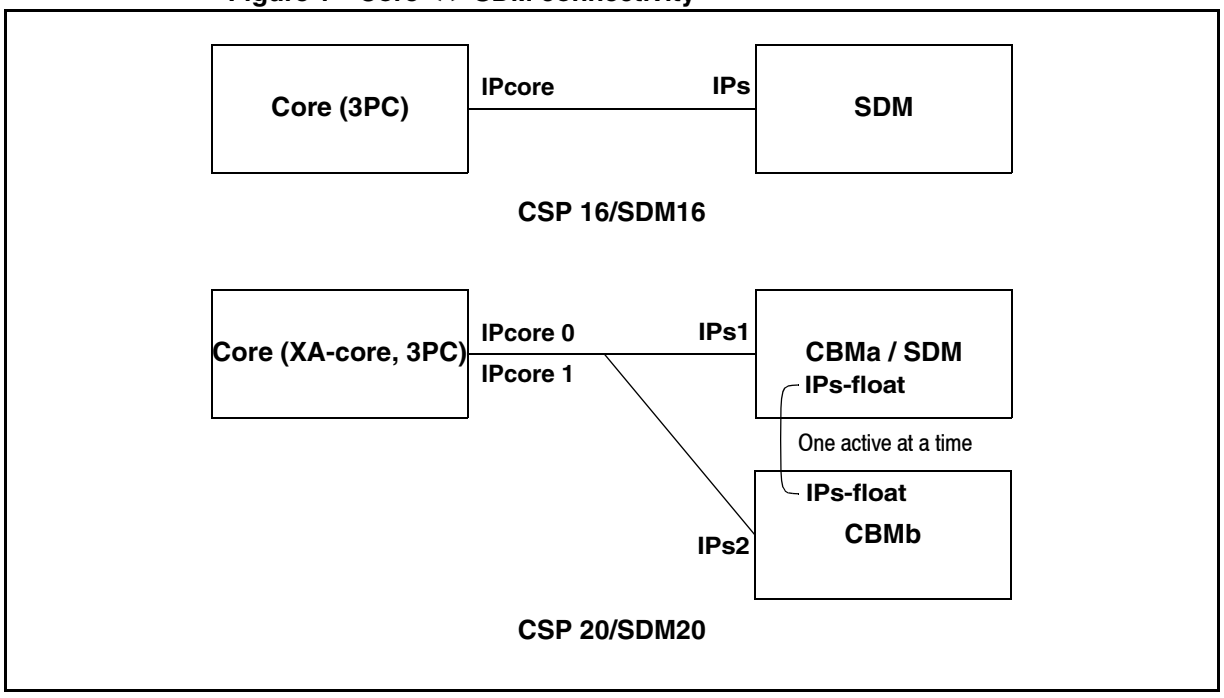
- a single SDM address (as seen by the core)
- a single Core IP address (There is support for a different Lancomm address.)

to:

- two Core IP addresses of which SDM/CBM will only use one.
- one floating IP address for the SDM/CBM cluster which is used by the active CBM node.
- one fixed IP address for each CBM node (for SDM the floating and fixed address would be the same)

The related core activity A00002510 routes messages between the legacy LANCOMM IP stack and the newer IRM IP stack. This activity identifies the SDM/CBM floating IP address to the A00002510 code so that applications using the LANCOMM stack can communicate with the SDM/CBM.

Figure 1 Core <-> SDM connectivity



In addition to the above, support is being added for core side applications to query the TCP port numbers and RPC service numbers of their peers on the SDM.

56.3 Hardware Requirements or Dependencies

None

56.4 Software Requirements or Dependencies

None

56.5 Limitations and restrictions

None

56.6 Interactions

None

56.7 Applicable customer facing sections

Fault Management

Logs ___X

Alarms ___N/A

Configuration

Data Schema ___N/A

User Interface ___N/A

Element Management ___N/A

Security ___N/A

Service Order ___N/A

Office Parameters ___N/A

Accounting (includes AMA billing) ___N/A

Performance (includes operational measurements) ___N/A

56.8 Glossary

Term	Description
CBM	Core and Billing Manager

57: FN: Node ISTB for SPM Carrier Outage: A00002858

57.1 Feature name

Mark SPM/STM1 Node ISTb under the PM banner whenever one of its carriers goes SysB or one of its line carriers has a remote alarm.

57.2 Description

57.2.1 Background

Nortel's customers have expressed the desire to have a SysB carrier cause its SPM node to go ISTb under the PM banner. This would provide the telco a visual MAP alert that a carrier outage may be causing multiple trunk failures. Adding this capability would make SPM work like DTC. But most importantly, this feature will reduce the chance of long duration outages when the telco is not aware that a carrier problem is disrupting service. This feature will also reduce the chance of problems during a Panther upgrade since these types of carrier problems can prevent sparing on the OC3.

Feature A59036987 attempted to address this concern by adding the display of S/P/D/d/R under the TRKS banner.

57.2.2 Operation

There will be two new "triggers" that can cause a SPM node to go ISTb under the PM banner:

57.2.2.1 Trigger 1: Check SysB Carrier on OC3 RM

When one of the OC3's carriers goes SysB, which corresponds to a Bellcore state of OOS-AU-FAF (which is same as OC3 carrier state of IS-UPS-FAF). FAF is FAcility Failure. Note that this trigger corresponds to "S/P/D/d" in the A59036987 feature. While the carrier is SysB, any of its trunks will be in the CFL condition and not able to bear traffic.

Here's an example of the existing log that will be seen when a carrier goes SysB:

MSH706BM * CARR511 JUN04 05:46:03 6200 **SYSB** CARRIER SPM 34
CKT: 13 CarrName: SPM34_STS1P_1_VT15P_3_DS1P_3
Carrier: STS1P 1 VT15P 15 DS1P 1
Previous State: **INSV**

This trigger clears when the carrier is no longer SysB (e.g. CARR510 log when the carrier is RTS'd and goes InSv).

For STM-1 international product, the trigger will occur when a STM-1 carrier goes SysB.

57.2.2.2 Trigger 2: Check RFI Alarm on STS3L Carrier

When one of the OC3'sInSv STS3L carriers has a RFI (Remote Failure Indication) alarm. Such an alarm can be caused by cutting the TX fiber on the OC3. Note that this trigger corresponds to "R" (for Remote alarm) in the A59036987 feature. Since OC3 sparing will not be allowed while the remote alarm condition is present on the line carrier, the OC3 is effectively in an E2 outage condition due to the loss of redundancy.

Here's an example of the existing log that will be seen when a remote alarm is raised on a line carrier. Note that the carrier data in table MNHSCARR would have to set the RFI alarm as reportable (RFI MN RPT) for this log to be seen.

```
MSH8_03BM   * CARR310 APR18 10:27:41 3204 FLT  CARRIER SPM  41
                CKT: 178  CarrName: ATM_STS3L_SPM_41_CKT_178
                Carrier: RM     2 OC3S   0 STS3L  0
                Failure: RFI     Set
```

If the RFI alarm is set as NRPT (non-reportable) for the carrier, then the log will not be seen but the trigger will still occur. Note that the CI command:

MAPCI;MTC;TRKS;CARRIER;POST {carrier};LISTALM

will always show the presence of the alarm, independent of whether MNHSCARR sets the alarm as RPT or NRPT for the carrier.

This trigger clears when the RFI alarm clears (as reported by a CARR310 "RFI Clear" log).

For STM-1 international product, trigger will occur when a InSv STM1M carrier has a RFI alarm.

57.2.3 MAPCI PM Display

When one of these triggers occur, the new ISTb reason string will appear in the existing SPM300 log that occurs whenever a OC3 RM goes ISTb. See Log section below for details. The severity off this ISTb MAP alarm will be minor, so it won't appear under the "1 SPM" display below.

Here's how the MAP's PM level will appear for the ISTb SPM when one of the above triggers has occurred. Note that the "S" under TRKS is part of an existing feature that indicates a section-level carrier (e.g. OCS3) is SysB.

```
XAC      MS     IOD     Net      PM      CCS     Lns     Trks    Ext     APPL
   .      .       .       .     1 SPM     .      . .     ..S .     .       .

                                SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit         PM                0       0       0       0       1     177
  2 Post_        SPM               0       0       0       0       1      77
  3 ListSet
  4 ListRes   SPM   20  ISTb  Class: SMG4
  5 Trnsl
  6          Shlf0 SL A Stat  Shlf0 SL A Stat  Shlf1 SL A Stat  Shlf1 SL A Stat
  7          -----  1 - ----  CEM 1  8 A ISTb  -----  1 - ----  -----  8 - ----
  8          -----  2 - ----  OC3 0  9 A ISTb  -----  2 - ----  ALM 0  9 A InSv
  9 OfClk     VSP 0  3 A InSv  OC3 1 10 I InSv  -----  3 - ----  DSP 3 10 I InSv
 10           VSP 1  4 A InSv  VSP 2 11 A InSv  -----  4 - ----  DSP 0 11 A InSv
 11 Disp_    -----  5 - ----  VSP 3 12 A InSv  VSP 6  5 A InSv  DSP 1 12 A InSv
 12 Next     -----  6 - ----  VSP 4 13 A InSv  VSP 7  6 A InSv  DSP 2 13 A InSv
 13 Select_   CEM 0  7 I InSv  VSP 5 14 A InSv  -----  7 - ----  VSP 8 14 I InSv
 14 QueryPM
 15 ListAlm
 16 Clock
 17 SPERFORM
 18 Upgrade_
```

57.2.4 QUERYPM FLT Display

The telco can use this command:

MAPCI;MTC;PM;POST SPM ISTB;QUERYPM FLT REASON

to show what faults caused the SPM node(s) to become ISTb. If one of the SPM's carriers has gone SysB, then the output will look like this:

>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check SysB Carrier
CEM 0 ISTb NonCritical faults:
Check Carrier on OC3 RM

The "Check SysB Carrier" is a new reason that can cause a OC3 RM to go ISTb, which results in the CEM going ISTb, and hence the node ISTb. The "Check Carrier on OC3 RM" is a new ISTb reason for CEMs that will only occur when one (or both) of our two triggers have occurred.

For the STM1 product, CEM ISTb reason will appear as "Check Carrier on STM RM".

If the 2nd trigger occurs (i.e. remote alarm on a line carrier), then the output will look like this:

```
>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check RFI Alarm on STS3L Carrier
CEM  0 ISTb NonCritical faults:
Check Carrier on OC3 RM
```

The “Check RFI Alarm on STS3L Carrier” is the other new reason that can cause a OC3 RM to go ISTb.

For the STM1 product, the STM ISTb reason will appear as “Check RFI Alarm on STM1M Carrier” and the CEM ISTb reason will appear as “Check Carrier on STM RM”.

Note that our two new “triggers” are the only RM ISTb reasons that can also cause the Node to go ISTb.

57.2.5 LISTALM Display

The LISTALM command for the ISTb SPM will produce this output when one of the triggers has occurred. Note that it just reflects the Minor alarm reason that caused the node to go ISTb.

```
ListAlm: SPM 26  CEM 0
SEVERITY    ALARM       ACTION
-----------------------------
Critical    None
Major       None
Minor       ISTB        RPT
No_Alarm    None
```

57.2.6 Logs

When one of the new triggers occur, the existing CARRxxx log will occur as shown above. In addition, the existing SPM300 log will occur to show the OC3 RM has gone ISTb for one of the new ISTB text reasons. The severity of these SPM300 logs will be non-critical for each new reason.

Note: the maximum length for an ISTb reason string is 64 characters, so we can make the reasons longer if that would help.

57.2.6.1 Check SysB Carrier

This log will occur if one of the SPM's carriers goes SysB:

```
STEC207AM   *  SPM300 MAY30 15:57:33 4093 TBL  Device Fault Report
      Location   : SPM : 26   OC3 : 0
      Status     : Alarm Raised
      Problem Description: Non Critical
       7A: Check SysB Carrier
      Action     : Refer to NTPs for Alarm Clearing Procedures.
      Cardlist   :
       No Cardlist Available.
```

57.2.6.2 Check RFI Alarm on STS3L Carrier

This log will occur if one of the SPM's STS3L line carriers recieves a RFI external alarm (e.g. due to TX fiber cut). Note that STS3L will be substituted with STM1M on STM1 nodes.

```
STEC207AM   *  SPM300 MAY30 15:57:33 4093 TBL  Device Fault Report
      Location   : SPM : 26   OC3 : 0
      Status     : Alarm Raised
      Problem Description: Non Critical
       7A: Check RFI Alarm on STS3L Carrier
      Action     : Refer to NTPs for Alarm Clearing Procedures.
      Cardlist   :
```

For the STM1 product, the 7A string above will instead appear as "Check RFI Alarm on STM1M Carrier".

57.2.6.3 OC3 ISTb Log

If the OC3 RM was previously InSv when the trigger occurred, then the following SPM500 "Device State Change" log will occur when the OC3 transitions to ISTb. There are no changes to this log. Here's an example:

```
STEC207AM   *  SPM500 MAY30 15:57:33 4194 INFO Device State Change
          Location: SPM : 26   OC3 : 0
          From    : InSv
          To      : ISTb
```

57.2.6.4 Node ISTb Log

If the SPM node was previously InSv when the trigger occurred, then the existing NODE500 “Node State Change” log will occur when the SPM node transitions to ISTb. There are no changes to this log. Here’s an example:

```
OLSC_SN06BT CM        * NODE500 JUN04 15:14:16 1000 INFO Node State Change
      Location: SPM 33 Unit 0
      From:     InSv ( Connected, Active )
       To:     ISTb ( Connected, Active )
```

57.2.7 Troubleshooting why SPM Node is ISTb

Determining which carrier caused the SPM Node to go ISTb depends on the type of reason given under QUERYPM FLT REASON:

57.2.7.1 Check SysB Carrier

Find which SPM is ISTb:

mapci;mtc;pm;post spm istb

then post the SysB carriers on the SPM:

trks;carrier;post spm {spm# from current post set} sysb

Then follow existing troubleshooting procedures for SysB SPM carriers.

57.2.7.2 Check RFI Alarm on STS3L Carrier

Find which SPM is ISTb:

mapci;mtc;trks;carrier;post spm istb

then post the line carriers on that SPM:

trks;carrier;post spm {spm# from current post set};next

The map will look something like this:

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 SysBTh    .     NODLOG    .      1 SPM     .       .     232CCS   3Crit    .
                                   *C*                      *C*     *C*
             CLASS    ML   OS ALRM  SYSB  MANB UNEQ OFFL  CBSY PBSY  INSV
  0 Quit     TRUNKS  176    0   95   201     0    0    0    88    0   746
```

```
 2 Post_      HSCARR  203     0    5     3     0    0    0    63    0   753
 3             STS3L
 4            N  CLASS  SITE SPM RM OC3S STS3L CKT STATE  TR MA
 5 Loop_      0  HSCARR HOST  12  0    0     0  89 INSV   .S ..
 6 Tst_       1  HSCARR HOST  12  1    0     0  90 INSV   .. ..
 7 Bsy_       2  HSCARR HOST  12  0    0     0  91 INSV   .. m.
 8 RTS_       3  HSCARR HOST  12  1    0     0  92 INSV   .S m.
 9 Offl_
10            SIZE OF POSTED SET  :  176                  MORE...
11 Disp_
12 Next
13
14 Detail_
15 ListAlm_
16
17 Perfmon_
18
```

The faulty line carrier will be the one with an alarm (e.g. “m”) under the “MA” column. Use LISTALM or PERFMON;PPQUERY to confirm the alarm. Then follow existing troubleshooting procedures for clearing alarms on a STS3L carrier. One thing to check for is a cut TX fiber on the OC3.

For the STM1 product, everythings the same except STM1M will appear instead of STS3L (and STM1R will appear instead of OC3S).

57.3 Hardware requirements

There are no new hardware dependencies introduced by this feature.

This feature will only work on TDM (legacy) SPM nodes (i.e. SPM and STM1). Anywhere that OC3 RM or STS3L carrier is referred to in this document for SPM, you can substitute STM RM or STM1M carrier when referring to a STM1.

Succession ATM/IP-based nodes (MG4K, IW, LSA, STS1) will **not** support this feature in the initial release.

57.4 Software Requirements or Dependencies

There are no new software dependencies introduced by this feature.

The feature will be “off” by default, but can be turned “on” by the customer.

This feature will impact Local CEM and RM loads for the SPM and STM1 products in the SN07/20 release, and will impact the SN07/20 (i.e. SHR20) Core load.

57.5 Limitations and restrictions

1. As stated above, the feature is only supported on TDM (legacy) SPM nodes, which includes the STM1.

2. Note that existing feature A59036987 will also show “P” for a ManB line carrier, whereas this new feature ignores any ManB carrier.
3. This feature will be “off” by default. An option will be provided (in Table OFCENG) for the customer to turn the feature “on” for all SPMs in the office. There will be no way to control the feature for individual SPMs. It is strongly recommended that the customer leave the feature “on” so they can avoid any long duration outages due to SPM carrier problems.
4. For the feature to be “on”, the new SN07/20 Core and Local loads must be running. If an upgrade is in progress where the customer is running the new SN07/20 Local loads but still has the pre-SN07/20 Core loads, then the feature will not activate until the new SN07/20 Core load is also running (e.g. after a No Restart SWACT).
5. While this feature is backwards compatible, it wil not be forwards compatible when the feature is enabled. For example, telco can run the new SN07/20 Local load with an older Core load as described above in #4 (this is “backwards compatibility”), but telco cannot run the new SN07/20 Core load with an older Local load when the feature is turned “on” in the new Core load (via Table OFCENG). If forward compatibility is needed, the feature must be turned “off” in the new Core load.
6. When the feature is activated or deactivated via Table OFCENG, it will take up to 45 minutes for this change to propagate throughout the system. The user will be warned about this delay time when the change is made. The same amount of delay will be incurred when the telco first upgrades the Core to the new SN07/20 load via NoRestartSWACT.
7. The carrier alarm level in Table MNHSCARR will not have an impact on whether a specific carrier can cause the node to go ISTb. So even if the carrier is set to NRPT (Non-Reportable), if it drops SysB, then it will cause the node to go ISTb. Same with the remote alarm trigger.
8. It only takes a single SysB carrier on the SPM node (including one DS1P or E1P path carrier) to cause the node to go ISTb. Any ManB or OFFL carrier will not cause the node to go ISTb.
9. If both “triggers” are present on the same OC3/STM at the same time, then only the last one reported will be shown when QUERYPM FLT REASON is done. If the last trigger is cleared, then QUERYPM FLT REASON will show the first trigger (until the first trigger is also cleared).

57.6 Interactions

This new feature works very similar to the 17/SN04 A59036987 feature that reports “S/P/D/d” under TRKS banner for a SysB carrier and “R” for a line carrier with a remote alarm. There are **no** interactions between them. Note that “S/P/D/d/R” will continue to be displayed under the TRKS banner.

With both features operating concurrently, the telco will have more info available on the MAP display to isolate the carrier issue *if* there is only *one* node ISTb. If the PM banner shows "1 SPM", then the telco will know this extra info by examing the right-most letter under the TRKS banner display:

1. "**S**": telco will know that a SysB section carrier (OC3S, STM1R) has caused the SPM to go ISTb.
2. "**P**": telco will know that a SysB line carrier (STS3L, STM1M) has caused the SPM to go ISTb. If "P" appears and there is no ISTb SPM, then we know there is a ManB line carrier on one of the SPMs. This ManB line carrier will prevent OC3 sparing so the SPM has a E2 loss of redundancy.
3. "**D**": telco will know that a higher-level path carrier (STS1P, DS3P, VC4P) going SysB has caused the SPM to go ISTb.
4. "**d**": telco will know that a lower-level path carrier (DS1P, VT15, VC12P, E1P, E1L) going SysB has caused the SPM to go ISTb.
5. "**R**": telco will know that a InSv line carrier (STS3L, STM1M) with remote RFI alarm has caused the SPM to go ISTb.

The TRKS letters above ("S/P/D/d/R") are shown in their priority order of precedence. This means that if a "S" and "D" fault exist concurrently, then the "S" preceeds the "D" so only "S" is shown.

If *more than one* SPM is ISTb, then the telco will still know the highest level carrier severity, but won't know which SPM it is on. For example, a "2 SPM" under PM banner and a "S" under TRKS banner means one SPM has a "S" fault and the other SPM has "S" or lower fault.

57.7 Applicable customer facing sections

Fault Management	
Logs	___X__
Alarms	__N/A_
Configuration	
Data Schema	__N/A_
User Interface	___X__
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	__X_
Accounting (includes AMA billing)	__N/A_

Performance (includes operational measurements) __N/A_

57.8 Glossary

Term	Description
New term	definition

57.9 References

A59036987 FN in PLS FMDOC - 17/SN04 release.

58: Functional Description (FN): A00002900

58.1 Feature Name

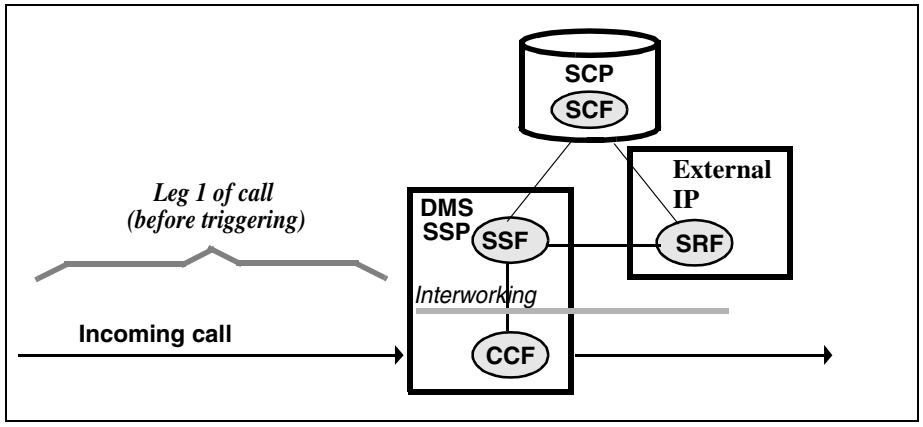
China INAP Compliance Enhancement Part 2

58.2 Description

58.2.1 Functional Overview

This feature will enhance the external IP capabilities and support multiple ApplyChargings on ISN07 TDM and CS2Kc platform for China market. The external IP supported in this feature has direct connection through China ISUP to SCP (as figure 1), SSP would not provide assisting SSP functionality.

Figure 2 Network diagram



This feature is based on feature A89008388: China IN SSP capabilities and feature AG5145: External IP, please see reference 7,10 for more information.

Two main functionalities are implemented in this feature:

- External IP enhancement

  For China INAP, several enhancements are made to fully support external IP:

  - Enhance operation EstablishTemporaryConnection
  - Enhance operation InitialDP

    Parameter iPAvailable and iPSSPCapabilities are required in IDP operation. SSP is able to set these two parameters by datafill.
  - Charging the temporary connection to external IP using ApplyCharging operation

    According to China requirement, charging to the temporary connection to external IP is required. Charging per duration and time are both supported in this feature.
  - Unsuccessful connection to external IP handling enhancement

    Several scenarios of unsuccessful connection to external IP are enhanced to comply with China requirement.
  - CISUP: Map the post answer ANM(CON) to CPG
- Multiple ApplyChargings support
  - Support up to 3 ACs

    Now up to 3 ACs can be accepted and handled simultaneously during an INAP call. For multiple ACs, corresponding ACRs can be sent to SCP if required.

Function ‘CISUP: Map the post answer ANM(CON) to CPG’ is for China ISUP originator only. The other functions are agent independent, i.e. they are supported on the originating agents with the condition: the originating agent <-> INAP interworking is ALREADY supported. For example, China ISUP, IBN lines, SIP-T (no ISUP), China PRI.

These functions are detailed in Section 2.2.2 to 2.2.3.

58.2.1.1 Functional Requirements

The functions to enhance China IN SSP capabilities are based on the following specification:

— China INAP specification (See reference 1)

— China INAP test specification (See reference 2)

— Supplementary Specification of China IN CS-1 INAP (See reference 3)

— Test specification of Supplementary Specification of China IN CS-1 INAP (See reference 4)

58.2.1.2 Data Requirement

The datafill is the same as that for normal IN call.

58.2.2 External IP enhancement

58.2.2.1 EstablishTemporaryConnection enhancement

The ETC is defined as below in China INAP specification:

```
EstablishTemporaryConnection OPERATION
  ARGUMENT
    SEQUENCE {
      assistingSSPIPRoutingaddress [0] IMPLICT OCTET STRING;
      correlationID[1] IMPLICT OCTET STRING OPTIONAL;
      legID [2] CHOICE{
        sendingSideID[0] IMPLICIT OCTET STRING( SIZE(1) )} OP-
        TIONAL;
      scfID [3] IMPLICT OCTET STRING(SIZE (3)OPTIONAL;
      .....}
```

Parameters scfID and legID are supported in this feature. legID indicates which leg of a call is connected to the SRF for user interaction. Currently, external IP can only be connected to calling party. This feature will only support the decode of parameter legID.

Parameter correlationID has fixed length 3 bytes.

Parameter assistingSSPIPRoutingAddress is checked according to China INAP requirement:

— the format is Generic number

— If scfID and correlationID are not contained in assistingSSPIPRoutingaddress, the NOA of assistingSSPIPRoutingaddress should be national number(0000011) or Subscriber number(0000001). For national number, it consists of the prefix 0, Area code and office code, the length of the number is 4~8. For Subscriber number, it consists of office code, the length of the number is 4~5.

For the outgoing IAM to external IP, the format of CDPN within IAM is different considering that the number of CDPN is even or odd. Examples are shown in table 1 and 2:

Table 1 CDPN with 8 digits assistingSSPIPRoutingAddress

	8	7	6	5	4	3	2	1
1	Even	Nature of Address						
2	INN indica-tor	Numbering Plan Indicator			Spare			
3	2nd Assisting Address Signal				1st Assisting Address Signal			
4	4th Assisting Address Signal				3rd Assisting Address Signal			
5	6th Assisting Address Signal				5th Assisting Address Signal			
6	8th Assisting Address Signal				7th Assisting Address Signal			
7	2nd SCF ID				1st SCF ID			
8	4th SCF ID				3rd SCF ID			
9	6th SCF ID				5th SCF ID			
10	2nd Correlation ID				1st Correlation ID			
11	4th Correlation ID				3rd Correlation ID			
12	6th Correlation ID				5th Correlation ID			

Table 2 CDPN with 7 digits assistingSSPIPRoutingAddress

	8	7	6	5	4	3	2	1
1	Odd	Nature of Address						
2	INN indica-tor	Numbering Plan Indicator			Spare			
3	2nd Assisting Address Signal				1st Assisting Address Signal			
4	4th Assisting Address Signal				3rd Assisting Address Signal			
5	6th Assisting Address Signal				5th Assisting Address Signal			
6	1st SCF ID				7th Assisting Address Signal			
7	3rd SCF ID				2st SCF ID			
8	5th SCF ID				4th SCF ID			
9	1st Correlation ID				6th SCF ID			
10	3rd Correlation ID				2nd Correlation ID			
11	5th Correlation ID				4th Correlation ID			

12	Filler (0)	6th Correlation ID

58.2.2.2 InitialDP enhancement

According to China INAP, IPAvailable and IPSSPCapabilities should be supported in IDP operation, SSP should fill these two parameters according to its abilities.

In order to build iPAvailable and iPSSPCapabilities into IDP, option INITDP_PARM of table SERVINFO is extended to add two new fields **IP_AVA** and **IPSSP_CAP** to indicate whether parameters IPAvailable and IPSSPCapabilities will be carried in IDP. These two fields should be datafilled at the same time. These two fields can also be datafilled for those variant other than China.

Meanwhile, option SRF_INFO is extended to add new filed **IP_INFO** to provide detailed information of the IP capability within SSP.

For China market, if IP_AVA and IPSSP_CAP are datafilled and IP_INFO is not datafilled, parameters iPAvailable and iPSSPCapabilities are set to default value according to China INAP, the default value of iPAvailable is ‘01’H (which indicates that the IP is available), the default value of iPSSPCapabilities is ‘#0C00’ (which indicates that DTMF digit collection and tone & announcement is supported). If IP_INFO is datafilled, then iPAvailable and iPSSPCapabilities are set according to this datafill. That means IP_INFO will take effect only if IP_AVA and IPSSP_CAP are datafilled, otherwise, the information of this datafill will not be carried in IDP.

IP_INFO contains two subfields: IP_AVAILABLE and IPSSP_CAPABILITIES, which contains values for parameter IPAvailable and IPSSPCapabilities respectively.

According to China INAP, there are 14 kinds of IP capabilities which are indicated by parameter iPSSPCapabilities. These capabilities can be datafilled in IPSSP_CAPABILITIES as shown in table 3:

Table 3 IP Capabilities defined in China INAP

IPSSPCapabilities parameter	Value	Meaning	IPSSP_CAPABILITIES selections
1st byte, bit 0	0/1	Not support/Support IPRoutingAddress	IPRA
1st byte, bit 1	0/1	Not support/Support VoiceBack	VOICE_BACK
1st byte, bit 2	0/1	Not support/Support VoiceInformation, recognize through voice, speech.	VOICE_INFO_SPEECH
1st byte, bit 3	0/1	Not support/Support VoiceInformation, recognize through voice, voice.	VOICE_INFO_VOICE

1st byte, bit 4	0/1	Not support /SupportText to Voice conversion.	TEXT_TO_VOICE
1st byte, bit 5	0/1	Not support/Support fax.	FAX
1st byte, bit 6	0/1	Not support/Support recorder.	RECORDER
1st byte, bit 7	0/1	Not support/Support script.	SCRIPT
2nd byte, bit 0	0/1	Not support/Support manual operator.	MAN_OPERATOR
2nd byte, bit 1	0/1	Not support/Support conference.	CONFERENCE
2nd byte, bit 2	0/1	Not support/Support tone & announcement.	TONE_ANNC
2nd byte, bit 3	0/1	Not support/Support DTMF digit collection.	DTMF_DIGCOL
2nd byte, bit 4	0/1	Not support/Support sending DTMF signal.	SEND_DTMF_SIG
2nd byte, bit 5	0/1	Not support/Support sending FSK signal.	SEND_FSK_SIG
2nd byte, bit 6,7	To be defined.		
3rd, 4th bytes	To be defined.		

Below is an example of datafill:

Table 4 SERVINFO datafill example

Example of datafill:
TABLE SERVINFO
200 (INITDP_PARMS (SERVKEY) (CDPA) (**IP_AVA**) (**IPSSP_CAP**) $)
(SRF_INFO (EARLY_ANS ANS_ON_ANNS)
(**IP_INFO Y** (**IPRA**) (**VOICE_INFO_SPEECH**)
(**TONE_ANNC**)(**DTMF_DIGCOL**)$)$)$

58.2.2.3 Charging the temporary connection to external IP using ApplyCharging operation

Currently, DMS SSP does not charge the temporary connection to external IP. According to China INAP:

If the charging is based on duration:

— SCP should send AC before ETC, and the startChargePattern is ‘AnswerReceived’

— When SSP receives AC and ETC, SSP begin to prepare for charging. SSP start charging after receiving answer message from external IP.

When originator abandon, SSP releases the connection to external IP or SSP receives release message, the charging is stopped, and ACR is sent to SCP.

— The other requirement of processing AC parameters are not changed.

If the charging is based on time:

— SCP can send AC before ETC or during the speech phase. If AC is sent before ETC, then the startChargePattern can be ‘Immediately’ or ‘AnswerReceived’. Otherwise, if AC is received during the speech phase, the startChargePattern should be ‘Immediately’.

— The fee is carried in surCharge parameter of AC, meanwhile AC does not carry chargeClass parameter.

— SSP can send ACR immediately or after the connection to external IP is released.

58.2.2.4 Unsuccessful connection to external IP handling enhancement

If the ETC is received between PA and SRR, SSP should report unexpected component sequence error.

58.2.2.5 CISUP: Map the post answer ANM(CON) to CPG

There are two conditions under which the mapping will occur:

— Condition 1: SSP has received an answer message from external IP or called party and transmitted it to the originating office, when the SSP connect to the external IP or the called party (if the first connection is to external IP) again, SSP will receive another answer message.

— Condition 2: SSP has received CTR and PCUI, SSP sent ACM and ANM to the originating office, when the called party answer, SSP will receive another answer message.

This functionality will implement that: if the second or later answer message is CISUP ANM containing BCI or CISUP CON, then it will be mapped to CPG and transmitted to the originating office.

58.2.3 Multiple ApplyChargings support

58.2.3.1 Support up to 3 ACs

In this feature, up to 3 ACs can be accepted and handled simultaneously during an INAP call. The number 3 is the maximum number of in-effect ACs, it does not include the number of expired(that is, a final ACR has been sent) ACs.

The chargeRecordIdentifier parameter is used to identify the AC operation, different ACs should have unique chargeRecordIdentifier. If two ACs have an identical chargeRecordIdentifier, then the newly received one will be rejected with ReturnError (UnexpectedDataValue).

If an AC with chargeUserIndicator equaling 1(calling party) or 2(called party) had been received, then any subsequent ACs with the same chargeUserIndicator will be rejected with ReturnError(TaskRefused(generic)). In orther words, on a call at most 1 AC is allowed for the calling/called party. However, this restriction does not apply to the specified charge number(chargeUserIndicator = 127).

If there are already 3 ACs in effect on the call, then all subsequent ACs will be rejected with ReturnError(TaskRefused(generic)).

For multiple ACs, corresponding ACR(s) can be sent respectively for each AC. ACR will be sent to SCP in three conditions:

1. If the calling/called party hangs up, the following actions are taken:

- The call (or only the called party, depending on the on-hook party and armed EDPs) is taken down
- ACR for each AC is sent respectively

2. If the cost/time limit for one of the ApplyChargings is reached, the following actions are taken:

- The call (or only the called party, depending on armed EDPs) is taken down
- The forceReleaseCause in the ApplyCharging whose charge/time limit is reached is stored in the backward release message
- ACR for each AC is sent respectively. If the supervisionMethod in the AC for which we are sending ACR is costGranted, the reasonForReport parameter in the ACR is ChargeLimitReached; if the supervisionMethod is timeGranted, the reasonForReport is TimeLimitReached.

3. If the heartbeat timer for one of the ApplyChargings expires, the following action is taken:

- An ACR for the AC is sent

Multiple treatments can be played if more than one ACs require warning tone/ announcement to be played at a desired time before the charge/time limit is reached, provided the restrictions below:

— All tones/announcements are only played to the calling party

— If multiple treatments are required to play at almost the same time, DMS SSP will play the 1st started treatment and suppress other

treatments which try to start at the time when the 1st treatment is playing.

58.3 Hardware Requirements or Dependencies

N/A.

58.4 Software Requirements or Dependencies

N/A.

58.5 Limitations and restrictions

N/A.

58.6 Interactions

N/A.

58.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

58.8 Glossary

Term	Description
ACH / AC	Apply Charging
ACR	Apply Charging Report
ACM	Address Complete Message
ANM	Answer Message
CDPN	Called Party Number
CISUP	China ISDN User Part
CODEC	Coder/Decoder
CON	Connect
DMS	Digital Multiplex System
ETC	Establish Temporary Connection
IAM	Initial Address Message
IDP	initial DP
IN	Intelligent Network
INAP	Intelligent Network Application Part
IP	Intelligent Peripheral
ISUP	ISDN User Part
SCP	Service Control Point
SSP	Service Switching Point

58.9 References

1. GF017-1995 China INAP Specification
2. YDN107.2-1999, INAP test spec - SSP part
3. Supplementary Specification of China IN CS-1 INAP (draft)
4. Test specification of Supplementary Specification of China IN CS-1 INAP (draft)
5. Requirement of China Telecom Intelligent Network Intelligent IP Establishment. China Telecom, 2002, January
6. SSP (IP related) INAP Specificationn and Signalling coorperation test specification of China Telecom Intelligent Network. China Telecom, 2001, January

7. AG5145 IN SSP REL 3.0 HLD: External IP
8. AG5089 WT IN SSP REL 3.0
9. A59039729 - CS1R China ISUP Calling Card Service
10. A89008388 - China IN SSP capability

59: Functional Description (FN): A00002901

59.1 Feature name

Activity A00002901 - Enhanced Meet-Me Conference (EMMC)

59.2 Description

59.2.1 Background

Existing Meet-Me Conference allows users to have a conference call without the conference setup time required with most other conferencing features. A directory number and a time is given to all conferees before the conference takes place. The conferees dial the directory number at the chosen time and are entered into the conference. This enables the conferees to quickly get on with the conference.

The user begins a Meet-Me conference by dialing the designated Meet-Me number. The maximum number of participants for a given conference is established in datafill and is associated with the customer group by the SUPERCNF option in table CUSTHEAD. As of BCS-25 it is datafillable whether the first caller must be a member of the Meridian Digital Centrex (MDC) customer group family. In either case if the first caller is a trunk it must have disconnect supervision. Note that other participants in the conference do not necessarily have to be members of the MDC customer group or have disconnect supervision if they are on incoming trunks. Other participants may always access the conference locally or from remote locations over all types of incoming trunk facilities if the datafill in table MMCONF allows them. The first caller receives audible ringing tone until the arrival of the second caller. The conference begins with the arrival of the second caller to the Meet-Me number. Each new participant to arrive on the bridge is announced with an audible confirmation tone to all the current participants. For each customer group, the number of 6-port conference circuits required by Meet-Me Conference are allocated for a customer group in table CUSTENG, option CONF6C.

But in the existing Meet-Me Conference feature, there is no security protection function provided to the conference. If a conference is reserved and datafilled in table MMCONF, anyone who knows the conference bridge DN can dial this DN and start a conference. Also, when a conference is in progress, anyone can enter the conference if he/she knows the conference DN and the conference is not being locked by other conferees. This leak makes the conference unsafe. Because of the limitation of associating the maximum number of 6-port conference circuits to customer group, the number of conference that can be reserved in one customer group is restricted too.

To resolve above limitations and leaks, this feature provides an Enhanced Meet-Me Conference with security protection and other functionalities.

59.2.2 Feature Requirement

Enhanced Meet-Me Conference service on CS2Kc provides a conference bridge which conference participants can enter by dialing a specific DN.

Conference is divided into 2 types: scheduled or timeless. A scheduled conference is the conference that predetermines conference date/time, conference elapsed time so that only within the reserved period of time could the conference be started. Scheduled conference has two sub-type: periodicity and non-periodicity conference type. The user can specify a scheduled conference as a periodically effective reserved conference, what means this conference is reserved with start date/time and elapsed time and the reservation can become effective daily/weekly/monthly. If the scheduled conference is reserved as non-periodicity, the reservation will get effective only once. With timeless conference, the conference DN is reserved timeless. Conference can be started whenever it is needed.

Conference participants are classified into 2 categories: chair-person and invited participants. Chair-person is the conference organizer, only one chair-person exists in one conference. Invited participants are the others invited to join the conference. The number of invited participants can be up to (N-1) per conference where N is the maximum number of conferees allowed in one conference session, it can be from 3 to 30. The chair-person and the invited participants are not necessarily subscribers from CS2Kc. The chair-person and the invited participants can dial into the conference from a IBN line and a CISUP/CTUP/SIP-T trunk.

Conference is secured by assigning conference password for all participants and chair-person. The chair-person and invited participants will have different passwords. The different passwords are the only means to distinguish the roles of chair-person and invited participants while conferees set up their calls to conference. These two password can not be the same. They are datafilled by the operator, and they are visible to operator. Please refer to section 2.2.3 for detail description.

It is optional for the conference organizer whether to let the conference starts without a chair-person. If so, the conference is allowed to start only after the chair-person arrives the conference. Otherwise, the conference can start when any conferee arrives.

In the case that the conference must start after the chair-person arrives, all invited participants arrives the conference before the chair-person will be given an announcement to declare that the chair-person has not arrived and the conference has not started. After that, the invited participants will be given

music and placed on hold. When the chair-person arrives, the on-hold participants will be placed into the conference.

In the case that allows the participants enter no matter whether chair-person has arrived, the situation is simpler. When a conferee arrives (if this is a timeless conference or it is in the reserved time of a schedule conference), just place him/her into the conference.

All conferees can have the conference through the conference bridge. In the progress of conference, if a new conferee enters the conference, all online conferees will hear a short ringing tone for announcing the arrival. Another short ringing tone will provide to the existing conferees if a conferee has disconnected. After at least two conferees have arrived and been placed into, the conference can really start.

Another option is given based on the status of the chair-person. The conference organizer can choose whether the conference will go on after the chair-person has disconnected while the conference is being reserved. If this option is set to TRUE, the conference can continue after the chair-person has disconnected from the conference. If this option is set to FALSE, the conference will end while the chair-person drops off even though there are still other conferees online.

For scheduled conference, System should play alarm tone or announcement to participants when time is expired before N minutes. (N is provisionable, e.g N=5 minutes.)

Every call into the conference DN should be mutual control or calling-party control. If a conference participant drops off, the corresponding conference port is automatically released.

Once the Enhanced Meet-Me Conference service is provisioned, it is available to the conference participants at any time, until the service provision is removed. However, the service provision can NOT be removed while the conference is still on.

59.2.3 Conference Provision

Enhanced Meet-Me Conference can be provisioned in a new table EMMCDATA with these aspects:

- Conference bridge DN
- Conference reservation type -- timeless, scheduled or periodicity conference
- Conference Date, Start Time, Elapsed Time. (If the conference type is timeless, this provision information is disable)

- Max number of ports available for the conference
- Invited participant password
- Chair-person password
- Quick start option: whether to allow the conference start if the chair-person has not entered
- ID of the Greeting to conference participants: operator can datafill a default greeting for each conference. If the customer has specific requirement for the greeting, and if software and hardware resource are enough, the operator can datafill a specific greeting for the customer. But this functionality is not guaranteed.
- Audio gruop number for playing music.
- System should play alarm tone to participants when time is expired before N minutes. N can be provisionable. (If the conference type is timeless, this provision information is disable.)
- Allow_to_continue option: whether to allow the conference to continue after the chair-person drops off
- Billing option: whether to generate a specific billing record for the conference

The provision capability is provided by a table EMMCDATA. The operator can datafill this table for each reserved conference session. The datafill examples of scheduled conference and timeless conference are shown below:

Figure 1 Datafill Example of Table EMMCDATA

```
TABLE: EMMCDATA
LKEY RESERVE SIZE CHRPSWD PARTPSWD QUICK GREETING AUDIOGRP ENDALARM CONTINUE
BILLING
-------------------------------------------------------------------------
28 801 9998 TIMELESS 6 111111 222222 Y EMMC1 AUDIO12 6 N N
28 801 9996 SCHEDULE NONPERIOD 2003 12 11 08:00 120 6 111111 222222 N EMMC1
AUDIO12 5 N N
28 801 9995 SCHEDULE DAILY 2003 12 02 19:00 300 6 111111 222222 N EMMC1
AUDIO12 6 N N
28 801 9994 SCHEDULE WEEKLY 2003 08 14 20:30 240 6 111111 222222 N EMMC1
AUDIO12 5 N N
```

Note: The key filed LKEY is composed of SNPA, OFCCODE and STNCODE (which form the bridge DN). The filed RESERVE denotes the reservation type of the conference.

The first tuple shows an example of timeless conference with bridge DN 28 8019998. The user can start a conference at any time from this bridge DN. The timeless conference type is denoted in the filed RESERVE with “TIMELESS“.

The second tuple of in this example is a scheduled conference which provides a conference bridge DN 28 8019996. This conference can support up to six conferees to arrives. It starts at 8:00 am on Dec. 11, 2003 and carries through

for 120 minutes. The schedule information is denoted by the field RESERVE with “SCHEDLED NONPERIOD 2003 12 11 08:00 60“. During this period of time, anyone with correct password can enter the conference if the number of the online conferees has not exceeded conference size (in this example, it is 6). This conference session allows the conference to start before the chair-person arrives. It will play a greeting (denoted by EMMCOMPA) to all conferees when they arrives. It allows the conference continue after chair-person disconnects from conference and it will generate a separate billing record for this conference session. Field ENDALLARM denotes that five minutes before the expired time of this conference (10:00 am), an alarm tone will be given to remind the conferees.

The third tuple is also a scheduled conference and it is reserved for periodically used. It is denoted in filed RESERVE with “SCHEDLED DAILY 2003 12 02 10:00 300“. The users can use this conference bridge at 19:00 for 5 hours each day from Dec. 02, 2003 until this tuple is removed by the operator.

The size of this table is up to 8192.

When datafilling a tuple in table EMMCDATA, a corresponding tuple is datafilled in table DNINV to make this feature can be triggered via dialling the conference bridge DN. A new feature name EMMC is defined for this feature. Figure 2 shows an example of traver from a line 82220008 to bridge DN 8015555 (the second conference datafilled in Figure 1).

Figure 2 Traver Example of Triggering Enhanced Meet-Me Conference Feature

```
>traver 1 8010008 8019000 b
TABLE IBNLINES
HOST 00 0 00 08 0 DT STN IBN 8010008 CSGRPTA 0 2 28 (FNT) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
CSGRPTA 2 0 0 CSXLTA ( ACR Y)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSGRPTA NXLA CSXLTA FEATXLA 0 CSDIG
TABLE DIGCOL
CSDIG 8 POTS N
TABLE IBNXLA: XLANAME CSXLTA
TUPLE NOT FOUND
Default from table XLANAME:
CSXLTA
    (NET N N 0 N NDGT N Y GEN (LATTR CSXLTA 842_NPRT_2 NLCA_NILLA_2) $ $)$ F
TABLE DIGCOL
NDGT specified: digits collected individually
```

```
TABLE LINEATTR
CSXLTA IBN NONE NT 1 0 NILSFC 0 PX CSXLTA NIL 00 CSXLTA CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
842_NPRT_2 NSCR 842 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_2 NLCA NIL NILLATA $
TABLE PXHEAD
CSXLTA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8019000
TABLE PXCODE
CSXLTA 801 801 CONT ( MM 7 7) ( CLASS NATL) ( XLT OFC CSTERMTA) ( LNET NATL1) (
MZONE 1)$
TABLE OFCHEAD
CSTERMTA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8019000
TABLE OFCCODE
CSTERMTA 801 801 RTE ( MM 3 9) ( DEST 801) ( CLASS LCL) ( LNET NATL1) ( MZONE 1)$
TABLE: OFCRTE
KEY: CSTERMTA  801
 . T OFRT 801
 .  . TABLE OFRT
 .  .  801 T IBNRTE 801
 .  .  . TABLE IBNRTE
 .  .  .  801 DN 28 801 N 0 4
 .  .  .  . TABLE TOFCNAME
 .  .  .  . 28 801 $
 .  .  .  . TABLE DNINV
 .  .  .  . 28 801 9000 FEAT EMMC 28 801 9000
TABLE DNFEAT
TUPLE NOT FOUND
 .  .  .  . TABLE DNATTRS
 .  .  .  . TUPLE NOT FOUND
 .  .  .  . TABLE DNGRPS
 .  .  .  . TUPLE NOT FOUND
 .  .  . EXIT TABLE IBNRTE
 .  . EXIT TABLE OFRT
EXIT TABLE OFCRTE
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.
INAP Termination Attempt TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 FEATURE               288019000                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 BUSY

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

59.2.4 Conference Processing

The conference should be protected to prevent any accidental or malicious invader. This function is implemented by assigning conference password for all invited participants and specific chair-person password. During dialling phase, after dialling conference bridge DN, all conferees (invited participants and chair-person) are required to input passwords. Only the ones having inputted correct passwords are guaranteed to enter the conference. Conferees

are guided by prompt and announcements when they dialling password. Conferees need input password once in dialling process if a correct password is inputted. Their roles are identified by passwords.

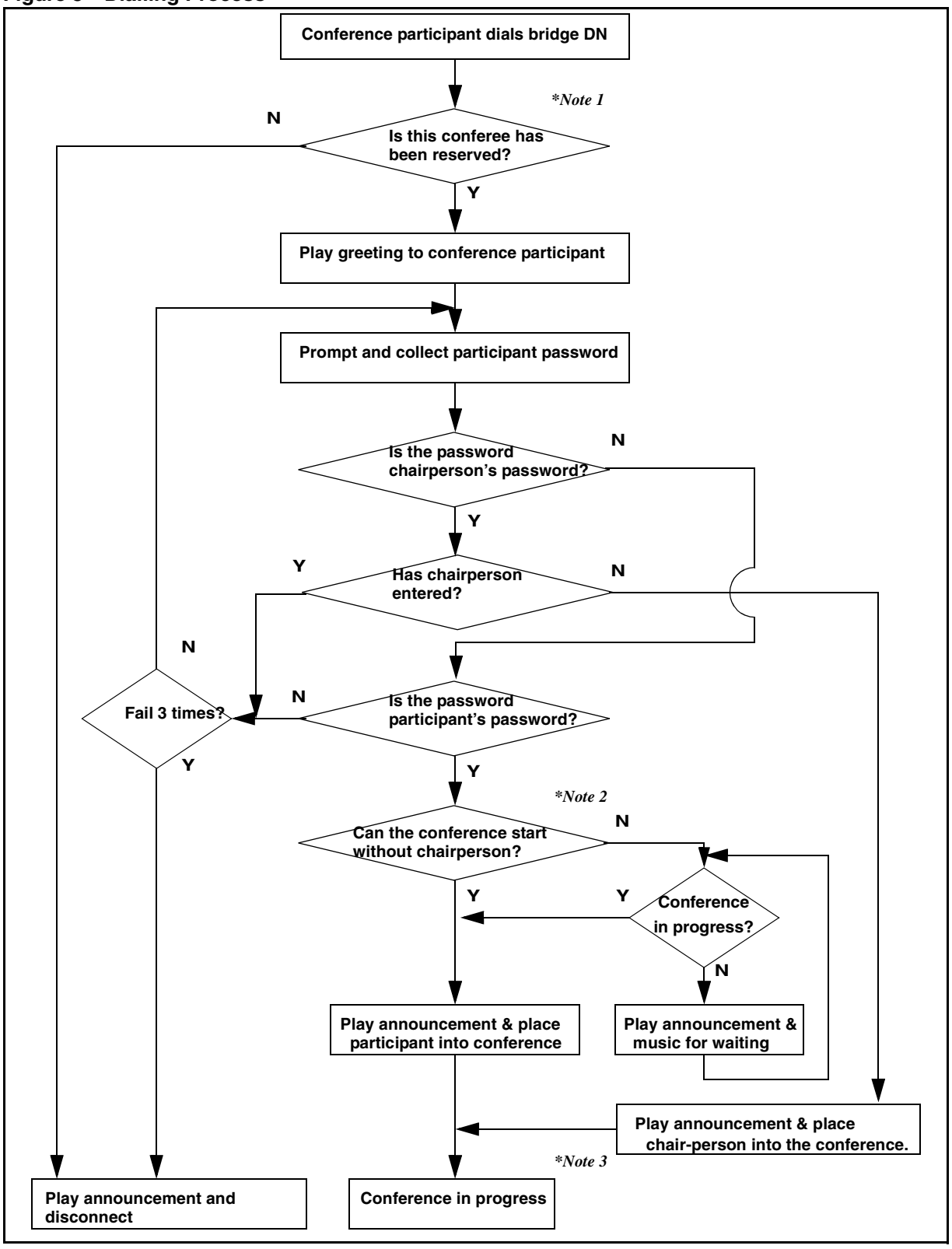
During the dialling process, some announcement are provided to guide the user how to execute following steps. The user can bypass the announcement by directly dialling any key. These announcements are:

- Greeting to welcome the user arrives the conference. This greeting can be datafilled on a per conference basis. So different conference may have different greeting.
- Prompt for collecting conferee's password.
- Prompt for reminding the user has inputted wrong password and to input again.
- Prompt for welcoming the chair-person enters the conference.
- Prompt for welcoming an invited participant enters the conference.
- Prompt for welcoming an invited participant but to place this participant on hold because the chair-person has not entered.
- Prompt for reminding the user has made some error and will be disconnected from the conference.

With the scheduled conference type, before N minutes to the end time (N is datafilled in field ENDALARM in table EMMCDATA), an announcement will play to all participants that the conference will end in N minutes.

The dialling conference DN and password process are shown in figure 1.

Figure 3 Dialling Process



Note: 1. If the conference type is scheduled and the dialling date/time is within the reserved conference start date/time and elapsed time, or the conference type is timeless, we think that the conference has been reserved.

Note: 2. Whether a conference can start without a chair-person is controlled by datafilling a quick start option for each conference session.

Note: 3. Under following two circumstance, we think that the conference is in progress: I. The chair-person has entered the conference. II. If the conference session has quick start option, an invited participant is the first conferee and is allowed to entered the conference.

After the conferee gets through the password verification and enters the conference, a conference port is allocated for this conferee. He/She will occupy one port of 6-port conference circuit mounted of CTM/MTM on TDM side or a member of UAS on IP side. The hardware resource will not be freed until the conferee drops off. If the conference reaches the maximum allowed size specified in table EMMCDATA, further call attempts will receive busy treatment. Until a conferee disconnects and thereby provides a vacant port on the conference, further user is allowed to enter. If the conference is under maximum size but it is unable to attach hardware resource, the user will receive NOSC treatment.

During conference processing, each new participant arriving on the bridge is announced with an audible confirmation tone to all the current participants. Similarly, A burst of dial tone is provided each time a conferee leaves the conference. When all conferees are dropped from the conference, all the conference circuits are freed. It is datafillable whether the conference will end after the chair-person disconnects.

For scheduled conference, an alarm tone will be played to all participants when elapsed time will be expired in N minutes. N is a number that When the predetermined elapsed time expires, the conference ends and all conferees (chair-person and invited participants) disconnect from the conference. For the timeless conference, the conference can keep on till all conferees drop off, no elapsed time limitation.

59.2.5 Conference Billing

When the billing option is datafilled, a billing record is generated for each session of the conference, and only one record is generated.

The billing record includes the following:

- Conference start date/time: the time that the first participant enters the conference if quick start option is set to TRUE, or when the chair-person is placed into the conference if quick start option is set to FALSE.

- Conference end time: the time all the participants have dropped off
- Conference port usage: the maximum number of ports used during the conference session. This is not the conference allowed size datafilled in the table, but the maximum actual used ports in conference progress.
- Conference bridge DN

According to different datafill of field QUICK in table EMMCDATA for different conference, conference start date/time have different definitions. If this field is set to TRUE, which means the conference can start without the chair-person entering, conference start date/time record the date and time when the first conferee enters the conference, no matter this conferee is a chair-person or an invited participant. If this field is set to FALSE, which means the conference can only start after the chair-person enters, conference start date/time record the date and time when the chair-person enters the conference.

Conference end time always records the time when the last conferee drops off from the conference.

A conference session denotes the period of time from conference start time to conference end time. In a scheduled conference, if all conferees drops off, it is considered that this conference session has completed. If the time hasn't expired, any user can still start the conference. But it will be thought as a new conference session. For each conference session, only one billing record is generated. And the billing record is only associated with this conference session.

Conference port usage records the maximum number of ports used during a conference session, i.e. the maximum number of online conferees at the same time during a conference session.

Conference bridge DN should also appear in the billing record.

One thing should be noticed, the control of generated billing record is per conference base, but not per conference session base. That means the field BILLING in table EMMCDATA can only control the generation of the billing record to the conference datafilled in the same tuple. If this conference has multi conference sessions, all sessions will (or will not) generate the billing records according to the filed BILLING.

An ama log will be generated as the billing record for each conference session. This ama log contains a structure code (the structure code can be selected from x0510, x0511, x0512, x0513 or x0514) and a module code (612) to record billing information. MC612 is appended to the structure code. The conference bridge DN is stored in the structure code, the other information are stored in the module code. One ama log is to be generated for one conference session.

Figure 4 is an example of a billing record, the module code 612 is appended to the structure code 40514.

Figure 4 An Example of Billing Record of a Conference Session

```
>calldump full
*
 HEX ID:                              AA
 STRUCTURE CODE:                      40514C
 CALL CODE:                           006C       STATION PAID
 SENSOR TYPE:                         036C       DMS 100F
 SENSOR ID:                           0250250C
 REC OFFICE TYPE:                     036C       DMS 100F
 REC OFFICE ID:                       0250250C
 DATE:                                30827C     AUGUST 27, 2003
 TIMING IND:
     TIMING GUARD FLAG                0          UNUSED
     SHORT CLD PARTY OFF-HOOK IND     0          UNUSED
     LONG DUR/SERV PTY CAPABILITY IND 0          UNUSED
     UNUSED                           0
     UNUSED                           0C
 STUDY IND:
     STUDY TYPE A                     0          UNUSED
     STUDY TYPE B                     2          NETWORK COMPLETION
     STUDY TYPE C                     0          UNUSED
     TEST CALL IND                    0          UNUSED
     UNUSED                           0
     ORIG/TERM NANP NUM IND           0          UNUSED
     OPERATOR SERV IND                0C         UNUSED
 CLD PTY OFF-HK:                      0C         CLD OFF-HOOK DETECTED
 SERVICE OBSERVED:                    0C         NONE
 OPER ACTION:                         0C         ANI, CUSTOMER DIALED CALL
 SERVICE FEATURE:                     000C       OTHER
 SIG DIGITS NEXT FIELD:               010C
 ORIG OPEN DIGITS 1:                  FFFFFFFFFF
 ORIG OPEN DIGITS 2:                  FFFFFFFFFF
 ORIGINATING CHARGE INFO:             FFFF
 DOMESTIC/INTL INDICATOR:             1C         DOMESTIC
 SIG DIGITS NEXT FIELD:               007C
 EXT TERM OPEN DIGITS 1:              000000008015555C
 EXT TERM OPEN DIGITS 2:              FFFFFFFFFFFFFFFF
 CONNECT TIME:                        1707089C   17:07:08.9
 ELAPSED TIME:                        000000026C 000000:02.6
 COMPLETION INDICATOR:                001C       COMPLETED: ANSWERED
 MODULE CODE:                         612C       EMMC
GENERIC DIGITS STRING 1:             308271706128000C
 GENERIC DIGITS STRING 2:            308271707086003C
MODULE CODE:                         000C       FINAL MODULE
```

The conference bridge DN is stored in the filed ‘EXT TERM OPEN DIGITS 1’ as 000000008015555c. In the module code 612 appended to the structure code, filed ‘GENERIC DIGITS STRING 1’ records the conference start date/time: 17:06:12.8 on Aug., 27, 2003. Field ‘GENERIC DIGITS STRING 2’

records the conference end date/time: 17:07:08.6 on Aug., 27, 2003 and the maximum ports used during this conference session: 3 ports.

59.3 Hardware Requirements or Dependencies

This feature uses conference circuits provide by six-party conference card on TDM side or UAS on IP side to implement conference bridge.

59.4 Software Requirements or Dependencies

N/A

59.5 Limitations and restrictions

- All changes to the conference bridge DN and other information should be done through table EMMCDATA. Any other method of changing the DN is not supported.
- The hardware resource in the switch is not guaranteed enough to support all reserved conference at the same time. If a large conference is supported by a UAS on CS2Kc, it is not possible to guarantee with absolute certainty that sufficient UAS ports will always be available to allow additional persons to join the conference. If an additional person tries to join a large conference at a time when a UAS port is not available, the system provides treatment (a reorder tone) to the user and leaves the existing conference intact. Same thing will happen on TDM side.
- Touch tone commands should be provided to the chair-person and invited participants to implement specific control to the conference. To provide touch tone commands, DTMF tone must be able to be detected during talking phase in a call. But implementing DTMF tone detection needs a lot of development effort, so touch tome commands functionality will leave as a potential function of this feature in the future.
- When a subscriber is being included in an Enhanced Meet-Me Conference, all flash activation/deactivation feature is forbidden.
- Multiple Appearance Directory Number (MADN) is forbidden while a subscriber is being included in the conference.

59.6 Interactions

- If these features have been activated (Three Way Call, Attendant Console, Station Controlled conference, Preset Conference, Directed Call Pickup, Call Forward, Simring) on a subscriber, it is not allowed to terminate on Enhanced Meet-Me Conference bridge DN.
- If a conferee has the call forward busy (CFB) feature, calls to the conferee are forwarded during the conference.
- 3-way call and call waiting will be disable if a user is in conference progress.

- When a subscriber is being included in an Enhanced Meet-Me Conference, feature Calling Number Delivery Blocking (CNDB), Calling Number Blocking (CNB), Calling Name and Number Blocking (CNNB) is allowed.

59.7 Applicable customer facing sections

Fault Management

Logs	__N/A__
Alarms	__N/A__

Configuration

Data Schema	__X___
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__

Accounting (includes AMA billing)	__X___
Performance (includes operational measurements)	__N/A__

59.8 Glossary

Term	Description
DN	Directory Number
EMMC	Enhanced Meet-Me Conference
UAS	Universal Access Server

59.9 Reference

a. AF1268FN - Executive Conference

b. AF6110FN - Meet-me Conference Enhancement

c. AMA Formatter User's Guide

d. A19013546FN - Announcement Provisioning

e. BR0781FN - Call Forwarding Remote Activation

59.10 Appendix

59.10.1 Datafill Example of UAS

To achieve proper audio node maintenance, the CM needs to know the number of conference and announcement terminals supported to allow this to be dynamically modified when needed.

```
TABLE SERVSINV
SRVSNAME SRVRNAME NUMTERMS OPTIONS
---------------------------------
AUD 1 GWC 96 2048 (3PORT 30) (6PORT 30) (ANNC 100) $

TABLE CLLI
CLLI ADNUM TRKGRSIZ ADMININF
---------------------------
UASCF6P 219 30 UAS_6_CONFERENCE
```

59.10.2 Example of Datafilling Conference Circuit on TDM Side

Enhanced Meet-Me Conference is based on six-way conferences. The example for datafilling conference circuit with a CTM card on TDM side is shown below:

```
TABLE CLLI
CLLI ADNUM TRKGRSIZ ADMININF
---------------------------
CF6P 110 20 6_CONF


TABLE PADDATA
PADKEY PAD1TO2 PAD2TO1
----------------------
CONF CONF 0 0


TABLE TMINV
TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS LKDATA EQPEC LOAD EXECS SCTMLOC
-----------------------------------------------------------------------
CTM 0 TME 0 32 1 BB 0 0 10 6 0 1X81AA MTMKA02 MTMEX SINGLE_CARD MTM 1 10


TABLE CONF6PR
CNFCKTNO EXTRKNM TMTYPE TMNO TMCKTNO CARDCODE PADGRP
-------------------------------------------------
0 0 CTM 0 24 1X81AA CONF
```

59.10.3 Datafill Example of Announcements

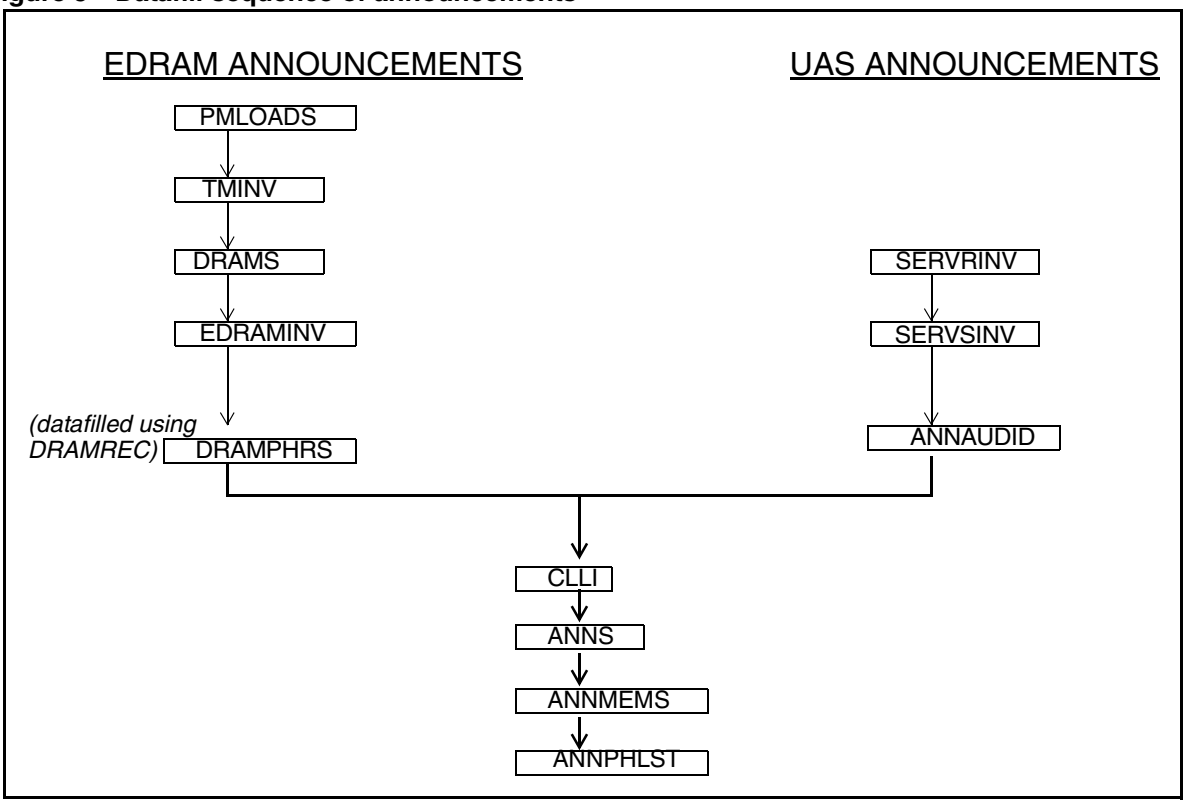
The datafill sequence for announcements are different on TDM side and IP side. Figure 5 shows the datafill sequence with EDRAM announcements (TDM side) and UAS announcements (IP side).

```
TABLE ANNAUDID                                  %% Only for UAS announcements
PHRASEKY AUDID
-------------
EMMCGREE1 1210
EMMCPSWD  1211
```

```
EMMCREINPUT 1213
EMMCCHAIR 1214
EMMCINVITED 1215
EMMCERROR 1216
EMMCHELD 1217

TABLE DRAMPHRS                                    %% Only for EDRAM announcements
DRAM PHRSNAME PHRASENO BLOCK LENGTH RECORDED
-------------------------------------------
0 EMMCEGREE 25 2 6 Y N 11
0 EMMCPSWD 26 2 5 Y N 17
0 EMMCREINPUT 27 2 5 Y N 22
0 EMMCCHAIR 28 2 3 Y N 27
0 EMMCINVITED 29 3 6 Y N 5
0 EMMCERROR 30 3 4 Y N 11
0 EMMCHELD 31 3 5 Y N 16


TABLE CLLI
CLLI ADNUM TRKGRSIZ ADMININF
----------------------------
EMMCDEFAULT 345 10 EMMC_DEFAULT_GREETING
EMMCANN 478 10 EMMC_ANNOUNCEMENT


TABLE ANNS
CLLI ANNARCH TRAFSNO CYTIME MAXCYC DATA
---------------------------------------
EMMCDEFAULT NETWK 0 10 2 STND Y 30
EMMCANN NETWK 0 3 1 EMMC 10


TABLE ANNMEMS
ANNMEM HDWTYPE CARD MEMINFO
---------------------------
EMMCDEFAULT 0 UAS AUD 0 AUD 0                   %% This is for UAS announcements
EMMCDEFAUTL 1 DRAM DRA (1 DTM 1 1)             %% This is for EDRAM announcements
EMMCANN 0 DRAM DRA (0 DTM 2 1)                 %% This is for EDRAM announcements
EMMCANN 1 UAS AUD 0 AUD 1                       %% This is for UAS announcements

TABLE ANNPHLST
ANNPHKEY PHSLIST
----------------
EMMCDEFAULT 1 (EMMCEGREE) $                      %% for EDRAM announcements
EMMCDEFAULT 0 (EMMCGREE1) $                      %% for UAS announcements
EMMCANN 1 (LANGUAGE 1) (EMMCPSWD) $
EMMCANN 2 (LANGUAGE 1) (EMMCREINPUT) $
EMMCANN 3 (LANGUAGE 1) (EMMCCHAIR) $
EMMCANN 4 (LANGUAGE 1) (EMMCINVITED) $
EMMCANN 5 (LANGUAGE 1) (EMMCERROR) $
EMMCANN 6 (LANGUAGE 1) (EMMCHELD) $
```

The datafill above that is not designated specific for EDRAM or UAS announcements are for both types.

Figure 5 Datafill sequence of announcements



59.10.4 Datafill Example of Music

The music playing for the held participant is defined with a new audio group, the datafill example is shown below:

```
TABLE AUDIO
AUDIOKEY ROUTES
---------------
AUDIO10 EMMC (MUSIC MUSIC1 0) $
```

60: Functional Description (FN): A00002960

60.1 Feature name

SN07:A00002960 - Originator Identification Screening

60.2 Description

This feature allows customers to block call terminations to certain ISUP EANT trunks when the Charge Number (CN) or Calling Party Number (CPN) identifiers is not available[1]. The intent of this new functionality is to allow only calls with one of the originating identifiers to complete over certain ISUP EANT trunks. All other calls will advance to the next trunk in the route list.

Please refer to the following sections for additional information:

- "SOC Control: UTRS0011" on page 611
- "Table TRKOPTS: ORIGIDSCR" on page 611.
- "Call Processing" on page 612

60.2.0.1 SOC Control: UTRS0011

The new SOC order code UTRS0011, UCS Orig ID Screen, is introduced by this feature. When UTRS0011 is IDLE calls will not be blocked on any ISUP EANT trunks when the CPN or CN is not available. The new ORIGIDSCR option in Table TRKOPTS can be datafilled when SOC is IDLE. When UTRS0011 is ON certain calls can be blocked. For more information see "Call Processing" on page 612.

The functionality introduced by this feature has been patched in older releases under password activated patch ATM51. During ONP processes UTRS0011 will have STATE set to 'ON' if the old side has patch ATM51 applied and activated. Otherwise, the SOC is set to IDLE.

60.2.0.2 Table TRKOPTS: ORIGIDSCR

A new trunk group option, ORIGIDSCR, is introduced in Table TRKOPTS for ISUP EANT trunks only. This allows the customer to specify which ISUP EANT trunks perform originator identification screening. For more information see "Call Processing" on page 612.

[1] For the purpose of this document the CN or CPN is considered available when at least the NPA is available. Refer to "60.2.0.3 Call Processing".

Figure 1 Table TRKOPTS Examples

TABLE: TRKOPTS

TRK1 ORIGIDSCR ORIGIDSCR

When an attempt to add ORIGIDSCR to a trunk other than EANT type or an MF EANT trunk the following error message is generated by table control:
TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can only be assigned to EANT ISUP trunks.

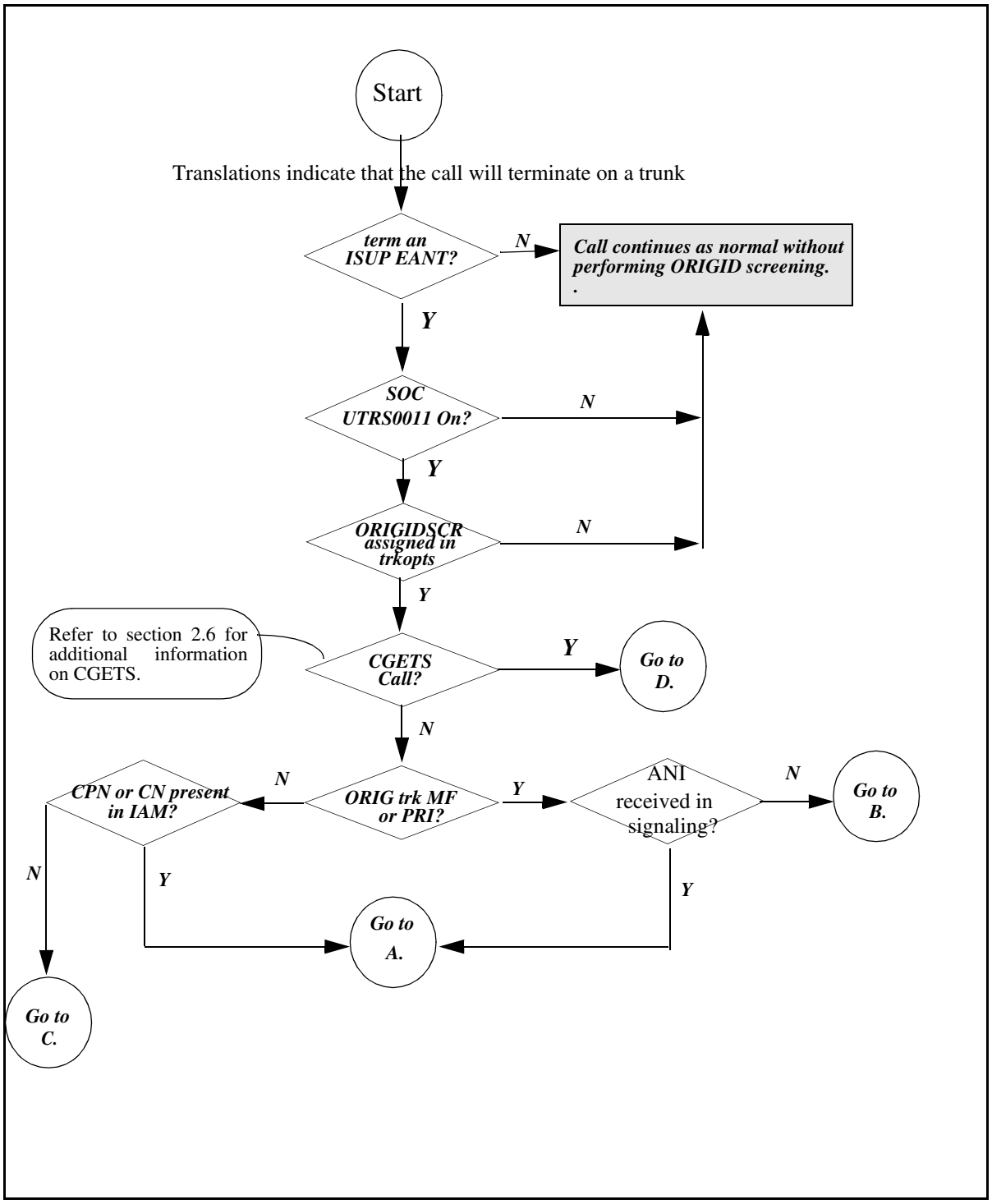
When an attempt to add ORIGIDSCR to an incoming trunk the following error message is generated by table control:
TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can not be assigned to Incoming trunks.

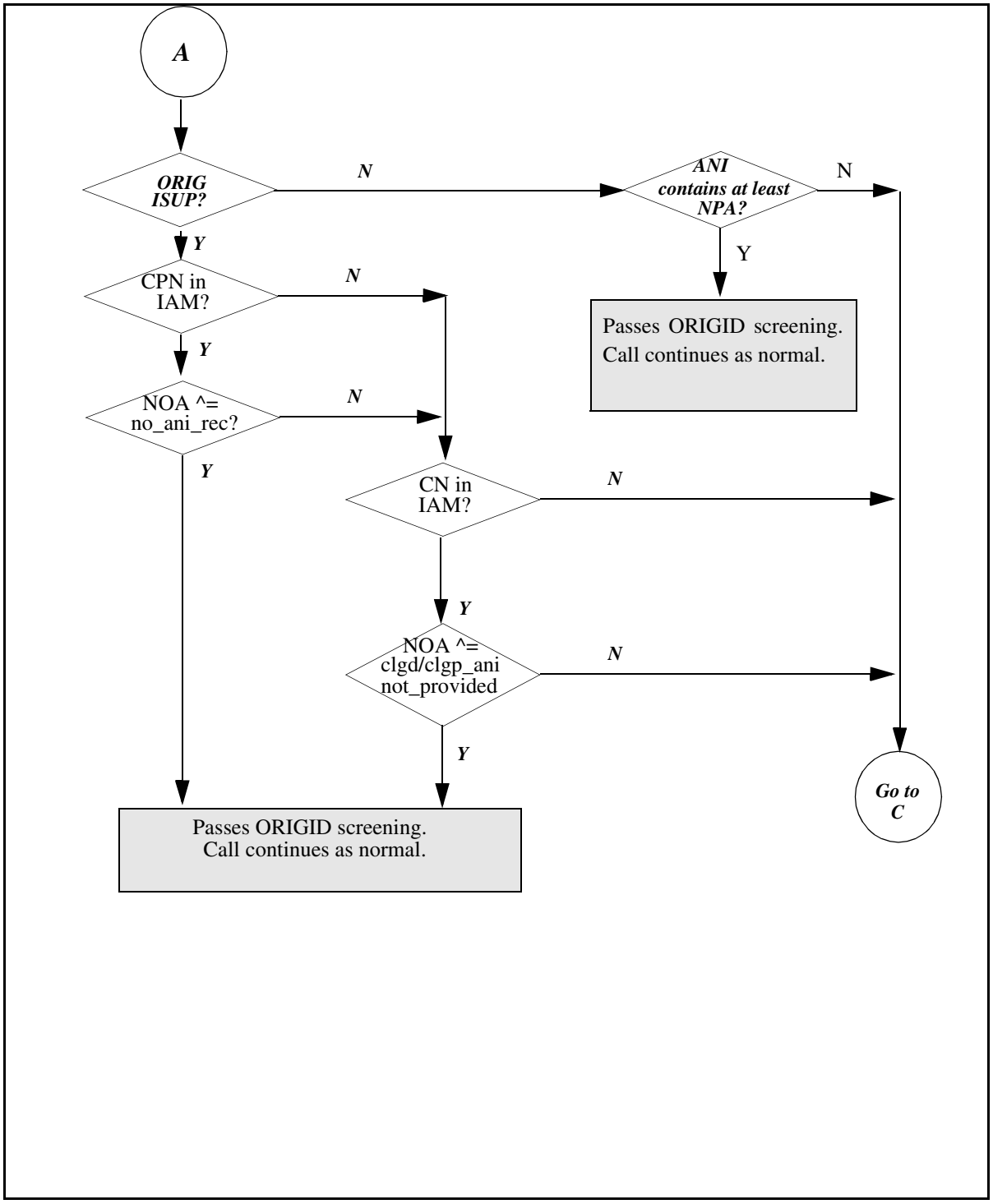
60.2.0.3 Call Processing

Call processing is enhanced to block call terminations on ISUP EANT trunks when ORIGIDSCR is assigned in Table TRKOPTS if the CN or CPN is not available from the incoming signaling or originator datafill. This feature is also controlled by SOC UTRS0011. Starting on page 613 is a detailed flow chart that describes the behavior of this feature.

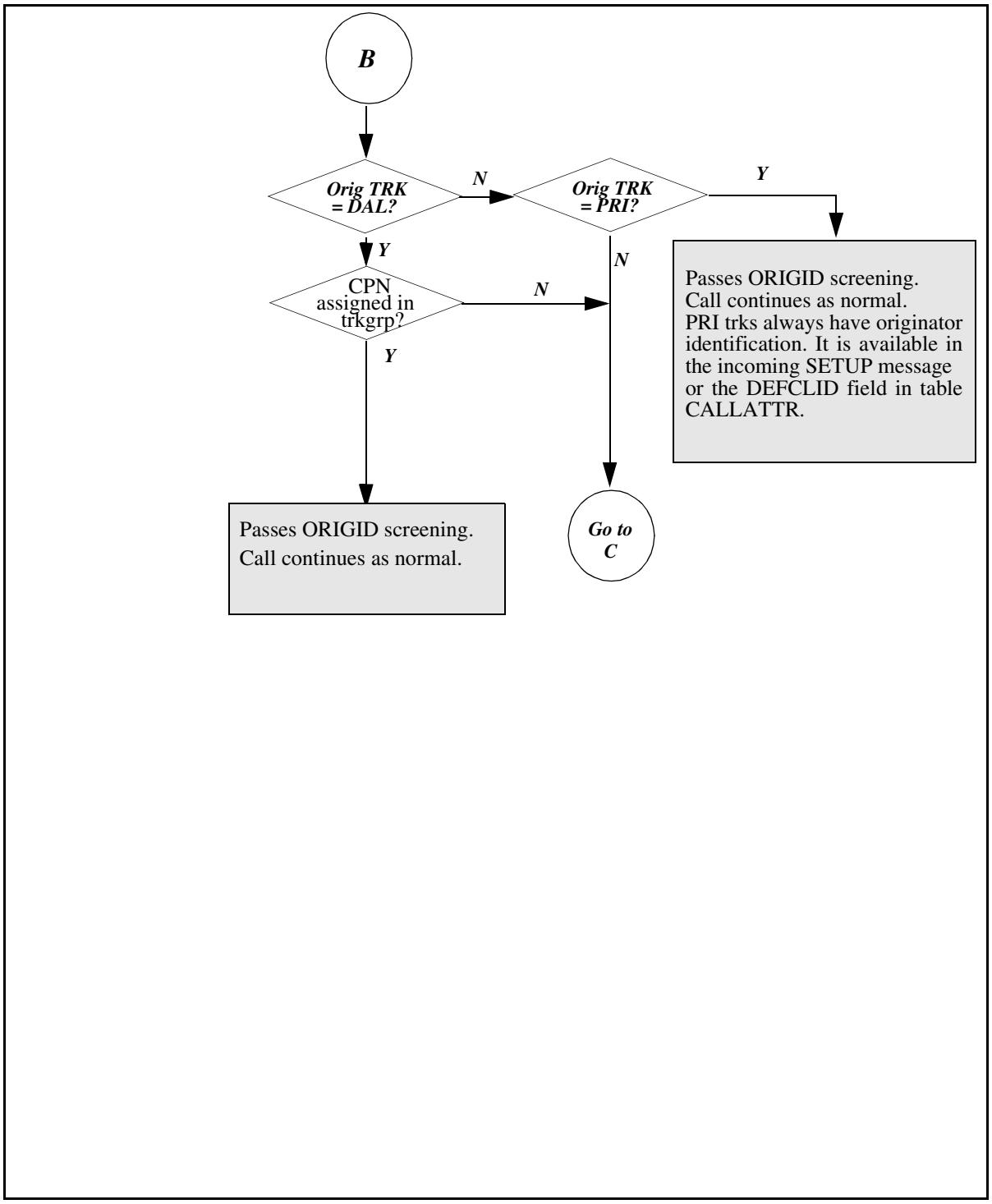
60.2.1 Originator Identification Screening Flow Chart



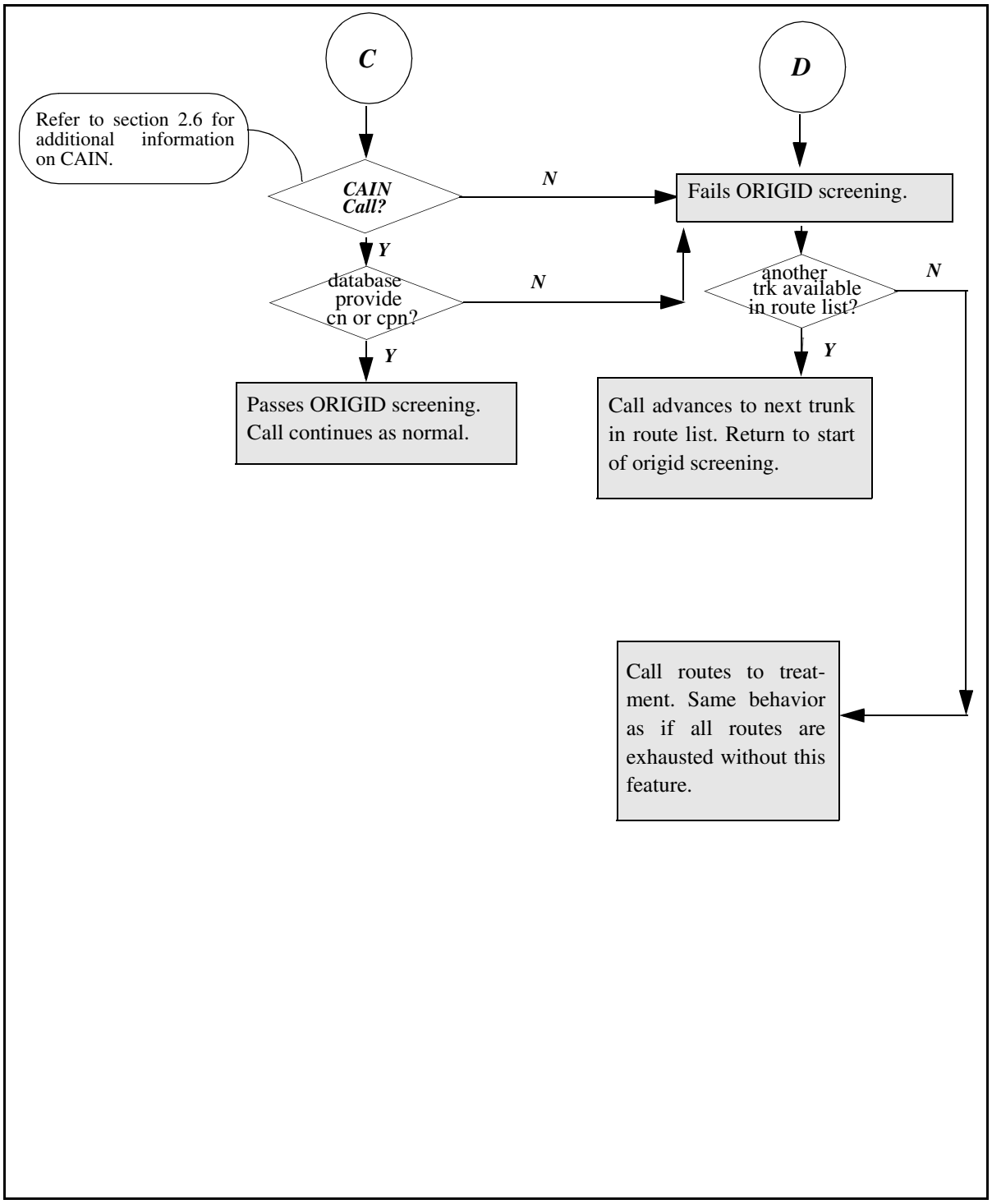
60.2.2 Originator Identification Screening Flow Chart - PART A



60.2.3 Originator Identification Screening Flow Chart - PART B



60.2.4 Originator Identification Screening Flow Chart - PART C & Part D



60.3 Hardware Requirements or Dependencies

None.

60.4 Software Requirements or Dependencies

None.

60.5 Limitations and restrictions

The new option ORIGIDSCR in Table TRKOPTS can only be assigned to 2w or outgoing ISUP EANT trunks. ORIGIDSCR can not be assigned to incoming ISUP EANT trunks.

This feature does not support interaction with Dynamically Controlled Routing (DCR.).

60.6 Interactions

Blocking of ANI delivery

This feature only considers if the CPN or CN is available from the incoming signaling or originator datafill. It does not consider if the originator or terminator has blocked delivery of this information in datafill. Therefore, the blocking of information has no impact on this feature. It is possible for originator screening to pass but the outgoing IAM to not contain CN or CPN because of one of the blocking features. Examples are:

Table RTEATTR	Datafill in Table RTEATTR can block sending out CPN, CN, and other parameters. It can also include CPN, CN, or other parameters.
IMT trunks: Table TRKGRP	Datafill in Table TRKGRP for IMT trunks can block sending out the CPN or CN with field CPIXFER.
EANT trunks: Table TRKGRP	Datafill in Table TRKGRP for EANT trunks can block sending out the CPN or CN with option TMANIDLV.
Tables ANIS-CUSP & UNIPROF	Datafill in both tables can block sending out the CPN or CN with field ANIDELV.

CAIN

CAIN calls can receive a CPN or CN from the SCP. If CPN and CN are not available from the incoming trunk then CAIN calls must check if the database supplied them.

Assume that SOC UTRS0011 is ON and the route determined by CAIN translations provides two possible trunks, TRK1 and TRK2. Only TRK1 has the new ORIGIDSCR option assigned in Table TRKOPTS which is discussed in "Table TRKOPTS: ORIGIDSCR" on page 611. Neither incoming signalling nor the originator datafill provided the CPN or CN but CPN or CN was supplied by the database so the call can terminate on TRK1. If the CAIN database had not supplied CN or CPN the call would route advance to TRK2.

CGETS

This feature does not support the termination of CGETS calls on trunks with ORIGIDSCR assigned. If a CGETS call attempts to route over a trunk that has this feature activated it will always route advance.

60.7 Applicable customer facing sections

Fault Management	
Logs	___N/A___
Alarms	___N/A___
Configuration	
Data Schema	___X___
User Interface	___N/A___
Element Management	___N/A__
Security	___N/A__
Service Order	___N/A___
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A__
Performance (includes operational measurements)	___N/A___

60.8 Glossary

ANI	Automatic Number Identification
CAIN	Carrier Advanced Intelligent Network
CGETS	Carrier Government Emergency Telecommunications System

CPN	Calling Party Number parameter of IAM
CN	Charge Number parameter of IAM
DAL	Dedicated Access Line
DCR	Dynamically Controlled Routing
EAEO	Equal Access End Office
EANT	Equal Access Network Trunk
IAM	Initial Address Message of the SS7 signalling
ISUP	Integrated Services digital network User Part
MF	Multi-Frequency
NOA	Nature Of Address
PRI	Primary Rate Interface
SOC	Software Optionality Control

61: Functional Description (FN): A00002970

61.1 Feature name

SMG4 Remote Site Provisioning

61.2 Description

SMG4s can be provisioned at multiple sites for a given CS2K. However, the SN06 and previous releases, have a limitation. SMG4s cannot be provisioned at multiple sites on the same floor, row, frame position and shelf position .

This feature aims at rectifying this limitation. As part of the feature enhancements, the following functionalities are introduced :

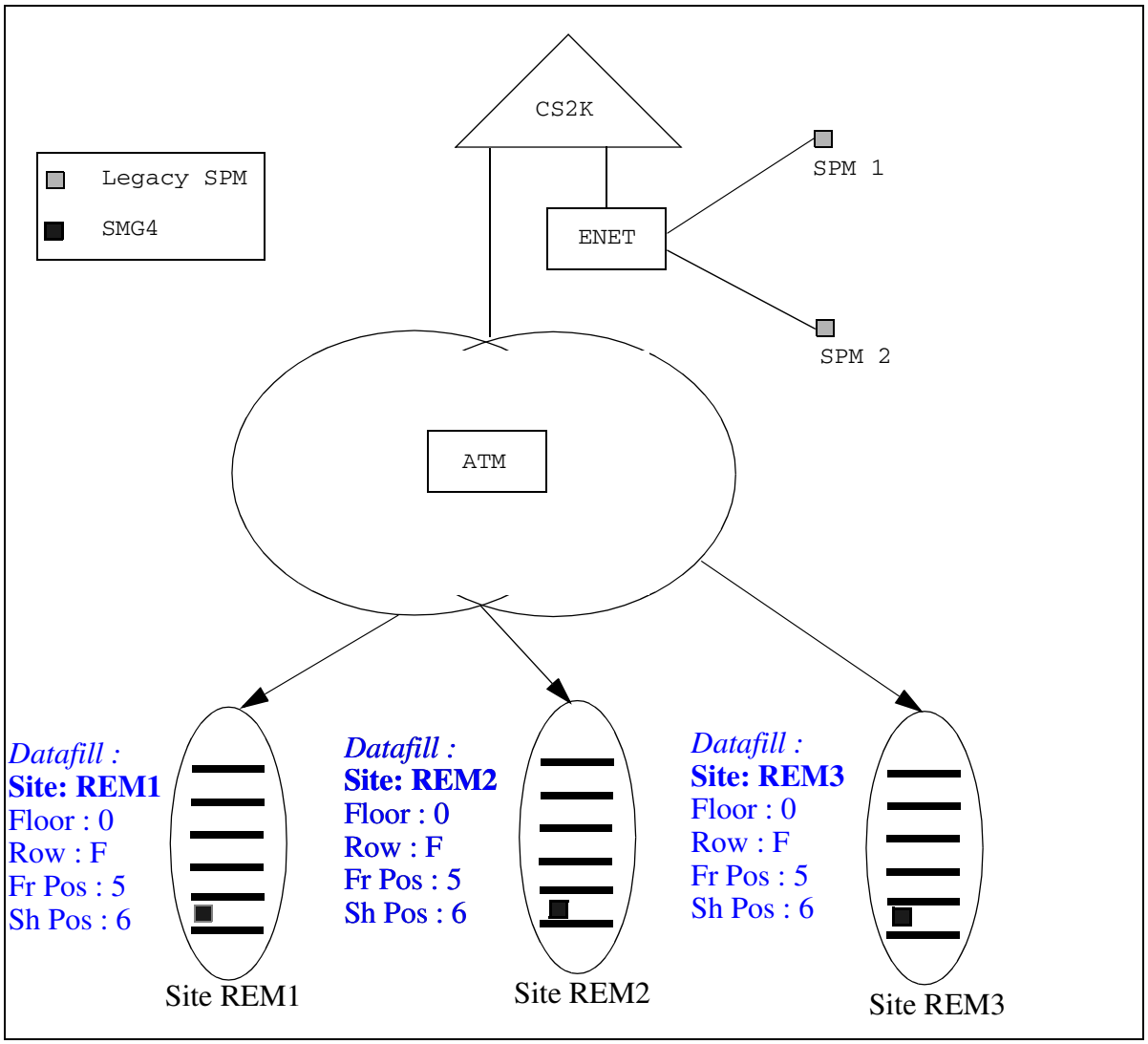
- Introduction of an inservice editable field, ‘SITE’ in Table MNNODE for SMG4s only.
- While datafilling the shelf position in the Table MNSHELF, the new field ‘SITE’(Table MNNODE) is also taken into consideration (for unique check of location) along with the fields, floor(Table MNNODE), row(Table MNSHELF), frame position(Table MNSHELF) and shelf position(Table MNSHELF).
- The ‘SITE’ field datafill in Table MNNODE is also reflected in the existing MAPs, Logs and Tools wherever the site name is displayed.

61.2.1 Functional Overview

This feature introduces an inservice editable field, ‘SITE’, in Table MNNODE. Hence, while datafilling the shelf position for an SMG4 in Table MNSHELF, a uniqueness check is performed taking the site also into consideration apart from the other fields. The other fields that determine the uniqueness of location are floor(TableMNNODE), row(Table MNSHELF), frame position(Table MNSHELF) and shelf position(Table MNSHELF).

Figure 1 shows how the fields - site, floor, row, frame position and shelf position determine the uniqueness of location of an SPM. Also, it is illustrated in the figure that as a result of this feature, SMG4s can now be provisioned at multiple sites on the same floor, row, frame position and shelf position.

Figure 1 The desired datafill behaviour

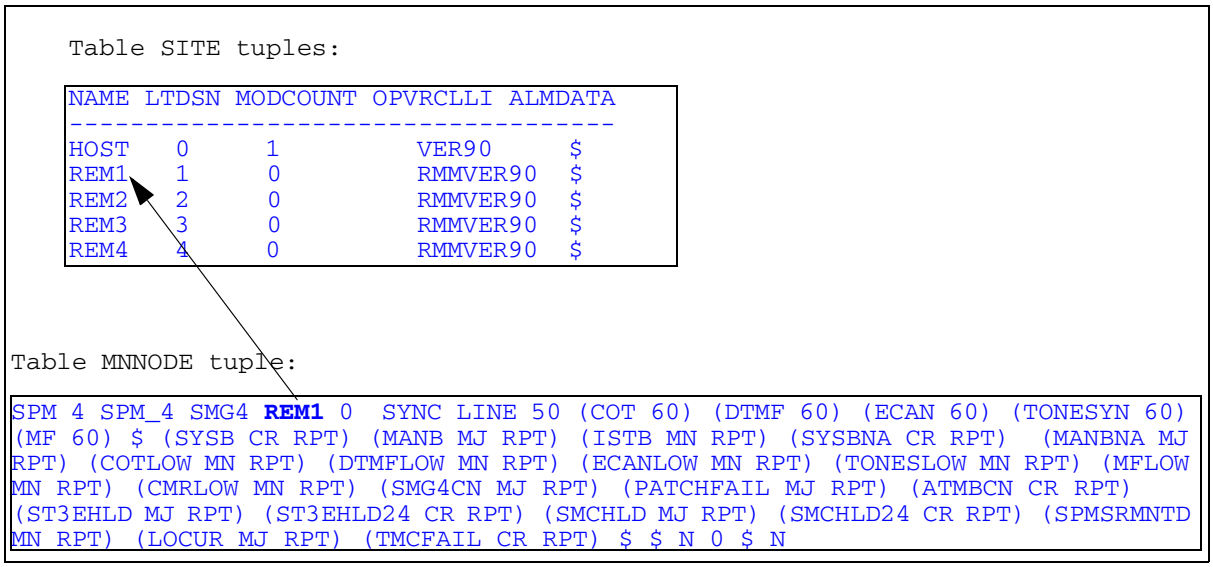


The major functionality changes as a result of this feature are :

61.2.1.1 Table MNNODE changes

A new field,'SITE' has been introduced in the Table MNNODE. This field accepts a four character site name while provisioning(add /modify) the table MNNODE. The allowed values for this field are the sitenames present in Table SITE. Any other sitename, not present in Table SITE, will fail the datafill operation. An example tuple with the new field, and its relationship with Table SITE is shown in Figure 2.

Figure 2 Table MNNODE tuple example with SITE field made editable



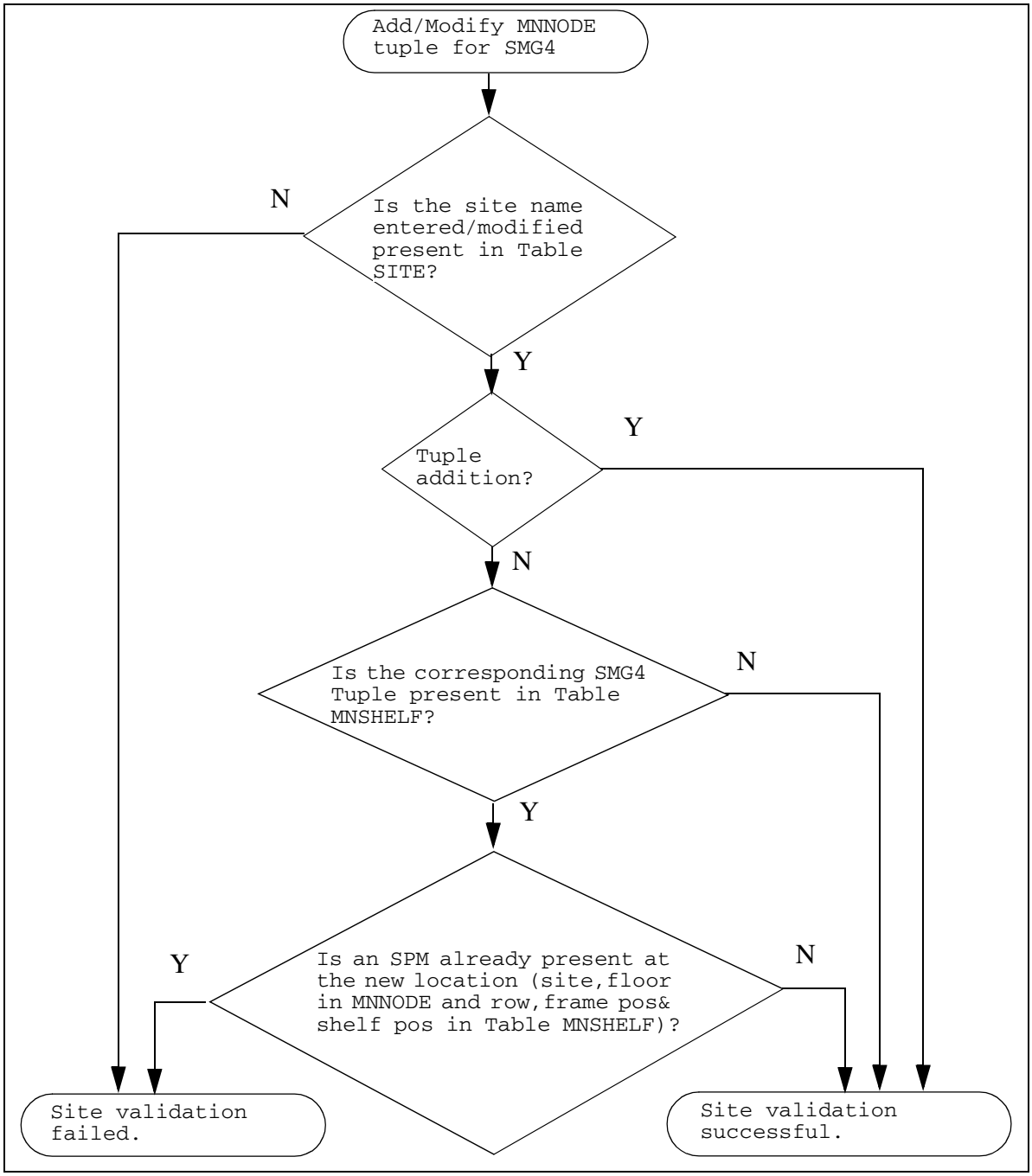
A provisioning example with reference to this feature is shown in Section 61.9 of this document.

Over ONP from previous releases, the value of this new field is defaulted to ‘HOST.’ After an ONP, for SMG4s that are located at a remote site, and are already provisioned, the provisioning information in MNNODE has to be modified appropriately.

This new field is independent of the existing field, ‘REMOTE’ in Table MNNODE. This is because, FSP alarms on remote SMG4 nodes will be reported at the core based on the REMOTE bool in table MNNODE and are not dependent on this new field, ‘SITE’.

Figure 3 shows a flow diagram of how the MNNODE datafill operation proceeds after adding this new field.

Figure 3 Flow Chart for Table MNNODE 'SITE' field validation



The new error messages introduced as a result of the site field validation have been described in the Data Schema in the Configuration document of A00002970.

61.2.1.2 Changes in MAPs, Logs and Tools

The feature also takes care of reflecting the data of the newly introduced field, ‘SITE’ in all the MAPs, Logs and Tools that display the site name for an SPM.

The MAPs and Tools that display site name have been listed in the CN document(Configuration) for this feature, i.e. A00002970.

The Logs that display site name have been listed in the FM document(Fault Management) for this feature, i.e. A00002970.

61.3 Hardware Requirements or Dependencies

None.

61.4 Software Requirements or Dependencies

None.

61.5 Limitations and restrictions

61.6 Interactions

61.7 Applicable customer facing sections

No new logs, alarms, MAPs or tools have been introduced as a result of this feature.

Fault Management	
Logs	__X__
Alarms	_N/A_
Configuration	
Data Schema	__X__
User Interface	__X__
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime _N/A_

Engineering Information _N/A_

61.8 Glossary

Table 1 Glossary

Term	Description
SPM	Spectrum Peripheral Module
SMG4	Succession Multiservice Gateway 4000
CS2K	Call server 2000

61.9 Appendix

61.9.1 Adding MNNODE tuple with ‘SITE’ information

61.9.1.1 ‘SITE’ already present in Table SITE

```
Table SITE datafill :

>lis all
TOP
NAME LTDSN MODCOUNT OPVRCLLI ALMDATA
-------------------------------------
HOST 0 1 VER90 $
REM1 1 0 RMMVER90 $
REM2 2 0 RMMVER90 $
REM3 3 0 RMMVER90 $
REM4 4 0 RMMVER90 $
REM5 5 0 RMMVER90 $
BOTTOM
```

```
Table MNNODE datafill :

>add SPM 62 SPM_62 SMG4 REM5 0 SYNC LINE 0 $ $ $ N 0 $ N N
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE ADDED:
SPM 62 SPM_62 SMG4 REM5 0 SYNC LINE 0 $ $ $ N 0 $ N N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

61.9.1.2 'SITE' not present in Table SITE

```
Table SITE datafill :

>lis all
TOP
NAME LTDSN MODCOUNT OPVRCLLI ALMDATA
-----------------------------------
HOST 0 1 VER90 $
REM1 1 0 RMMVER90 $
REM2 2 0 RMMVER90 $
REM3 3 0 RMMVER90 $
REM4 4 0 RMMVER90 $
BOTTOM
>add REM5 5 0 RMMVER90 $
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE ADDED:
REM5 5 0 RMMVER90 $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

```
Table MNNODE datafill :

>add SPM 62 SPM_62 SMG4 REM5 0 SYNC LINE 0 $ $ $ N 0 $ N N
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE ADDED:
SPM 62 SPM_62 SMG4 REM5 0 SYNC LINE 0 $ $ $ N 0 $ N N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

61.10 References

1. A00002970 in PLS FMDOC.

62: Functional Description (FN): A00002966

62.1 Feature name

Base Re-architecture Phase 2

62.2 Description

The feature is a follow-up to Base Re-architecture Phase 1 which re-architected the SDM platform software to decouple the AIX specific software from the common base software and port it from AIX compiler to open sourced GCC compiler. The common base software can be compiled across multi-platforms, such as AIX, Sun, and be used by SDM and CBM products.

The following major functions are expected to be ported from the SDM to the CBM in the feature:

- **Passthru users using SSH/telnet:** this functionality enables customers to access the Core/CM by logining the CBM through telnet/SSH client software. The user will be automatically forwarded to the Core/CM or the destination configured for the user. No command can be initiated on the CBM by passthru class users. The user interface for managing the passthru users is described in the FN of the feature A00002822 - User Interface Manager for CBM.
- **Restrict shell for maint class users:** all maint class users on the CBM are using the restrict shell to meet security requirement. It uses pretty much the same mechanism as in the SDM except that unix standard man pages are used instead of SDM-own fashioned help command. The user interface for managing the maint class users is described in the FN of the feature A00002822 - User Interface Manager for CBM.
- **Cbmgather tool:** an equivalent platgather tool, which is called cbmgather, is developed on the CBM. The difference from platgather is that the cbmgather doesn't collect the platform specific information, such as splitmode related log, FXgather, etc.

In addition to the porting work, the following new enhancements to the SDM or/and the CBM are expected to be completed in the feature:

- Add querytape subcommand in the apply level of sdmmtc for the SDM to retrieve the version information from the specified tape. It has the following syntax:

  querytape <dat0 | dat1 >

  dat0: tape drive in the domain 0

dat1: tape drive in the domain 1

The help information can be obtained through the help subcommand in the apply level.

- Add a new option to platgather/cbmgather to specify number of days' logs to be collected in order to accommodate some special need when the entire custlog and designlog files are expected to be collected. The new option looks like as follows:

  platgather -n <# of days' log> for the SDM

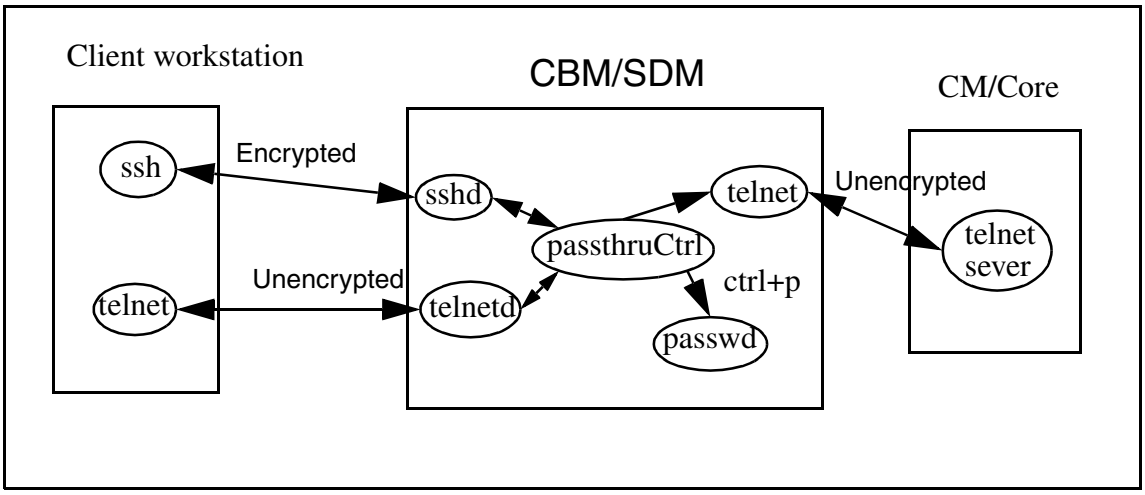
  cbmgather -n <# of days' log> for the CBM

  Where the number ranges from 1 to 7.

- Provide the capability for the passthru users themselves to change their own passwords for the SDM and the CBM. The functionality is requested from our customers and will eliminate the need of administrative users to change the passwords for the passthur users when they want.

  Figure 1, "Functional behavior diagram for passthru users using telnet/ssh" shows how the passthru users work on the CBM/SDM.

Figure 1 Functional behavior diagram for passthru users using telnet/ssh



- List, add, change and modify the passthru users through the command line tool - passthru.

62.3 Hardware Requirements or Dependencies

SSPFS platform hardware and FX

62.4 Software Requirements or Dependencies

SSPFS platform software and SDM

62.5 Limitations and restrictions

Passthru users don’t support the slicing on the CBM in the current release

62.6 Interactions

62.7 Applicable customer facing sections

Fault Management

- Logs __N/A____
- Alarms __N/A____

Configuration

- Data Schema __N/A____
- User Interface __N/A____
- Element Management __N/A____
- Security __N/A____
- Service Order __N/A____
- Office Parameters __N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) __N/A____

62.8 Glossary

Term	Description
New term	Definition
CBM	Core and Billing Manager
CM	Computing Module
SDM	Supernode Data Manager

63: Functional Description (FN): A00002979

63.1 Feature name

A00002979: Panther Electronic Software Delivery

63.2 Description

The PMUPGRADE DMS tool is part of the PANTHER initiative to automate the peripheral module (PM) software upgrade process for DMS switches. PM software upgrades are tedious and time consuming for Nortel customers, usually performed over several off-hour maintenance shifts. PANTHER's goals with respect to the PM software upgrade process are to:

- simplify
- reduce interval
- reduce cost
- improve quality

The purpose of this feature (Feature Number: A00002979) is to update and verify the unreleased CSP10 feature SD0910 so that it is able to be safely released and sustained in the current TDM and Succession environments. This is necessary to ensure the proper working of this feature with the new products and functionality that have been introduced since SD0910 was originally developed (e.g. SPM, XA-Core, etc.)

The purpose of the original CSP10 feature SD0910 is to supplement the PMUPGRADE tool for the electronic delivery of PM upgrade files to the DMS switch. Electronic software delivery (ESD) will contribute to interval and cost reduction of the PM upgrade process. This will allow Nortel customers to deploy new services and conform to changing regulatory requirements in a timely fashion and at a reasonable cost.

The PM upgrade process consists of three phases:

- administration of the new PM upgrade release files (PM load files, PM patch files, and the PM patch cross-reference file) by the PMUPGRADE tool
- production of a recommended PM upgrade plan by the PMUPGRADE tool
- execution of this upgrade plan by the SWUPGRADE PM tool

Feature SD0910 was designed to supplement the PMUPGRADE tool to support the electronic delivery of new PM upgrade files to the DMS switch during the file administration phase of the PM upgrade. The PMUPGRADE design component which deals with physical DMS volumes and files is extended to handle connections to remote FTP volumes. The traditional tape delivery of PM upgrade files remains fully supported by PMUPGRADE. Electronic software delivery helps reduce the need for site access to the DMS switch by customer personnel during the PM upgrade process. This promotes remote activation and supervision of the PM upgrade process.

63.2.1 Feature Limitations

Panther does not handle electronic software delivery of DMS-Core load files. Only PM loads and patches are handled by Panther. However, it is possible to manually transfer DMS-Core load files via FTP when initiating the file transfer from the DMS.

Secure File Transfer (SFT - NTP 297-5051-304 “SuperNode Data Manager Secure File Transfer User Guide” for more information) is currently not supported to transfer files between the DMS-Core and SDM when the file transfer is initiated from the DMS-Core. Therefore, in order for Panther ESD to access the SDM remote FTP volumes, the SDM will need to support normal or anonymous FTP protocol.

63.3 Hardware Requirements or Dependencies

None

63.4 Software Requirements or Dependencies

None

63.5 Limitations and restrictions

The electronic software delivery capabilities provided to PANTHER by features SD0910 and A00002979 is only supported on DMS switches which have TCP/IP connectivity via a SDM.

63.6 Interactions

None.

63.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface __X___

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

63.8 Glossary

Term	Description
CSP	Communications Services Platform
DMS	Digital Multiplexing System
ESD	Electronic Software Delivery
FTP	File Transfer Protocol
PANTHER	PM upgrade automation initiative
PM	Peripheral Module
PMUPGRADE	DMS tool for PM upgrade automation (file administration and upgrade planning phases)
SDM	SuperNode Data Manager
SPM	Spectrum Peripheral Module
SWUPGRADE PM	DMS tool for PM upgrade automation (upgrade execution phase).
TDM	Time Division Multiplexing
XA-Core	Extended Architecture Core

64: Functional Description (FN): A00003073

64.1 Feature name: SimRing Deny Redirection (SRDR)

64.2 Description

SimRing is a terminating end office feature. It resides in the Pilot DN's terminating end office and allows a user defined group of up to five DNs to be alerted simultaneously when a specific member (pilot DN) of this group is called. The SimRing group is comprised of a single Pilot DN (PDN) and up to 4 Non-Pilot Member DNs (NPMDNs or MDNs). The first alerted DN that answers the call is connected to the calling party, and the other alerted DNs are released.

This feature, SimRing Deny Redirection (SRDR), enhances SimRing by providing an optional method to allow a SimRing call to forward based only on the Pilot DN's call forwarding options. The NPMDNs are not allowed to forward the call. Without this option the NPMDNs behavior is unchanged, i.e., they are allowed to forward based on the call forwarding options on the NPMDN.

64.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced by this feature.

64.4 Software Requirements or Dependencies

Redirection Framework.

64.5 Limitations and restrictions

1. The NPMDN's terminating switch must not forward a call which has been marked as having been previously forwarded five (5) times.

This feature relies on the terminating switch of the NPMDN to adhere to the following standards by not forwarding a call which has already been forwarded five times.

— GR-586-CORE, *LSSGR: Call Forwarding Subfeatures (FSD 01-02-1450)*

3.1.1.2.A *Subfeature Construction and Assignment* CFDA: The sequential forwarding limit is five.

— TR-NWT-000972, *Call Forwarding Subfeatures: Switching System Requirements Using Signaling System No. 7 (SS7)*

3.1.1.4.D *Sequential Forwarding* Within the SS7 network or tandem SS7 networks the total number of all (intra and inter-switch) forwardings for each call should be limited. A count of the number of sequential forwardings is kept in the Redirection Counter field in the Redirection Information parameter.

3.1.3.1 *Sequential Forwarding Limit Reached* When the call ... has already been forwarded five times which is the sequential CF limit ... the call should not be forwarded...

2. SRDR is not compatible with a NPMDN terminating end office that uses any overflow or redirection that ignores the redirection/sequential-forwarding counter (for example RCF).

3. SRDR is not compatible with any SCP query/response which results in the modification of the redirection count.

For example, after the PDN-NPMDN call leg leaves the PDN's office, it is possible for an SSP (i.e., a tandem office in the network or the NPMDN's terminating office) to query an SCP and receive a message, analyze_route for example, with instructions for the SSP to reset the redirection count.

4. For inter-office PDN-NPMDN call legs, SRDR is supported when the connection between the Pilot DN's office and the NPMDN's office is ISUP all the way, PRI all the way, or ISUP/PRI interworking. It is not supported for any other network topology.

5. For inter-office PDN-NPMDN call legs, the existing office parm REDIRECTION_FRAMEWORK in table OFCVAR must be set to Y.

6. SRDR is not compatible with the following features when NPMDN and forwarded to DN are in the same office:

- RCF (Remote Call Forwarding)
- LOD (Line Overflow to Directory number)
- LOR (Line Overflow to Route)
- SCMP (Series Completion)
- DNH (Directory Number Hunt)
- KSH (Key Short Hunt)

64.6 Interactions

1. For the PDN-NPMDN leg, when member_dn_redir_allowed is set to NO, the call is made to look as if five redirections have taken place. Therefore, subsequent AIN queries on the PDN-NPMDN leg will include redirection parameters.
2. For calling number delivery, the EBS NPMDN will display the pilot DN and No Ans Fwd as the redirecting DN/reason when the pilot and NPMDN are in the same customer group but in separate offices connected over an ISUP IBN trunk.
3. If the Simring Redirection bool is set to 'NO' on a Simring group that has member DNs that route via ISUP/PRI trunk to a business set agent capable of displaying a REASON, then that set will display a REASON of Call Forward Don't Answer along with the calling party ID. With the Simring Redirection bool set to 'YES' the display of the terminating business set will not display a REASON of Call For -ward Don't Answer.

64.7 Applicable customer facing sections

Fault Management

- Logs ____n/a__
- Alarms ____n/a__

Configuration

- Data Schema ____x__
- User Interface ____n/a__
- Element Management ____n/a__
- Security ____n/a__
- Service Order ____x__
- Office Parameters ____n/a__

Accounting (includes AMA billing) ____n/a__

Performance (includes operational measurements) ____n/a__

64.8 Glossary

Term	Description
DNH	Directory Number Hunt

Term	Description
EBS	Electronic Business Set
KSH	Key Short Hunt
LOD	Line Overflow to Directory number
LOR	Line Overflow to Route
MDN	Member Directory Number
NPMDN	Non Pilot Member Directory Number
PDN	Pilot Directory Number
RCF	Remote Call Forwarding
SCMP	Series Completion
SCP	Service Control Point
SimRing	Simultaneous Ringing
SRDR	SimRing Deny Redirection feature
SSP	Service Switching Point

65: Functional Description (FN): A00003154

65.1 Feature name

MG9000 Manager Capacity Increase

65.2 Description

In the SN07 release the MG9000 Manager will be required to support a maximum capacity of 110,000 H.248 native lines and 75 MG9000 network elements. The pre-SN07 maximum capacity for the MG9000 Manager is 55,000 lines and 60 MG9000 network elements. The recovery time for the 55,000 line configuration is 90 minutes per SN06 Engineering Guidelines. This feature by requirement will meet or exceed the current documented SN06 recovery time, under the new extended capacity requirements.

The reason for the long recovery times is that per the current software architecture, managed objects have to be instantiated within the EM to allow OAM&P. To achieve the SN07 requirements specific managed objects in the MG9000 Manager design will be collapsed. These objects will have their data persisted to the Oracle database and their business logic collapsed into a container class. This design simplifies the recovery of the “leaf nodes” in the system, which require the most memory footprint and instantiation resources during application startup.

Included as part of this design, all configurable MG9000 data will be persisted and restored from the Oracle database. There will also be work required to support maintenance release and major release upgrades.

65.3 Hardware Requirements or Dependencies

This feature will apply to all supported hardware platforms, per SN07 Succession Server Platform Foundation Software specification.

65.4 Software Requirements or Dependencies

None

65.5 Limitations and restrictions

MG9000 provisioning actions will not be accepted in the event of a loss of communication with the Oracle Database hosted on the CS2M host.

65.6 Interactions

None.

65.7 Applicable customer facing sections

Fault Management	
Logs	__N/A____
Alarms	__N/A____
Configuration	
Data Schema	__N/A____
User Interface	___X___
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____
Accounting (includes AMA billing)	__N/A____
Performance (includes operational measurements)	__N/A____
Realtime	__X____
Engineering Information	___X___
Performance (includes operational measurements)	N/A
Real-time	N/A
Engineering Information	N/A

65.8 Glossary

66: Functional Description (FN): A00003154

66.1 Feature name

SN07 Take Back and Transfer Enhancements - A00003154

66.2 Description

Tack Back and Transfer (TBT) is a service which allows a terminator to initiate a conference call or transfer the call to another party using the Switch_Hook_Flash (SHF) capability.

This activity, A00003154, provides the following new capabilities in a TBT call:

1. A **Connect_To_Resource** (CTR) message requesting an internal switch resource for only digit collection.
2. A PRI connection between a UCS DMS-250 switch and an external resource (i.e Intelligent Peripheral -IP).
3. The interaction context between the SCP and IP can be specified as Connect_1129_style.

In addition to supporting additional CTR scenarios, this feature addresses all of the issues associated with the CAIN OMs for Take Back and Transfer calls.

For additional information concerning Tack Back and Transfer, refer to feature A89008913, Take Back and Transfer Feature Sourcing and Re-Engineering.

66.3 Connect To Resource Overview

Take Back and Transfer supports the receipt of the **Connect_To_Resource**(CTR) message in response to the Switch-Hook_Flash Event Request message sent at the **O_Mid_Call** EDP.

Connect_To_Resource message allows connection of a resource to an existing two-party call, which can be used for applications that need to provide announcements and/or collect digits from the user, such as with debit card calls. The SCP may return a CTR message to request the SSP to route the call or a leg of the call to a resource.

For detailed information about the **Connect_To_Resource** message, refer to feature AX0974 which implemented the **Connect_To_Resource** message as defined by GR-1298 CORE AIN Switching Systems Generic Requirements, Issue 7.

66.3.1 Internal Resource

This activity provides the capability for TBT calls to connect to an internal resource for only digit collection using a **Connect_To_Resource** message.. The SSP interprets a **Connect_to_Resource** message without a Destination Address parameter as a request to access an internal switch resource. The connection to an internal resource for a TBT call is requested through a Conversation package.

If a LegID is specified and a non-specified leg abandons the call, the following actions are performed:

— The switch cancels the resource interaction

— The switch sends a CTR_Clear in a response package with a ClearCause parameter set to userAbanodon

If a LegID is specified and the user on the leg abandons or is disconnected in some other way before the Connect_To_Resource is complete:

— The UCS DMS-250 switch cancels the resource interaction.

— The UCS DMS-250 switch sends a CTR_Clear in a response package with a ClearCause parameter set to userAbandon.

66.3.2 PRI Support for Intelligent Peripheral Connection

In SN06, activity A89008913 provided support for a SS7- IMT connection between the DMS-250 and the external resource (i.e. Intelligent Peripheral - IP). This SN07 activity provides the functionality that allows a PRI connection between the DMS-250 and the IP for TBT calls. When the Destination Address parameter is included in the **Connect_to_Resource** message, the SSP interprets the message as a request for an IP. For TBT calls, the **Connect_to_Resource** message must be designated as a Conversation package.

When an SCP requests a local SSP to make a connection to an IP and the local SSP has a direct ISDN or SS7connection to the IP, the indicated IP is referred to as a local IP. The local IP is designated in datafill by the IPTRUNK option in table TRKGRP. PRI can only be used for local IP connections.

66.3.3 Connect_1129_style support for Intelligent Peripheral Interface (IPI)

In SN06, activity A89008913 provided the Connect_only capability. This SN07 activity provides Connect_1129_style functionality for TBT calls. Connect_1129_Style provides the capability to allow for an SSP to interwork an exchange of data between an IP and SCP. During the active connection to an IP, data may be exchanged between the SCP and IP using certain PRI

message or a certain ISUP message, the **Call_Info_From_Resource** message and the **Call_Info_To_Resource** message.

With Connect_1129_style, the IP can be used to collect digits from the end user. After the digits have been collected, the IP sends the collected digits to the SSP within the Remote Operation (RO) parameter.

For PRI, the RO parameter can be sent with:

- Disconnect message
- Facility message

For IMT, the RO parameter can be sent with:

- ISUP FAR message
- ISUP Release message.

Data can be passed between the SSP and the SCP using the **Call_Info_From_Resource** and **Call_Info_To_Resource** message. Upon receipt of a valid FAC or FAR message, the UCS DMS-250 switch builds a **Call_Info_From_Resource** message, containing the IPReturnBlock parameter.

The expected response to the **Call_Info_From_Resource** message is the **Call_Info_To_Resource** message.

For detailed information concerning Connect_1129_style, refer to AX0974, Networkbuilder Connect_to_Resource.

66.3.3.1 Determination of IPI

The CONNECT_1129_STYLE method can be specified by one of three ways:

- The CAINSTRConnectionType extension parameter in the Connect_To_Resource message. Refer to UCS08 feature AX0190.
- The STR_CONNECTION_TYPE in table CAINXDFT for the associated CAINGRP.
- The tuple STR_CONNECTION_TYPE in table CAINPARM. Refer to UCS08 feature AX0190 for more information.

66.3.3.2 Timers

With the CONNECT_1129_Style, the timer TSTRC provides a maximum time limit for a CTR-Connection to an IP. It is started when the IP answers and canceled with the CTR-Connection is cleared, either by the SSP or IP. The TSTRC_TIMER field in table CAINPARM determines the time duration for the TSTRC timer. The following are the values for the TSTRC_TIMER:

- Range - 0 to 60 minutes, with the value of 0 disabling the timer
- Default - The timer will have a default value of 6 minutes.

66.3.3.3 Call_Info_From_Resource message

The Call_Info_From_Resource message is sent by the SSP to send intermediate information from an IP to the SCP during the Connect_1129-style connection.

The IPReturnBlock parameter is used to send the result of any user-interaction with the IP to the SCP.

Table 1 indicates the parameters supported by the Call_Info_From_Resource message.

Table 1 Call_info_From_Resource Message Parameters

Call_Info_From_Resource Message
IPReturnBlock
ExtensionParameter

66.3.3.4 Call_Info_To_Resource message

The Call_Info_To_Resource message is sent by the SCP. This message is used to provide a response to the intermediate information received from the IP through the UCS DMS-250 switch during an active Connect_1129_style connection. This message is used in response to the Call_Info_From_Resource.

Table 2 indicates the parameters supported by the Call_Info_To_Resource message.

Table 2 Call_info_To_Resource Message Parameters

Call_Info_To_Resource Message
ResourceType
StrParameterBlock
ExtensionParameter

66.4 Operational Measurements support for Take Back and Transfer

OMs – Operational Measurements of data that are collected and displayed as the switch performs various operations. The affected CAIN OM groups that are addressed by this re-engineering activity for TBT functionality are listed below:

- CAINAGOM
- CAINMSGR
- CAINMSGS
- CAINTRIG

The scope of this activity is limited to the above mentioned CAIN OM groups and the associated Registers for TBT functionality.

66.4.1 Group: CAINAGOM

The Carrier Advanced Intelligent Network Per-Agency Operational Measurements (CAINAGOM) group provides threshold reporting of OMs on a per agency basis.

CAINAGOM consists of eight tuples:

• TOTAL - represents the sum of OM tuples pegged on a per agency basis.

• DAL - represents measurements occurring on DAL originating or terminating agencies.

• EANT - represents measurements occurring on EANT originating or terminating agencies.

• ONAL-represents measurements occurring on ONAL originating or terminating agencies.

• ONAT-represents measurements occurring on ONAT originating or terminating agencies.

• PRI - represents measurements occurring on PRI originating or terminating agencies.

• IMT - represents measurements occurring on IMT originating or terminating agencies.

For Call Configurations (CC) between CC4 (ThreePartySetup) to CC11 (Transfer) the controlling leg i.e, TermA being the controlling leg shall be the originating agent for the following registers:

- AGRESPR

- AGEDPRCD
- AGEDPREQ
- AGCTRCNV
- AGCTRCLR

In CC11 (Transfer), if TermB initiates SHF (Switch_Hook_Flash) for Multiple transfer, then TermB would become the new controlling leg and hence TermB shall be considered as the originating agent for the above mentioned registers.

66.4.1.1 Register: AGRESPR

Counts the number of responses the switch receives from the SCP for calls originating on the agent type of the associated tuple. This register is pegged when the switch receives successfully decoded messages.

When we transition from CC2 (StableTwoParty) to CC4 by means of Originate_Call response for O_Mid_Call query, Orig being the originator of the first leg and the only leg at this point shall be pegged for this register.

66.4.1.2 Register: AGEDPRCD

Counts the number of times a valid Request_Report_BCM_Event component is received.

This register is pegged after the successful validation of the RRBCME component.

66.4.1.3 Register: AGEDPREQ

Counts the number of EDP requests sent for calls originating on the agent type of the associated tuple.

This register is pegged after the successful launch of EDP request form the SSP to the SCP.

66.4.1.4 Register: AGCTRCNV

Counts the number of conversational Connect_To_Resource messages received by each type of CAIN agent on the SSP.

This register is pegged after the successful decoding of CTR in conversation message.

The registers AGRESPR in group CAINAGOM and RESPRCVD in group CAINTRIG are not pegged when CTR message is received in conversation

package. These registers are pegged only when CTR message is received in response package.

66.4.1.5 Register: AGCTRCLR

Counts the number of CTR_Clear messages sent by CAIN agents on the SSP.

This register is pegged after the successful launch of CTR_Clear message form the SSP to the SCP.

66.4.2 Group: CAINMSGR

The Carrier AIN Messages Received (CAINMSGR) group reports the number of CAIN TCAP messages received from the Service Control Point (SCP) related to call processing.

When an unarmed event processing happens then the register corresponding to the SSP's action taken is not pegged.

For ex: In CC6 (PARTYONHOLD) call configuration if the Passive Leg 1 (Orig) disconnects, then the SSP performs disconnect leg processing with LegID 1 and the call transitions to CC2 (STABLE2PARTY). In this scenario, the register DISCLEG is not pegged.

To make it clear, a register of this OM group is pegged only when the corresponding message is received by SSP from the SCP and not when the SSP internally performs that message action due to unarmed event processing.

66.4.2.1 Register: CONTINUE

Counts the number of Continue messages received by the switch.

This register is pegged after the successful decoding of CONTINUE message.

66.4.2.2 Register: DISCON

Counts the number of Disconnect messages received by the switch.

This register is pegged after the successful decoding of DISCONNECT message.

66.4.2.3 Register: RRBCMEVT

Counts the number of Request_Report_BCM_Event operations received by the switch.

This register is pegged after the successful decoding of RRBCME component.

66.4.2.4 Register: CON2RSRC

Counts the number of Connect_To_Resource messages received by the switch.

This register is pegged after the successful decoding of CTR message.

This register will be pegged for CTR message both in response and conversation package.

66.4.2.5 Register: ORIGCALL

Counts the number of Originate_Call messages the switch receives.

This register is pegged after the successful decoding of ORIGINATE_CALL message.

66.4.2.6 Register: MERGECL

Counts the number of Merge_Call messages the switch receives.

This register is pegged after the successful decoding of MERGE_CALL message.

66.4.2.7 Register: DISCLEG

Counts the number of Disconnect_Leg messages the switch receives.

This register is pegged after the successful decoding of DISCONNECT_LEG message.

66.4.2.8 Register: ACKNOW

Counts the number of Acknowledge messages the switch receives.

This register is pegged after the successful decoding of ACKNOWLEDGE message.

66.4.3 Group: CAINMSGS

The Carrier AIN Message Sent (CAINMSGS) group provides OMs for TCAP messages sent to the Service Control Point (SCP) for CAIN processing.

66.4.3.1 Register: ODISC

Counts the number of O_Disconnect messages sent to the SCP.

This register is pegged after the successful encoding of O_DISCONNECT message.

66.4.3.2 Register: OMIDCALL

Counts the number of O_Mid_Call messages sent to the SCP.

This register is pegged after the successful encoding of O_MID_CALL message.

66.4.3.3 Register: CTRCLR

Counts the number of CTR_Clear messages sent to the SCP.

This register is pegged after the successful encoding of CTR_CLEAR message.

66.4.3.4 Register: OABANDON

Counts the number of O_Abandon EDP-Request messages the switch sends to the SCP.

This register is pegged after the successful encoding of O_ABANDON message.

66.4.3.5 Register: FAILUREO

Counts the number of Failure_Outcome messages the switch sends to the SCP.

This register is pegged after the successful encoding of FAILURE_OUTCOME message.

66.4.4 Group: CAINTRIG

The Carrier AIN Trigger (CAINTRIG) group provides OMs for each Carrier Advanced Intelligent Network (CAIN) trigger and Event Detection Point.CAINTRIG consists of 24 tuples on each DMS switch.

The OMs related to a TBT call are listed below:

• ODISC - represents OMs relating to calls that encounter the O_Disconnect event

• OABANDON-represents OMs relating to calls that encounter the O_Abandon event.

• SHF-represents OMs relating to calls that encounter the Switch_Hook_Flash event.

66.4.4.1 Register: RESPRCVD

Counts the number of responses the switch receives from the SCP that can be decoded and the requested action attempted.

This register is pegged after successful decoding of the message and the requested action being attempted.

66.4.4.2 Register: EDPSRCVD

Counts the number of times the switch receives a valid Request_Report_BCM_Event component.

This register is pegged after successful validation of the RRBCME component.

66.4.4.3 Register: EDPREQ

Counts the number of EDP requests sent to the SCP.

This register is pegged just before the successful launch of EDP request form the SSP to the SCP.

66.4.4.4 Register: CTRCONV

Counts the number of conversational Connect_To_Resource messages the switch received from the SCP.

This register is pegged after the successful decoding of CTR in conversation message.

The registers AGRESPR in group CAINAGOM and RESPRCVD in group CAINTRIG are not pegged when CTR message is received in conversation package. These registers are pegged only when CTR message is received in response package.

66.4.4.5 Register: CCLRCONV

Counts the number of CTR_Clear conversational messages sent to the SCP.

This register is pegged after the successful launch of CTR_Clear message from the SSP to the SCP.

66.5 Hardware Requirements or Dependencies

None

66.6 Software Requirements or Dependencies

None

66.7 Limitations and restrictions

None

66.8 Interactions

None

66.9 Applicable customer facing sections

Fault Management

- Logs __N/A____
- Alarms __N/A____

Configuration

- Data Schema __N/A____
- User Interface __N/A____
- Element Management __N/A____
- Security __N/A____
- Service Order __N/A____
- Office Parameters __N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) __N/A____

66.10 Glossary

Term	Description
SCP	Service Control Point
SSP	Service Switching Point
OM	Operational Measurements
CAIN	Carrier - Advanced Intelligent Network
TBT	Take Back & Transfer
CC	Call Configuration

Term	Description
SHF	Switch_Hook_Flash
CTR	Connect_To_Resource

67: Functional Description (FN): A00003233

67.1 Feature name

LANComm Tool Enhancements.

67.2 Description

This feature will provide necessary enhancments to existing LANComm tools. The following tools will be addressed: ARPMONCI, IPROUTCI, NETMAN, SNPINGCI, UDPCI, and IPOMSCI. The operation of existing Command Increments (CI) will not be changed. However NETMAN's 'FREE' CI, IPROUTCI's 'ROUTER' CI, SNPINGCI's REG and DEREG CI have been limited to the lab environment. IPROUTCI's 'DELROUTE' CI, ARPMON's 'DEQ' and 'CACHE QUEUE' CI have been created and secured by ToolSup.

The new ARPMON CI 'DEQ' has been implemented to remove entries from the ARP Cache. This will allow the user to invalidate specific ARP Cache entries.

UDPCI's UCBDUMP will be enhanced to display additional information.

The existing tool IPOMSCI will undergo no functional changes.

67.3 Hardware Requirements or Dependencies

Not applicable.
There are no new Hardware dependencies.

67.4 Software Requirements or Dependencies

Not applicable.
There are no new Software dependencies.

67.5 Limitations and restrictions

Limitations: (Secured by ToolSup)

- IPROUTCI's DELROUTE
- ARPMONCI's DEQ

Restrictions: (Lab environment only)

- NETMAN's FREE CI
- IPROUTCI's ROUTER
- SNPINGCI's REG
- SNPINGCI's DEREG

67.6 Interactions

Use of any ToolSup secured command will impact DMS operations. A complete understanding of not only TCP/IP, but also DMS operations and DMS specific implementation characteristics is required to use these tools.

67.7 Applicable customer facing sections

Fault Management

Logs	__N/A__
Alarms	__N/A__

Configuration

Data Schema	__N/A__
User Interface	___X___
Element Management	__N/A__
Security	___X___
Service Order	__N/A__
Office Parameters	__N/A__

Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	___X___

67.8 Glossary

Term	Description
EIU	Ethernet Interface Unit

Term	Description
LANComm	Local Area Network Communication pertains to the EIU hardware and the TCP/IP suite of protocols on the DMS Supernode and XA-Core.
ARP	Address Resolution Protocol.
ARPMONCI	A tool for debugging and monitoring ARP.
DEQ	This command invalidates the specified ARP Cache entry.
IPROUTCI	A tool for debugging and monitoring IP routing and throttling.
ROUTER	Adds a Router to the Router table (not the route table).
DELROUTE	Deletes a route from the route table.
IPOMSCI	A tool for monitoring internal OM's generated by the different layers of the protocol stack.
IPD	Display information about an Operational Measurement group.
NETMAN	A network management tool that displays information about TCP and UDP connections.
FREE	Deallocates a bound TCP/UDP endpoint.
ToolSup	A Tool Supervisor that controls command execution by password protection.

68: Functional Description (FN): A00003273

The FN for this feature document is located in activity A00003933 in PLS FMDOC. The A00003933 document contains the FN for the Session Server project.

69: Functional Description (FN): A00003277

69.1 Feature name

Documentation for this activity can be found in activity A00003393.

69.2 Description

69.3 Hardware Requirements or Dependencies

69.4 Software Requirements or Dependencies

69.5 Limitations and restrictions

69.6 Interactions

69.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

69.8 Glossary

Term	Description
New term	Definition

70: Functional Description (FN): A00003279

70.1 Feature name

Documentation for this activity can be found in A00003933 SIP on SP2000 Drop 1 ICAF in PLS FMDOC.

70.2 Description

70.3 Hardware Requirements or Dependencies

70.4 Software Requirements or Dependencies

70.5 Limitations and restrictions

70.6 Interactions

70.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

70.8 Glossary

Term	Description
New term	Definition

71: Functional description (FN): A00003280

71.1 Feature name

A00003280 - SIP on NGSS Tracing/Debug Framework

71.2 Description

This activity SIP on NGSS Debug and Tracing is a stand alone tool. It controls the Radvision SIPT Toolkit log module and filters the internal NGSS traces which are written into the tracing files.

This feature is primarily targetted to Customer Support groups like GNPS. While the tool will be available in the field, due to the impact of running the tracing session on the capacity of the field office, it should not be done on a regular basis or at high traffic levels.

71.2.1 Overview

This tool can run in these two mode:

1. Simple Mode - straightforward usage tracing SIP messages
2. Prompt Mode - more sophisticated usage, needs a deeper knowledge what to trace and how to used this tool.

71.2.1.1 Simple Mode

The following is an overview of a typical Simple Mode tracing session.

1. user needs a telnet session to the NGSS
2. start a Simple Mode by a command **/opt/apps/bin/sp2ktrace start**
3. stop a Simple Mode by a command **/opt/apps/bin/sp2ktrace stop**
4. tracing file is located in NGSS directory **/opt/apps/logs** with the name as siptrace.YYYYMMDD.MSG.00001 (example **siptrace.20040318.MSG.00001**)
5. the siptrace file contains the SIP messages provided by Radvision Transport layer:

```
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -
T  88b63c8 03/19/2004 14:09:13 DEBUG  - TRANSPORT    -
TransportCallbackMsgToSendEv: Application did not register to call back, default
bSendMsg = 1
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportUdpSendMessage
- Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportSendMessage -
About to send message with size = 335
```

```
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - --> OPTIONS sip:1.2.3.4
SIP/2.0
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     From:
<sip:MGCA>;tag=40c0a8c0-13c4-405afefd-49811d5-18457876
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -    To: <sip:CCAONE@1.2.3.4>
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Call-ID: 8909008-
40c0a8c0-13c4-405afefd-49811d5-16ba7f11@MGCA
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     CSeq: 30 OPTIONS
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Via: SIP/2.0/UDP
192.168.192.64:5060;branch=z9hG4bK-405afefd-49811d5-218c6e77
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Max-Forwards: 70
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Supported: 100rel
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Content-Length: 0
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -
T  88b63c8 03/19/2004 14:09:13 DEBUG  - TRANSPORT    -
TransportCallbackMsgToSendEv: Application did not register to call back, default
bSendMsg = 1
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportUdpSendMessage
- Sending message. local-address=192.168.192.64:5060. remote-
address=192.168.192.59:5060
```

6. for continuous tracings you can type command on NGSS:

> tail -f /opt/apps/logs/siptrace.20040318.MSG.00001

to get traces onto the screen.

71.2.1.2 Prompt Mode

The following is an overview of a Prompt Mode tracing session.

1. user needs a telnet session to the NGSS

2. enter a Prompt Mode (command line interface) by a command **/opt/apps/bin/sp2ktrace** as example:

```
root@unit0 root]# /opt/apps/bin/sp2ktrace
```

3. type **help** to see which commands are available

```
SIPTRACE> help
These commands are provided:
  Help
  set (layer<1-19>  filter<0-63>)
  status
  start
  stop
  Users
  display <all | Session Server Name> - for IP address status
  prtcache
  Quit
-------------------------------------------------------------
Additional info for SET command:
  Layers and their corresponding numbers are shown by
  STATUS command.
  1 - all layers (ex. SET 1 2 sets all layers filter=INFO=2).
  There are 6 Filters as:
  DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32.
  Filters can be logically combined - if you want to trace for ex.
  layer PARSER (7) with filters ERROR (8) and EXCEP (16)
```

```
  SET 7 24
  For cleanup use filter 0 (example SET 7 0 for above).
  Use SET 1 63 (to set tracing for everything)
  use SET 1 0  (to cleaunp everything).
  Please be aware SET command only sets tracing.
  You must use START command to start tracing
  and use STOP command to end it.
Tracing files are in the directory /opt/apps/logs/.

SIPTRACE>
```

4. type **status** command to see all available Layers and Filters:

```
SIPTRACE> status

Active Users: 1         Radvision    L  o   g   F   i   l   t   e   r   s
[pid:15734]  active=OFF ----------------------------------------------------
        RV Layers       DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
=============================================================================
 1      all             -       -       -       -       -       -
 2      core            -       -       -       -       -       -
 3      msg             -       -       -       -       -       -
 4      transport       -       -       -       -       -       -
-----------------------------------------------------------------------------
 5      transaction     -       -       -       -       -       -
 6      call            -       -       -       -       -       -
 7      parser          -       -       -       -       -       -
 8      stack           -       -       -       -       -       -
-----------------------------------------------------------------------------
 9      msgBuilder      -       -       -       -       -       -
10      authenticator   -       -       -       -       -       -
11      regClient       -       -       -       -       -       -
12      subscription    -       -       -       -       -       -
++++++++++++++++++++++ S P 2 K     L  o  g    F   i   l   t   e   r   s
13      callpAppMTC     -       -       -       -       -       -
14      GCP             -       -       -       -       -       -
15      other           -       -       -       -       -       -
16      sipmsg          -       -       -       -       -       -
17      gcpmsg          -       -       -       -       -       -
18      gcpmtcmsg       -       -       -       -       -       -
19      linkmtc         -       -       -       -       -       -
=============================================================================
SIPTRACE>
```

5. type **set** command to set Layers/Filters selection (in this example you chose to trace a **transport** layer (4) for **filters** DEBUG (1), INFO (2) and ERROR (8) and the another layer msgBuilder (9) for ERROR (8) only. Thus type two command: **set 4 11** (4-transport, 11= 1+2+8) and **set 9 8**

```
Active Users: 2         Radvision    L  o   g   F   i   l   t   e   r   s
[pid:22958]  active=OFF ----------------------------------------------------
        RV Layers       DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
=============================================================================
 1      all             -       -       -       -       -       -
 2      core            -       -       -       -       -       -
 3      msg             -       -       -       -       -       -
 4      transport       x       x       -       x       -       -
-----------------------------------------------------------------------------
 5      transaction     -       -       -       -       -       -
 6      call            -       -       -       -       -       -
```

```
 7      parser          -       -       -       -       -       -
 8      stack           -       -       -       -       -       -
-------------------------------------------------------------------------
 9      msgBuilder      -       -       -       x       -       -
10      authenticator   -       -       -       -       -       -
11      regClient       -       -       -       -       -       -
12      subscription    -       -       -       -       -       -
++++++++++++++++++++++ S P 2 K     L  o  g    F   i   l   t   e   r   s
13      callpAppMTC     -       -       -       -       -       -
14      GCP             -       -       -       -       -       -
15      other           -       -       -       -       -       -
16      sipmsg          -       -       -       -       -       -
17      gcpmsg          -       -       -       -       -       -
18      gcpmtcmsg       -       -       -       -       -       -
19      linkmtc         -       -       -       -       -       -
=========================================================================
SIPTRACE>
```

Please note “x” at the transport and msgBuilder Layer.

6. start the tracing by a **start** command

```
SIPTRACE> start
```

7. type **users** command to see overall tracing activity

```
SIPTRACE> users

                                  R   a   d   v   i   s   i   o   n    S  P  2  K
                          Layers:  1   2   3   4   5   6   7   8   9   10 11 12   13  14
15  16     17     18        19
                                  al co ms tp tr ca pa st mB au rC su   MTC GCP
oth SIPMSG GCPMSG GCPMTCMSG LINKMTC
User                pid     active
-------------------------------------------------------------------------------
-------------------------------------
server              15704   1       0  0  0  31 0  0  0  0  0  0  0  0    0   0
0   0      0       0         0
mtc                 16802   0       0  0  0  0  0  0  0  0  0  0  0  0    0   0
0   0      0       0         0
MSG                 00001   1       0  0  0  31 0  0  0  0  0  0  0  0    0   0
0   0      0       0         0
SIPTRACE>
SIPTRACE> stop
```

In the example above you can see three users. A server is a permanent thread with a pid (processID=15704), your session with a userID mtc and pid 16802and one Simple Mode with userID MSG and hardcoded pid 00001. The “00001”s behind a pid column belong to the active column indicating that this session is active - it means it collects data.

8. the siptrace file for the above tracing session (pid 22958) is located in NGSS directory /oipt/apps/logs/siptrace.20040319.mtc.22958 with few first lines as:

```
=== SESSION ENTERED: [pid:22958/mtc]  Fri Mar 19 14:17:19 2004
=== MONITOR UPDATED: [pid:22958/mtc]  Fri Mar 19 14:38:53 2004
  Filters: 0  0  0  11 0  0  0  0  0  0  0  0 ::0  0  0  0  0
=== MONITOR UPDATED: [pid:22958/mtc]  Fri Mar 19 14:38:59 2004
  Filters: 0  0  0  11 0  0  0  0  8  0  0  0 ::0  0  0  0  0
```

```
=== MONITOR STARTED: [pid:22958/mtc]  Fri Mar 19 14:42:27 2004
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
TransportMultiThreadTimerEventHandler - Allocating timer expired event for timer
0x88dafe4
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
TransportProcessingQueueTailEvent - TIMER_EXPIRED_EVENT 0x8906a20
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
TransportProcessingQueueDispatchEvents - TIMER_EXPIRED_EVENT 0x8906a20
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - SipTransportUdpSendMessage
- Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - SipTransportSendMessage -
About to send message with size = 335
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - --> OPTIONS sip:1.2.3.4
SIP/2.0
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     From:
<sip:MGCA>;tag=40c0a8c0-13c4-405b06b8-4b643e6-4fdb17be
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     To: <sip:CCAONE@1.2.3.4>
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Call-ID: 890bb28-
40c0a8c0-13c4-405b06b8-4b643e6-69016e79@MGCA
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     CSeq: 30 OPTIONS
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Via: SIP/2.0/UDP
192.168.192.64:5060;branch=z9hG4bK-405b06b8-4b643e6-5c79301f
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Max-Forwards: 70
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Supported: 100rel
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Content-Length: 0
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -
```

9. stop the session by the **stop** command.

10. exit session by a **quit** command.

71.3 Hardware Requirements or Dependencies

Customer offices without the Session Server will not have the functionality delivered by this feature.

71.4 Software Requirements or Dependencies

71.5 Limitations and restrictions

This tool has the following limitations:

1. Tool is currently configured for 10 concurrent Trace Clients. The Simple Mode is counted as a Client.

2. The user of this tool needs an access (a telnet session) to the NGSS machine.

3. There can run only one Client in the Simple Mode at a time.
(it would not have a sense to duplicate very same tracing)

4. Every Trace Client gets own output trace file which is being used until the Trace Client session ends (by **quit** command in the Prompt Mode or ***sp2ktrace stop*** in the Simple Mode). It means if a user starts a session on Monday and runs it over 3 days - there will be only one Trace Client file with a creation date i.e. Monday date.

5. The Trace Server trace file. In contrast of the Trace Client trace file, the Trace Server trace file is created on every day. The trace file creation is not done few seconds after midnight but by the first event recorded into the server file (after midnight - which can be few hours from the midnight) depending on tracing activities/setup.
6. If the size of any client output file (siptrace) created by this tool (in the directory /opt/apps/logs) exceeds limit (default is 10 MBytes) then this file will be over written from the beginning. This event is recorded together with the overwritten counter.
7. All siptrace* files in the directory /opt/apps/logs/ older than 3 days will be deleted automatically by the tracing tool. This removal is triggered by new sp2ktrace session.
8. Other files in the directory /opt/apps/logs need to be deleted manually. Please note the file created by monitoring in the Simple Mode is appended every time when tracing starts (by a command ***sp2ktrace start***) on the same date.
9. **WARNING**: Do not delete active/current (today) server file and prevent deletion of the active Trace Client's files. Deleted files will not be re-created.
10. **SWACT:** the current version of the tracing tool does not automatically swact when NCGL platform does a swact. The sp2ktrace tool needs to be started on both units (active/inactive) prior a swact if tracing over the swact is required. In a case of a application swact the sp2ktrace tool needs to be restarted manually.
11. **Configuration:** The configuration file sp2ktraceConfig is created when tool runs for very first time in the directory /opt/apps/logs. This file has currently two (default) parameters:

- NUMBEROFINITLOGS 300
- CLIENTFILESIZEMB 10

The first parameter configures the number of logs to be printed into the server siptrace file during the initialization (when SIP Gateway is Unsuspended). The default value is 300 logs but can be increased up to the maximum of 25000.

The second parameter allows to increase the size of the client siptrace file from the default value 10 Mbytes up to the maximum of 500 Mbytes.

These parameter must be changed prior the SIP Gateway is Unsuspended to be used.

71.6 Interactions

Not applicable.

71.7 Applicable customer facing sections

Fault Management

- Logs _____N
- Alarms _____N

Configuration

- Data Schema _____N
- User Interface _____N
- Element Management _____N
- Security _____N
- Service Order _____N
- Office Parameters _____N

Accounting (includes AMA billing) _____N

Performance (includes operational measurements) _____N

71.8 Glossary

Term	Description
NGSS	Another acronym for the Session Server
SIP	In-band signally protocol, RFC 2962

71.9 References

- SP2K_CGRD - SP2K DID A00003933 (PLS FMDOC)
- Radvision SIP Toolkit - Programmer Guide
- Radvision SIP Toolkit - Reference Guide
- Radvision SIP Stack - Porting Guide
- A00003698 - FMDOC - SIP Msg trace

72: Functional Description (FN): A00003371

72.1 Feature name

The activity name for this task is Common Inventory and Data Consolidation A00003371.

72.2 Description

This feature introduces a Common Inventory data schema and eliminates redundant data. It provides for creation of new components and modification of a number of existing components summarized as follows:

- a new centralized inventory database schema in Oracle representing network element data and its relationships (logical and physical associations) with other entities in the system.
- a new JDBC-based API that allows applications to add, modify, remove, and retrieve inventory information from the schema.
- a new event notification and registration component for applications to register for data addition/deletion/modification events.
- an new inventory schema upgrade infrastructure for supporting upgrades from one release of the inventory schema to another.
- Modification of all relevant applications in the SESM package to use the new common inventory, including the elimination of the NETWORK and PROXY schema data. Affected applications are: GWC Manager, UAS Manager, Alarm Manager, Proxy Agent, Data Engine, NetworkView, Service Broker, Line Provisioning, Trunk Provisioning, LMM, Cs2kCfgMgr, V52CfgMgr ProfileManager and TMM.

Part of the effort in providing this feaure includes generation of IEM compliant customer logs. This is the only customer visible aspect of this feature and is captured in an accompanying Fault management document.

72.3 Hardware Requirements or Dependencies

NA

72.4 Software Requirements or Dependencies

NA

72.5 Limitations and restrictions

NA

72.6 Interactions

NA

72.7 Applicable customer facing sections

Fault Management

- Logs ___X___
- Alarms ___N/A__

Configuration

- Data Schema ___N/A_
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

72.8 Glossary

Term	Description
New term	Definition

73: Functional Description (FN): A00003452

73.1 Feature name

Intelligent Portal insertion for low portal density networks.

73.2 Description

This feature enables Network Operators to reduce the provisioning of Media Proxies/Portals (MP)in the network, as implemented by Activity A90007980.

MP are now only mandatory on the following GWC types:

- Line GWC with GW behind NAT or GW external to the CS2K core.
- SIP-T GWC

MP provisioning against all other GWC types is optional, and require no additional provisioning to support this new functionality.

[APG provisioning is subject to change once feature reaches DID_R state]

73.3 Hardware Requirements or Dependencies

Not applicable.

73.4 Software Requirements or Dependencies

Not applicable

73.5 Limitations and restrictions

Not applicable

73.6 Interactions

Not applicable

73.7 Applicable customer facing sections

Fault Management

Logs	__N/A_
Alarms	__N/A_

Configuration

Data Schema	__N/A_
User Interface	__N/A_

Element Management __N/A_
Security __N/A_
Service Order __N/A_
Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

73.8 Glossary

Term	Description
MP	Media Proxy/Portal.
GWC	Gateway Controller

74: Functional Description (FN): A00003454

74.1 Feature name

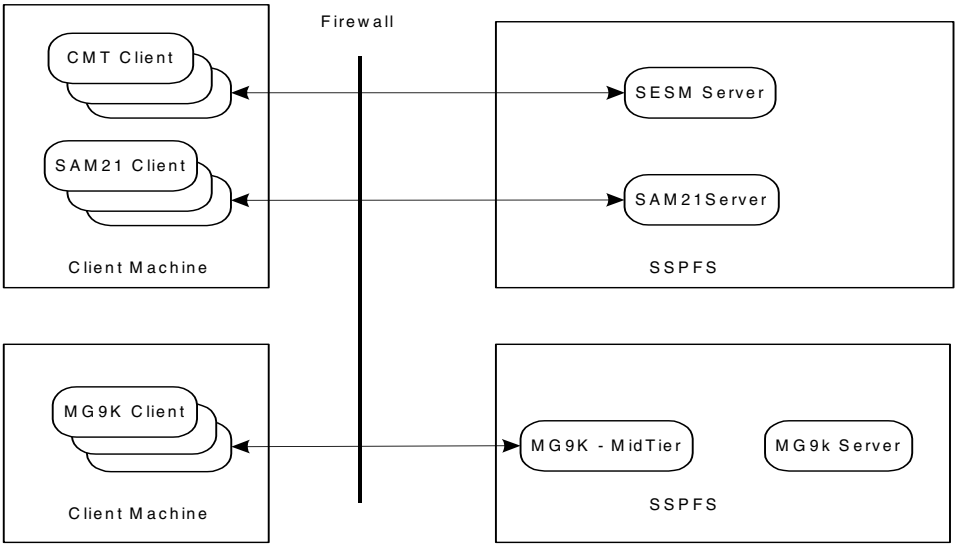
Secure_and_Firewall_Compatible_CS2M_and_UE9KEM_Client_GUI_Communication, A00003454.

74.2 Description

74.2.1 Purpose:

The primary purpose for this feature is to facilitate firewall protection for traffic for the Succession OAM&P GUI Client/Server communication, the Succession GUI's will work even with the addition of a firewall in the customer network. Along with sending the data through a firewall, the data will also be encrypted.

Figure 1 Purpose of A00003454



This was done with the addition of a SOCKS proxy on the client and server machines. The Succession GUI's will send all messages to a SOCKS proxy listening on a specific port on the client machine. The client SOCKS proxy will send all the messages to a SOCKS proxy listening on a specific port on the server machine.

There are two compents that have customer impact.

1. Configuring the client and server ports.

2. Starting, stopping, and getting the status of the SOCKS proxy on the server machine.

The applications that are covered with this activity include the CMT, SAM21 EM, and MG9K EM GUI's.

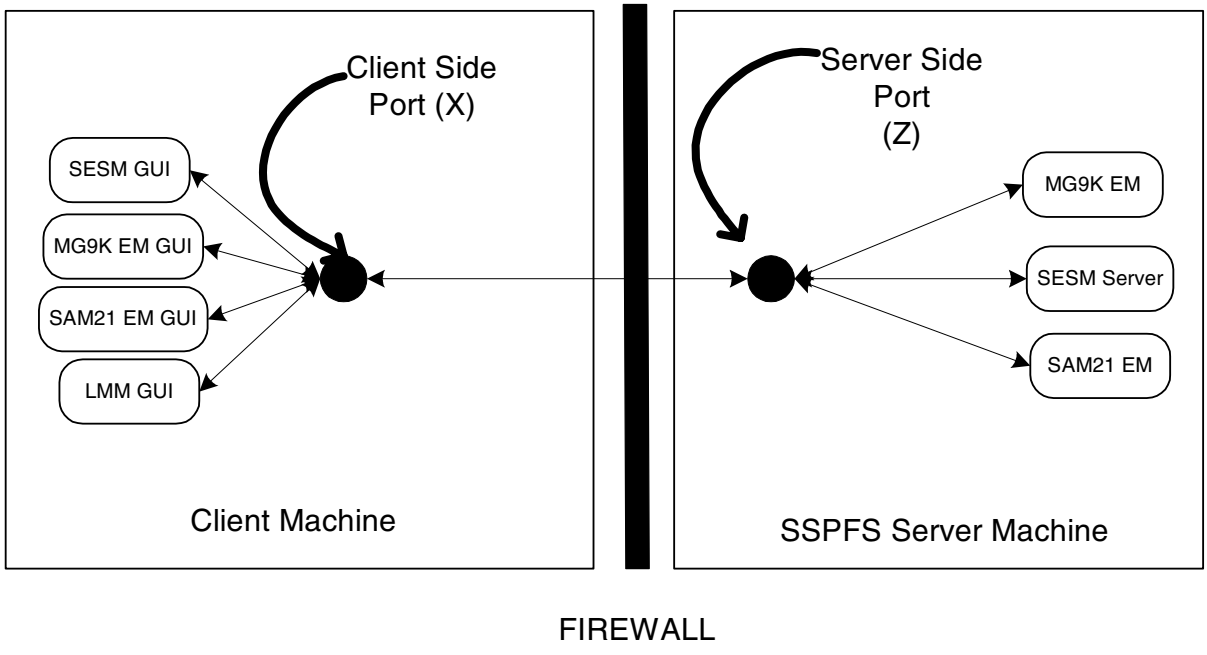
74.2.2 Configuration

There is one changed command the customer will use to configure this feature, the *cli* command. The functions that will be added is to configure the port and to list the currently used ports

- A port on the SSPFS server machine used to receive all requests from clients.
- A port on the client machine that concentrates all requests from the client to the server.
- A port on the client machine to receive all the requests from the Succession GUI applications.

The following figure depicts the ports configured. Each of the ports has a default value. If the default value is acceptible, it is not necessary to configure the ports with the cli command. If the default value is not the value required, the cli command is used to change these ports.

Figure 2 Ports configured



The port configuration takes place on each SSPFS server the SOCKS software is used on. The SSPFS machines that would require configuration are those that contain the GUI's covered by this feature.

As shown, the Server Side Port, referenced as Z will be configured using the *cli* command. This is the port that requests from all client machines will be concentrated to. If a firewall is in place, the Server Side port Z must be opened to allow these messages through. The default value for this port is 10080. It is recommended that port 10080 is used, but if it is necessary to change, the software on the server machine will ensure there are no port collisions on the SSPFS machine by verifying that the port is not in file /etc/services. All SSPFS server machines must configure this to the same value.

The Client Side port, referenced as X will also be configured using the *cli* command. Upon startup of the client machines, the Succession GUI will connect to that port. This port is an internal port used only on the client machine. There is no firewall configuration necessary. All SSPFS machines must be configured to the same value. The default value for this port is 10080 and may be configured to a different value.

74.2.2.1 Consistent configuration of ports

The ports configured through the offices must be configured consistently across all offices in the network. If the ports are not configured consistently, the GUI's will not function correctly. See the troubleshooting section for information on incorrect behavior.

74.2.2.2 Port conflicts on server side

The ports on the server side will be added to the file /etc/services. If the port is already bound into /etc/services, the configuration will not be allowed. The list of ports in /etc/services is not exhaustive, and the customer should know the site specific configuration of the SSPFS ports.

Note that in the MG9K case, the database host machine (as defined in the DB_HOST variable) must be upgraded to SN07 before the MG9K Midtier.

74.2.3 Start and Stop of server component

There is a new command added to start, stop, and restart the server side component that is listening on the Server Side port.

If the *cli* command is used to change the Server Side Port, the change takes effect immediately, as the the SOCKS server on the SSPFS machine is restarted.

74.2.3.1 Impacts to restarting SOCKS server

If the server side component is reconfigured or restarted, the clients GUI's covered by this feature will need to be restarted. Also, the following server's

on the SSPFS where the SOCKS proxy is restarted will need to be restarted as well.

- MG9K Mid-Tier
- SAM21 EM
- Notification Service
- SESMService
- NPM
- PSE

74.2.4 Starting and stopping the SOCKS process using *servman*

The socks process is a run level command, which means that any time the server is restarted for any reason socks will be automatically started. There should be no reason for the customer to start or stop socks except in Nortel directed troubleshooting.

If the SOCKS server is stopped and then started, the Succession servers running on the same SSPFS machine will need to be restarted. The GUI clients that are active and communicating with the server will also need to be restarted.

74.2.4.1 Starting the SOCKS server

/etc/init.d/socks start

```
SOCKS server successfully started
```

```
If servstart SOCKS does not work the following error
will be displayed.
```

```
The SOCKS server could not be started due to the port
<port number> is already in use. Verify the port is
not configured for another use.
```

74.2.4.2 Stopping the SOCKS server

/etc/init.d/socks stop

```
SOCKS server successfully stopped
```

74.2.4.3 Querying the SOCKS server

s/etc/init.d/socks status

```
SOCKS server RUNNING
```

If the SOCKS server is not running the result will be:

```
SOCKS server STOPPED
```

74.3 Hardware Requirements or Dependencies

There are no new hardware requirements added with the introduction of this feature.

74.4 Software Requirements or Dependencies

There are no new software requirements or dependencies added by this feature.

74.5 Limitations and restrictions

The Client Side ports as shown in figure 2 must be free for the Succession GUI's shown to operate.

The Server Side port as shown in figure 2 must be opened on a firewall that supports stateful packet inspection.

Reconfiguration of Server Side port requires server side Socks Proxy restart, EM restart, and client application restart.

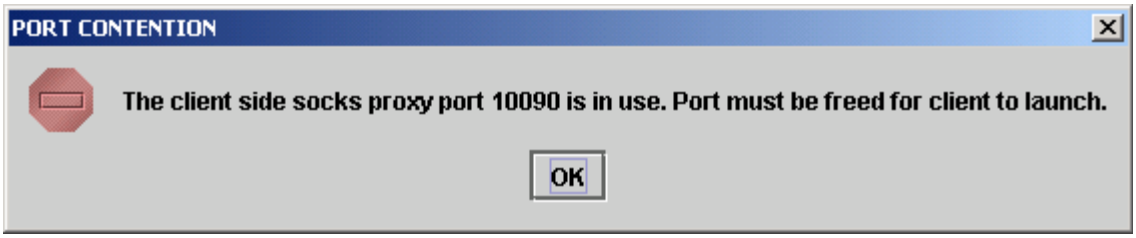
74.6 Troubleshooting

At times, there may be configuration errors which cause port contention on the client machine or servers configured with different ports. In both these cases a failure by the client to launch or connect will be encountered.

74.6.1 Client Port Binding Error

If the port on the client machine is already bound to another process then the client GUI will fail to start. If the port is already bound to another process, and the client will not start successfully, the following dialog to show there is a problem with a port contention:

Figure 3 Dialog specifying port contention upon startup on the client machine



The solution to this is to free the port in the client machine. Depending upon what type of client machine used, the solution will differ. Closing the application will free the port.

74.6.2 Server Configuration Errors

If there are server side configuration differences between offices there will be a failure of the GUI to connect to the server machine. If office A is configured for the server to listen on port 10080, and office B is configured for the server to listen on port 10090. If there are only GUI's launched to communicate with either office A or office B, there will be no problems. If GUI's are launched to communicate with both office A and B, then there will be a failure to communicate with one of the offices. The GUI that is launched to communicate with one office, say office A will work. If there are other GUI's launched to communicate with office A, those will also work. If there is a GUI launched to communicate with office B, those communications will fail.

The recourse to solving this problem is to verify if there is in fact a configuration error. If there is a configuration error, there are two ways to get the GUI's to launch correctly.

74.6.2.1 Re-Launch GUI's

If the GUI to server B, as described in the previous section needs to be launched, and the desire is to not reconfigure the server, the GUI's launched that are communicating with office A need to be closed.

After all the GUI's have been closed, re-launch the GUI to office B.

74.6.2.2 Re-Configure server

Reconfiguring the server is the best solution to this problem. Configure all the server side ports to the same value on all offices. Please see the CN section to determine how to reconfigure the server side ports.

74.6.3 Server side Socks Proxy not running

If the Socks Proxy is not running on the server side, the following dialog will be displayed.

Figure 4 Dialog specifying server side.socks proxy is not running

74.7 Interactions

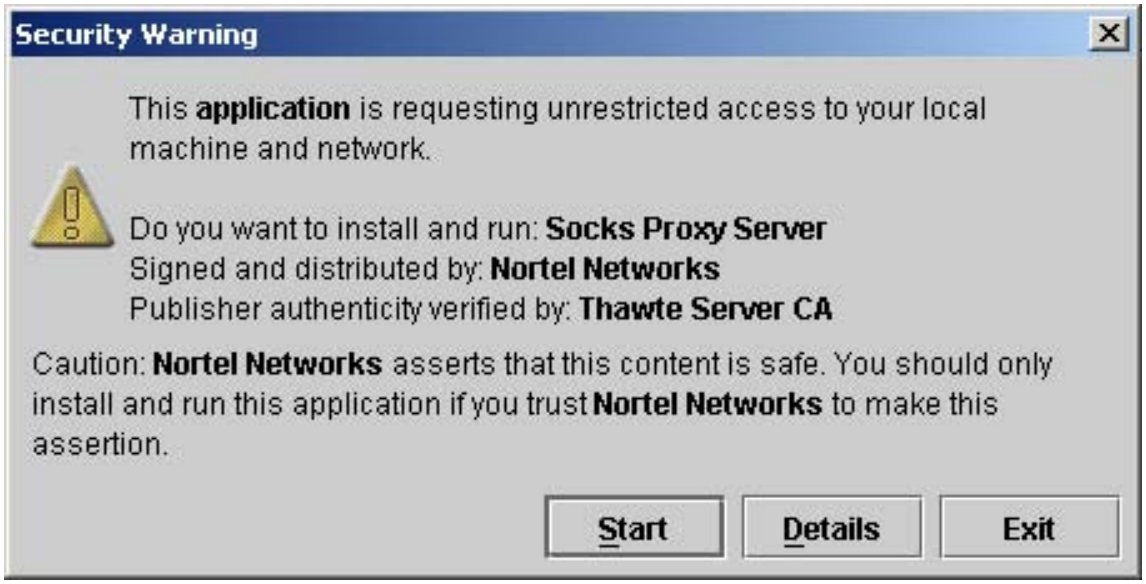
74.7.1 Launch sequence

When launching a Succession GUI the succession GUI outline will launch and a new dialog will be shown. This dialog is shown so the user knows that the Client Side Socks Proxy is being launched. The following dialog

Figure 5 Dialog shown when Client Socks Proxy is being launched

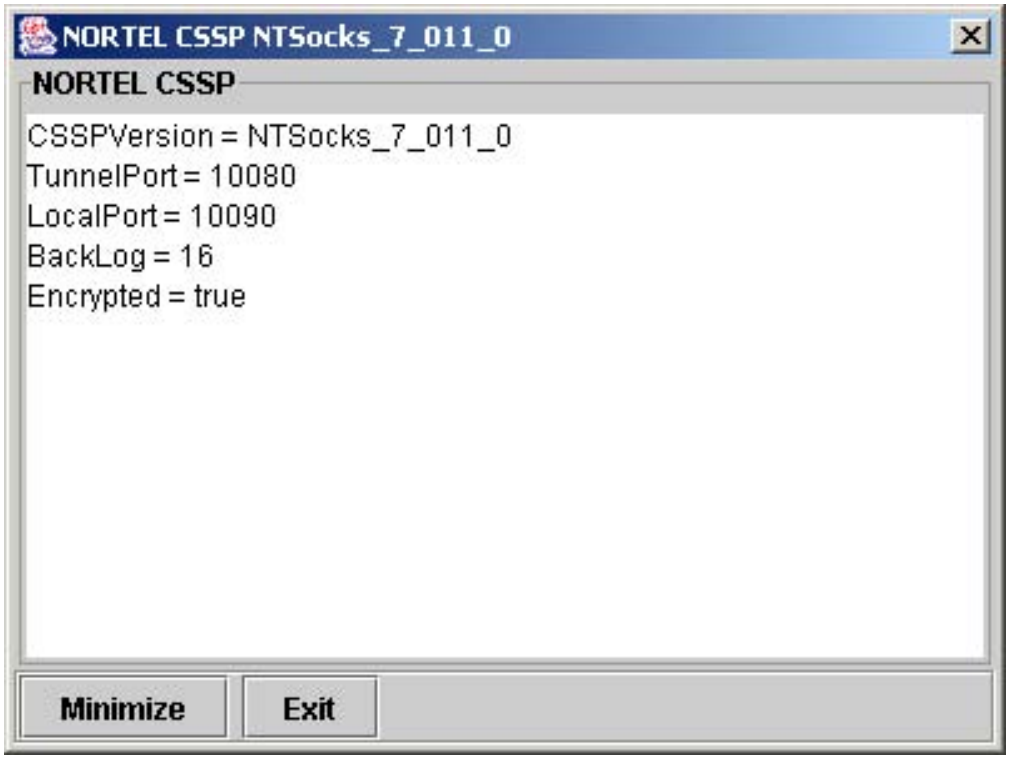
When launching an application after starting this feature, the user will be prompted to allow a new Java Web Start application unrestricted access to the client machine, prior to launching a Succession GUI as follows:

Figure 6 Added Security Warning dialog when starting Succession GUI's



The client side SOCKS proxy has a small GUI that automatically opens up at the start of the first client application on the client machine. The GUI will automatically minimise itself, but may be opened to see parameters of the connection. The client side SOCKS proxy may be terminated also from this GUI by hitting the 'Exit' button. Note that hitting the 'Close' button only re-minimises the GUI; it does not terminate the client side SOCKS proxy. Note that the parameters cannot be changed; they are shown for reference only. Figure 7 shows an example of the GUI.

Figure 7 Nortel Client Side SOCKS Proxy GUI



74.7.2 Nortel CSSP

The NORTEL CSSP is iconified at startup. The Minimize button will iconify the window as will the x on the top right of the window.

The Exit button will exit the process, and any GUI's that are using the NORTEL CSSP will need to be restarted from the application launch point.

The NORTEL CSSP will remain open until the Exit button is pressed. The NORTEL CSSP will be shared by all the Succession GUI's that use it.

75: Functional Description (FN): A00003459

75.1 Feature name

A00003459 - SSC re-architecture

Activity 1: SYSB Line alarm/log and LGRP alarm/pm map support

75.2 Description

This activity covers a part of the SSC re-architecture work. It has four main design components:

- Add new alarm for succession SYSB line.
- Generate a new log when the above alarm is raised/cleared.
- Add a new pm sublevel for LGRP and
- Raise alarm when there are LGRPs in SYSB state.

75.2.1 New alarm for SYSB lines

This alarm will only be supplied to Succession office. The class of the alarm (MINOR, MAJOR, or CRITICAL) will be displayed in the system status display area under the header Lns of the mapci display (i.e. under Lns header of mapci;mtc). Here is the map window:

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
 .        .        .        .         .        .      LGRP       .        .        .
                                                      *C*
   MTC
  0 Quit
  2
  3 MTCNA
  4 SRSTATUS
  5 BERP
  6 CAPACITY
  7
  8
  9 XAC
 10 MS
 11 IOD
 12 Net
 13 PM
 14 CCS
 15 Lns
 16 Trks
 17 Ext
 18 APPL
   YD
 Time  10:56  >
```

Currently, the alarm for Lns has four types: CUT, DF, HAZ, PSPD. Accordingly, the alarm is displayed using the following characters for the combination of alarms of the same severity:

{ 1}: ' CUT '
{ 2}: One of the following diagnostic failure alarms: 'Diag', 'Fac ', 'SDiag', ...
{ 3}: 'CT DF'
{ 4}: ' HZD '
{ 5}: 'HZ CT'
{ 6}: 'HZ DF'
{ 7}: 'H C D'
{ 8}: 'PSPD '
{ 9}: 'CT PS'
{10}: 'PS DF'
{11}: 'C P D'
{12}: 'HZ PS'
{13}: 'H C P'
{14}: 'H P D'
{15}: 'HCPD '

With the new addition of SYSB alarm, the following character display will be used to indicate the multiple alarms occuring at a given time:

Table 1 new alarm display

	CUT	DF	HAZ	PSPD	SYSB
'SYSB '					X
'CT SB'	X				X
'DF SB'		X			X
'CD SB'	X	X			X
'HZ SB'			X		X
'CH SB'	X		X		X
'DH SB'		X	X		X
'CDHSB'	X	X	X		X
'PS SB'				X	X
'CP SB'	X			X	X
'DP SB'		X		X	X
'CDPSB'	X	X		X	X
'HP SB'			X	X	X

Table 1 new alarm display

	CUT	DF	HAZ	PSPD	SYSB
'CHPSB'	X		X	X	X
'DHPSB'		X	X	X	X
'CDHPS'	X	X	X	X	X

The alarm will only be applied to succession lines (excluding ABI) in the entire office. The severity of the alarm is based on the alarm thresholds, which are set independently. A new office parameter **SYSBALARM** will be created in table OFCVAR. The new office parameter will have a default value {10, 20, 30} which will be set at IPL time and will survive all restarts.

AlmStat at the LTP level will be changed to display and modify the threshold of SYSBALARM. The new display of this command without parameter will look like the following:

```
OFFICE TOTALS

             OFFICE LINE FAILURE TOTALS

                        OFFICE   OFFICE OFFICE OFFICE
                        CURRENT  MINOR  MAJOR  CRITICAL
 Ext   Diag Fail  (D)     1       10     20      30
 Facility Fault   (F)     0       10     20      30
 Short Diag Fail  (S)     0       10     20      30
 Needs Ext  Diag  (N)     0       10     20      30
 Set Missing   (MSET)     0       10     20      30
 Card Missing (MCARD)     7       100    150     200
 Shower Queue (QUEUE)     0       100    150     200
 Major ICMOLINE(IMAJ)     0       100    150     200
 Minor ICMOLINE(IMIN)     0       100    150     200
 Loop Sig Set  (LSET)     0       100    150     200
 Loop Sig Card(LCARD)     0       100    150     200
 TCM sync loss    (T)     0       100    150     200
 Loop Performance (P)     0       100    150     200
 Major CPERROR (CMAJ)     0       5      10      15
 Minor CPERROR (CMIN)     0       5      10      15
 Major RapidMSG(OMAJ)     0       10     20      30
 Minor RapidMSG(OMIN)     0       10     20      30
 Utility Card     (U)     0       100    150     200
 State = PLO   (PSPD)     6       10     20      30
 State = HAZ (HAZARD)     0       0      1       10
 State = SYSB (SYSB)      6       10     20      30

......
```

where 6 in this example is the total number of SysB lgrp lines in the office.

Use the following command to change the SYSB threshold:

AlmStat SYSB minor_value major_value critical_value

The input values must be in ascending order, or the command will be rejected. User could also change the threshold via table OFCVAR, but a warning will be displayed on the MAP: “WARNING : This parameter should only be changed using the ALMSTAT command at the LTP”.

This alarm can be disabled by changing the threshold to (0 0 0) via table control on table ofcvar. Again, a warning message will be displayed for this action.

75.2.2 New log for SYSB line alarm

A new log LINE 811 will be generated when the alarm is raised or cleared. The format of the log will be as below:

RTP7 *** LINE 811 DEC01 17:45:14 2000 THR LNS ALARM
Category: Communications
Cause: thresholdCrossed
Severity: CRITICAL
ThresholdID: SYSB_LINES

RTP7 ** LINE 811 DEC01 17:45:14 2000 THR LNS ALARM
Category: Communications
Cause: thresholdCrossed
Severity: MAJOR
ThresholdID: SYSB_LINES

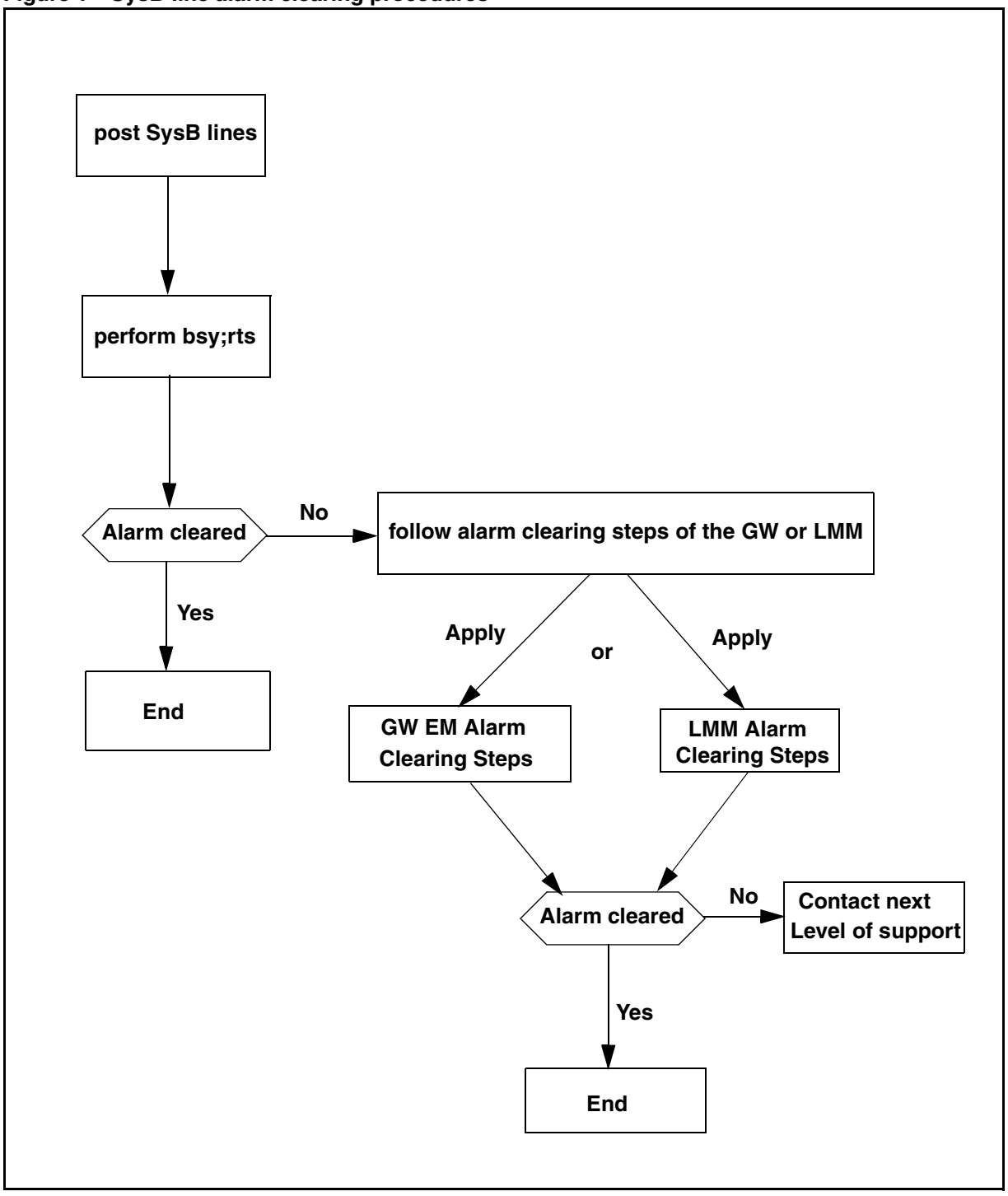
RTP7 * LINE 811 DEC01 17:45:14 2000 THR LNS ALARM
Category: Communications
Cause: thresholdCrossed
Severity: MINOR
ThresholdID: SYSB_LINES

RTP7 LINE 811 DEC01 17:45:14 2000 THR LNS ALARM
Category: Communications
Cause: thresholdCrossed
Severity: CLEAR
ThresholdID: SYSB_LINES

75.2.3 SysB lns alarm clearing procedures

Please refer to the summary flowchart depicted in the following figure to clear the SysB Lns alarm:

Figure 1 SysB line alarm clearing procedures



Note: For MG9K, the alarm clearing procedures are documented in A00005016.

75.2.4 LGRP maintenance

This feature will provide a new lgrp maintenance support on the core. The following lists the work items to be done:

- lgrp pm map interface support to allow user to post lgrp nodes and perform maintenance action against the posted lgrp node
- lgrp SysB alarm support
- support for new lgrp map maintenance commands: bsy, rts, offl and QueryPM

75.2.4.1 New pm map level for lgrp

User will be able to post LGRP under the PM maintenance level. The map window is very similar to other LCDs:

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .        .        .        .       2lgrp     .        .        .        .        .
                                      *C*
LGRP                                  SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit           PM                    4        0        0        0        0        0
 2 Post_          LGRP                  2        0        0        0        0        0
 3 Listset
 4             LGRP: LG   00 0         SysB
 5
 6             POST:
 7 Bsy
 8 Rts
 9 OffL
10
11 Disp_
12 Next
13
14 QueryPM
15
16
17
18
  YD
Time  09:05  Pref>
```

The state of the posted lgrp will be displayed, so does the total numbers of LGRPs in each state.

Command Bsy, Rts, and Offl can only be issued for the large node lgrp (i.e. only for a lgrp of S type).

75.2.4.2 Bsy command

Command Bsy will send a man_bsy message to GWC. The map will wait for an ACK from gwc with 5 second timer. Upon receiving man_bsy message, GWC will disable the heartbeat between MG9K and GWC, and send an man_bsy_ack message back to the core. Upon receiving the ACK, Bsy command will kill all the calls and change the node state to ManB. If timeout occurs, the core will send bsy force request to gwc and change the node state to ManB.

Bsy nowait command will also be supported. This command does the same thing as Bsy command but user gets the prompt back immediately.

This command can only be issued on a node state of OFFLINE, SYSTEM BUSY, or INSERVICE.

75.2.4.3 Rts command

Command Rts will send man_rts message to gwc and wait for an ACK. Upon receiving man_rts message from the core, gwc will reenable the heartbeat between MG9K and GWC, and send man_rts_ack (if service-change-disconnected message is received from MG9K) back to the core.

If man_rts_ack message is received, the map process will handle it as tid-idle message is received (i.e. change the state to Insv and send down the line state table to gwc, etc). Map display will be updated accordingly.

If 90-second timeout occurs, a “TIMEOUT ON WAIT FOR REPLY FROM GWC” message will be displayed on the map and no state change will occur.

Rts force command will do the same thing as Rts, except that it does not wait but immediately change the node state to SysB.

Rts nowait command allows the user to get the prompt back immediately.

Rts force nowait command does the same thing as Rts force.

Rts command can only be issued on a ManB state.

75.2.4.4 Offl command

Command Offl will take the lgrp posted to unequipped state. It can only issued from ManB state.

> ***Note:*** The lgrp node state will be set to OFFL (like most of the PM nodes are) after the node provisioning. User will need to perform manual action in order to bring the node into service.

75.2.4.5 QueryPM command

Command QueryPM will show the posted LGRP node data information:

```
  XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
   .       .       .       .      2lgrp    .       .       .       .       .
                                   *C*
 LGRP                             SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit          PM                4       0       0       0       0       0
  2 Post_         LGRP              2       0       0       0       0       0
  3 Listset
  4             LGRP: LG   01 0      SysB
  5
  6             QueryPM
```

```
 7 Bsy       PM Type: LGRP  PM No: 81  Int. No: 1  HOSTNN: 72
 8 Rts       Cside Host Name: GWC  6
 9 OffL      Cside Host IP:  172.16.112.56
10           FrmType   Flr   RowPos   FrmPos   ShlfPos
11 Disp_     MG9F        2     ZZ       3        0
12 Next
13
14 QueryPM
15
16
17
18
  YD
Time  09:12  Pref>
```

75.2.4.6 New pm alarm for LGRP

The new alarm will be displayed under the PM banner and will be raised when there are LGRP nodes that are in SysB (machine busy).

The severity of this alarm will follow the rule of existing PM alarms: If the number of SysB lgrp exceeds 10 percent of the total pm in the office of all types, set the alarm class to CRITICAL. Otherwise, set the alarm to MAJOR if there is at least one SysB lgrp. The alarm will be cleared only when the state of all lgrp nodes is changed to other state (via Bsy or Offl command).

75.2.4.6.1 lgrp alarm clearing procedures

The most common reason of lgrp sysb alarm is due to OOS (Out of Service) of MG9K or due to state mismatch between the lgrp node in the core and the MG9K VMG the lgrp represents. User should use the alarm clearing procedure in A00005015 as the guild for clearing the alarm. If none of them clears the sysb alarm in the core, call GNPS for next level support.

75.2.4.7 Software upgrade for LGRP

Since the initial LGRP node state will be set to OFFL upon provisioning, swact applications needs to be provided for core upgrade from SN06 to SN07 and from SN07 to SN07.

75.2.4.7.1 Swact from SN07 to SN07

An swact application for LGRP node state transfer will be provided such that InSv state will be transfered to the inactive side during ONP. The following table dictates the preswact node status check for LGRP:

Table 2

	Inactive Side (states)				
Active side (state)	OFFL	INSV	SYSB	MANB	CBSY
OFFL	match	---	---	---	---
INSV	match	match	---	---	match
other state	---	---	---	---	

Only the entry marked as “match” will pass the preswact node status check.

75.2.4.7.2 Swact from SN06 to SN07

In SN06, the initial LGRP node state is InSv or SysB. A patch will be required to bypass the node status check for LGRP so that preswact will always pass for LGRP node status check.

75.3 Hardware Requirements or Dependencies

N/A

75.4 Software Requirements or Dependencies

N/A

75.5 Limitations and restrictions

N/A

75.6 Interactions

N/A

75.7 Applicable customer facing sections

Fault Management

- Logs __X____
- Alarms __X____

Configuration

- Data Schema __X____
- User Interface __X____
- Element Management _____
- Security _____

Service Order _____

Office Parameters __X____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

75.8 Glossary

Term	Description
New term	Definition
LMM	Line Maintenance Manager
GW	Gateway

75.9 References

1. "New VMG Out of Service Alarm", A00005016MG9000_FM.fm from http://triweb/smg5000/Succession/subdir/document_mirror/mg9k_07/

2. "CS2000 Line Test for MG9000 Lines" A00001888 in FMDOC

76: Functional Description (FN): A00003485

76.1 Feature name

A00003485 - ISUP 200,000 Ports Trunk Support.

76.2 Description

76.2.1 ISUP 200K Ports Trunk Support

This feature increases the limit on the size of table C7TRKMEM for a standalone SSP from 165,000 tuples to a maximum of 200,000 tuples.

The constraints which will allow table C7TRKMEM to realize an increased maximum number of tuples from 165,000 to 200,000 are:

- Switch is a stand-alone SSP.
- Universal Signaling Platform.

If an attempt to exceed the above maximum of 200,000 tuples is made, a pre-existing error message is printed which states that the number of tuples in table C7TRKMEM is at the supported limit.

When ISUP, PRI, DPT, and PTS ports are provisioned the total ports for the SSP can not be above 200,000 total trunk ports.

76.2.2 EPUTIL

EPUTIL is a CI tool in the CM(Type EPUTIL on the CI prompt to access the tool) tool which allows a user to capture and display maintenance messages sent from the GWCs to the CM. This tool has been available as a lab-only tool until now. This feature will make this tool field ready.

Given below is a list of the various commands that will be available to the user in EPUTIL.

1. **EPTRACE**: This is the main test tool available to the user. It provides the user with commands to turn ON/OFF the trace, display the captured messages etc. Given below is a list of the sub-commnads available at this level:
   a. **SELECT**: Allows the user to select a node for the trace. The user has an option of selecting all nodes or a specific node.
      eg SELECT ALL : selects all nodes
      SELECT GWC <GWC NO> : selects the specified GWC

      Note : A maximum of seven nodes can be selected at a given time(applicable only when specific nodes are being selected)

b. **REMOVE**: Allows the user to remove a selected node. The user can remove all nodes, or can remove a specific node
   eg REMOVE ALL : removes all selected nodes
   REMOVE GWC <GWC NO> : removes the specified GWC

c. **START**: Starts the TRACE

d. **STOP**: Stops the TRACE

e. **LIST**: Lists all the captured bundle messages
   eg LIST ALL : Lists all the captured messages
   LIST GWC <GWC NO> : Lists all the captured messages for the specified GWC

f. **SHOW**: Shows the details regarding the specified bundle message

   Figure 1 below displays a sample output for the SHOW command

Figure 1 Sample Display for SHOW command

```
**********************************************************
Msg Received at: 2004/01/13 11:14:47.206 TUE.
 GWC Number: 80(0x0050), Node Number: 28(0x001C)
Bundle Count: 3, (0x0003)
Sequence No: 6, (0x0006)

       Individual Messages
      ===============

       Message 1 <==
      Received from Node 28(0x001C)
      Terminal Number: 801 (0x0321), CPID: CKT ETSIV2OG 1
       Individual message type: um_car (0x0003)
       Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)

       Message 2 <==
      Received from Node 28(0x001C)
      Terminal Number: 804 (0x0324), CPID: CKT ETSIV2IC 1
       Individual message type: um_car (0x0003)
       Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)

       Message 3 <== Received from Node 28(0x001C)
      Terminal Number: 807 (0x0327), CPID: CKT ETSISPAREOG 1
       Individual message type: um_car (0x0003)
      Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)
**********************************************************
```

g. **STATUS**: Displays the current status of the TRACE(displays whether the TRACE is ON/OFF, and all the GWCs selected for the TRACE).

h. **COUNT**: Displays the total number of messages captured

i. **HELP**: Provides the user with the list and a brief description of all available commands at the EPTRACE level

1. **EPPTABLE**: Displays the details regaring all the processes in the input handler. The details include the Process ID, the In Use Queues and the Mailbox ID
2. **FQTABLE**: Lists the free queues
3. **NODEMAP**: Displays the node to process mapping
4. **HELP**: Provides the user with the list and a brief description of all available commands at the EPUTIL level

76.3 Hardware Requirements or Dependencies

This increased limit of table C7TRKMEM can only be realized for Succession offices with Universal Signaling Platform is being used as SS7 network interface.

76.4 Software Requirements or Dependencies

None

76.5 Limitations and restrictions

76.5.1 ISUP 200K Ports Trunk Support

- Support of only 64k of trunks being transfered during upgrades in the states, INB, RES, or MB.
- When ISUP, PRI, DPT, and PTS ports are provisioned the total ports for the SSP can not be above 200,000 total trunk ports.

76.5.2 EPUTIL

- A maximum of 1024 messages can be captured by EPUTIL if the trace is turned on for all GWCs. In case the trace is turned on for specific nodes, then a maximum of 512 messages can be captured for each of the selected nodes.
- EPUTIL captures the messages at the input handler, and hence turning on the trace might have some real time impact. It is recommended that this tool be used at off-peak hours
- EPUTIL does not keep track of all the users that are logged into the tool simulaneously. Care should be taken when multiple users use this tool.

76.6 Interactions

None

76.7 Applicable customer facing sections

Fault Management

- Logs __NA__
- Alarms __NA__

Configuration

- Data Schema __NA__
- User Interface __NA__
- Element Management __NA__
- Security __NA__
- Service Order __NA__
- Office Parameters __NA__

Accounting (includes AMA billing) __NA__

Performance (includes operational measurements) __NA__

76.8 Glossary

Term	Description
USP	Universal Signaling Platform
CM	Central Module
GWC	Gateway Controller

77: Functional Functional Description (FN): A00003486

77.1 Feature name

A00003486 - Gateway location information

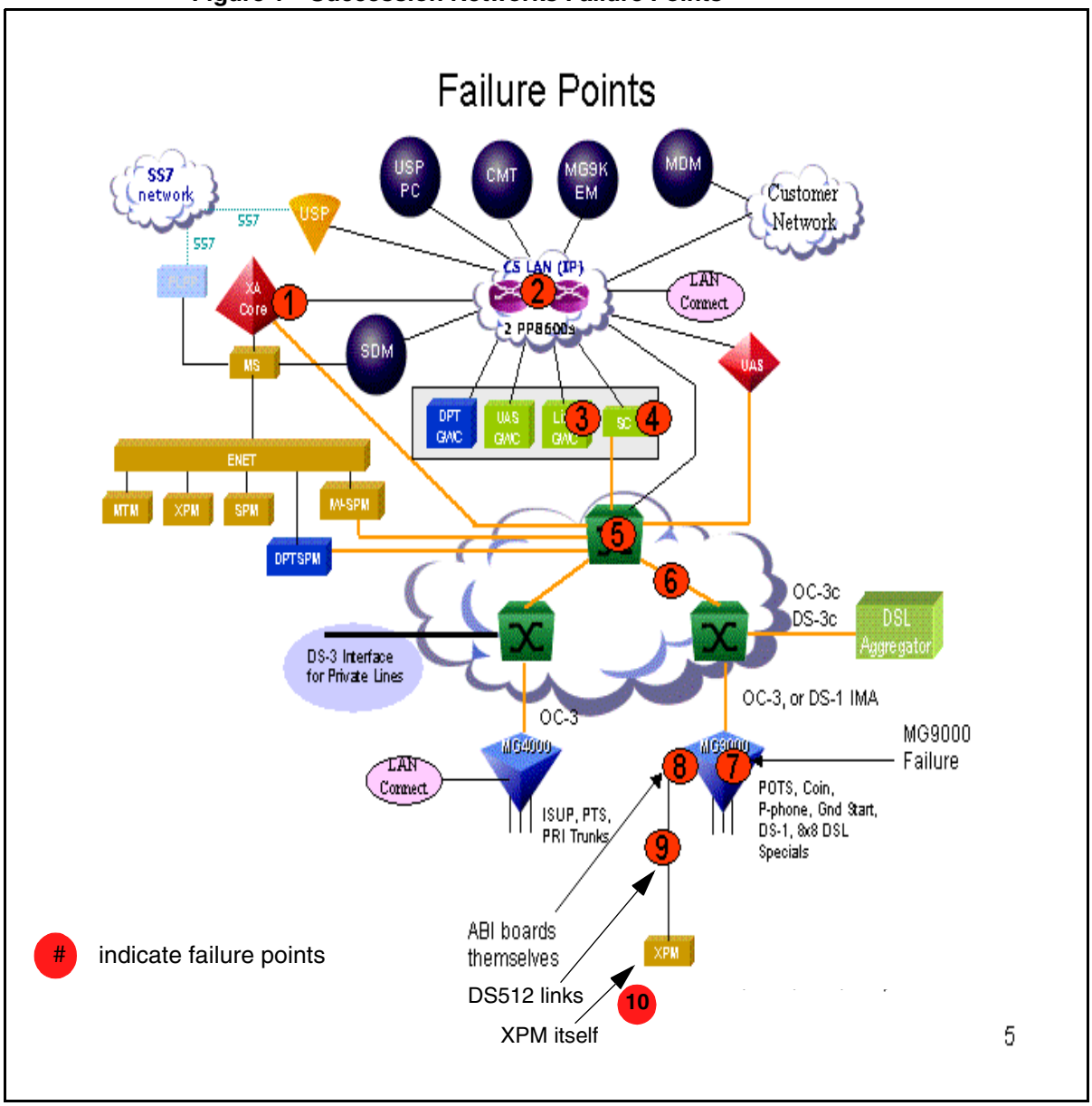
This Core feature is available in the SN07 release.

77.2 Description

The purpose of this feature is to provide physical location data for MG9K gateways which host only ABI XPMs to aid in the determination and ultimately the resolution of ABI XPM and line troubles on the Core where applicable.

Currently, these service impacting failures can occur in many different points in the Succession networks. Please refer to Figure 1 on page 697.

Figure 1 Succession Networks Failure Points



The ability to identify MG9Ks involved in the ABI configurations and their lines and their physical location was not easily determined.

This feature will aid in identifying the failure points detectable by the Core by providing necessary and accurate location data. Then using this newly provisioned data to correctly report and identify problem areas in the form of Logs, OMs, and Mapci commands.

In order to provide these new functionalities, the customer will see changes in the following areas:

- operation of Table LTCINV
- introduction of new Table GATWYINV
- display of the QueryPM command for ABI XPMs

77.2.1 Table LTCINV

The impact to this table consists of moving most of the ABI gateway information out of the EXTDS512 option and replacing it with a key to the ABI gateway information provisioned in table GATWYINV. For details on what/how this is provisioned, refer to the CN section of this feature.

77.2.2 Table GATWYINV

This is a new table on the Core designed to house gateway related information. The term gateway in this context has a flexible meaning. Gateway could refer to the physical gateway, where the hardware and call processing entity are the same. Gateway could also refer to a logical gateway, where the hardware contains many call processing entities each of which are considered a gateway. Therefore the meaning you choose depends on the construction of the "gateway".

For our more experienced DMS customers, provisioning of "gateways" in this table does not result in node creation, even though the name "INV" might suggest otherwise. Therefore the maintenance and management of the gateway is still performed from the Element Manager.

For details on what/how this table is provisioned, refer to the CN section of this feature.

77.2.3 ABI QueryPM

The impact to this command is a change in the amount of data displayed as a result of issuing the command. The command itself has not changed. For details on how this functionality has changed, refer to "Map Level: QUERYPM MAPCI command" in the CN section of this feature.

77.3 Hardware Requirements or Dependencies

There is no hardware dependencies required to execute this feature.

77.4 Software Requirements or Dependencies

This feature requires the Core load to be a Succession load. Specifically Succession release SN07 or later.

77.5 Limitations and restrictions

The new GATWYINV table will not have flow through provisioning in this release. There are plans to have flow through for this table in a future release.

For our more experienced DMS customers, provisioning of “gateways” in this table does not result in node creation, even though the name “INV” might suggest otherwise. Therefore the maintenance and management of the gateway is still performed from the Element Manager.

As is the current functionality today, flow through provisioning for this ABI Gateway and its corresponding location information is not available in this release. There are plans to have this ABI gateway data flow through in the future.

Although the new GATWYINV table is being designed for many different types of Gateways, for this initial SN07 release, only ABI gatways are allowed to be provisioned.

As is the currently functionality today of table LTCINV, the ability to change the hosting GWC once provisioned in the new GATWYINV table is not allowed.

77.6 Interactions

The following are the feature interactions for this feature:

- Features which this feature is dependant on:
  - — none
- Features which are dependent on this feature:
  - — A00004430 - ATM SVC ATM606 logs (Mike Domino)

    This feature possibly will need access to the Location information to format logs accurately.
- Features which have an interaction with this feature:
  - — A00003490 - Network Change and ABI XPM Migration (Kim Newnam)

    This feature plans to allow change to GWC host and ABI IP address data. This data will be moving to the new GATWYINV table and this functionality will have to be addressed from the new table.
  - — A00002380 - ABI ESA Logs (Diane Williford)

    This feature is possibly changing the Mapci levels for ABI. This may impact ABI QueryPM and ABI Link Mtc which is being impacted by this feature.

77.7 Applicable customer facing sections

Fault Management

- Logs ___n/a___
- Alarms ___n/a___

Configuration

- Data Schema ___X___
- User Interface ___X___
- Element Management ___n/a___
- Security ___n/a___
- Service Order ___n/a___
- Office Parameters ___n/a___

Accounting (includes AMA billing) ___n/a___

Performance (includes operational measurements) ___n/a___

77.8 Glossary

Term	Description
VMG	Virtual Media Gateway - this is a logical representation of a gateway.
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512. These XPMs are physically connected to MG9K Gateways via a DS512 interface.

78: Description (FN): A00003487

78.1 Feature name

Tri-modal provisioning - A00003487 in FMDOC library.

Note that this Functional Description covers all the SN07 Trimodal Call Server Features:

- a00003488: TriModal Call Signaling and Connectivity
- a00003662: TriModal Call Server Bridge Maintenance
- a00003509: TriModal Support for Lawful Intercept
- a00003947: TriModal Logs and OMs
- a00003948: TriModal GWC EM
- a00004046: TriModal ECAN support

78.2 Description

78.2.1 Existing Functionality

Prior to SN07, the CS2000 call server had very limited knowledge about the packet bearer network. Only a single packet bearer network was supported along with the legacy ENET bearer network. Individual agents were associated with a bearer network based upon the connectivity of the node that hosted the agent. For example, a trunk member that was assigned to a DTC would be associated with the legacy ENET bearer network. A trunk member that was assigned to either a GWC or an MG4K would be associated with the packet bearer network. Since both the GWC and the MG4K tag their hosted agents as ‘packet bearer network’, the core connectivity cannot distinguish between the various types of packet bearer networks are are available (i.e., IP, AAL1, AAL2). This is the basis for the CS2000 call server restriction that it can only support a single packet bearer network prior to SN07.

78.2.2 Feature Functionality

In the SN07 release, work is being started in the CS2000 Call Server to support multiple bearer networks. These bearer networks include both the legacy ENET bearer network and up to seven additional packet bearer networks.

In the SN07 release, a bearer network framework is implemented but full integration of all possible supported configurations will not be supported in this release. In SN07, the focus will be on supporting three bearer networks with full interworking between them[1]:

- ENET

- AAL1 packet network
- IP packet network

The main focus in SN07 is to support a Universal Access (UA)- AAL1 and a Universal Access (UA) - IP configuration with a single CS2000 Call Server. In addition, there are requirements to support some limited Carrier Hosted Services (CHS) functionality as well (i.e., H.323 and Media Call Server 5200 (MCS5200).

Interworking between the UA-AAL1 and UA-IP configurations in a multi-bearer network configuration is supported in SN07. However, interworking with the CHS agents is limited in SN07. In SN07, there is no support for interworking between the H.323 gateway (using a Media Portal) and the IP IW SPM. For this reason, a loop around trunk, hosted by a PVG on the CHS bearer network and hosted by a PVG in the UA IP bearer network or an MG4K in the UA AAL1 bearer network or an SPM/DTC in the ENET network, must be used to provide connectivity between the H.323 GW and all other agents on the CS2000 Call Server.

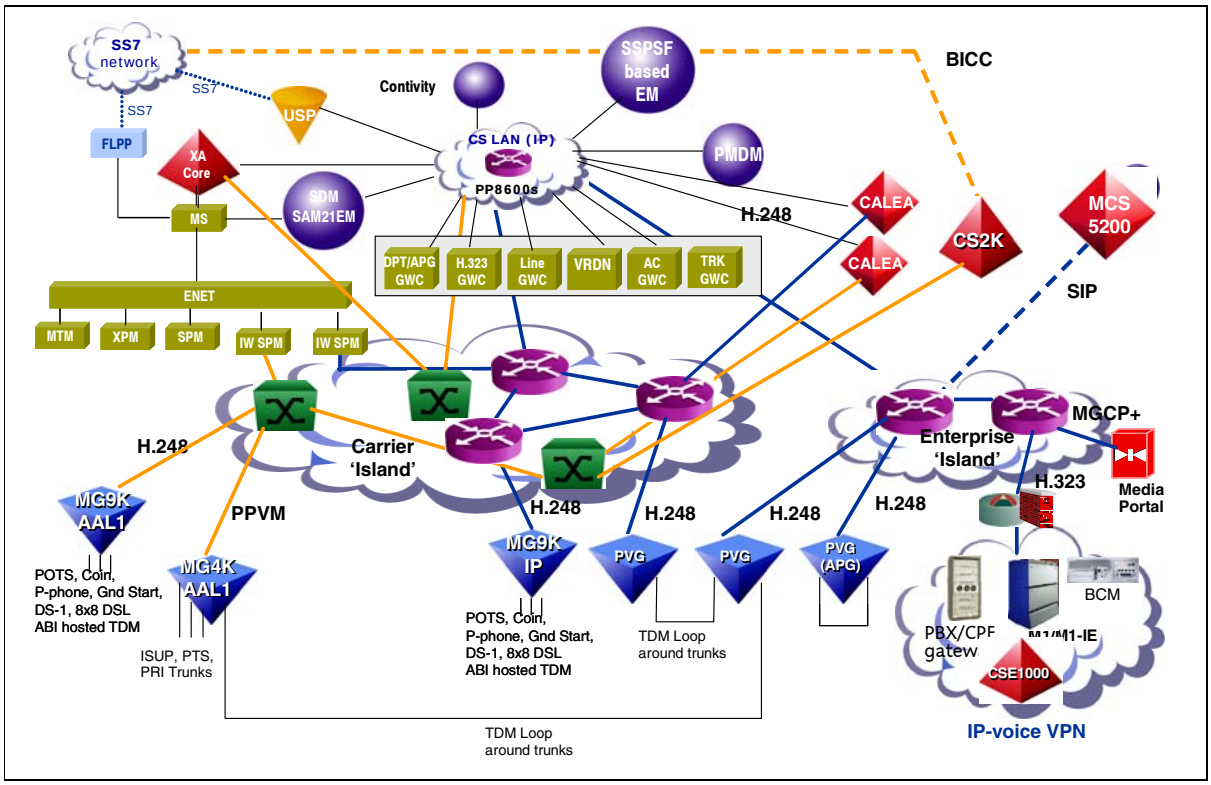
The following list provides a view of the limitations associated with H.323 calls in this configuration:

- Multiple billing records generated - A call from am H.323 agent to an MG9000 AAL1 native line would be represented as two calls in the CS2000 call server, each generating its own billing record.
- H.323 agent access to announcements - Since there is no announcements accessible to the CHS IP network (i.e., no IP IW bridge supported), announcements cannot be played to the H.323 agent. Any CS2000 Call Server services will not be able to use announcements and any treatments will have to be configured to ‘release with cause’ and the announcement would be provided by the enterprise bearer network.
- H.323 agent access to conferencing - Since there is no conference circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), conferencing services cannot be supported to the H.323 agent.
- H.323 agent access to test trunk facilities - Since there is no test trunk circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), trunk tests cannot be supported to the H.323 gateway.

A diagram of the network topology is shown in the following figure.

[1]AAL2 packet networks are not going to be tested in a multi-bearer network configuration, but there is nothing to block this type of bearer network from being configured.

Figure 1 SN07 supported multi-bearer network topology



In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Table 1 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	None[a]	supported SN07 legacy peripherals which includes both lines and trunk

Table 1 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC[b]	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
IP (CHS)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	GWC[c]	SIP-T DPT trunks
	H.323 GWs (Cisco, Westel, BCM, M1)	PRI trunks

a. There are no ‘gateways’ support on the ENET. However, there is a list of supported legacy peripherals for Succession Call Servers. This list remains unchanged by this feature.
b. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk.
c. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk.

Connectivity between the supported bearer networks is accomplished by using IW SPM bridges. The CS2000 Call Server is modified to allow support of both the ATM AAL1 based IW SPM and the IP based IW SPM at the same time. Prior to SN07, the CS2000 Call Server could only support one type of IW SPM. A single IW bridge pool was supported. In SN07, support for multiple bridge pools is introduced.

Control is given to the Succession customer to configure how the supported bearer networks in the CS2000 Call Server connect to each other. This is controlled by provisioning the types of interworking bridges needed to connect one bearer network to another. The interworking bridges available in SN07 are the following:

- IW SPM AAL1 - connects an AAL1 bearer network to the ENET
- IW SPM IP - connects an IP bearer network to the ENET

Prior to SN07, Succession configurations used the IW SPM AAL1 to connect an AAL1 bearer network to the ENET and used the IW SPM IP to connect an IP bearer network to the ENET. This is still supported in SN07 with multi-bearer network support. In this multi-bearer network configuration, a connection between an AAL1 bearer network and an IP bearer network will use two IW bridges (i.e., 1 IW SPM AAL1 and 1 IW SPM IP using the ENET to connect the two packet bearer networks). The following figures illustrate the connection topologies[1].

[1]Note that thesefigures are logical representations and are not meant to imply physical connectivity of the bearer networks.

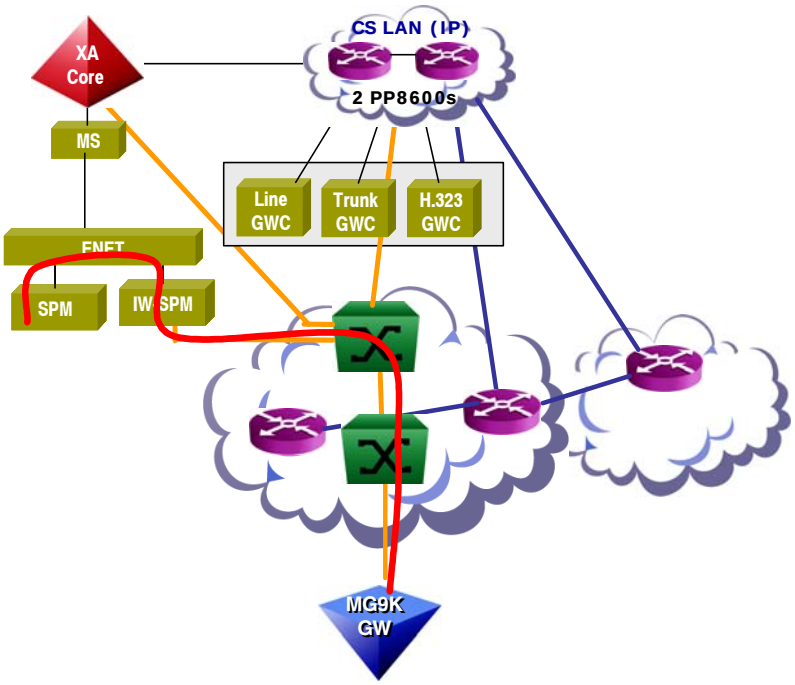


Figure 2 ATM AAL1 (UA) to ENET connection topology

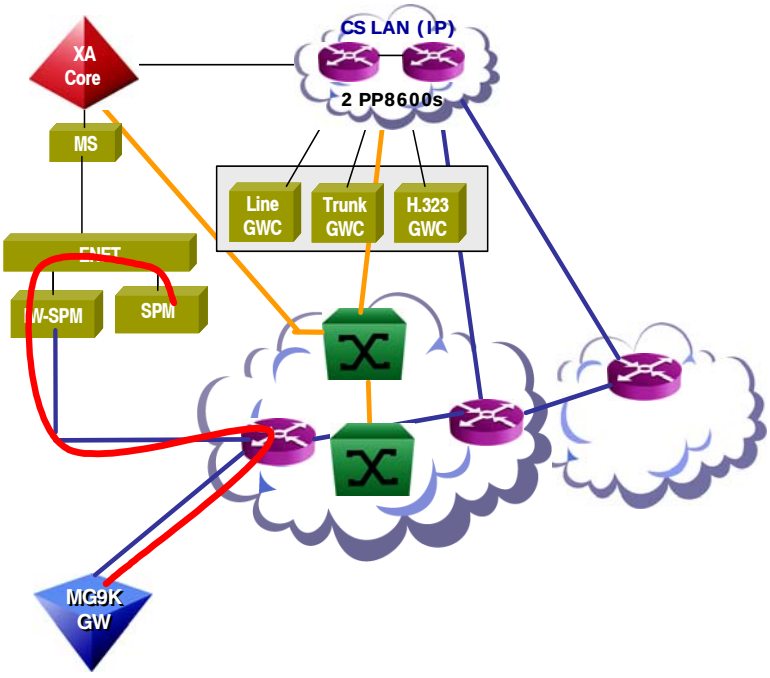


Figure 3 IP (UA) to ENET connection topology

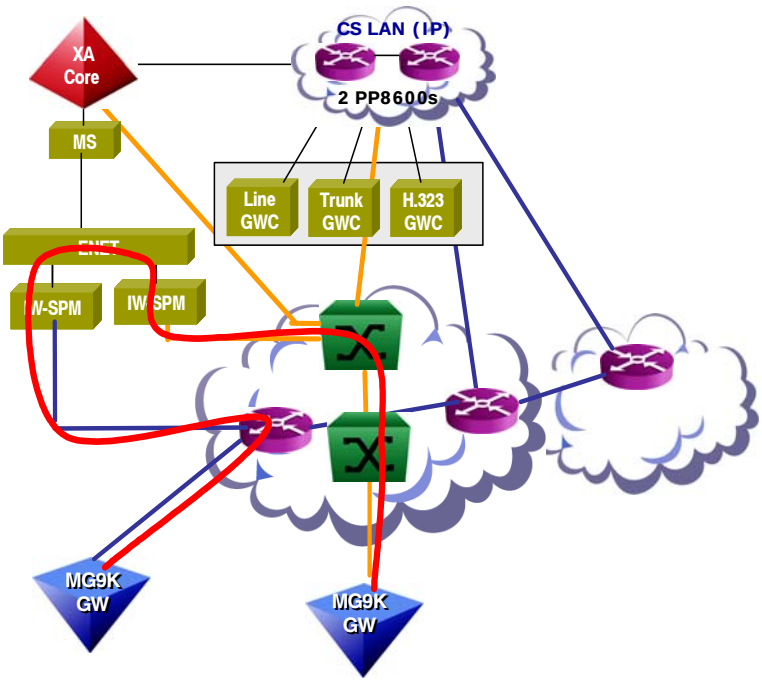


Figure 4 ATM AAL1 (UA) to IP (UA) connection topology

The following areas will be addressed in more detail in the following sections:

- Bearer network and connectivity provisioning
- Multiple bearer network support in the GWC EM
- Core connectivity connection management
- IW Bridge management
- OAMP changes on the CS2000 Call Server
- Lawful Intercept
- Service circuit support
- Groups with members in multiple bearer networks
- Trunk selection (like network selection)
- DPT (BICC and SIP-T) interworking including audible ringing support
- Translations and Routing changes
- USP messaging
- ECAN across multiple bearer networks
- Voice quality

- ONP
- Capacity

78.2.2.1 Bearer network and connectivity provisioning

The purpose of the provisioning changes are to allow bearer networks to be defined and associated to individual agents. Once this is accomplished, there are rules created that define which bearer networks can connect to each other and how that connection is accomplished.

When the CS2000 Call Server is requested to make a connection between two endpoints, it needs to know the bearer network associated with each endpoint. If this model were followed for provisioning, then each line and trunk member datafill would have to include an indication of the bearer network. This level of provisioning is cumbersome and very repetitive in most cases. For this reason, a hierarchical model is used in SN07. An assumption is made that a node (either an SPM node or a line/trunk GWC) supports one and only one bearer network. This allows the bearer network to be associated with the node and then this information is applicable to all the endpoints associated with that node. In other words, the bearer network for the endpoint is derived from the bearer network of the node that hosts the endpoint. Note that endpoints that are hosted on legacy peripherals which are then hosted on MG9000 ABI, will derive their bearer network from the GWC that hosts the MG9000 ABI.

There is one exception to the above behavior and it is in the area of DPT trunk support. Given the dynamic endpoint association that is made between the hosting node and the DPT trunk member, GWCs configured as DPT GWCs will not have an associated bearer network at the node level. The bearer network is associated with the DPT trunk group. The DPT endpoint obtains its associated bearer network from the DPT trunk group that is associated to it on a call-by-call basis.

The following provisioning changes are made by this activity:

- Bearer network definition
- Bearer network node association
- Bearer network DPT trunk group association
- IW bridge pool definition
- IW bridge pool assignment
- Bearer network connectivity

78.2.2.1.1 Bearer network definition A new table is introduced (Table BEARNETS) that defines the bearer network and the bearer fabric associated with this bearer network. The key to the table is a bearer network index. This index is needed to make it easy to change the bearer network name (i.e.,

without having to delete and re-add the entry). Index 0 is always reserved for the ENET tuple, if it exists.

The OPTIONS field in this table identifies an optional bearer network characteristics. In SN07, the following options are supported:

- Default packet network - specifies the default packet bearer network in the office. This is used during the ONP process as well as an endpoint bearer network designation if a node-based bearer network cannot be determined.

Table BEARNETS supports up to eight bearer networks in the CS2000 Call Server. Refer to the Configuration section for more details on Table BEARNETS.

Figure 5 Table BEARNETS example datafill

```
TABLE: BEARNETS
NETIDX BNETNAME     DISPLAY FABRIC OPTIONS
-----------------------------------------
NET 0  TDM_ENET     ENET    ENET   $
NET 1  NET_AAL1     ATM     AAL1   (PACKET_NETWORK_DEFAULT)$
NET 2  NET_IP       IP      IP     $
NET 3  NET_AAL2     AAL2    AAL2   $
```

78.2.2.1.2 Bearer network node association Association of the bearer network is done at the node level in the CS2000 Call Server. In order to minimize table changes and to provide minimal impact to DMS legacy offices, legacy peripheral nodes do not require an explicit association to the ‘ENET’ bearer network. This will be assumed in within the CS2000 Call Server.

However, any node that hosts packet bearer network endpoints requires that the bearer network be associated with the node. This is applicable to the following nodes:

- GWC (Table SERVRINV) - GWCs host many types of endpoints: lines and trunks)
- MG4K (Table MNNODE)
- DPT SPM (Table MNNODE)

Table SERVRINV is modified to include a new field BEARNETS. This field lists all the supported bearer networks associated with the GWC. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. This information is populated by the GWC Element Manager when a GWC is defined in SN07. Refer to the Configuration section for more details on Table SERVRINV.

Figure 6 Table SERVRINV example datafill

```
TABLE: SERVRINV
SERVRNAME SERVRADDR SERVREXEC SERVRTONE BEARNETS SERVROPTS
-----------------------------------------------------------
GWC 0     IP  47 192 48 24 (POTS POTSEX)  (KEYSET  KSETEX)  $
NORTHAA (NET_AAL1 Y) $ $
```

Table MNNODE is modified for ‘SMG4’ class of SPM’s (i.e., MG4Ks) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the MG4K. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Figure 7 Table MNNODE example datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM  1             SPM_1          SMG4   0   SYNC   LINE   50
(COT 60)  (DTMF 60)  (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT)  (MANB MJ RPT)  (ISTB MN RPT)  (SYSBNA CR RPT)(MANBNA MJ
RPT)  (COTLOW MN RPT)  (DTMFLOW MN RPT)(ECANLOW MN RPT)  (MFLOW
MN RPT)  (CMRLOW MN RPT)(TONESLOW MN RPT)  (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT)(ATMBCN CR RPT)  (STE3HLD MJ RPT)  (STE3HLD24
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  (SPMSRMNTD MN RPT)
(LOCUR MJ RPT)  (TMCFAIL CR RPT)  $ $  N  0  $  N  N  (NET_AAL1 Y) $
```

Table MNNODE is modified for ‘IW’ class of SPMs whose DPT_INFO indicates a DPT SPM (i.e., DPT SPMs) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the DPT SPM. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Figure 8 Table MNNODE example datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM 1   SPM_1   IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $ (SYSB CR RPT)  (MANB MJ RPT)  (ISTB MN RPT)
(SYSBNA CR RPT)(MANBNA MJ RPT)  (DTMFLOW MN RPT)  (ECANLOW MN RPT)
(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN CR RPT)(SMCHLD MF
RPT)  (SMCHLD24 CR RPT)  $ DPT_ONLY  (NET_AAL1 Y) $
(SPMECIDX 0)$
```

78.2.2.1.3 Bearer network DPT trunk group association DPT trunk groups require an association to the bearer network. Changes are made to

Table TRKOPTS where the DPT trunk groups are defined. As part of this change, it was decided to change the option used to indicate a DPT trunk group. The DPT application is removed from the DYNAMIC option. A new DPT option is created to define a DPT trunk group. This new option contains a field to designate the associated bearer network. Other application users for the DYNAMIC option remain unchanged. Refer to the Configuration section for more details on Table TRKOPTS.

Figure 9 Table TRKOPTS example datafill

```
TABLE: TRKOPTS
OPTKEY          OPTINFO
----------------------------------------
DPTTRK DPT      DPT BICC NET_AAL1 1
SIPTRK DPT      DPT SIPT NET_IP N MGC2 PROF MGCTWO Y
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC
```

78.2.2.1.4 IW bridge pool definition A framework is needed to allow multiple bridge pools to be defined in the CS2000 Call Server. This framework is intended to support any type of bridge that may be used to connect two bearer networks together.

In SN07, there is only one bridge type supported, the core-managed IW SPM bridge. In defining a bridge pool of this type, the two bearer networks that this bridge can connect together are specified. Other types of bridges may require additional information to be defined.

The bridge pool name is first defined in Table CLLI. Note that the number of members in the CLLI is not applicable to the bridge pool. New table NETBRDGE is created to define the bridge pool and its type. Refer to the Configuration section for more details on Table NETBRDGE.

Figure 10 Table CLLI and Table NETBRDGE example datafill

```
TABLE CLLI
CLLI          ADNUM   TRKGSIZ                    ADMININF
-----------------------------------------------------
ENET_TO_AAL1  321     0       ENET_TO_AAL1_BRIDGE_POOL
ENET_TO_IP    322     0       ENET_TO_IP_BRIDGE_POOL

TABLE: NETBRDGE
BRDGCLLI      TYPE        DISPLAY BEARNETS
-------------------------------------
ENET_TO_AAL1  CORE_BRDGE  E-A1    (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDGE  E-IP    (TDM_ENET NET_IP)   $
```

78.2.2.1.5 IW bridge pool assignment Once a bridge pool has been defined, the individual IW SPM bridge nodes needs to be associated with a bridge pool. Table MNNODE is modified for ‘IW’ class of SPM’s whose

DPT_INFO indicates an IW SPM (i.e., not a DPT SPM) to include a new field BRDGCLLI. This field lists all the supported bridge pools associated with the IW SPM. In SN07, only one entry for this field is supported. Refer to the Configuration section for more details on Table MNNODE.

Figure 11 Table MNNODE example datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-----------------------------------------------
SPM  1 SPM_1  IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $(SYSB CR RPT)  (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT)(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

78.2.2.1.6 Bearer network connectivity Now that the bearer networks have been defined and the bridge pools have been defined, the next step is to define the connectivity rules between the bearer networks. An assumption is made that a connection between two endpoints on the same bearer network will always be allowed to proceed. The rules being discussed here apply only to a connection request made between two endpoints that are associated with different bearer networks. These rules answer the following questions:

- Can a bearer network connect to another bearer network?
- What bridge pool or bridge pools are used to support a connection between two bearer networks?
- With trunk groups that support members in multiple bearer networks, what order, within trunk group member selection, should the bearer networks be attempted

Two new tables are created to allow the customer to provide answers to these questions. Table NETPATH provides a set of bridge pool combinations. These can be thought of as ‘connectivity routes’ and assist in answering the second question posed above. Note that it is possible to create a NETPATH entry that contains more than one bridge pool which would instruct connectivity to obtain multiple bridges for the connection. Note that this is also possible to create a NETPATH entry that conatins no bridge pools which would instruct connectivity to allow the connection to proceed with no bridgese needed.[1]

Table NET2NET allows the customer define which bearer networks connect to other bearer networks, the order that trunk group member selection uses and what ‘connectivity route’ should be used (i.e., points to an entry in Table NETPATH). If there are no connecting networks specified in Table NET2NET, then a connection request from that bearer network to any other bearer network

[1]The customer may use this option when there are two bearer networks that have the same fabric. No bridge is needed to connect the two bearer networks.

will be denied. Refer to “Trunk selection (like network selection)” on page 743 for more information on using the bearer network ordering in Table NET2NET.

Refer to the Configuration section for more information on Tables NETPATH and NET2NET.

Figure 12 Table NETPATH example datafill

```
TABLE: NETPATH
PATHIDX       NETBRDGE
----------------------------------------
  0           $
  1           (ENET_TO_AAL1)  $
  2           (ENET_TO_IP)    $
  3           (ENET_TO_AAL1) (ENET_TO_IP)$
```

Figure 13 Table NET2NET example datafill

```
TABLE: NET2NET
BNETNAME             CONNETS
-------------------------------------------------
  TDM_ENET         (NET_AAL1 1)    (NET_IP 2)    $
  NET_AAL1         (TDM_ENET1)     (NET_IP 3)    $
  NET_IP           (NET_AAL1 3)   (TDM_ENET 2)   $
```

78.2.2.2 Multiple bearer network support in the GWC EM

As described in the previous section, the bearer network needs to be associated with the GWC. New GWCs are added using the GWC Element Manager (EM). Information input using the GWC EM GUIs is then automatically updated in CS2000 Call Server tables (such as Table SERVRINV).

Prior to SN07, the GWC EM supported only one packet network. Characteristics about that packet bearer network were defined and associated with all the GWCs in the office.

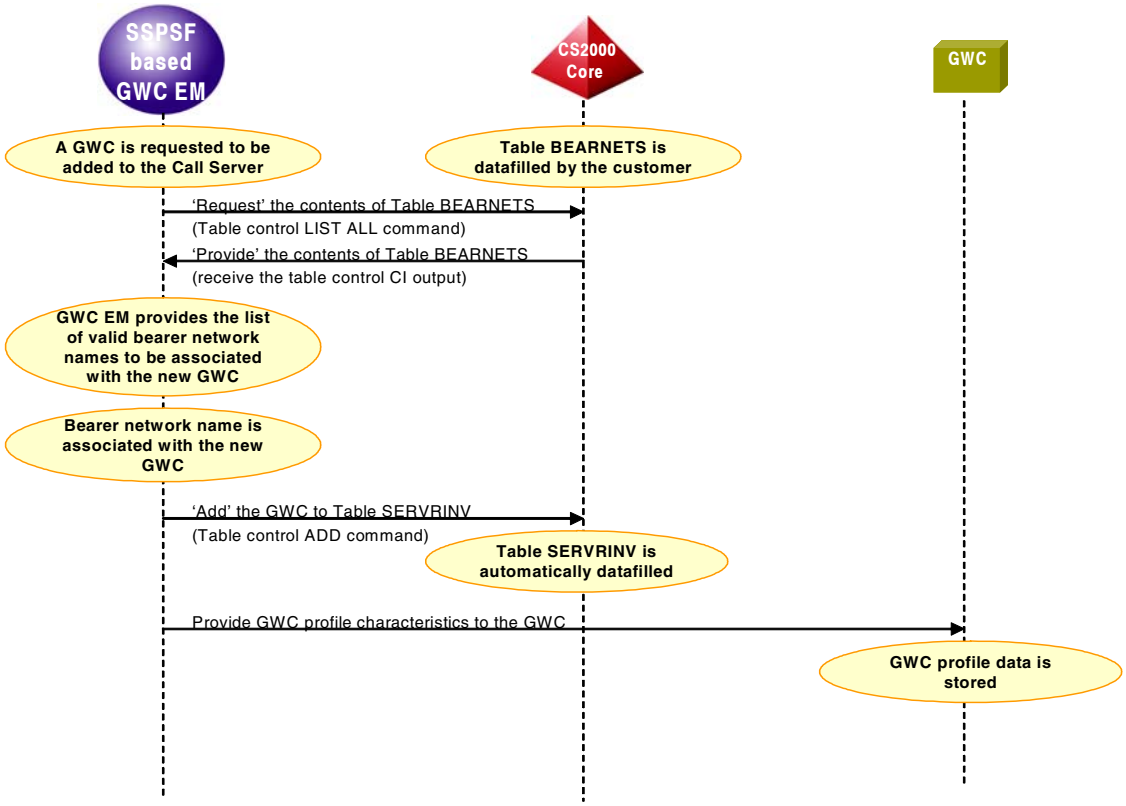
In SN07, changes are made to the GWC EM to support multiple bearer networks. These changes involve the following:

- Support the provisioning of multiple bearer network codec profiles.
  - — Display bearer network codec profile on GWC-EM GUI.
  - — Add bearer network codec profile from GWC-EM GUI.
  - — Delete bearer network codec profile from GWC-EM GUI.
  - — Change bearer network codec profile from GWC-EM GUI.

- Support the specification of a bearer network and a bearer network codec profile for each GWC.
  - — Display the bearer network and network codec profile of each GWC on GWC-EM GUI.
  - — Associate the bearer network and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
  - — Change the associated bearer network codec profile of one GWC node from GWC-EM GUI.
- Support population of the selected bearer network in the CS2000 Call Server table SERVRINV

The following figure illustrates the steps involved in flowing the data from the GWC EM to the CS2000 Call Server. Refer to the Configuration section for more information on the GWC EM GUI screens that are available in SN07.

Figure 14 GWC EM flow through provisioning for bearer network



78.2.2.3 Core connectivity connection management

Core connectivity is a function in the CS2000 Call Server that handles connection requests that are made from the CallP and Services applications. Prior to SN07, core connectivity processed requests to make a connection between endpoints. Endpoints were designated as being ‘internal’ (i.e., connected to the ENET) or ‘external’ (i.e., connected to the packet bearer network). Core connectivity knew that if a request was made to connect and ‘internal’ endpoint to an ‘external’ endpoint, then an IW bridge was needed. It would request a bridge from the office-wide IW bridge pool.

In SN07, core connectivity is changed to support multiple bearer networks and multiple bridge pools. Rather than making assumptions that a bridge from a bridge pool is needed to make a connection, core connectivity references tables NET2NET and NETPATH when a connection between two unlike bearer networks is requested. If these tables indicate that a connection should not be made, then core connectivity denies the connection request to the CallP application. The CallP application would then route the call to a Network Blocking (NBLH) treatment causing the call to not be completed.

The following figures provide examples on how core connectivity uses the datafill to process a connection request from the CallP application.

Figure 15 ATM AAL1 (UA) to ENET connection request

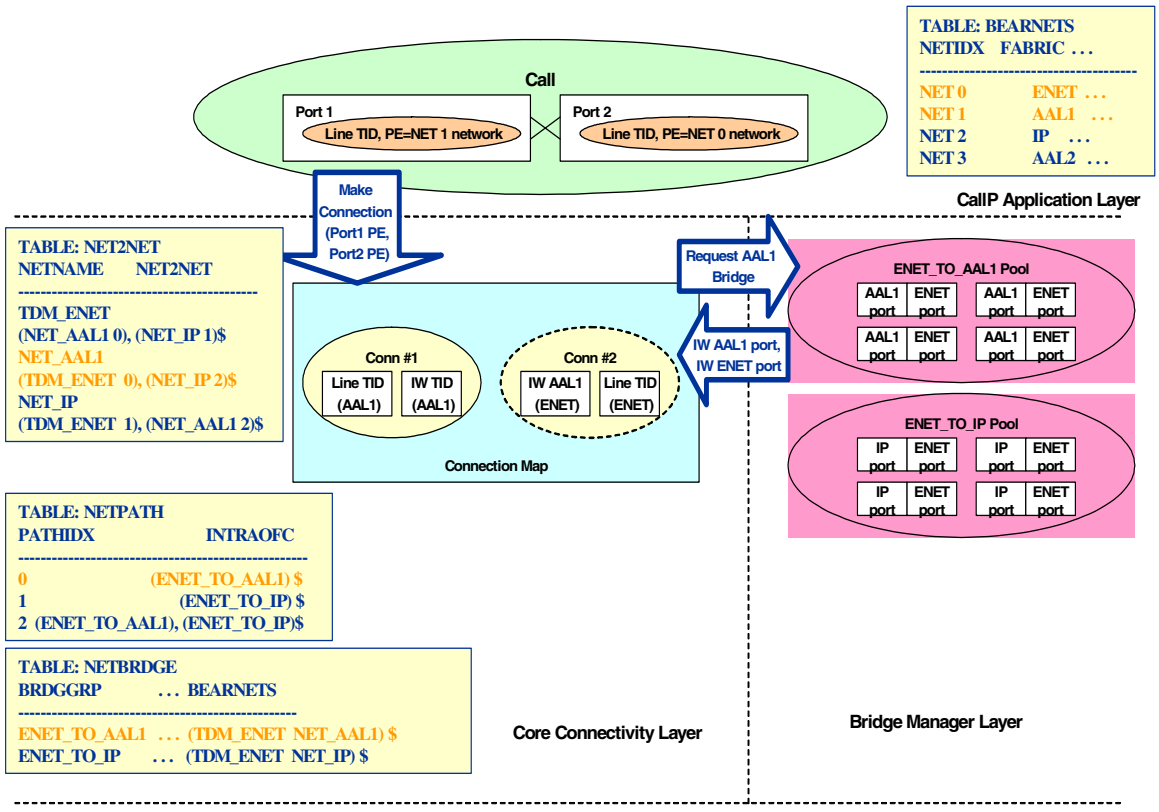


Figure 16 IP (UA) to ENET connection request

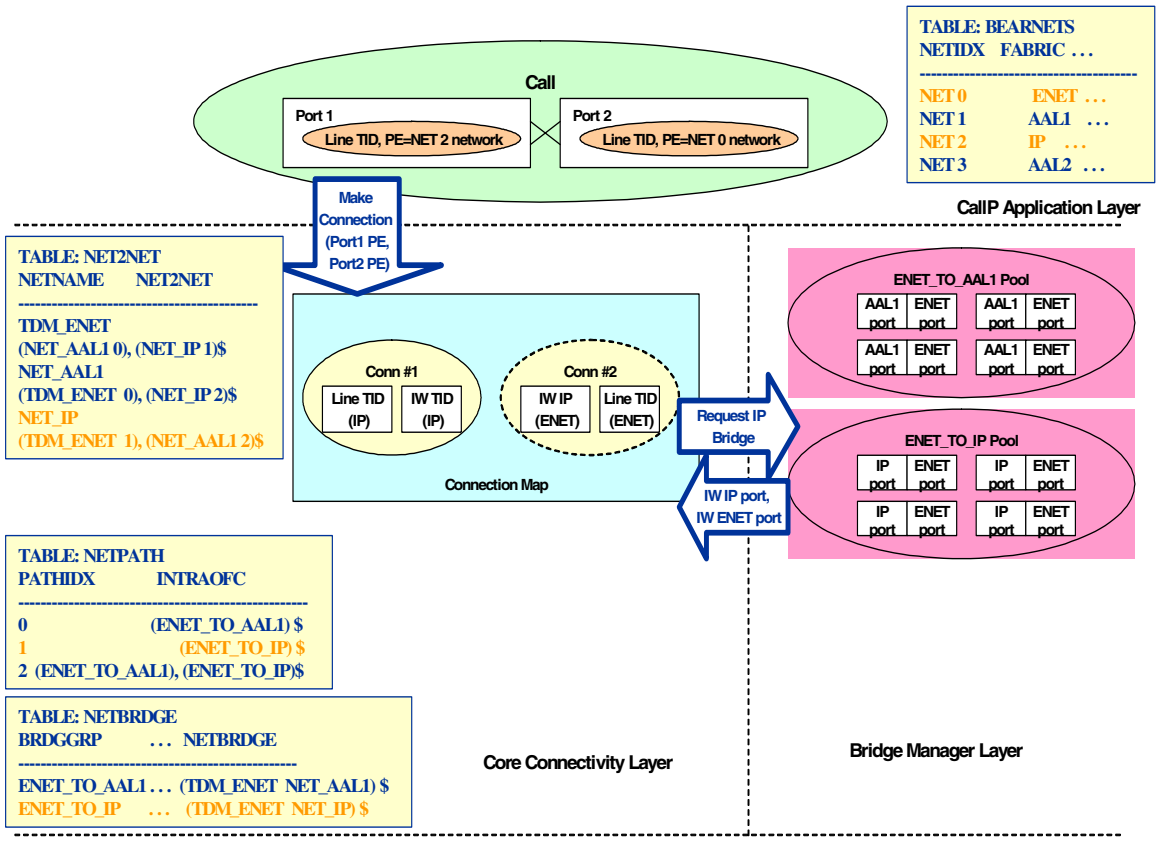


Figure 17 ATM AAL1 (UA) to IP (UA) connection request

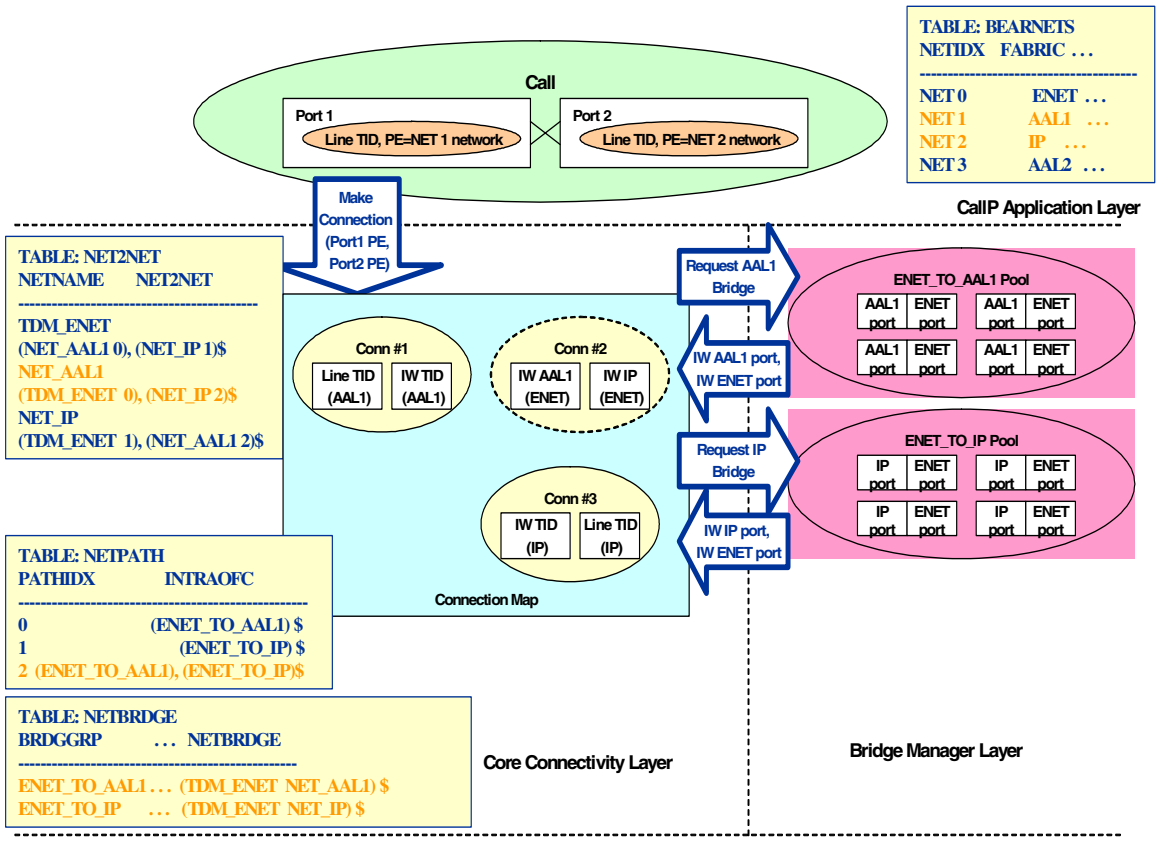
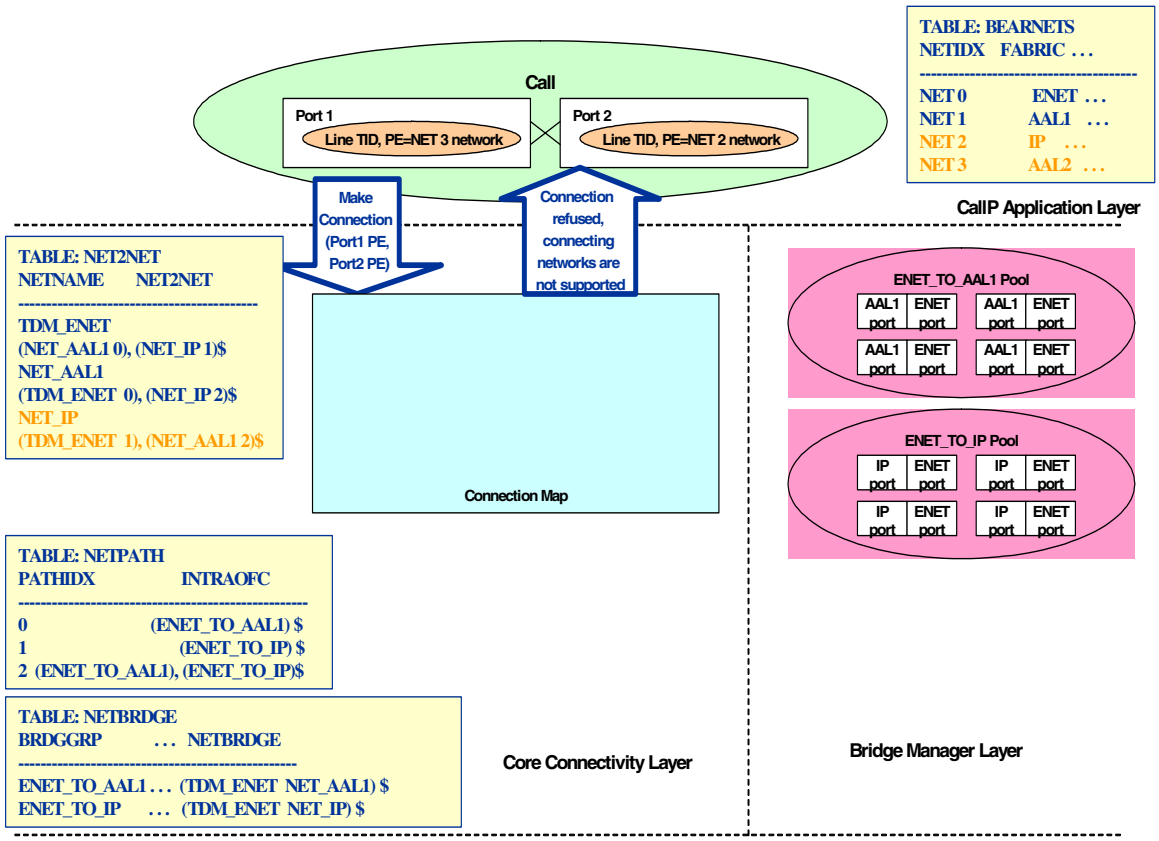


Figure 18 ATM AAL2 to IP (UA) connection request



Core connectivity supports a set of connection operations. All of the possible connection requests that the CallP application may request in support of the services supported on the CS2000 Call Server map to one of these connection operations.

- Make a connection
- Break a connection
- Hold a connection
- Restore a connection
- Move a connection

These connection operations can be performed multiple times on a single call depending upon the services that are invoked. Each time a connection operation is performed, the connectivity datafill is consulted to determine how the connection map should be modified. IW bridges may be added or removed to maintain the most optimized connection topology for the call.

The following is an example of a 3-way call. The originating line (A) is on the AAL1 bearer network. The first terminating line (B) is on the IP bearer network and the second terminating line (C) is on the ENET network.

Table 2 Example 3-way call

Step	Description	Connectivity Operation	Connection Map
1	'A' calls 'B'	Make connection	Connection 1 : active • 'A' endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 : active • 'B' endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 : active • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
2	'A' flashes and puts 'B' on hold	Hold connection	Connection 1 : held • 'A' endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 : held • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 : freed • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
3	'A' calls 'C'	Move connection	Connection 1 : active • 'A' endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 : held • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 4: active • Bridge #1 endpoint (ENET) • 'C' endpoint (ENET)

Table 2 Example 3-way call

Step	Description	Connectivity Operation	Connection Map
4	'A' flashes and connects to 'B' and 'C'. A conference circuit is obtained on the MTM.	Move connection	Connection 1 : active • 'A' endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 : active • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 4: freed • Bridge #1 endpoint (ENET) • 'C' endpoint (ENET) Connection 5: active • Bridge #1 endpoint (ENET) • CF3P(0) endpoint (ENET) Connection 6: active • Bridge #2 endpoint (ENET) • CF3P(1) endpoint (ENET) Connection 7: active • 'C' endpoint (ENET) • CF3P(2) endpoint (ENET)
5	All parties disconnect	Break connection	Connection 1 : freed • 'A' endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 : freed • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 5: freed • Bridge #1 endpoint (ENET) • CF3P(0) endpoint (ENET) Connection 6: freed • Bridge #2 endpoint (ENET) • CF3P(1) endpoint (ENET) Connection 7: freed • 'C' endpoint (ENET) • CF3P(2) endpoint (ENET)

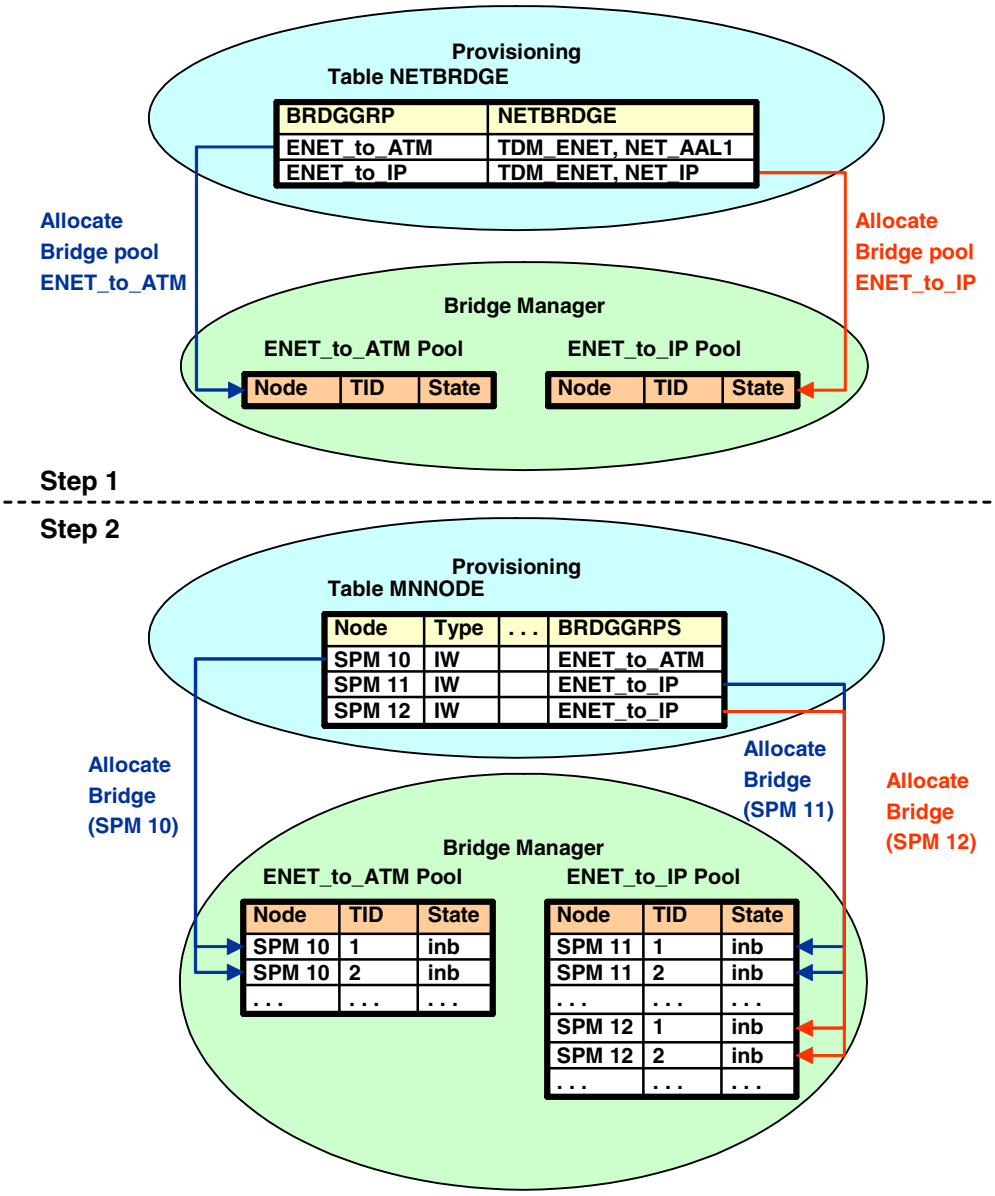
78.2.2.4 IW Bridge management

IW bridge management is a function in the CS2000 Call Server that manages the pool of IW SPM bridges. Prior to SN07, a single, office-wide pool of available IW bridges was managed by this utility. Each IW bridge node is composed of four groups of 504 bridge endpoints each. When an IW bridge node was provisioned in Table MNNODE, a set of four groups of 504

endpoints were added to the bridge pool. As the group of 504 endpoints was brought into service, these endpoints became available for Core Connectivity to use. The bridge manager function interfaced with maintenance and Core Connectivity to manage the set of available IW bridge endpoints in the office.

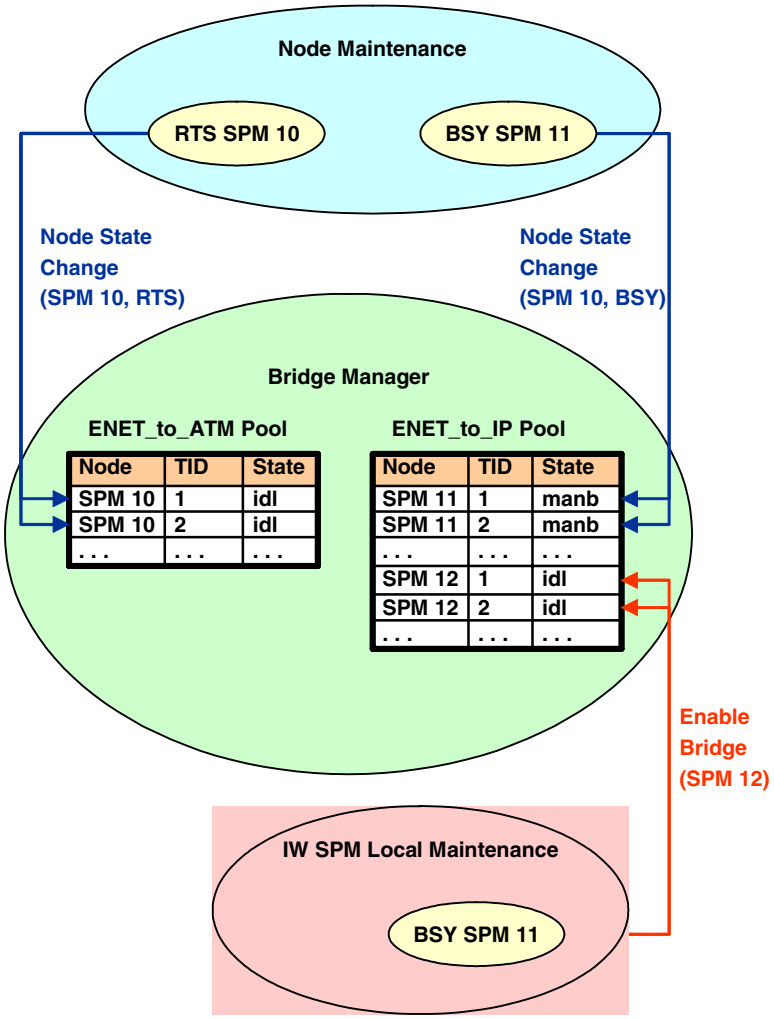
In SN07, the office-wide, single bridge pool is changed to support multiple bridge pools in a single CS2000 Call Server. A bridge pool is created when it is datafilled in Table NETBRDGE and the first IW SPM node is defined in that bridge pool in Table MNNODE. Additional individual IW bridge nodes are added (still in the 4 groups of 504 endpoints each) as they are provisioned in Table MNNODE against the newly created bridge pool.

Figure 19 IW bridge pool creation



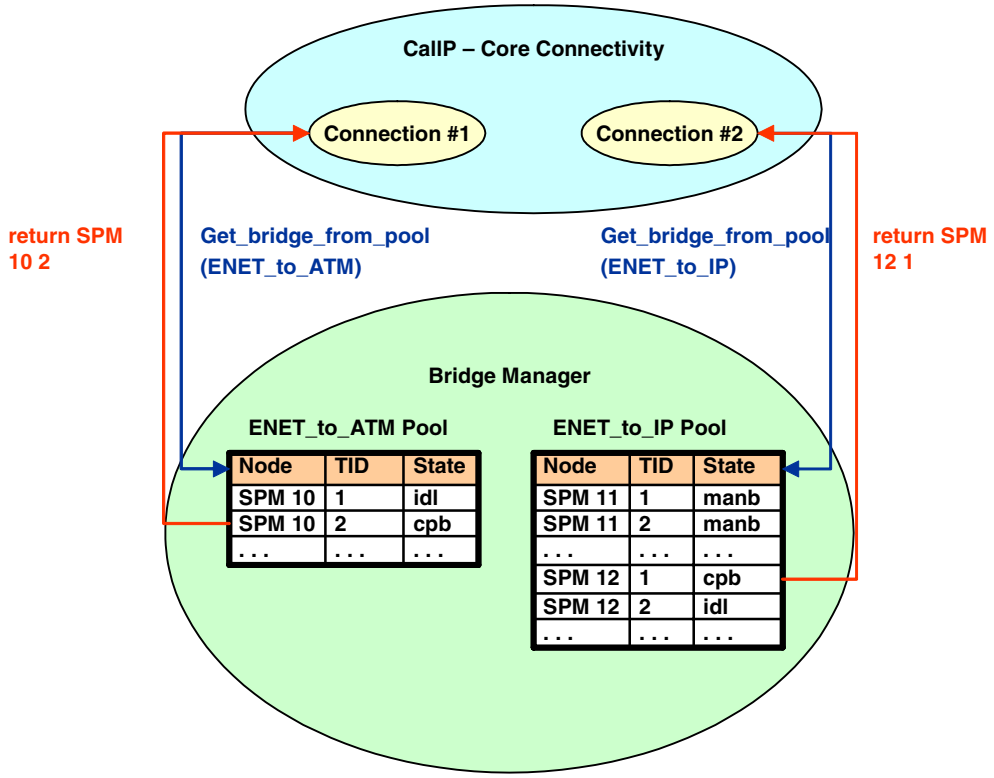
Once the bridge pools are created through provisioning, the individual IW bridge nodes are brought into service. This causes the nodes in the associated bridge pool to become available for use.

Figure 20 IW bridge maintenance



With idle IW bridge endpoints available in their associated bridge pools, the Bridge Manager can respond to requests from Core Connectivity to get a bridge. If more that one bridge is needed for a connection request, the Core Connectivity makes a request for each bridge needed.

Figure 21 IW bridge request



78.2.2.5 OAM changes on the CS2000 Call Server

OAM changes associated with the support of multiple bearer networks are limited in SN07. It is recognized that many additional requirements should be implemented and will be addressed in a future release.

In SN07, this feature does address the following areas:

- IW bridge OAM
- Trunk group OAM
- DPT OAM
- Office-wide usage OAM

Since many of these changes have impacts to customer OSSMINE interfaces, the activation of these changes is controlled by a new office parameter, MULTINET_DISPLAY_ACTIVE. Setting this parameter to ‘Y’ allows these changes to be visible. Setting this parameter to ‘N’ hides these changes. Note that this parameter does not impact the ability to support call connections between multiple bearer networks.

78.2.2.5.1 IW bridge OAM In SN07 with the support of multiple bridge pools, changes are made to the IWBM 800 series logs. These logs are

generated to monitor the usage thresholding of the bridge pools in the office. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then a new information line is output indicating the associated bridge pool that is causing the generation of the log. Refer to the Fault Management section of the document for more information.

Figure 22 IWBM 800 log example

```
RTP7  **  IWBM800 SEP17  12:16:55  6600  1st Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 70 percent of all bridges in the pool.
           Total number of IW bridges:  2016
           Number of available IW bridges: <NN>
           Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

In addition to the modified IWBM 800 logs, the existing OM group IWBM is modified to provide a set of registers for each bridge pool that is defined in Table NETBRDGE. In addition to the registers that were present in the OM group prior to SN07, additional call type usage registers are added. IWBM contains registers to monitor the following usage information:

- Number of attempts to get a bridge from the associated pool
- Number of failures to get a bridge from the associated pool
- Number of get bridge aborts from the associated pool
- Number of attempts to free a bridge from the associated pool
- Number of failures to free a bridge from the associated pool
- Number of free bridge aborts from the associated pool
- Indicates when the number of 'in use' bridges exceeds 70% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges exceeds 90% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges falls below 65% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges falls below 85% of the total bridges in the associated pool
- Number of times a bridge from the associated pool was used to connect to a test facility
- Number of times a bridge from the associated pool was used to connect to an announcement or conference facility

Refer to the Performance Management section of the document for more details.

Note that the value of MULTINET_DISPLAY_ACTIVE office parameter does not impact the availability of this OM group. It is always available in SN07.

78.2.2.5.2 Trunk group OAM With support for multiple bearer networks, a trunk group can be configured to have members is multiple bearer networks. The existing TRK and TRNK2 OM groups only provide data on a per trunk group basis. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then new OM groups (TRK2NET1 and TRK2NET2) are created to provide a per trunk group and per bearer network view of the trunk group usage.

OM group TRK2NET1 contains the same set of registers that existing OM group TRK contains. It contains registers to monitor the following usage information:

- Automatic congestion control
- Invalid or no automatic number identification (ANI)
- Number of calls answered
- Automatic number identification (ANI) office failure
- Number of successful connections
- Network management reroutes
- Glare
- Answer messages sent and received on incoming trunks
- Answer messages sent and received usage on incoming trunks
- Total incoming attempts
- Incoming failures
- Invalid authorization code
- Maintenance busy usage
- Maximum busy circuits
- Total outgoing attempts
- No answer on trunk (timed out)
- Number of overflows, all trunks busy
- Answer messages sent and received on outgoing trunks
- Outgoing failures
- Outgoing matching failures

- Pre-route abandons
- System busy usage
- Number of tandem calls
- Total usage
- Traffic busy usage

Figure 23 TRK2NET1 OM group example

```
>omshow trk2net1 active
TRK2NET1
CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;  FASTSAMPLES:          29 ;
   KEY (COMMON_LANUAGE_NAME_BEARNETS)
   INFO (OM2TRKINFO)
       INCAATT   PRERTEA1    NINFAIL     NATMPT
       NVFLATB     GLARE1      OUTFL    CADEFLD
       TRFCU      SBSYU      MBSYU   TRKNWBLK
       CNCTAT    TNDMATT   ANIOFCFL       NANF
       TOTBSYU    NANSWER  INVATHCD     MAXBSY
       NACCCNG    NOANSWR
100   TRK_TO_A NET 0 TDM_ENET 2W    0      0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0
100   TRK_TO_A NET 1 NET_AAL1 2W    0      0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0
100   TRK_TO_A NET 2 NET_IP 2W    0      0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0
```

OM group TRK2NET2 contains the same set of registers that existing OM group TRNK2 contains. It contains registers to monitor the following usage information:

- Number of calls answered (extension from TRK2NET1)
- Number of successful connections (extension from TRK2NET1)
- Network management reroutes (extension from TRK2NET1)
- Total incoming attempts (extension from TRK2NET1)
- Total outgoing attempts (extension from TRK2NET1)
- System busy usage (extension from TRK2NET1)
- Number of tandem calls (extension from TRK2NET1)
- Total usage (extension from TRK2NET1)
- Traffic busy usage (extension from TRK2NET1)

Figure 24 TRK2NET2 OM Group Display

```
>omshow trk2net2 active

TRK2NET2

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   KEY (TRK2NET_KEY)
   INFO (OM2TRKINFO)
            INCAATT2        NATMPT2        CADEFLD2       TRFCU2
            SBSYU2          CNCTAT2        TNDMATT2       TOTBSYU2
            NANSWER2

100   TRK_TO_A      NET 0 TDM_ENET 2W    0      0
            0               0               0               0
            0               0               0               0
            0

100   TRK_TO_A      NET 1 NET_AAL1 2W    0      0
            0               0               0               0
            0               0               0               0
            0

100   TRK_TO_A      NET 2 NET_IP 2W      0      0
            0               0               0               0
            0               0               0               0
            0
```

78.2.2.5.3 DPT OAM In providing support for multiple bearer networks, a requirement to support both BICC and SIP-T DPT protocols in the same office was also requested. Prior to SN07, the DPT OM groups did not indicate the associated DPT protocol.

In SN07, when office parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’, then the following changes are made:

- Provide an office-wide, per-protocol DPT performance summary

- Provide a per-DPT node, per-protocol DPT performance summary

A new OM group (DPTOFCP) is created to provide an office-wide, per-DPT protocol performance summary. This group is modeled after the DPTOFC OM group and contains the same set of registers. Two DPT protocols are supported: BICC and SIP-T. The following registers are included per protocol:

- Get DPT terminal attempts
- Get DPT terminal failures
- Get DPT optimized terminal failures
- DPT terminal usage
- DPT terminal usage high water mark
- DPT port depletion

Figure 25 DPTOFCP OM group example

```
>omshow dptofcp active

DPTOFCP

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PROTOCOL_INFO)
            DPGTATT       DPGTATT2      DPGETFL       DPGETFL2
            DPUSAGE       DPUSAGE2      DPOTFLO       DPOTFLO2
            DPHWTR        DPHWTR2       DPRTDPL       DPRTDPL2

0
   BICC
            0             0             0             0
            0             0             0             0
            0             0             0             0

1
   SIPT
            0             0             0             0
            0             0             0             0
            0             0             0             0
```

Changes are made to the existing DPTNODE OM group. This OM group provides a per-DPT node performance summary. In SN07, each DPT node can only support one DPT protocol. For example, a DPT capable MG4K node can only support BICC. DPT GWC nodes can support either BICC or SIP-T but not at the same time. When MULTINET_DISPLAY_ACTIVE is set to 'Y', additional information is added to the DPTNODE OM group to display the following additional information:

- DPT protocol
- For SPM-type nodes, the associated bearer network and SPM node type are also displayed[1]

[1]DPT GWCs are considered bearer independent, so the associated bearer network is not included for DPT GWCs.

Figure 26 DPTNODE OM group example

```
>omshow dptnode active

DPTNODE

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PM_INFO)
            DPTGTAT        DPTGTAT2       DPTGTFL        DPTGTFLO
            DPTUSAG        DPTUSAG2       DPTHWT

0
   GWC  3    93 BICC
            0                 0              0              0
            0                 0              0

1
   GWC   4   94 SIPT
            0                 0              0              0
            0                 0              0

2
   SPM    1   70 NET 2 NET_AAL1 BICC SMG4
            0                 0              0              0
            0                 0              0
3
   SPM    2   71 NET 0 ENET_TO_AAL1_DPT   BICC      DPT
            0                 0              0              0
            0                 0              0
```

78.2.2.5.4 Office-wide usage OAM With support for multiple bearer networks, it is a requirement to be able to monitor the performance of the traffic over each bearer network. The existing OFZ and OFZ2 OM groups only provide an office-wide view. When office parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’, then new OM groups (OFZ2NET1 and OFZ2NET2) are created to provide a per bearer network view of office traffic.

OM group OFZ2NET1 contains the same set of registers that existing OM group OFZ contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- Incoming trunk subscriber abandoned calls
- Incoming trunk switch abandoned calls
- Incoming trunk calls routed to an announcement
- Incoming trunk calls routed to a tone
- Incoming trunk calls to lock-out
- Incoming trunk calls to outgoing trunk calls
- Incoming trunk calls to terminating line calls
- Lines manual busy
- Number of incoming trunk calls
- Number of originating line calls
- Originating line switch abandoned calls
- Originating line calls routed to an announcement
- Originating line calls to lock-out
- Originating line calls to outgoing trunk calls
- Originating line calls routed to a tone
- Originating line calls to terminating line calls
- Outgoing trunk match failures
- Outgoing trunk network attempts
- Outgoing trunk original seize failures
- Outgoing trunk retrial match failures
- Outgoing trunk retrial seize failures
- Terminating line blocked
- Terminating line match failures
- Terminating line network attempts

Figure 27 OFZ2NET1 OM group example

```
>omshow ofz2net1 active
OFZ2NET1
CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;
   INFO (BEARNETS_INFO)
          ICANN          ICLKT          NICOG          NICOG2
          ICTONE         TRKORIG        TRKORIG2       OGNWAT
          OGNWAT2        OGTMFL         OGTRMFL        OGOSF
          OGROSF         ICABNM         ICABNC         LINEANN
          LINELKT        LINEOG         LINEOG2        LINETRM
          LINETRM2       LINETONE       LINEUSG        LINEUSG2
          ICTRM          ICTRM2         TRMLNAT        TRMLNAT2
          TRMMCHFL       TRMBLCK        LNMBSYPC       LINEABDN
0
     NET 0 TDM_ENET
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
1
     NET 1 NET_AAL1
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
2
     NET 2 NET_IP
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
```

OM group OFZ2NET2 contains the same set of registers that existing OM group OFZ2 contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- No circuits available on business network trunks
- No circuits available on inward dial trunks
- No circuits available on intermachine trunks
- No circuits available on intertoll trunks
- No circuits available on local tandem trunks
- No circuits available on offnet trunks
- No circuits available on connect trunks
- No circuits available on toll completing trunks
- No circuits available on circuit trunks
- No circuits available on all other trunks
- Calls routed to GNCT treatment
- Switch originated partial dial calls
- Switch originated calls to permanent signal treatment

Figure 28 OFZ2NET2 OM group example

```
>omshow ofz2net2 active
OFZ2NET2

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (BEARNETS_INFO)
            NCKTIT          NCKTTC          NCKTLT          NCKTBN
            NCKTID          NCKTOSC         NCKTOT          NCKTRT
            NCKTIM          NCKTON          NCKTOF          MDPSIG
            MDPD            DPTRC           DPTRC2

0
NET 0 TDM_ENET
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
1
NET 1 NET_AAL1
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
2
NET 2 NET_IP
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
```

78.2.2.6 Lawful Intercept

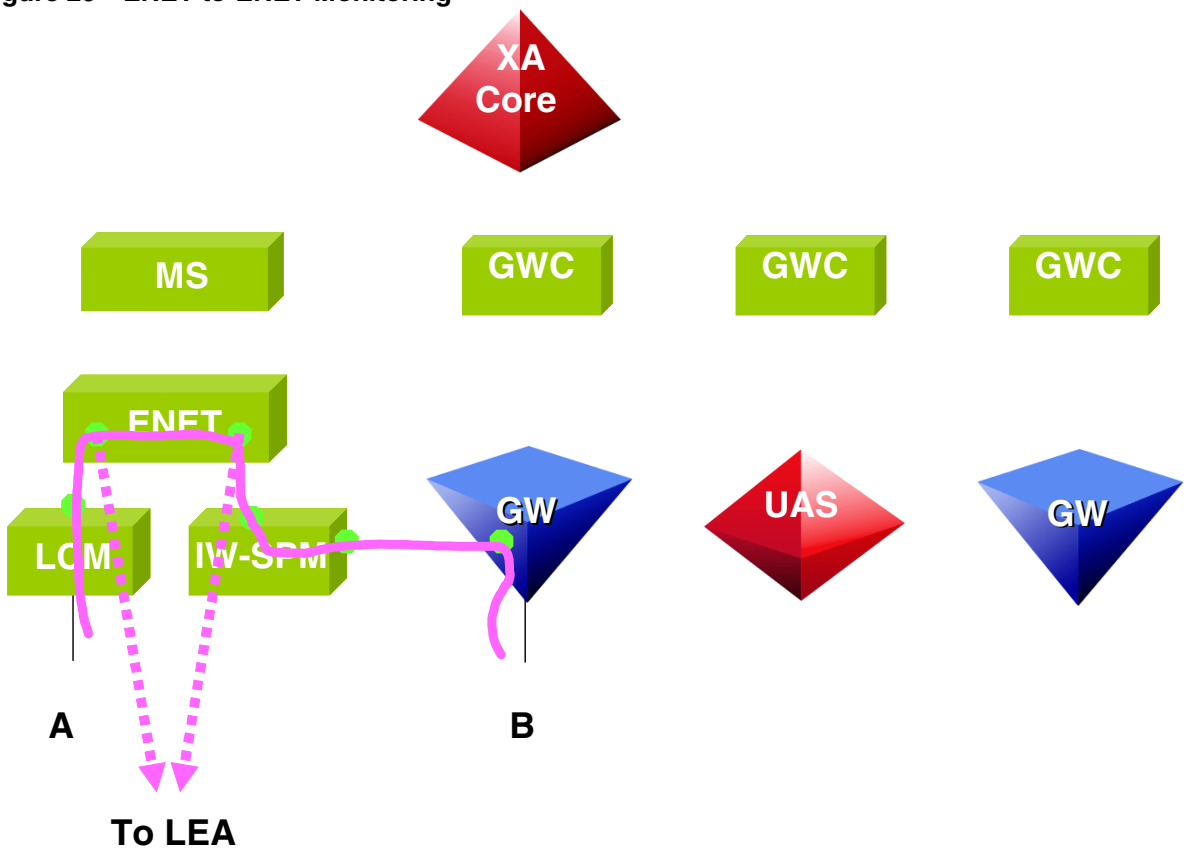
Lawful Interception is the ability to perform call monitoring on selected agents. Call monitoring includes:

- Call Data monitoring - reporting details about monitored calls (e.g. time of the call, dialled digits, parties involved, etc.)
- Call Content monitoring - delivery of both sides of a monitored conversation to law enforcement

With support for multiple bearer network in a single CS2000 Call Server, lawful intercept must provide the ability to do Call Content monitoring on all required call types and all supported bearer connections. Previous to SN07, Call content monitoring was supported for the following call types:

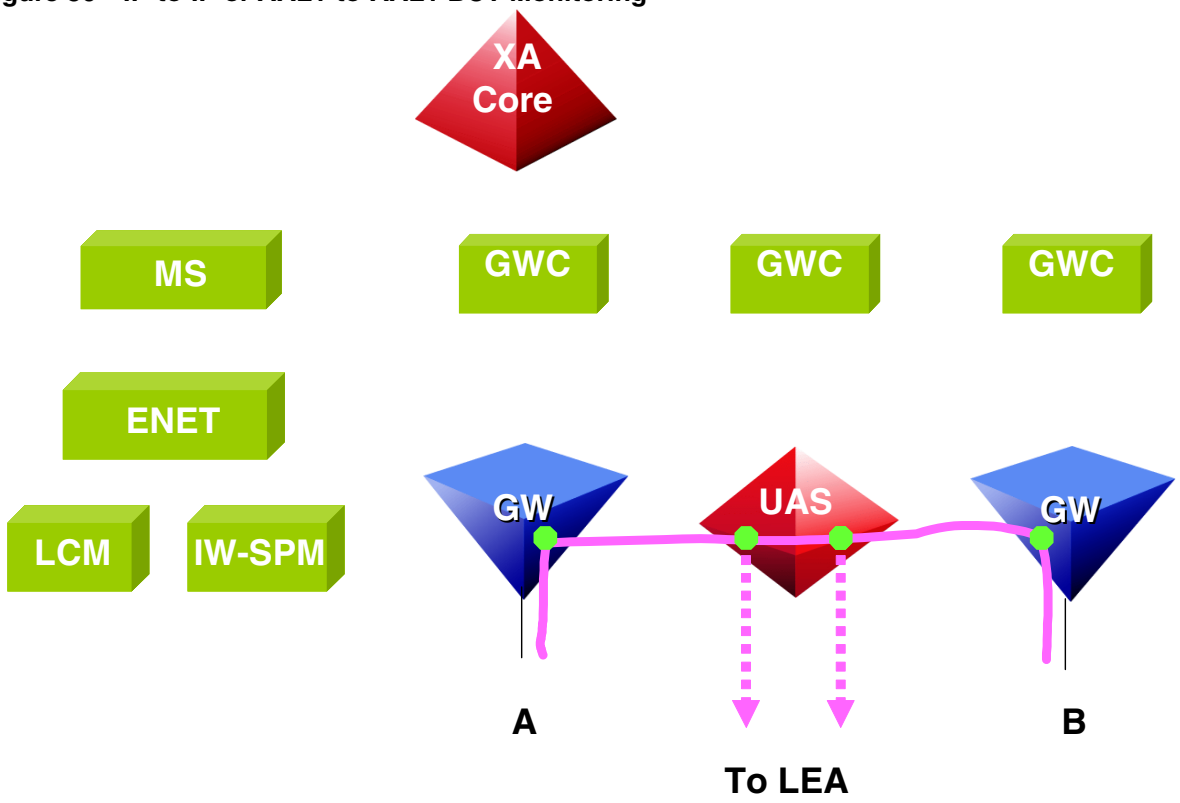
- ENET-to-ENET: replicas are attached to the primary ENET pathends which broadcast the transmit of each endpoint (legacy monitoring)

Figure 29 ENET-to-ENET Monitoring



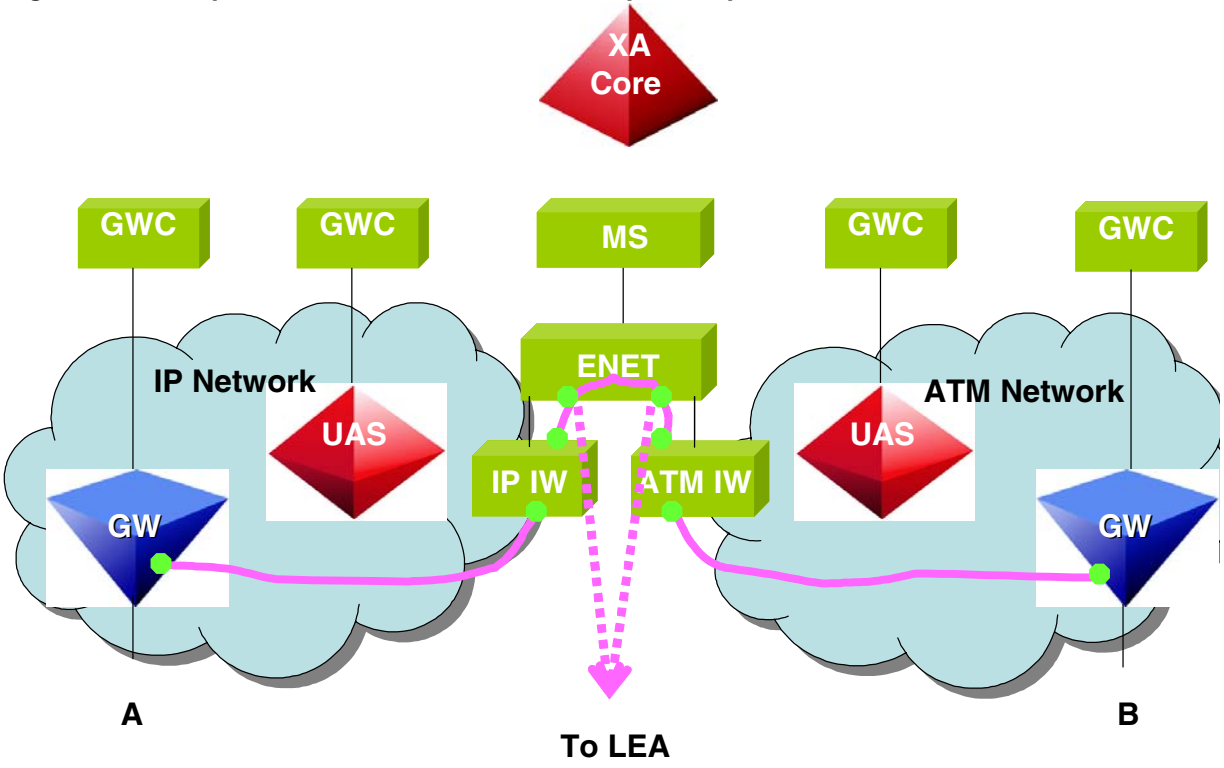
- IP-to-IP: primary call is tandemed through a Centralized Replicator (CR) to which replicas are attached. This functionality is known as Bearer Channel Tandeming (BCT).
- AAL1-to-AAL1: when BCT is active, the same strategy is used as in IP-to-IP calls. If not, then broadcast connections are attempted. This works for Packet Trunking - AAL1 solutions where the only AAL1-to-AAL1 calls involve MG4Ks which support broadcast connections.

Figure 30 IP-to-IP or AAL1-to-AAL1 BCT Monitoring



In SN07, there are no impacts to the replication models that are used to lawful intercept. Since the connection model for supporting a packet bearer network 1 to packet bearer network 2 connection involves using 2 IW SPM bridges, lawful intercept will used the ENET-to-ENET model to perform replication. Also, there is no impact to the connections made to the Law Enforcement Agency (LEA). A single interface is supported for all the replication methods. Refer to the following figure for an example connection with lawful intercept.

Figure 31 Multiple bearer network lawful intercept example



In summary, this means that in a CS2000 Call Server that supports three bearer networks (ENET, AAL1 and IP), that the following replication points will be used:

- ENET
  - — for ENET-to-ENET calls
  - — for AAL1-to-IP calls
  - — for ENET-to-AAL1 calls
  - — for ENET-to-IP calls
- UAS IP
  - — for IP-to-IP calls
- UAS AAL1
  - — for AAL1-to-AAL1 calls[1]

78.2.2.7 Service circuit support

Service circuits include specialized components needed to support the following:

- Announcements

[1]If the call involves only 2 MG4Ks, then the UAS is not needed (MG4Ks can broadcast the bearer path). But if an MG9K is involved, then the UAS is required.

- Conferencing
- Line and trunk test facilities

Each Succession configuration provides support for these service circuits in different ways. The following table provides a view of how these components are supported prior to SN07.

Table 3 Pre-SN07 service circuit support

Succession Configuration	Service Circuit Type	Service Circuit Support
PT-AAL1	announcements	ENET-based MTM
	conferencing	ENET-based MTM
	line/trunk test facilities	ENET-based MTM
UA-AAL1	announcements	ENET-based MTM
	conferencing	ENET-based MTM
	line/trunk test facilities	ENET-based MTM
PT-IP (XA Core)	announcements	ENET-based MTM and/or UAS (IP)[a]
	conferencing	ENET-based MTM and/or UAS (IP)[b]
	line/trunk test facilities	ENET-based MTM
PT-IP (CS2Kc)	announcements	UAS (IP or AAL2)
	conferencing	UAS (IP or AAL2)
	line/trunk test facilities	UAS (IP or AAL2) with Sage box
UA-IP (XA Core)	announcements	ENET-based MTM and/or UAS (IP)
	conferencing	ENET-based MTM and/or UAS (IP)
	line/trunk test facilities	ENET-based MTM
UA -IP (CS2Kc)	announcements	UAS (IP)
	conferencing	UAS (IP)
	trunk test facilities	UAS with Sage box
	line test facilities	AccessCare

a. Directed terminations for announcements is used if both platforms are present. ENET originating agents use the announcements on the MTM and IP originated agents use announcements on the UAS.

b. Directed terminations for conferencing is used if both platforms are present. ENET requesting agents use the conference ports on the MTM and IP requesting agents use conference ports on the UAS.

In SN07, in order to support multiple bearer networks and multiple service circuit platforms, then the directer terminations function would have to be changed to take into account multiple packet bearer networks. This work is not being done in SN07. This means that only a single platform for providing announcements, conferencing and test facilities is supported in a multple packet bearer network configuration. Since full service circuit functionality is provided when using the MTM as the platform, this is the configuration that is supported. This means that all packet bearer networks must allow connectivity to the ENET network in order to obtain announcements, conference ports and test facilities. If this network connectivity is not in place, then services that requires these facilities will fail.

78.2.2.8 Groups with members in multiple bearer networks

The CS2000 Call Server maintains line group types and trunk group types. These groups are comprised of individual members. Here are some examples of these groups:

- Centrex customer group
- Hunt group
- MADN group
- Trunk group

There is no restriction in place to require that all the members of the line group types be assocaited with a single bearer network. For example, a hunt group can can members in all supported bearer networks. There are connectivity implications to consider in the case. In order to ensure seemless group functionality among all its members, then the associated bearer networks must be able to connect to each other (i.e., Table NET2NET must indicate connectivity between the bearer networks). If connectivity is not fully supported, then some group services may fail.

There is no restriction in place to require that all the members of a trunk group be assocaited with a single bearer network. Refer to the next section for more details on like network selection for trunk groups.

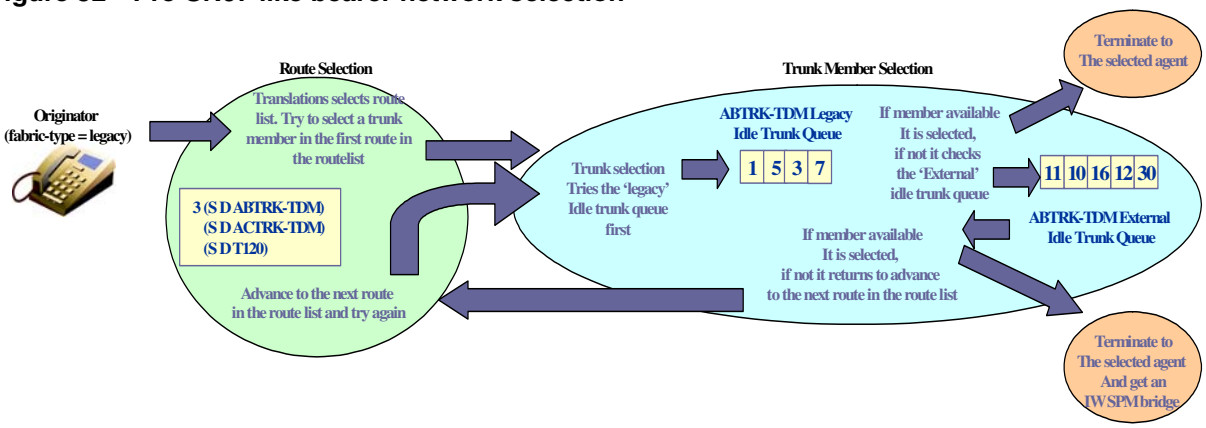
78.2.2.9 Trunk selection (like network selection)

Prior to SN07, the CS2000 Call Server tried to optimize bearer network connections by trying to select a trunk member whose bearer network matched the bearer network of the originating agent. Since there were only two bearer networks supported (‘internal’ and ‘external’), the trunk selection utility internally maintained an idle trunk queue for each of the two bearer networks. When a request was made to select a trunk member, the trunk selection utility would determine the bearer network of the originating agent and then traverse the ‘matching’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP

which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

If it did not find a member, it would search the ‘other’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If both queues are checked and no available member can be found, then the request is returned with an indication that the call should advance to the next route in the route list.

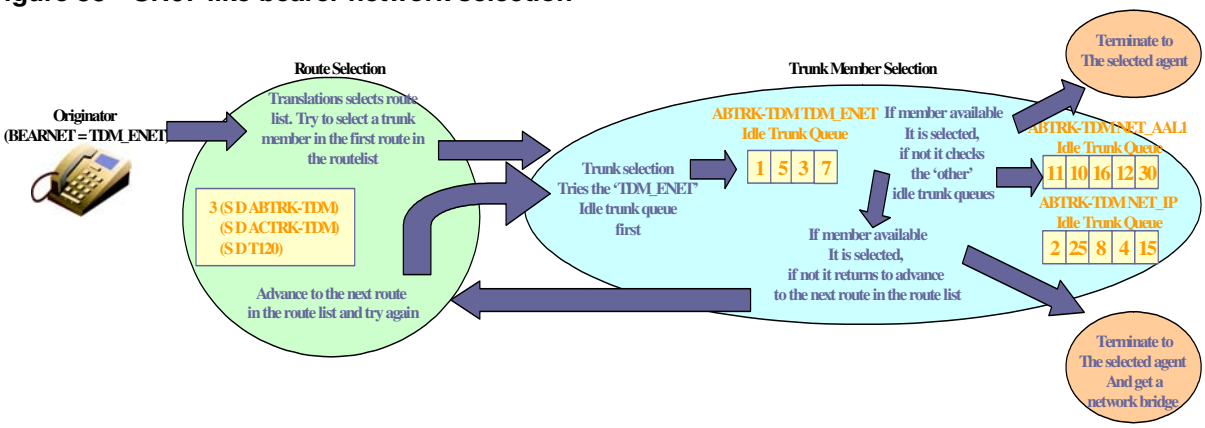
Figure 32 Pre-SN07 like bearer network selection



In SN07, the trunk selection utility is changed to support multiple bearer networks (i.e., more that two). When a request was made to select a trunk member, the trunk selection utility determines the bearer network of the originating agent and then traverses the ‘matching’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

If it did not find a member, it would search the ‘next’ bearer network’s idle trunk queue looking for an available trunk member. The ‘next’ bearer network is determined by the order that the connecting bearer networks are datafilled in Table NET2NET. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If it did not find a member, it would continue searching it’s idle trunk queues in the Table NET2NET bearer network order until it either found an available member or exhausted all of its bearer networks. If all bearer networks are exhausted, then the request is returned with an indication that the call should advance to the next route in the route list.

Figure 33 SN07 like bearer network selection



The following is an example trunk selection request.

- Originating agent's bearer network = NET_AAL1
- Table NET2NET datafill
  - NET_AAL1 -> (TDM_ENET 0) (NET_IP 2)
- Terminating trunk group has members in all three bearer networks

The following is the order that the trunk selection utility will try to find an available trunk member:

1. Trunk group members in the NET_AAL1 bearer network
   - This is first because this is the originator's bearer network.
2. Trunk group members in the TDM_ENET bearer network
   - This is second because it is the first entry in Table NET2NET.
3. Trunk group members in the NET_IP bearer network
   - This is third because this is the second entry in Table NET2NET.

78.2.2.10 DPT (BICC and SIP-T) interworking including audible ringing support

Providing support for both BICC and SIP-T DPT protocols in the same CS2000 Call Server impacts the following areas:

- DPT terminal selection
- DPT audible ringing support

78.2.2.10.1 DPT terminal selection The algorithm for determining which node to host a DPT trunk call differs for BICC and SIP-T. Now that both are supported in the same CS2000 Call Server, this feature must ensure that both function properly.

Changes are needed for the BICC DPT terminal selection algorithms to make sure the bearer network of the hosting DPT capable node matches the bearer network of the DPT trunk group that was selected in translations.

The following table defines the algorithms for each protocol.

Table 4

DPT Protocol	Direction	Algorithm
SIP-T	outgoing	CS2000 Call Server selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRINV and SERVSINV). Note that the bearer network of the DPT trunk group does not factor into the selection process.
SIP-T	incoming	The VRDN GWC selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRINV and SERVSINV). The VRDN GWC builds it list of available SIP-T GWCs because the SIP-T GWCs register with it. BICC GWCs do not register with the VRDN GWC.
BICC	outgoing	CS2000 Call Server tries to put the DPT trunk on the most optimized BICC DPT capable node. BICC DPT capable nodes include the following: • BICC GWCs (bearer network independent) • MG4Ks (with an associated bearer network) • DPT SPMs (with an associated bearer network) If the originating agent is on the MG9K, then a BICC GWC is selected. Note that the bearer network of the DPT trunk group does not factor into the selection process because BICC GWCs can support any bearer network. If the originating agent is on the MG4K, then that same MG4K is selected provided the bearer network of the DPT trunk group matches the bearer network of the MG4K. If the bearer network of the DPT trunk group does not match the bearer network of that same MG4K, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get another MG4K that does support the DPT trunk group's bearer network. If the originating agent is on a legacy peripheral, then the DPT SPM is selected (if present) provided the bearer network of the DPT trunk group matches the bearer network of the DPT SPM. If the bearer network of the DPT trunk group does not match the bearer network of any DPT SPM in the office, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get any MG4K that does support the DPT trunk group's bearer network.

Table 4

DPT Protocol	Direction	Algorithm
BICC	incoming	Prior to SN07, the CS2000 Call Server attempts to initially put the DPT terminal on an MG4K for message normalization and then will move it to the most optimized location based upon what agent the call terminates to. The reason for doing this was to provide a hosting node that had the ability to play tones and collect digits in the case where a service was invoked prior to digit translations and line/trunk termination. In SN07, the CS2000 Call Server continues to place the DPT terminal on an MG4K or DPT SPM for normalization. However, this MG4K/DPT SPM's associated bearer network must now match the bearer network of the incoming BICC DPT trunk group. If no match can be found, then the call is sent to a BICC GWC to be normalized. Note that this leaves no place to support tones and digit collection for those services that may be invoked prior to agent termination. Once the DPT call is normalized, the CS2000 Call Server attempts to optimize the location of the DPT context based on the terminating agent in the call. If the terminating agent is on an MG9K, then the DPT context is moved to a BICC GWC. Note that the bearer network of the BICC DPT trunk group does not factor into the optimization process because BICC GWCs can support any bearer network. If the terminating agent is on an MG4K, then the DPT context will be moved to that MG4K provided the bearer network of the terminating agent's MG4K matches the bearer network of the BICC DPT trunk group. If it does not match, then the DPT context remains where it is (i.e., where it was normalized). If the terminating agent is on a legacy peripheral, then the DPT context will be moved to a DPT SPM (if present) provided the bearer network of the DPT SPM matches the bearer network of the BICC DPT trunk group. If a DPT SPM cannot be found, then the DPT context is moved to a BICC GWC and an IW SPM bridge from the associated bridge pool is used to connect the bearer network of the DPT trunk group and the legacy peripheral. If a BICC GWC is not present, then the call remains where it is (i.e., where is was normalized) and an IW SPM bridge from the associated bridge pool is used.

78.2.2.10.2 DPT audible ringing support The means for providing audible ringing on egress DPT trunk calls differs based upon the DPT protocol being used. Now that both protocols are support in the same CS2000 Call Server, care is taken to ensure that audible ringing functions properly is all scenarios, including bearer network interworking scenarios.

On an incoming DPT SIP-T trunk call where the DPT SIP-T trunk is asked to apply audible ringing, the DPT SIP-T trunk uses Remote Bearer Control (RBC) to ask the originating call server to apply the audible ringing tone on its behalf. On an incoming DPT BICC trunk, the DPT BICC trunk uses Bearer Channel Proxy - No-Anchor (BCP-NA) to ask the terminating gateway to apply audible ringing back towards the originating call server. The following table illustrates the scenarios and how audible is applied.

Table 5 DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
Line (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Line GW towards the line agent
Trunk (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Trunk GW towards the trunk agent
DPT BICC (NET_AAL1)	Line (TDM_ENET)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	Line (NET_AAL1)	BCP-NA used to ask the MG9K to apply audible ringing towards the AAL1 network

Table 5 DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
DPT BICC (NET_AAL1)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	Line (NET_IP)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (TDM_ENET)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_AAL1)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_IP)	BCP-NA used to ask the line gateway to apply audible ringing towards the IP network. If it cannot accomodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.
DPT BICC (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
DPT SIP-T (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.

78.2.2.11 Translations and Routing changes

With support for multiple bearer networks, there is an assumption that calls should remains on the same bearer network as much as possible. Given this assumption, the following changes are made in SN07:

- Routing based upon the bearer network
- TRAVER modifications to support multiple bearer networks

78.2.2.11.1 Routing based upon the bearer network Prior to SN07, the CND/NOT PKT conditional route selector allowed the customer to force routing between the ENET and the packet bearer network. In SN07, this selector is replaced by new conditional route selectors:

- CND/NOT
- FABRIC
- BEARNET

The FABRIC conditional route selector replaces the PKT conditional route selector. During translations and routing, the fabric of the originating agent's bearer network is examnied and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network fabric. During the ONP to SN07, the FABRIC selector replaces any PKT selectors found.

The BEARNET conditional route selector is new in SN07. During translations and routing, the originating agent's bearer network is examnied and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network.

Refer to the Configuration section of the document for additional information.

Figure 34 Conditional routing example datafill

```
TABLE: OFRT
-----------------------------------------------------------
100 (CND FABRIC ENET ST 200) (CND FABRIC AAL1 ST 201)
    (CND FABRIC IP ST 202) $
101 (CND BEARNET TDM_ENET ST 200) (CND BEARNET NET_AAL1 ST 201)
    (CND BEARNET NET_IP ST 202) $
```

78.2.2.11.2 TRAVER modifications to support multiple bearer networks In order to support the new conditional route selectors described above, changes are needed in TRAVER to provide the correct route selection. In SN07, TRAVER needs to determine either the fabric or the bearer network of the originating agent.

If the originating agent is a line, then TRAVER will identify the fabric or bearer network and apply that knowledge to any FABRIC or BEARNET conditional route selectors that it finds.

If the originating agent is a trunk group, then TRAVER cannot automatically identify the fabric or the bearer network information. This is because this designation is not made at the trunk group level but is made at trunk member level.. Therefore, changes are made to TRAVER to allow either a trunk member to be specified explicitly or to specify the bearer network to use for the originating trunk group. The existing TRAVER option TRKMEM is modified to include the determination of the associated bearer network. A new option, BEARNET, as added to support the bearer network designation for a trunk group[1].

[1]TRAVER determines the fabric based upon the associated bearer network.

Refer to the Configuration section of the document for additional information.

78.2.2.12 USP messaging

In SN07, the USP is an optional component. When it is present, it provides the connection from the CS2000 Call Server to the SS7 network. ISUP signaling messages and TCAP transaction messages traverse through the USP interface.

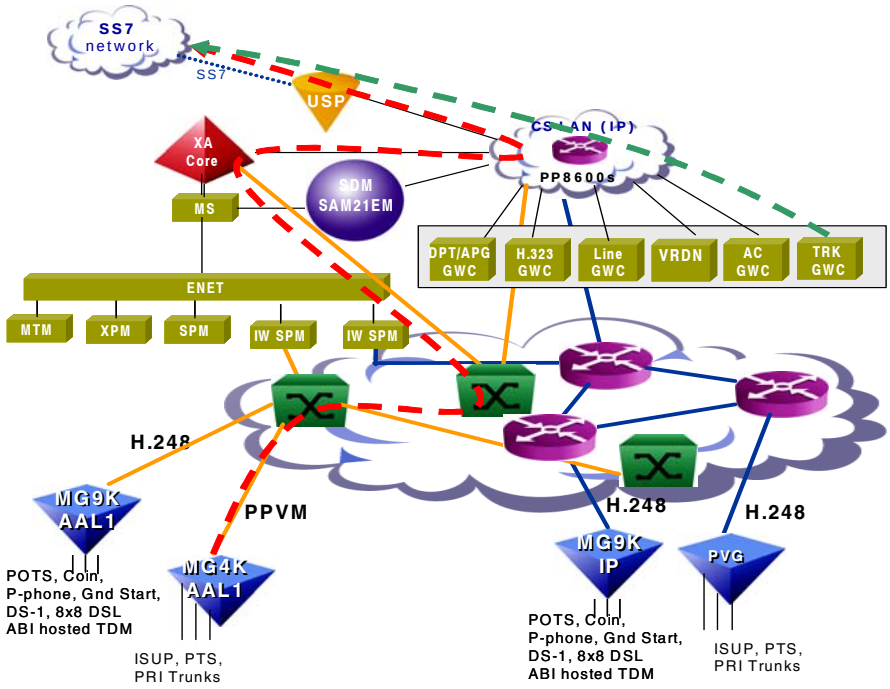
TCAP transaction messages are always generated by the CS2000 Call Server. However, ISUP signaling messages are generated from the ISUP trunk peripherals. The path that the ISUP message takes to get to the USP varies based upon the type of trunk peripheral.

Table 6 USP messaging path for ISUP signaling messages

ISUP trunk peripheral	USP messaging path
GWC	GWC -> CS LAN -> USP
MG4K (AAL1)	MG4K -> AAL1 bearer network -> CS2000 -> CS LAN -> USP
DPT SPM (AAL1)	DPT SPM -> CS2000 -> CS LAN -> USP
legacy peripheral	Legacy peripheral -> CS2000 -> CS LAN -> USP

The USP supports multiple messaging paths and defines them on a per node basis.

Figure 35 USP messaging paths



78.2.2.13 ECAN across multiple bearer networks

Echo cancellation (ECAN) can be applied differently in each bearer network. In an IP bearer network, the packet latency is generally large enough to require 100% ECAN. ECAN is only turned off if an individual call requires that it be turned off (i.e., FAX call).

In an AAL1 bearer network, the packet latency may not be large enough to require ECAN. ECAN in the AAL1 network is generally expensive hardware to purchase and would like to be avoided, if possible. The existing office parameter, ECAN_EDGE_STRATEGY, determines the ECAN strategy used for the AAL1 networks.

Refer to feature A00004046: Echo Cancellation Support for TriModal Call Server 2000 for more information on ECAN.

78.2.2.14 Voice quality

In supporting the connections between packet bearer networks using multiple IW bridges, the voice quality may experience some degradation. The area of concern is in packet latency and delay.

Latency and delay are concerned with how long it takes for a packet of voice to transit the bearer network(s) from end to end. Generally, there is a budget of

150 ms given to a packet. If the delay increases past 150 ms, then the possibility of the end subscribers talking over top of each other increases. The following factors effect the latency and delay that a packet experiences:

- packetization rate and jitter buffer
- transcoding delay
- ECAN
- IP routers
- overall distance travelled

The following tables provide a few examples of latency.

Table 7 MG9K IP to MG9K AAL1 call analysis

MG9K IP to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
MG9K IP packetization	10	20
Leg 3 router hops, assume 3 routers	3	3
IP IW SPM jitter buffer	30	60
ENET	1	1
AAL1 IW packetization	6	6
MG9K AAL1 jitter buffer	2	2
Total latency	52	92

78.2.2.15 ONP

Due to the nature of the changes made to the connectivity function in the CS2000 Call Server, they are applicable to all Succession configurations in SN07, regardless of how many bearer networks are supported. In order to preserve call processing over the ONP, the provisioning of Tables BEARNETS, NETBRDGE, NETPATH and NET2NET must be accomplished during the table transfer.

Refer to the Configuration section for more details on the ONP procedures.

78.2.2.16 Capacity

In general, there are no changes to the capacity parameters for a CS2000 Call Server that supports multiple bearer networks. The total number of endpoints (i.e., lines and trunks) supported remains unchanged. The BHCA capacity of the call server remains unchanged.

The only capacity change is the number of IW SPM bridge nodes supported in a singel office. Prior to SN07, there was a limit of 14 IW SPM bridge nodes supported in an office. In SN07, this limit is removed. The limitation that the CS2000 Call Server can support only 78 SPM nodes of any type is the only remaining capacity limitation for IW SPM nodes. In other words, all the SPM nodes in the office must sum to less that (or equal to) 78 nodes. This includes all the legacy SPMs, MG4Ks, DPT SPMs and IW SPMs in the office.

78.3 Hardware Requirements or Dependencies

In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Table 8 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	None[a]	supported SN07 legacy peripherals which includes both lines and trunk
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC[b]	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk

Table 8 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
	GWC[c]	SIP-T DPT trunks

a. There are no ‘gateways’ support on the ENET. However, there is a list of supported legacy peripherals for Succession Call Servers. This list remains unchanged by this feature.
b. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk support.
c. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk support.

78.4 Software Requirements or Dependencies

This feature requires SN07 North America XA-CORE load or later.

78.5 Limitations and restrictions

In SN07, only one bearer network entry will be supported in table SERVRINV and it will be restricted to the default network because SESM will only support a single bearer network per GWC.

In SN07, an IW bridge will be restricted to a single bridge pool.

In SN07, only one bearer network entry will be supported for DPT SPM and it will be required to be the default network.

In SN07, only one bearer network entry will be supported for MG4K and it will be required to be the default network.

In SN07, the DPT trunk groups datafilled in table TRKOPTS will be restricted to a single network protocol.

In SN07, networks must be configured with full inter-connectivity in table NET2NET.

Customer groups may contain agents from various bearer networks, but all agents within a customer group must be fully inter-connected via NET2NET.

The maximum size of the table BEARNETS will be 8 tuples.

The maximum size of the table NETBRDGE shall be 64 tuples.

Carrier Hosted Services (MCS, H.323, and Centrex IP) are not supported in SN07.

In a multiple packet bearer network configuration, it is expected that the service circuits (i.e., announcements, conference ports and test facilities) be accessed on the MTM (via the ENET).

E911 is a regulatory service that requires all lines to have access to a PSAP. This feature introduces a means to block connectivity between agents that are on different bearer networks. Care should be taken when engineering the office to ensure that all lines have connectivity access to an E911 PSAP. Line PSAPs are not supported.

Operator services is a regulatory service that requires all lines to have access to an operator. This feature introduces a means to block connectivity between agents that are on different bearer networks. Care should be taken when engineering the office to ensure that all lines have connectivity access to operator services access points.

Hyper-PRI is not supported for packet based agents. Multiple fabrics are not supported within a PRI group.

SIP-T is supported on a single IP network only, as the APG resource selection is not supported across mutliple bearer fabrics.

This feature does not support in-service line/trunk migrations or cutovers from one bearer network to another bearer network.

This feature does not support in-service node migrations or cutovers from one bearer network to another bearer network.

78.6 Interactions

N/A

78.7 Applicable customer facing sections

Fault Management	
Logs	___X__
Alarms	_____
Configuration	
Data Schema	___X___
User Interface	___X___
Element Management	___X__
Security	_____
Service Order	__n/a_
Office Parameters	___X__
Accounting (includes AMA billing)	__n/a_

Performance (includes operational measurements) ___X___

78.8 Glossary

Term	Explanation
AAL1	ATM Adaptation Layer 1
AAL2	ATM Adaptation Layer 2
ABI	Access Bridging Interface
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
CODEC	Coder DECoder
CS2K	Call Server 2000
CS2K - MT	Communication Server 20000 Management Tool
DPT	Dynamic Packet Trunk
DPT-SPM	Interworking SPM (ENET interface on the c-side, packet network on the p-side)
ECAN	Echo Cancellation
ENET	Enhanced Network
GUI	Graphic User Interface
GW	GateWay
GWC	GateWay Controller
GWC-EM	Gateway Controller Element Manager
H.323	ITU-T “umbrella” standard for multimedia communications.
IDL	Interface Definition Language
IP	Internet Protocol
IW	Interworking
IW-SPM	Interworking SPM (ENET interface on c-side, packet network on p-side)

JNET	Junctored Network
LGRP	Logical Group
MG4K	Media Gateway 4000 - SPM capable of supporting TDM trunks and DPTs. External network only, no ENET.
MSH	Multi-Service Hub Layer
NA	North America
NV	Network View
OSSDI	Operations Support System DAta Interface
SESM	Succession Element Sub-element Manager
SHR	SHaRed Layer
SIP-T	Session Initiated Protocol - Trunking
SMG4	SPM Media Gateway 4000
SNMP	Simple Network Management Protocol
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
TL	Telecom Layer
TRKOPTS	TRunK OPTionS

79: Functional Description (FN): A00003489

79.1 Feature name

A00003489 - ABI SMS Support

79.2 Description

This activity adds support for the SMS and its subtending SLC-96s to the list of legacy PMs supported by the ABI program. The ABI program allows legacy host XPMs to be connected to the packet network without use of an ENET and an I/W Bridge. Instead the XPM is connected to an ABI card in the MG9K via its legacy DS-512 interface. The MG9K in turn provides connectivity to the packet network. This feature will support Mode 1 and Mode 2 SLC-96s. It will work with both the existing ATM MG9K and be integrated with the new IP version.

The main customer viable changes for this activity will be the ability yo provision the EXTDS512 optional field as part of the tuple in table LTCINV for the SMS Peripheral Type. The optional field is used to identify the IP Address of the ABI Card and the Gateway Controller that the peripheral is 'hosted' off (the GWC must be datafilled in table SERVRINV prior to entering this information). A full description of the table control changes is available in the Data Schema section of this document (part of the Configuration chapter).

79.3 Hardware Requirements or Dependencies

There are no hardware requirements for this project. Integration with the IP project will require the new IP MG9K.

79.4 Software Requirements or Dependencies

The CM changes will go directly into SN07. The SMS load is currently frozen. The last load was built in the XPM14 time frame out of the XPM13BC context. The load will be brought on stream in XAX20 to add this new functionality.

79.5 Limitations and restrictions

- Only Mode 1 and Mode 2 SLCs will be supported. Mode 3 SLCs might also work, but, they will not be tested.
- RMM support will not be added to the SMS.
- Line Test will therefore only be supported using RMMs located in other XPMs at the site with the SMS or via DIal Up External test sets.

79.6 Interactions

This new code will need to interact with the existing ABI framework for link maintenance, packet connection setup, and MG9K ESA.

79.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema ___X__
- User Interface ___X__
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

79.8 Glossary

Term	Description
ABI	Access Bridging Interface
SLC	Subscriber Loop Carrier
SMS	Subscriber Module for SLC-96/RT
XAX	Current XPM design stream for MX77 loads

80: Functional Description (FN): A00003490

80.1 Feature name

Feature A00003490 - Support for ABI XPM tuple Change - XA-Core

This feature is sourced in the Succession SN07 release.

80.2 Description

This feature provides the ability:

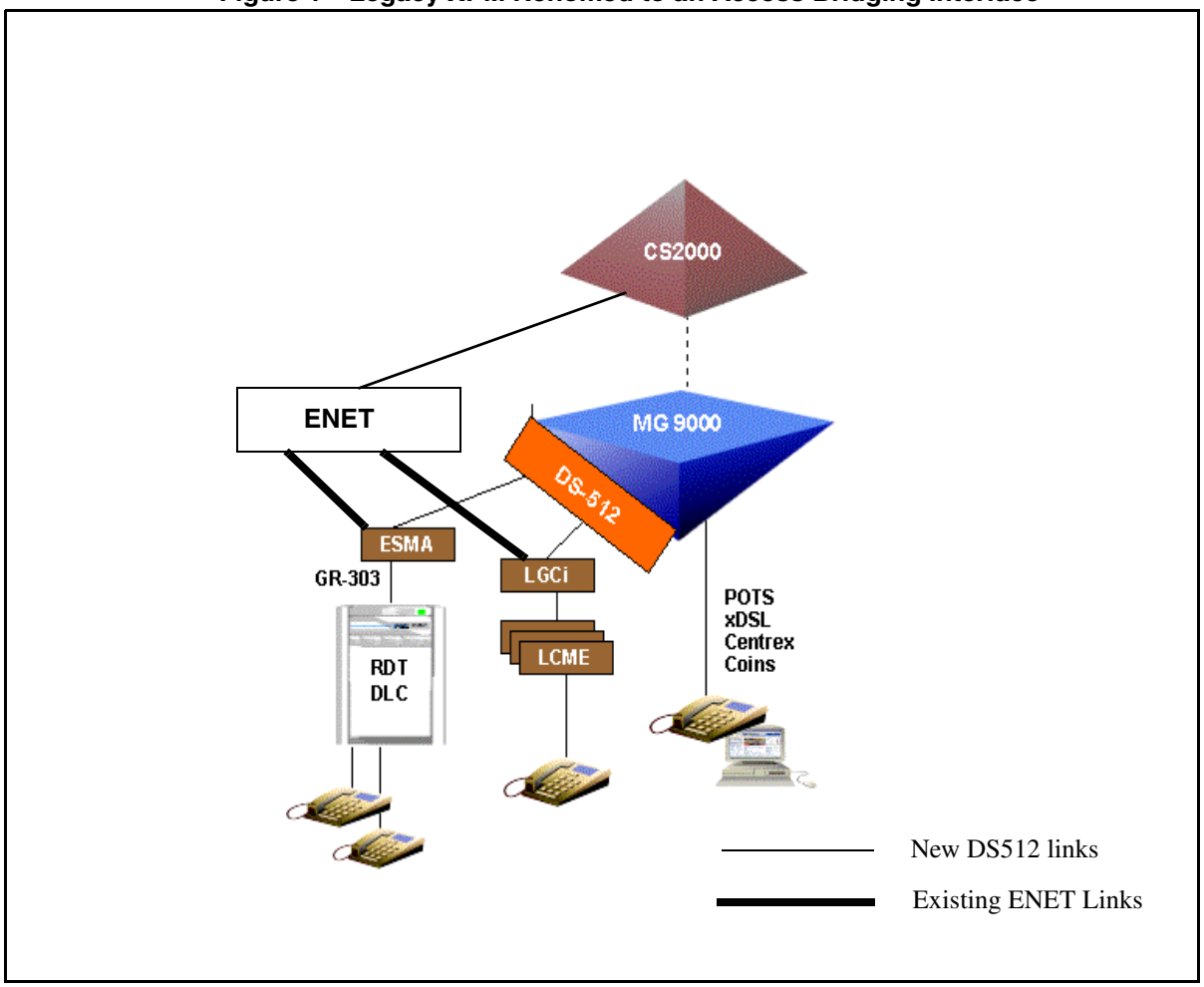
- to change the network fabric for a TDM based XPM from Enet/Jnet to DS512 interface
- restrict the use of this change only during the XPM rehome procedures

Currently, legacy XPMs are connected to either a ENET or JNET network. Rehome of the legacy XPMs to the ABI configuration is accomplished by connecting the XPM to the DS512 interface in a MG9000 gateway. The DS512 serves as the interface between the TDM links to the XPM and the OC3 interface coming out of the MG9000 and into the ATM network. Please refer to “Figure 1 Legacy XPM Rehomed to an Access Bridging Interface” on page 762.

The ability to perform a network interface change has the following benefits:

- simplifies the ABI XPM rehome methods and procedures
- in some instances, this may be the only way to change to an ABI network interface. Offices with a fully configured network cannot datafill a “fake” XPM because there is no free network links

Figure 1 Legacy XPM Rehomed to an Access Bridging Interface



The ability to change the network interface via the table control change operation is only available during the XPM rehome activity. To control the activation of the table control change operation, the installation personnel utilizes the TOOLSUP and ABIREHOME CI tools. Please refer to "Command interface changes" in the configuration (CN) section of this feature for detailed command information. This table control operation is merely one piece of the overall installation and rehome process. For the complete installation process, please refer to Installation Method 72-1682 XPM to MG9000 DS-512 Rehome. Optionally, a secondary capability to rehome an ABI XPM to a different gateway with a new IP address, will also be provided.

For a complete list of restrictions associated with the ABI XPM rehome operation, please refer to "80.5 Limitations and restrictions" on page 765.

In order to provide these new functionalities described above, the customer will see changes in the following areas:

- operation of table LTCINV

- operation of new ABIREHOME CI tool

80.2.1 Table LTCINV Impacts

Table LTCINV changes consist of modifications to the original SN05 ABI XPM tuple change operation restrictions. No other changes have been made to the table. For a complete list of the current ABI XPM tuple operation restrictions, please refer to “80.5 Limitations and restrictions” on page 765.

For a change operation on XPM tuple in LTCINV, the following four types of change are allowed:

1. **ENET change** - This is an existing functionality that has not been altered. In this type of change, the ENET links of the XPM can be changed to any available valid ENET links.

2. **ABI change** - In this type of change, the XPM can be moved to a different ABI on the same GWC.

3. **ENET to ABI change** - In this type of change, the ENET links of the XPM are removed and an attribure EXTDS512 is added which indicates that the XPM is being moved from ENET to ABI. The EXTDS512 attribute has the information about which ABI the XPM is being moved to.

4. **ABI to ENET change** - In this type of change, the attribute EXTDS512 is removed and ENET links are added which indicates the XPM is being moved from ABI to ENET.

When change operation is not successful there is a need to rollback the changes that have been done. The rollback is done based on the type of change.

80.2.2 New ABIREHOME CI Tool

The ABIREHOME CI tool is intended to be used by qualified personnel only. Therefore, the ABIREHOME tool must be enabled via the TOOLSUP password control mechanism.

The ABIREHOME CI directory contains commands specific to the rehoming process. This directory will contain only the following commands in SN07:

- Rehome query commands
  - QUERY_ABI_REHOME_STATUS/QRS: This command displays the status of the ABI rehome control mechanism. Several commands can only be executed when the Rehome State is ON.

- QUERY_IMPACTED_NODES/QIN: This command is used to display all the nodes currently marked as impacted.
- FIND_AFFECTED_NODES/FAN: This command is used to display all the nodes impacted by rehome of given XPM node. This does not show that the given XPM has been marked as impacted by Rehome, rather it only displays the node and those subtending nodes which would be affected if this node is rehomed.
- SHOW_NODE_STATUS / SHOWNS: This command displays the current status, through ABI rehome, of a specified XPM node, or all rehoming XPM nodes.
- DISP_LINK_CHANNEL_MAP/DLC: This command displays the link channel map for a specified XPM node.
- DISP_LINK_INFO/DLI: This command displays the status of a specified node and the status of that node's links.
- DISP_IOUI_ROUTE_DATA/DRD: This command displays the IO Routing data for a specified node.

• INVASIVE rehome commands

- SET_ABI_REHOME_STATUS: This command turns on the functiality for all the following invasive commands, and the overall ABI Rehome procedure. This status must be ON during the execution of the ABI Rehome procedure, as indicated in the Installation Method.
- MARK_NODE_DS512_RESULT: This command sets the DS512 Link Verified bit for the specified node. If the node is marked PASS for the DS512 Link Verification test, the XPM and its subtended nodes are marked as 'Affected By Rehome.' If the XPM is marked FAIL for the DS512 Link Verification test, the XPM and its subtended nodes are cleared from being marked as 'Affected By Rehome.' This permits the user to clear a node that was errantly marked as PASSed.
- ADJUST_FRAME_SYNC/AFS - This command is used to adjust the frame sync on the ABI cards to sync to the inactive XPM unit.
- SEND_GWC_STATIC_DATA/GWCSD : Send GWC Static Data. This command is used to send a limited static data update request to GWCs with new or deleted ABI XPMs.
- ABORT_GWC_STATIC_DATA/ABORT_GWCSD : Abort GWC Static Data. This command is used to send a limited static data update request to UNDO the recent GWC static data updates, following and AbortSwact ONLY.

  - LINE_STATUS_CHG : This command provides the ability to input a range of LENs and either display all line states in that range, or change the line states from one state to another.

- HIDDEN commands
  These commands SHOULD NOT BE EXECUTED. These commands are only intended for use by Nortel GNPS personnel in a recovery and/or data collection situation.
  - SLC: Set Link Channels Idle. This command sets the link and channel maps to Idle, for a specified node. Thiscommand will cause call deaths, if there are active calls on the node at the time.
  - SAN: Set Affected Nodes. This command is used to set the protected rehome bit for each node impacted by rehoming the given XPM.
  - CAN: Clear Affected Nodes. This command is used to clear the protected rehome bit for each node impacted by rehoming the given XPM.
  - SHOW_GWCSD: Show GWC Static Data. This command displays the GWC Static Data transactions that have been captured via LTCINV table control operations. This static data is automatically sent to the GWC following the XACore Swact, or AbortSwact.
  - CLEAR_GWC_SD_TABLE: This comand clears the GWC Static Data transactions that have been captured via LTCINV table control operations. If this command is executed prior to the XPM Rehome XACore SWACT, the GWC will not be updated with appropriate static data, and the GWC must be Node BSY and RTS'ed to recover the correct static data.

80.3 Hardware Requirements or Dependencies

While this feature does allow for the change to the network interface for an existing XPM, it does not require that the hardware be present in order to perform this operation.

80.4 Software Requirements or Dependencies

This feature does require the Core load to be a Succession load. The Succession load contains the MSH DRU. The MSH DRU is where key software resides for this feature functionality.

80.5 Limitations and restrictions

It was thought to be beneficial to list the ABI XPM provisioning limitations and restrictions which existed before and after this feature.

ABI XPM Provisioning Limitations and Restrictions	SN05	SN06	SN06.2	SN07
LTCINV tuple must be entered with ENET CSLNKTAB links or the EXTDS512 option, but not both.	X	X	X	X
EXTDS512 option may be assigned to LGCI and SMA2	X	X	X	X
EXTDS512 option may be assigned to LGC, LTC, LTCI			X	X
EXTDS512 option may be assigned to SMS				X
Add/Change/Delete of the derived C-side links in CSLNKTAB for ABI XPMs is not allowed.	X	X	X	X
Change of the GWC of the External XPM is not allowed.	X	X	X	X
Change of the External XPM to a gateway on a different GWC, as defined in GATWYINV, is not allowed.				X
Change of an LTCINV tuple from ENET to EXTDS512, or EXTDS512 to ENET, is allowed if the following conditions are true: - Change is being performed on the Inactive XACore, - ABI XPM Rehome is in progress, - The XPM is out of servic, and the XPM's ENET C-side links are OFFL or UNEQ. - The XPM either has no ISDN datafilled -or- has ISDN and is capable of doing pside-to-pside switching (has an NTAX78BA timeswitch or similar timeswitch with pside-to-pside switching capable) - The XPM (e.g. LTC) has no trunks datafilled on it.				X
IP address associated with the EXTDS512 option must be unique for each External XPM.	X	X	X	X
Change of the IP address associated with the EXTDS512 option (either in LTCINV or in GATWYINV) is allowed, if the XPM is MANB or OFFL. This can be performed on the Active XACore, or on the Inactive XACore as part of the ABI Rehome process.	X	X	X	X
XPM Rehome from ENET to ABI should NOT be executed over ONP.	X	X	X	X
TRNSL C, TRNSL MSG C and TRNSL EMSG C directs the user to the MG 9000 Element Manager. No C-side link information maintained in the Core.	X	X		

80.6 Interactions

This feature introduces the capability to change network interfaces for existing XPMs via a table control change operation during the rehome process. It is designed to have no impact on existing XPMs that will not be rehomed.

80.7 Applicable customer facing sections

Fault Management

Logs ___n/a___

Alarms	___n/a___
Configuration	
Data Schema	___X__
User Interface	___X___
Element Management	___n/a___
Security	___n/a___
Service Order	___n/a___
Office Parameters	___n/a___
Accounting (includes AMA billing)	___n/a___
Performance (includes operational measurements)	___n/a___

80.8 Glossary

Term	Description
Rehome	Moving of XPMs from one network to another network. More specifically from the ENET to the ABI or vice-versa Also, Moving of subtending devices from one XPM to another XPM. In the case of an ABI configuration, the XPM is considered a subtending device to the GWC.
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512
network change	When the network interface type of an XPM is changed via the Table Control Change operation in Table LTCINV.

81: Functional Description (FN): A00003495

81.1 Feature name

APG integration with MP for NAT traversal.

81.2 Description

This feature is an enhancement of the CS 2000 Media Proxy NAT (Network Address Translator) traversal solution. It adds support for the APG (Anchor Packet Gateway) to this solution.

The MP (Media Proxy) NAT traversal solution was developed in SN06 under activity 89007980. It involves proxying a media path through an MP if the calling agents are in different IP (Internet Protocol) address domains, in order to ensure that media can flow between both parties.

The APG is a network device needed to support certain SIP-T (Session Initiation Protocol for Telephony) features on the CS 2000, mainly those that require the SIP-T leg to collect digits or play tones. The APG is inserted into the media path whenever SIP-T control logic determines that it is needed. The APG was developed in SN04 under activity 59031163.

Previous to this feature, calls requiring both an MP and an APG were not supported.

81.3 Hardware Requirements or Dependencies

None, apart from the hardware requirements and dependencies inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

81.4 Software Requirements or Dependencies

None, apart from the software requirements and dependencies inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

81.5 Limitations and restrictions

None, apart from the limitations and restrictions inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

81.6 Interactions

None.

81.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

81.8 Glossary

Term	Description
APG	Anchor Packet Gateway
CS 2000	Communications Server 2000
IP	Internet Protocol
MP	Media Proxy
NAT	Network Address Translator
SIP-T	Session Initiation Protocol for Telephony

81.9 References

a. FN section of ACT.89007980 (NAT Traversal feature)

b. FN section of ACT.59031163 (APG feature)

82: Functional Description (FN): A00003496

82.1 Feature name

Control of Shasta Media Proxy

82.2 Description

This feature implements the Nortel proprietary protocol MPCP 4.0 for the CS2K GWC platform.

MPCP is a simple protocol that is very loosely based on the IETF protocol MGCP. It uses a small subset of the MGCP messages, which are modified and extended with experimental parameters and proprietary interpretation of existing parameters. It is used by the GWC to control a Shasta BSN 5000 Media Portal as a Media Proxy (MP).

82.2.1 References

a. Media Proxy Contol Protocol 4.0 Specification: http://eur-livelink.europe.nortel.com/livelink/livelink.exe/8440318/MPCP_4.0?func=doc.Fetch&nodeid=8440318

82.3 Hardware Requirements or Dependencies

None

82.4 Software Requirements or Dependencies

None

82.5 Limitations and restrictions

None

82.6 Interactions

None

82.7 Applicable customer facing sections

Fault Management

Logs	__N/A__
Alarms	__N/A__

Configuration

- Data Schema __N/A__
- User Interface __N/A__
- Element Management __N/A__
- Security __N/A__
- Service Order __N/A__
- Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

82.8 Glossary

Term	Description
BSN	Business Service Node
GWC	Gateway Controller
IETF	Internet Engineering Task Force
IMS	Interactive Multimedia Server
ITA	Internet Transparency Application
MGCP	Media Gateway Control Protocol
MP	Media Portal
MPCP	Media Portal Control Protocol
RTP	Real Time Protocol
TAPI	Telephony Application Programming Interface

83: Functional Description (FN): A00003506

83.1 Feature name

Activity A00003506 - H.248 Per Trunk Signalling (PTS) Development

83.2 Description

This SN07 activity provides PTS trunking capabilities for the Succession Call Server 2000 (CS2K). Specifically, this activity provides incoming, outgoing, and two-way interconnections from a North American End Office (EO), Access Tandem (AT), or InterExchange Carrier (IEC) to the Public Switch Telephone Network (PSTN) as well as Private Branch eXchange (PBX) systems.

Figure 1 illustrates the CS2K network components that are applicable to this activity. The PSTN interconnection is provided using PTS trunk groups configured on a Gateway Controller (GWC) peripheral type where H.248 protocol is supported between the GWC and the Media Gateway (MG). The specific MG planned to provide this PTS functionality is Nortel's Passport Voice Gateway (PVG). The PVG load that will support PTS trunks is planned to be available in the SN07.1 release time frame.

The PTS trunk group types providing interconnection to the PSTN and PBX's are listed in Table 1, "Supported GWC PTS Trunk Group Types," on page 772.

Table 1 Supported GWC PTS Trunk Group Types

Trunk Group Type	Direction
OP	IC,OG,2W
ES	IC,OG,2W
PX	IC,OG,2W
IBNTI	IC
IBNTO	OG
IBNT2	2W
ATC	IC,OG,2W
IT	IC,OG,2W
SC	IC,2W
CELL	IC,OG,2W
DAL	IC,OG,2W

Table 1 Supported GWC PTS Trunk Group Types

Trunk Group Type	Direction
EANT	IC,OG,2W
ONAT	IC,OG,2W

This activity supports the following pulse types:

- MF - Multi-Frequency
- DP - Dial Pulse (for PX, DAL, IBN2W, IBNTO, and IBNTI only)
- DT - DigiTone (for PX, DAL, IBN2W, IBNTO, and IBNTI only)
- NP - No Pulse (For Outgoing FXS signalling only)

This activity supports the following Start Signal types:

- WK -WinK
- IM - IMmediate
- DD - Delay Dial
- GS - Ground start fxS
- LS - Loop start fxS

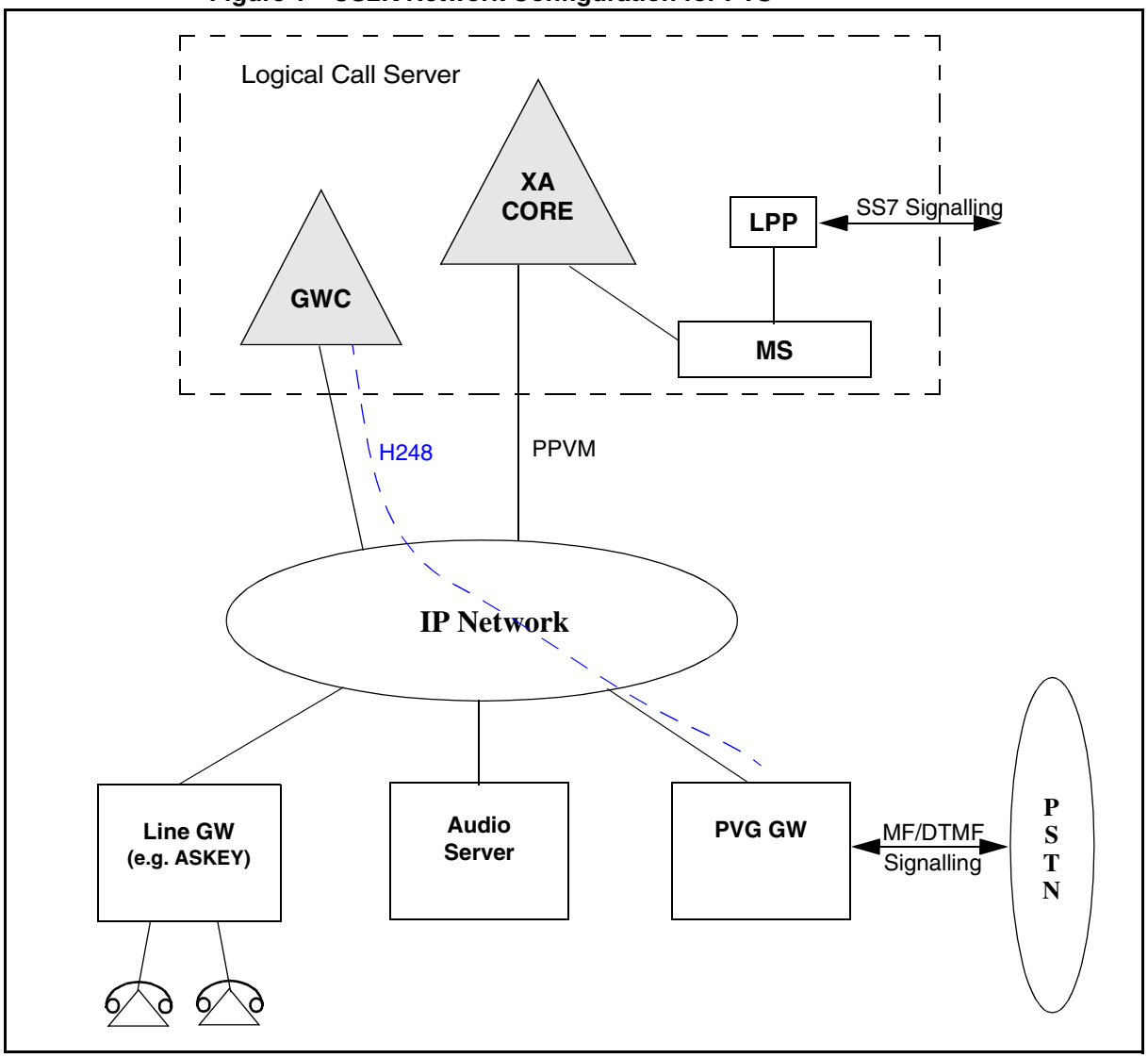
This activity supports the following Card Codes:

- DS1SIG
- FXSLS
- FXSGS

The supported combinations of trunk group type, pulse type and start signal type for this activity include the same combinations as supported in the legacy DM100 Switching System. Any restrictions or limitation from that support are included in section “83.6 Limitations and Restrictions” on page 785.

The base framework for H.248 PTS on GWC was established by prep features A89007187 and A89007652 in SN06. These prep features introduced limited PTS support for Outgoing Operator (OP), Emergency Services (ES), Direct Access Line (DAL), and Equal Access Network Trunk (EANT) trunk group types. This current activity in SN07 builds upon this base framework established in SN06.

Figure 1 CS2K Network Configuration for PTS



83.3 Functional Description

83.3.1 CS2K Provisioning Overview

As with the legacy DMS100 switching system, the GWC PTS trunk related data is provisioned on the CS2K core using the same data tables. These data tables include tables CLLI, TRKGRP, TRKSGRP, TRKOPTS, and TRKMEM. In addition, GWC node and endpoint provisioning is required and is accomplished using the Call Server 2000 Manager (CS2M).

When provisioning PTS trunks on a GWC, there are no restrictions regarding the distribution of the trunk members. Trunk members can be distributed over more than one GWC, over more than one MG, and can consist of any number of channels on a T1. However, if a T1 is to have its channels divided across trunks groups, those trunks groups must have the same card code provisioned in table TRKSGRP (e.g. DS1SIG, FXSLS, or FXSGS).

Also, a combination of trunk groups with different signalling types, on the same GWC, is supported. For example, ISUP and PTS trunks on the same GWC is a supported configuration.

Hybrid PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are ***not*** supported.

83.3.2 CS2M GWC Node and Endpoint Provisioning

The CS2M provides the capability to configure a GWC by selecting the ADD GWC NODE command under the Configuration tab. The subsequent popup window allows the user to provision the GWC name, IP and router IP. In addition, the user provisions the Gateway controller profile and associated profile data information including Tone data, Exec data, and Type list for the GWC node being added. This activity provides the capability to select a specific GWC profile and profile data to configure GWCs to support PTS trunks.

The CS2M also provides the capability to configure an MG by selecting the Associate Media Gateway command under the configuration tab. The subsequent popup window allows the user to provision the GW name, IP, GWC name, and Gateway Profile name. For this activity the Gateway Profile name specified must be PVG. In addition, the user must also select the protocol type. For this activity, Megaco (4) must be selected to indicate H.248 protocol.

The CS2M also provides the capability to add carriers to a GWC. This is accomplished by first selecting a specific GWC, then selecting the provisioning tab. Once under the provisioning tab, the carrier tab can then be selected. Once under the carrier tab, the user can click the ADD button which triggers a POPUP where the user provisions the Carrier Name and Gateway Name. This carrier provisioning task accomplishes the provisioning of 24 PTS endpoints at a time on the specified GWC and carrier. The endpoints and

subsequent node and terminal numbers are mapped in the CS2K to a trunk group and member in table TRKMEM. See section “83.3.7 Table TRKMEM” for information regarding provisioning of table TRKMEM.

The capabilities to configure an MG and add carriers to a GWC are not introduced by this activity, but are included here to clarify the specific field values required to support PTS trunking.

83.3.3 Table SERVRINV Provisioning

When a GWC node is added from the CS2M, a subsequent and corresponding tuple is added to table SERVRINV. This tuple contains GWC name, network type, IP address, exec lineups and termtypes, tone set value, and options. This activity provides the capabilities to add a GWC node to table SERVRINV, either manually or via the CS2M tool that will support new exec_lineups for GWCs configured as PTS GWCs. The following table includes the new exec_lineup and termtype combinations which are supported for the PTS GWC.

Table 2 Supported PTS Exec Lineup/Term Type Combinations

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWC250	All GWC PTS trunk groups except for PX trunk groups using FX signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FX signalling except for for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FX signalling and EANT, ONAT, and DAL trunk groups.

83.3.4 Table TRKOPTS Provisioning

This activity enhances the functionality of table TRKOPTS by adding the capability to provision option GWCPTSTK to any PTS trunk group identified in Table 1, “Supported GWC PTS Trunk Group Types,” on page 772 Figure 2 below shows an example tuple in table TRKOPTS with the GWCPTSTK option provisioned and highlighted.

In addition, the GWCPTSTK option contains a single sub-option, PRELOADANI. This sub-option is a boolean value which identifies GWC PTS trunk groups which support a call model that allows the ANI digits to be sent from the Core to the GWC prior to receiving any ANI request from the peripheral. The SN07 Feature A00003630 TGCP for the Cable Market introduced this PRELOADANI sub-option. This sub-option is currently only applicable to OP and ES trunk group types and will not be allowed to be set to

Y for any other GWC PTS trunk group type. Please refer to the feature documentation for activity A00003630 for additional information.

Figure 2 Table TRKOPTS GWCPTSTK Option

```
TABLE: TRKOPTS

                    OPTKEY
                                                                        OPTINFO
-------------------------------------------------------------------------------
        GWCPTSCLLI GWCPTSTK
                                                                    GWCPTSTK N
```

The GWCPTSTK option can only be added to a trunk group after the trunk group has been provisioned in table TRKGRP and before any trunk members of that group are provisioned in table TRKMEM.

In addition, the GWCPTSTK option is incompatible with some of the existing TRKOPTS options. Restrictions are added to prevent the incompatible options from being added together with the GWCPTSTK option on the same trunk group.

Table 3 TRKOPTS Options Incompatible with GWCPTSTK

TRKOPTS Option	Incompatibility Reason
Q118OPT	This activity supports IBN basic call only. No option support
SUPVOPT	This activity supports IBN basic call only. No option support
DPT	ISUP Specific Option
DYNAMIC	ISUP Specific Option
CNAMINGN	ISUP Specific Option
RLT	ISUP Specific Option
OSNC	ISUP Specific Option
DLYFWDXMT	Not supported for GWC PTS trunks
BLOCKLNP	ISUP Specific Option
VOICELAW	ISUP Specific Option
CGETSRESP	ISUP or ISDN Specific Option

Table TRKOPTS is also used to restrict trunk group, subgroup, or member capabilities non-compatible with the GWCPTSTK option.

The trunk group restrictions enforced by the GWCPTSTK option are unique for each supported GWC PTS trunk group type. These trunk group restrictions are discussed in section “83.3.5 Table TRKGRP”, section “83.6 Limitations and Restrictions”, and in the Configuration customer facing section.

The trunk subgroup restrictions enforce by the GWCPTSTK option are discussed in section “83.3.6 Table TRKSGRP”, section “83.6 Limitations and Restrictions”, and in the Configuration customer facing section.

The trunk member restrictions enforced by the GWCPTSTK option are discussed in section “83.3.7 Table TRKMEM”, section “83.6 Limitations and Restrictions”, and in the Configuration customer facing section.

83.3.5 Table TRKGRP

The TRKGRP tuple for a GWC PTS trunk is unchanged from the legacy DMS100 switching system. However, restrictions are enforced on GWC PTS trunk groups in table TRKGRP when the GWCPTSTK option is added to the trunk group in table TRKOPTS. Refer to section “83.6 Limitations and Restrictions” and the Configuration customer facing section for further information.

83.3.6 Table TRKSGRP

The TRKSGRP tuple for a GWC PTS trunk is unchanged from the legacy DMS100 switching system. However, with an IP network configuration, the responsibility of providing low level PTS signalling requirements is delegated to the MG. As a result, there is data currently provisioned in table TRKSGRP that is not applicable to PTS trunks configured on a GWC. Specifically, the IDGTIME and TRKGRDTM fields are not used by the CS2K in this configuration. In addition, other tuple field restrictions are enforced on GWC PTS trunk subgroups when the GWCPTSTK option is added in table TRKOPTS. Refer to section “83.6 Limitations and Restrictions” and the Configuration customer facing section for further information.

83.3.7 Table TRKMEM

The provisioning of a GWC PTS tuple in table TRKMEM requires a node number and a terminal number on the GWC. The node and terminal numbers are mapped to the specific endpoints during endpoint provisioning from the CS2M. Provisioning of the endpoints on the CS2M is recommended prior to table TRKMEM provisioning in order to map trunk members to specific carriers. Refer to section “83.3.2 CS2M GWC Node and Endpoint Provisioning” for additional information on GWC PTS endpoint provisioning.

Before a GWC PTS trunk member is allowed to be provisioned in table TRKMEM, the GWCPTSTK option must be present on the trunk group in table TRKOPTS. Table control enforces this restriction. In addition, if option GWCPTSTK exist on a trunk group, table control will disallow the addition of trunk members on non-GWC peripheral types, such as a DTC. Hybrid GWC

PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are ***not*** supported. Please refer to section “83.6 Limitations and Restrictions” and the Configuration customer facing section for further information.

83.3.8 Echo Cancellation

This activity restricts the ECSTAT field in table TRKSGRP to allow only values of EXTERNAL or INTERNAL for GWC PTS trunk groups. The ECSTAT value of INTERNAL signifies that echo cancellation is to be performed by the MGs where this trunk group is provisioned. The ECSTAT value of EXTERNAL signifies that echo cancellation is NOT to be performed by the MG where the trunk group is provisioned. The ECSTAT field value of UNEQ is not supported. Field ESUPR is also restricted to allow only a value of ‘N’ for GWC PTS trunk groups.

83.3.9 Padding

Padding data is provisioned on the CS2K core in table PADDATA. For each GWC PTS trunk group in table TRKGRP, field PADGRP is provisioned. When a call is established, the padgrp for each agent involved in the call is retrieved and mapped in table PADDATA to determine the gain or loss. This gain or loss is specified to the MG via H.248 signalling. The PADGROUP ETLL should be used for PTS trunks configured on a GWC. Please refer to the SN06 PT-IP Engineering Guidelines for additional information on padgroup values.

83.3.10 H.248 Package Requirements

In order to support PTS trunks configured on a GWC using H.248 protocol between the GWC and MG the following H.248 packages are supported:

- Basic Channel Associated signalling (CAS) Package ITU-T Recommendation H.248.25 (7/2003)
- Robbed Bit Signalling (RBS) Package - ITU-T Recommendation H.248.25 (7/2003)
- Generic (G) Package -ITU-T Recommendation H.248.1 (03/2002)
- TDM Circuit (TDMC) Package - ITU-T Recommendation H.248.1 (03/2002)
- DTMF Detection (DD) Package - ITU-T Recommendation H.248.1 (03/2002)
- Extended DTMF (XDD) Package - ITU-T Recommendation H.248.16 (11/2002)
- Enhanced DTMF (EDD) Package - ITU-T Recommendation H.248.16 (11/2002)
- Basic Call Progress Tones Generator (BCG) Package - ITU-T Recommendation Q.1950 (12/2002)

- Call Progress Tones Generator (CG) Package - ITU-T Recommendation H.248.1 (03/2002)
- Extended Call Progress Tones (XCG) Package - ITU-T Recommendation Q.1950 (12/2002)
- Basic Service Tones (SRVTN) Package - ITU-T Recommendation Q.1950 (12/2002)
- Network (NT) Package - - ITU-T Recommendation H.248.1 (03/2002)
- H.248 Inactivity Timer (IT) Package - ITU-T Recommendation H.248.14 (03/2002)

Both the Basic CAS and RBS package include properties which the MG, to be compliant, must provide at least a default value for each of the properties. For interoperability with the CS2K, a set of these properties are provisioned on the MG.

83.3.11 PVG Profiles

For the PVG, a profile is provisioned on a DS1 carrier basis during installation of the PVG by Nortel Networks. Currently there are four profiles which support PTS trunks and are dependent on the supported cardcode and pulse types provisioned in table TRKSGRP. A PVG profile table mapping is shown below in Table 4, “PVG DS1 Profile Mapping,” on page 780.

Table 4 PVG DS1 Profile Mapping

PVG Profile Name	TRKSGRP Cardcode	TRKSGRP InComing Pulsetype	TRKSGRP OutGoing Pulsetype	Trunk Group Restrictions
ds1sig_mfr1.prof	DS1SIG	MF,DT, DP	MF,DP	None
ds1SigMwMfr1.prof *	DS1SIG	MF,DT, DP	MF,DP	None*
ds1sig_dtmf.prof	DS1SIG	DT,DP	DT,DP	Not Supported for OP, SC, ES, ATC, IT, ONAT, and EANT.
fxsls.prof	FXSLS	DT,DP	DT,DP	Supported for DAL and PX groups only
fxsgs.prof	FXSGS	DT,DP	DT,DP	Supported for DAL and PX groups only

* should be used in place of ds1SigMfr1.prof, if the far-end trunk group is setup to generate the multi-wink operator ringback signal.

Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. The affected office parameters are listed in section “83.6.1 Office Parameters”.

83.3.12 Trunk Maintenance

83.3.12.1 Trunk Maintenance Manager (TMM) Support

The following commands will be supported on the TMM for GWC PTS trunks. No changes were introduced to provide this functionality for GWC PTS trunks.

- POST
- BSY
- BSY ALL
- FRLS
- RTS
- RTS ALL

83.3.12.2 Trunk Test Position (TTP) Level Support

Support for the following TTP level commands for PTS trunks configured on GWCs is provided.

- QUIT
- Post_
- BSY [<STATE>] [<ALL or A>] where STATE is MB, SB, or INB. SB is not supported for GWC trunks
- BSY [<ALL or A>]
- RTS with opts RTS, ALL, RES, INI, IDL, RLS, C (M, CP, BOTH)
- Hold
- NEXT
- RLS
- CktInfo
- Level_
- FRLS
- SEIZE

The following TTP level commands are not supported for PTS trunks configured on GWCs:

- TST
- Ckt_

NOTE: The T108 test is supported for PTS incoming trunks. Note: special translations are required to support an incoming T108 test (e.g. call translated to CLLI TRKLPBK).

The following TTP level commands are not supported for all trunks configured on GWCs (PTS, ISUP, etc.):

- BSY SB
- CktLoc
- TrnslVf_
- StkSdr_
- Pads

83.3.12.3 TTP MANUAL Level Support

The following MANUAL level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the MANUAL level as exist in the TTP level for GWC PTS trunks.

- QUIT
- Post_
- BSY
- RTS
- Hold
- NEXT
- OP_
- FRLS
- SGNL
- RLS

The following MANUAL level commands are not supported for PTS trunks configured on a GWC:

- TST

The following MANUAL level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- LOSS
- TGEN

- Noise
- TDet
- Hset

The following MANUAL level commands are not supported for all trunks configured on a GWC (PTS, ISUP, etc.):

- Jack_
- CallTrf

83.3.12.4 TTP MONITOR Level Support

The following MONITOR level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the MONITOR level as exist in the TTP level for GWC PTS trunks.

- QUIT
- Post_
- BSY
- RTS
- Hold
- NEXT
- RLS
- FRLS

The following MONITOR level commands are not applicable to PTS trunks configured on a GWC:

- CPos_
- CktMon
- TST

The following MONITOR level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- MonTalk
-

The following MONITOR level commands are not supported for all trunks configured on a GWC (PTS, ISUP, etc.):

- MONPOST
- MONLINK

83.3.12.5 TTP DATATTP Level Support

The following DATATTP level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the DATATTP level as exist in the TTP level for GWC PTS trunks.

- Quit
- Post_
- Seize
- BSY
- RTS
- HOLD
- Next
- Rls

The following DATATTP level commands are not applicable to PTS trunks configured on a GWC and are restricted from use.

- BTerm_

The following DATATTP level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- BERT_

83.3.12.6 GWC Swact Support for PTS Trunks

This activity provides for the support of PTS trunks during GWC swact. Any stable call over a PTS trunk configured on a GWC, which performs a warm swact, will remain active over the warm swact. All stable calls are torn down over a GWC cold swact.

83.3.12.7 CS2K Restart Support for PTS Trunks

This activity provides for the support of PTS trunks configured on a GWC over all core restarts. Any stable call will remain active over a warm restart. For any other core restart type, all calls are torn down as expected.

83.3.12.8 CS2K SWACT Support for PTS Trunks

This activity provides support for PTS trunks configured on a GWC during all CS2K swact activities including norestartswact, restartswact, and abortswact.

83.4 Hardware Requirements or Dependencies

Succession Network Hardware

- CS2K
- CS2M
- GWC
- PVG with VSP3-0
- IP Router (i.e. Passport 8600)

83.5 Software Requirements or Dependencies

This activity makes changes to the CS2K core, GWC, and PVG software loads. In addition, changes are made to the CS2M software.

This activity has the following software dependencies:

- CS2K North American load - SNNCSH07
- GWC load - GC070
- SN07.1 PVG load - availability TBD
- SN07 CS2M load - CSM0007

83.6 Limitations and Restrictions

83.6.1 Office Parameters

Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. This chart will show which key PTS office parameters are not applicable to GWC PTS trunks.

Office Parameter	Still applicable to GWC PTS trunks?	Notes

PRE_SND_WK_DD_TIME (OFCSTD)	Yes	On originating wink start or delay dial trunks, this is the amount of time that the switch waits (minimum) before sending the leading edge of the start signal (either wink or DD) after origination has been detected. This parameter is in 10 millisecond granularity. This timing is not started until after the origination has been filtered (see ORIGFLTR in TRKGRP datafill).
REC_MAX_DD_TIME (OFCSTD)	No	Maximum duration Delay Dial recognized. On terminating DD trunks, any start signal with an off-hook duration of greater than this value will be considered glare. This is in 160 millisecond granularity.
REC_MAX_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_MIN_DD_TIME (OFCSTD)	No	Minimum duration Delay Dial recognized. On terminating DD trunks, any start signal with an off-hook duration of less than this value will be ignored (probably resulting in a 'no start dial' condition with a route advance). This parameter is in 10 millisecond granularity.
REC_MIN_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_PRE_DD_TIME (OFCSTD)	No	Timeout for receiving Delay Dial signal leading edge. On terminating DD trunks, the leading edge of the start signal must be received within this time or a "no start dial" condition will be experienced. This parameter is in 150 millisecond granularity. A value of 10 is recommended for GWC based and legacy trunks inter-connection.
REC_PRE_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
SND_DD_TIME (OFCSTD)	No	For DP trunks, this is the start signal duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.

SND_MF_WK_TIME (OFCSTD)	No	For non-DP trunks (MF trunks), this is the start signal wink duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_DP_WK_TIME (OFCSTD)	No	Same as above except for DP originators.
WK_DD_PRE_DIAL_ DELAY (OFCSTD)	Yes	On terminating wink and delay dial trunks, this is the time delay after the trailing edge of the start signal before outpulsing begins.
EA_REC_MAX_WK_T IME (OFCSTD)	Yes	Equal Access Receive Maximum Wink Time - This parameter specifies the maximum time for recognition of wink for ATC type trunk groups, in 10-ms intervals.
EA_REC_SUB_PRE_ WK_TIME (OFCSTD)	Yes	Equal Access Receive Subsequent Pre-wink - This parameter specifies the timeout for receiving the leading edge of next wink signals for ATC type trunk groups, in 160ms intervals.
EA_REC_1ST_PRE_W K_TIME (OFCSTD)	Yes	Equal Access Receive First Pre-wink Time - This parameter specifies the timeout for receiving the leading edge of the first wink signal for ATC type trunk groups, in 160-ms intervals.
EAEO_REC_1ST_PRE _WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive First Pre-wink Time - This parameter specifies the time of the first pre-wink delay associated with outpulsing from an equal access end office (EAEO), in 160 ms intervals.
EAEO_REC_2ND_PRE _WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive Second Pre-wink Time - This parameter specifies the time of the second pre-wink delay associated with outpulsing from an Equal Access End Office (EAEO), in 160-ms intervals.

IMMED_PRE_DIAL_DELAY (OFCSTD)	No, GWC PTS trunks will use a value of 1 second.	Two-way Immediate Start Trunks Pre-dial Delay - This parameter only applies to two-way immediate start and outgoing trunks. This parameter specifies the delay between seizure and outpulsing of digits, in 10-ms intervals.
MIN_REC_DP_PULSE_WD (OFCSTD)	No	Minimum Received Dial Pulse Width - This parameter allows variable settings for the minimum received dial pulse (DP) width.
PRE_ANI_SPILL_DELAY (OFCSTD)	Yes	Pre-automatic Number Identification Spill Delay - Switching units with outgoing trunks that perform wink and reversal signal calling number outpulsing require this parameter. This parameter specifies the delay between receiving the calling number request signal (wink), and outpulsing the calling number.
DPREC_INTER_DGT_TIMING (OFCSTD)	No	Interdigit timing in DP reception. This parameter specifies the end of digit timing value between two consecutive digits.
SHORT_TIMED_RELEASE_DISC_TIME (OFCSTD)	Yes	Disconnect timing performed on terminator disconnect. The Short TRD is typically used for unbilled calls.
LONG_TIMED_RELEASE_DISC_TIME (OFCENG)	Yes	Disconnect timing performed on terminator disconnect. The Long TRD is typically used for billed calls.
MF_LAST_DIGIT_DELAY (OFCENG)	No	This is a special interdigit delay between the second-to-last and last digit of an MF outpulsing stream. A value of 0 means the delay is no different than between other digits. This parameter is in 10 millisecond granularity.
ACK_WINK_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the delay between the end of the address stream and the leading edge of the acknowledgment wink. This parameter is in 10 millisecond granularity.

ANS_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the minimum delay between the trailing edge of the acknowledgment wink and offhook indicating answer. This parameter is in 10 millisecond granularity. 500 milliseconds seems large; however, in many cases the in-switch delay to route the call may be greater than 1/2 second.

83.6.2 Hybrid Office Restriction

A hybrid office configuration is not officially supported by this feature. Interworking Legacy agents with GWC PTS trunks require the use of an IW-SPM which is outside the scope of this development. This includes, but not limited to any test equipment that resides in an MTM shelf.

83.6.3 Universal Audio Server Restriction

The UAS does not support H.248 GWC PTS trunks since these trunks require support of the EG (Emergency) parameter. The UAS does not support use of the EG parameter and no further UAS development is planned. The AMS, Audio Media Gateway currently supports H.248 PTS GWC trunks and the EG parameter.

83.6.4 Dialtone Restriction

On some PTS trunk group types, EANT, DAL, ONAT, and possibly others, DIALTONE can be provisioned to values of S, C, or N, respectively Standard, Carrier, or None. The value of C is not restricted from provisioning, but when provisioned it will provide standard dialtone and not carrier dialtone. This restriction is based on the current limitations of the PVG.

83.6.5 Table DIGMAN Restriction

This feature does not support use of the DIGCOM field value of SIG in table DIGMAN with a pulse type of DT.

83.6.6 Table TRKGRP Restrictions

The following trunk group restrictions are enforced by the GWCPTSTK option in table TRKOPTS or the functionality has been determined to be unsupported for this feature.

83.6.6.1 OP Trunk Group Restrictions

- ANITYPE values of WK, REV, and NO are allowed but are restricted based on the value of the DIRection and MODE fields. The table below

provides a support matrix for the combinations of DIRection, ANITYPE, MODE.

Table 5 OP Trunk ANITYPE/Mode Support

DIR	ANITYPE	MODE	Supported
OG	REV	N/A	YES
OG	NO	N/A	NO
OG	WK	N/A	YES
2W	REV	AR/CR	YES
2W	REV	CV	YES
2W	REV	VF	NO
2W	NO	AR/CR	NO
2W	NO	CV	NO
2W	NO	VF	YES
2W	WK	AR/CR	YES
2W	WK	CV	YES
2W	WK	VF	NO

- HOLDTYPE value of JNTHOLD is disallowed for all OP groups.
- EAOSS value of N is allowed. Value of Y is disallowed.

83.6.6.2 ES Trunk Group Restrictions

- FDISCTIM is restricted to allow a value of 0 only.
- SWST is restricted to allow a value of DC only. AC and ADC are disallowed.
- ANI is restricted to allow a value of ANISPILL only. OUTPULSE and NOANI are disallowed.
- RMB has to be set to YES. A value of NO is disallowed.

83.6.6.3 PX Trunk Group Restrictions

No support for the TRKOPTS option DLYFWDXMT for PX trunks is provided by this feature.

83.6.6.4 IBNTI/IBNTO/IBNT2 Trunk Group Restrictions

This activity provides support for “basic call” only on IBN trunk groups. The following fields are restricted with table control, however, if any other field is outside the scope of “basic call”, then no support is implied.

Note: These 1st four fields conflict with requirements. Unsure how the support of these fields was agreed to as a requirement.

- DTI value is restricted to allow value of N. Value of Y is disallowed.
- TRKDSR value is restricted to allow value of N. Value of Y is disallowed.
- REORIG value is restricted to allow value of N. Value of Y is disallowed.
- FLASH value is restricted to allow value of N. Value of Y is disallowed.
- Disallowed IBN OPTIONS include PROPANS, ANISEND, ANIREC, ANIFAIL, DNIS, CLID, and OUTSCHM.

83.6.6.5 ATC Trunk Group Restrictions

None identified

83.6.6.6 IT Trunk Group Restrictions

None identified

83.6.6.7 SC Trunk Group Restrictions

- Option NOUTR is disallowed.

83.6.6.8 CELL Trunk Group Restrictions

None identified

83.6.6.9 DAL Trunk Group Restrictions

None identified

83.6.6.10 EANT Trunk Group Restrictions

None identified

83.6.6.11 ONAT Trunk Group Restrictions

None identified

83.6.7 Table TRKSGRP Restrictions

The following trunk subgroup restrictions are enforced by the GWCPTSTK option in table TRKOPTS and are common to subgroups of all GWC PTS trunk group types.

- SGRP field is restricted to a value of 0 only.
- CARDCODE field is restricted to values of DS1SIG, FXSLS, or FXGLS.
- SGRPVAR is restricted to a value of STD only
- IPULSTYP/OPULSTYP are restricted to allow values of MF, DP, NP, or DT only. Each trunk group type may have additional restrictions.
- Pulse type NP is only supported for Outgoing FXS trunks.

- Pulse types DP and DT are only supported for DAL, PX, and IBN trunk group types.
- ISTARTSG/OSTARTSG are restricted to allow values of WK, IM, DD, GS, or LS. Each trunk group type may have additional restrictions.
- CCONT is restricted to allow values of MW or NO.
- RNGBCK is restricted to allow values of MW or NO.
  - — Note: For GWC PTS trunks the CCONT and RNGBCK functionality is a function of the GW.
  - — Note: Selecting the MW value for RNGBCK is equivalent to turning ON the ringback feature on a particular GWC PTS trunk group. But the physical characteristics of the ringback signal are dictated by the PVG CAS profile associated with a particular carrier (that belongs to the same trunk group via provisioning)

    The PVG supports both types of physical ringback signalling - Expanded In-Band (EI) and Multi-Wink (MW). PVG CAS Profiles to Operator Ringback signalling types are mapped as:

    ds1sigMfr1.prof -> sets the operator ringback signal to EI

    ds1sigMwMfr1.prof -> sets the operator ringback signal to MW

    For the GWC PTS trunks to interact properly with external operator signalling equipment, the proper profile has to be set on that particular carrier on the PVG. This is a per-carrier restriction.
  - — Note: Operator Ringback functionality is only supported while using MF signalling.
- ESUPR is restricted to allow a value of N only.
- ECSTAT is restricted to allow values of EXTERNAL or INTERNAL only.
- Option SPMECIDX is disallowed on GWC PTS trunks.

83.6.8 Table TRKMEM Restrictions

Hybrid GWC PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are ***not*** supported.

83.6.9 GWC PTS Trunks Capacity/Engineering Restrictions

A maximum of 42 DS1s or 1008 DS0s worth of NA PTS trunks are supported on a per GWC basis.

For every PTS halfcall, H248/Megaco messages convey PTS trunk signalling and also the bearer path manipulation information to the PVG. This extensive messaging puts constraints on the GWC resources. Hence every GWC PTS trunk datafilled will use GWC resources equal to that of four (4) GWC ISUP trunks.

Table 6, “GWC Trunks Capacity And PTS trunks,” on page 793is meant to illustrate this restriction, in the context of supporting multiple trunk types on the GWC.

Table 6 GWC Trunks Capacity And PTS trunks

Number of PTS trunks Datafilled	Number of other (e.g. ISUP) trunks supported	Total GWC Trunks Capacity.
1008	0	1008
504	2078	2582
350	2694	3044
200	3294	3494
0	4094	4094

Note: This feature does not restrict the support of different trunk types on the GWC, it only restricts the number of other trunk types ‘members/end-points’ that can be datafilled along with the PTS trunk ‘members/end-points’.

83.7 Interactions

The goal of this activity is to provide transparency with the legacy DMS100 Switching System. The same service interactions and service restrictions that exist with legacy non-gwc PTS trunks will also apply to PTS trunks configured on a GWC.

This activity supports interworking with the following agent types during regular call processing as well as when a service interaction, such as three way calling or call transfer, results in a connection with a supported GWC PTS trunk.

- Line
- ISUP Trunk
- PRI Trunk
- SIPT Dynamic Packet Trunk (DPT)

83.8 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

- Data Schema __X___
- User Interface _____
- Element Management __X___
- Security _____
- Service Order _____
- Office Parameters __X___

Accounting (includes AMA billing) _____

Performance (includes operational measurements) __X___

83.9 Glossary

Term	**Description**
AMA	Automatic Message Accounting
ANI	Automatic Number Identification
B911	Basic 911
CAS	Channel Associated Signalling
CFL	Carrier Failure
CLI	Calling Line Identification
CS2K	Call Server 2000
DAL	Direct Access Line
DMS	Digital Multiplex System
DN	Directory Number
DP	Dial Pulse
DPT	Dynamic Packet Trunk
DTC	Digital Trunk Controller
E911	Emergency 911
EANT	Equal Access Network Trunk
EAOSS	Exchange Access Operator Services Signalling
EO	End Office

Term	**Description**
ES	Emergency Service
FGC	Feature Group C
GWC	Gateway Controller
I	Information (I) digit
IEC	Inter-Exchange Carrier
IETF	Internet Engineering Task Force
II	Information (II) digits
IP	Internet Protocol
LEC	Local Exchange Carrier
MAP	Maintenance and Administration Position
MF	Multi-Frequency
MG	Media Gateway
MG2000	Media Gateway 2000
OM	Operational Measurement
OP	Operator
OSS	Operator Services Signalling
PBX	Private Branch Exchange
PPVM	Peripheral Processor Virtual Machine
PRI	Primary Rate Interface
PTS	Per Trunk Signalling
PSTN	Public Switched Telephone Network
RBS	Robbed Bit Signalling
SESM	Succession Element and Sub-Element Manager
SS7	Signalling System Number 7
TMM	Trunk Maintenance Manager
TTP	Trunk Test Position

84: Functional Description (FN): A00003531

84.1 Feature name

MG9K EM – Frame location enhancements (A00003531)

This feature involves work in both MG9K-EM and SESM.

84.2 Description

This feature consists of following deliverables;

1. Office Frame number is displayed in MG9K EM Alarm browser, IEMS alarm browser and any other alarm browser/s provided by OSS.
2. Internal frame number is hard-coded to zero in VMG name, while provisioning VMG.
3. In MG9K-EM Frameview, frames are displayed without gap. However, any gap present between shelves will continue to be displayed.

   With this change, MG9K-EM Frame view is displayed in a cleaner way. Some of the examples for this cleaner display are;

- MG9K-EM Craft-person can see Master frame as and when he/she opens the Frame view, even when Master frame has two or more empty frames to its left side.
- MG9K-EM Craft-person can see adjacent frames, without scrolling to right in Frameview, even when there is gap between the frames.

4. In MG9K-EM Frameview, Master frame is shown far left and all subtending frames are shown to the right of Master frame going by following logic.

   - Show Master frame far left.

   - Show other frames, whose frame number is higher than that of Master frame on right of Master frame, in increasing order of their Internal frame number (IFN).

   -And then, show other frames, whose IFN is lower than that of Master frame, in increasing order of their IFNs.

As a result of the deliverables #3 and #4, Frameview may not be a mirror reflection of actual line-up of frames in MG9K.

Note that, as in SN6.2, in MG9K-EM Frame view, Internal frame number is shown at the bottom of each frame and Office frame number is shown at the top of each frame. With this, Craft-person can map the MG9K-EM Frame view to actual line-up of frames in MG9K.

5. Office Frame number is used in place of Internal frame number in OMC CSV OM file

6. A *complete* flow through provisioning is supported for ITP VMGs. With this, Frame location information, which is specified in MG9K-EM while provisioning ITP VMGs, is sent to SESM. SESM in turn, updates XA-CORE table LGRPINV.

   With these changes, Craft-person need not manually fill Frame location information in the table LGRPINV. Craft-person just need to provision Frame location information at MG9K-EM

7. A *partial* flow through provisioning is supported for ABI VMGs. With this, Frame location information, which is specified in MG9K-EM while provisioning ABI VMGs, is sent to SESM. However, SESM does not in turn updates XA-CORE table GWINV.

   There is no impact on the way Craft-person handles ABI VMGs, because of these changes. i.e., he/she still needs to manually fill Frame location information in the table GWINV, apart from provisioning Frame location information at MG9K-EM.

   Note: GWINV is a new table, which will be supported in SN07 through the Core feature A00003486 (Gateway location information).

84.2.1 MG9K-EM Frame view

This section gives example screen shots for the deliverable #3 and #4, which are explained in 2.1. For this, two different scenarios are considered.

84.2.1.1 Scenario 1

Let us consider a scenario wherein frames are lined-up from left to right as follows;

- First frame is numbered as 1 and is Master frame
- Second frame is numbered as 3 and is subtending frame

For this scenario, in SN06.2, craft-person need to use horizontal scroll bar to see the non-empty frames (frame #1 and frame #3) and MG9K-EM Frame view would looks like figure #1 and figure #2.

For this scenario, in SN07, craft-person see the non-empty frames as and when he/she opens the Frameview and MG9K-EM Frame view would looks like figure #3.

Even when frames are lined-up from right to left, in both SN06.2 and SN07, Frame view will look the same way as in left to right lineup.

Figure 1 MG9K-EM Frame view in SN06.2 and prior – when Frame view comes up

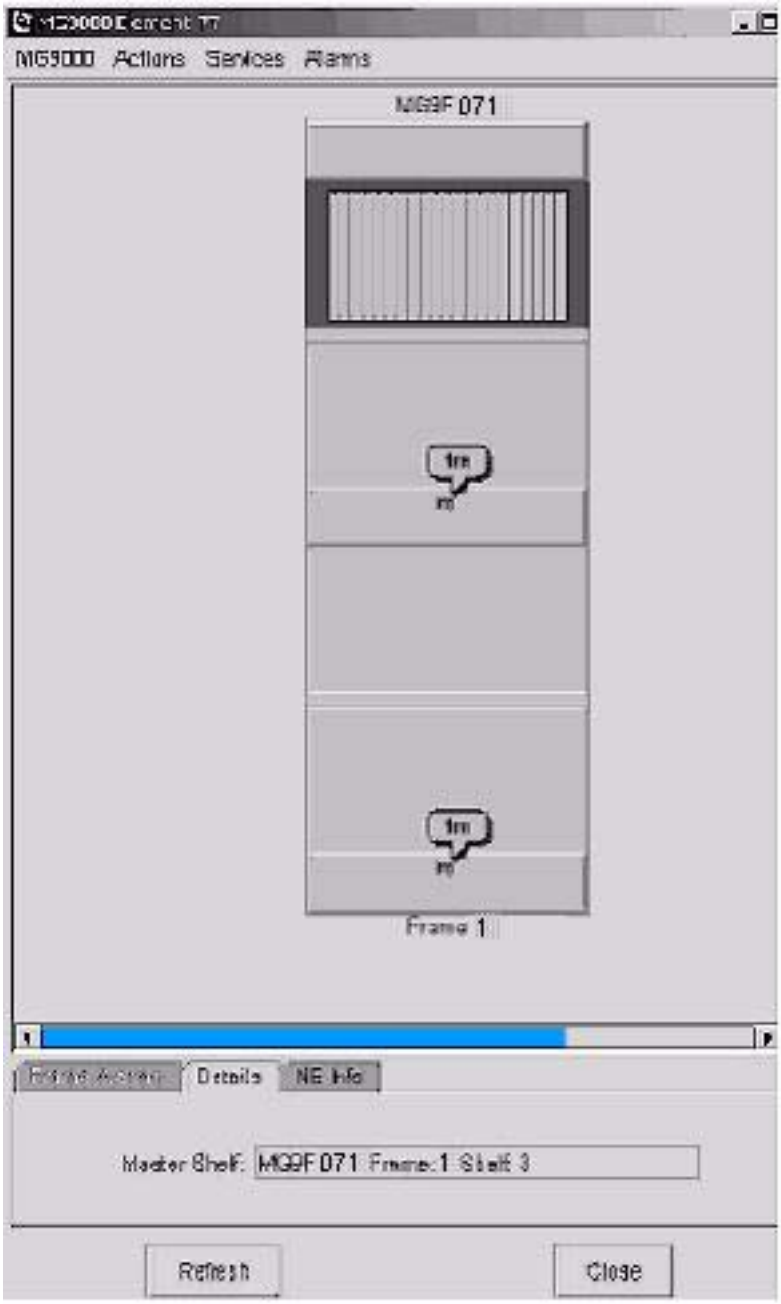


Figure 2 MG9K-EM Frame view in SN06.2 and prior – Horizontally scrolled far right

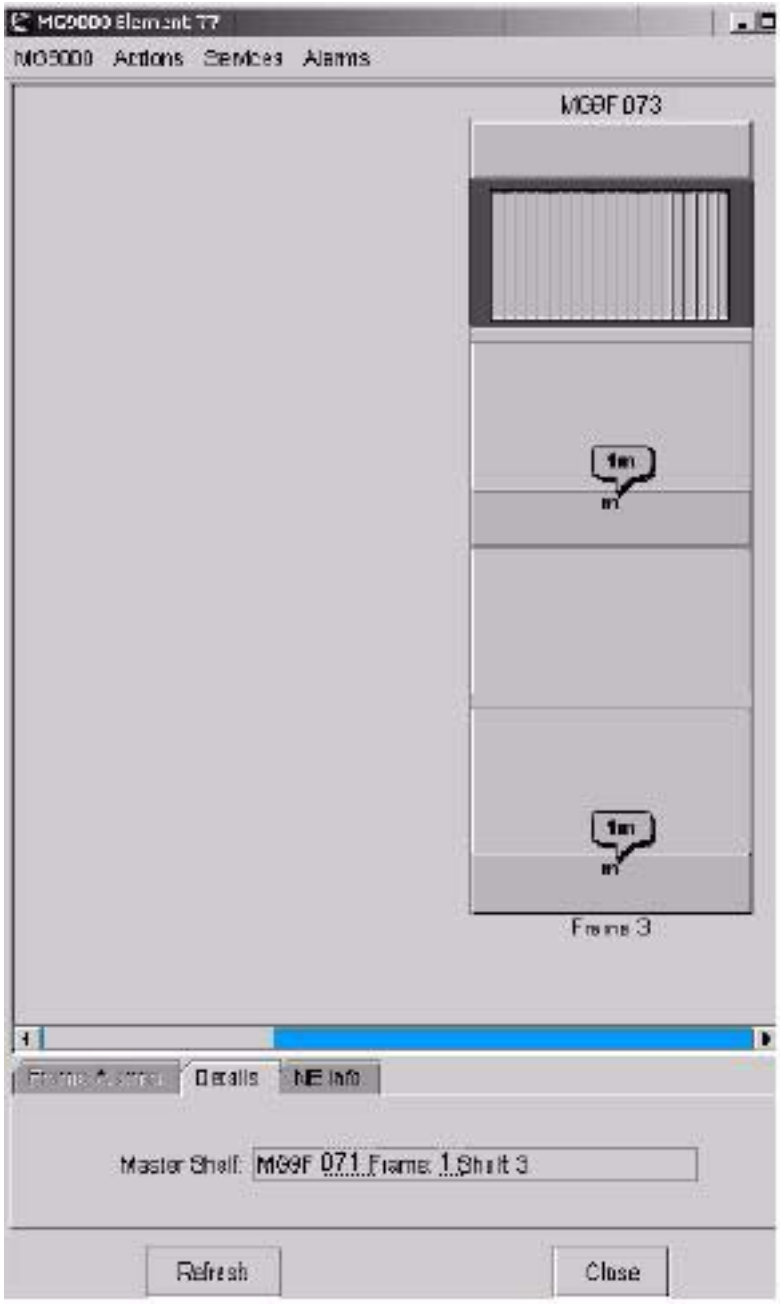
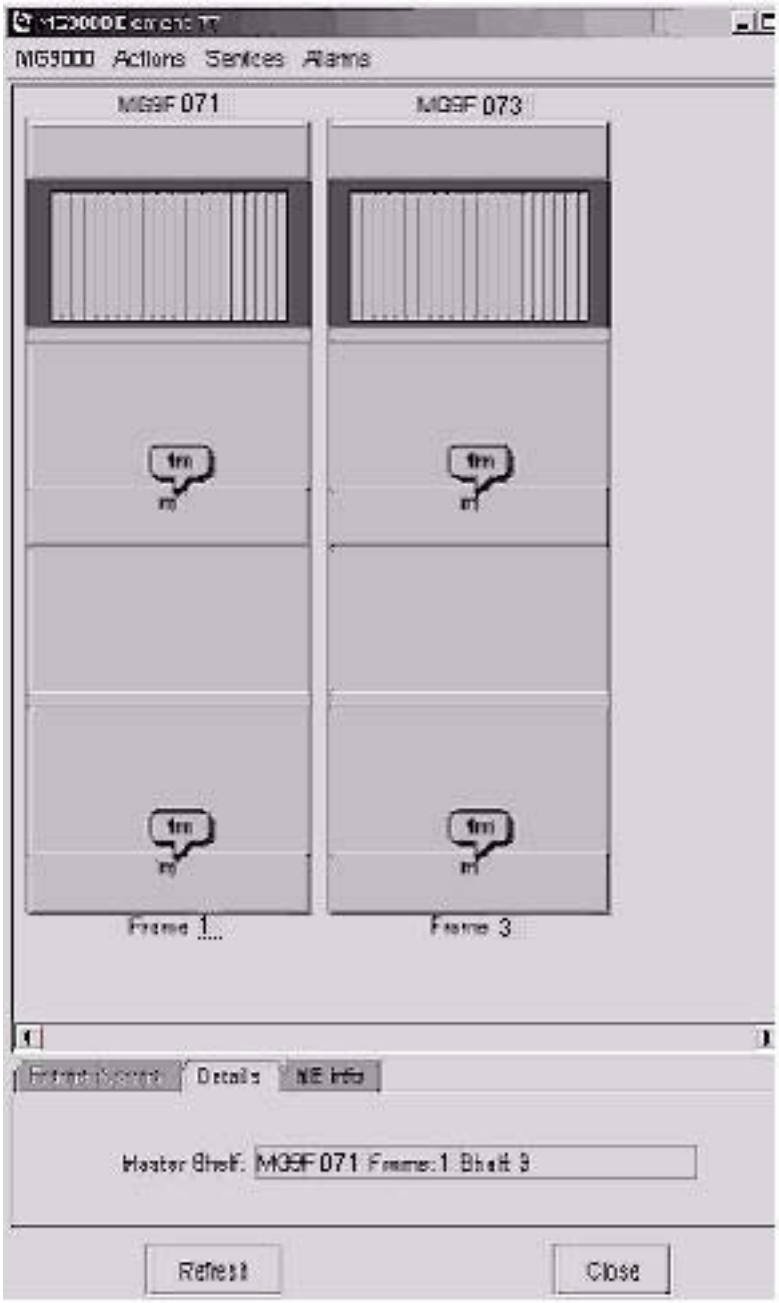


Figure 3 MG9K-EM Frame view in SN07



84.2.1.2 Scenario 2

Let us consider a scenario wherein frames are numbered as follows;

- First frame is numbered as 5 and is Master frame
- Subsequent three subtending frames are numbered as 7, 0 and 2 .

For this scenario, in SN06.2, frames would be shown in increasing order of their Internal frame numbers. i.e, as [frame #0][frame #2][frame #5][frame #7]).

For this scenario, in SN07, frames would be shown as [frame #5][frame #7][frame #0][frame #2]); refer to the logic given in section 2.2 point #4.

84.2.2 MG9K-EM Alarm browser

Following figure is an example screen shot for the deliverable #1, which is explained in section 2.1. Note that, without Frame location information being provisioned, 'Description' field in the Alarm browser is shown with default filler 'F' in following format;

Site Flr RPos Bay_id

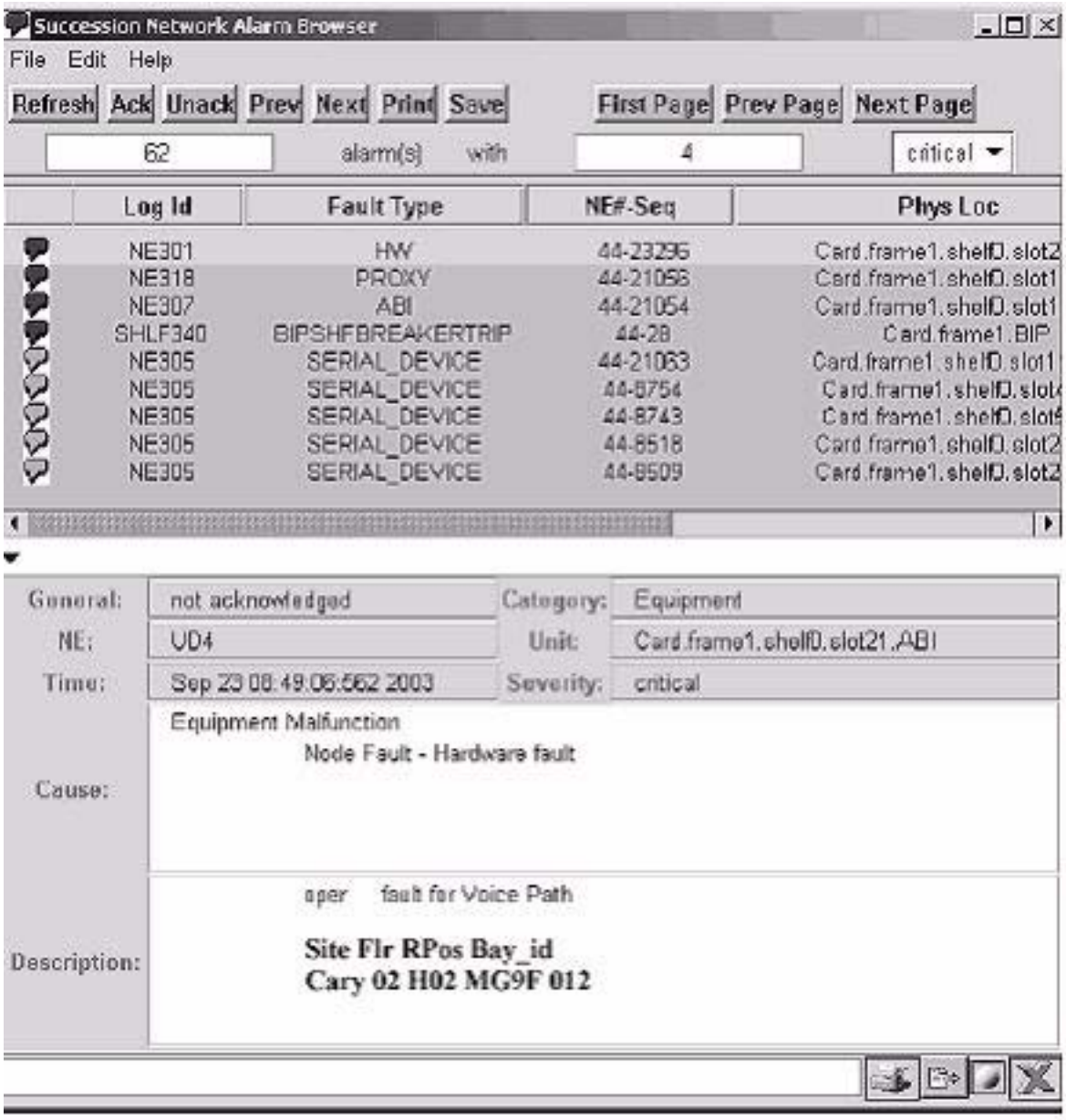
FFFF FF FFFF MG9F FFF

i.e., <Site=FFFF><3 blank space><Flr=FF><2 blank space><RPos=FFFF><3 blank space><Bay-id=MG9F FFF>

When Frame location information is (re)provisioned for a Master frame, all alarms (both Gateway alarms and EM alarms) reported on components in the frame are updated with latest frame location information.

When Frame location information is (re)provisioned for a subtending frame, only Gateway alarms reported on components in the frame are updated with latest frame location information.

Figure 4 MG9K-EM Alarm browser GUI

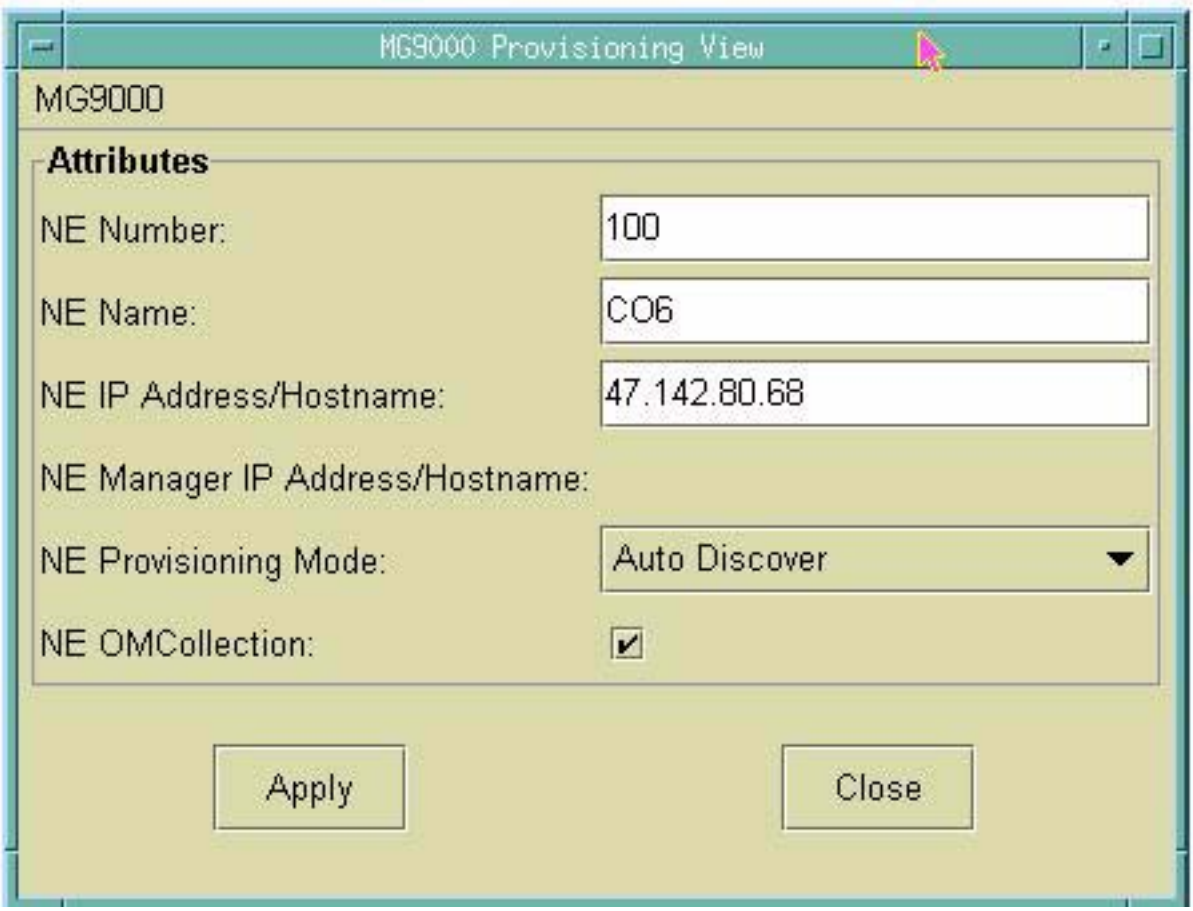


84.2.3 MG9K EM MG9000 Provisioning view

In SN07, a new checkbox “NE OMCollection” is introduced in MG000 Provisioning GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection

cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

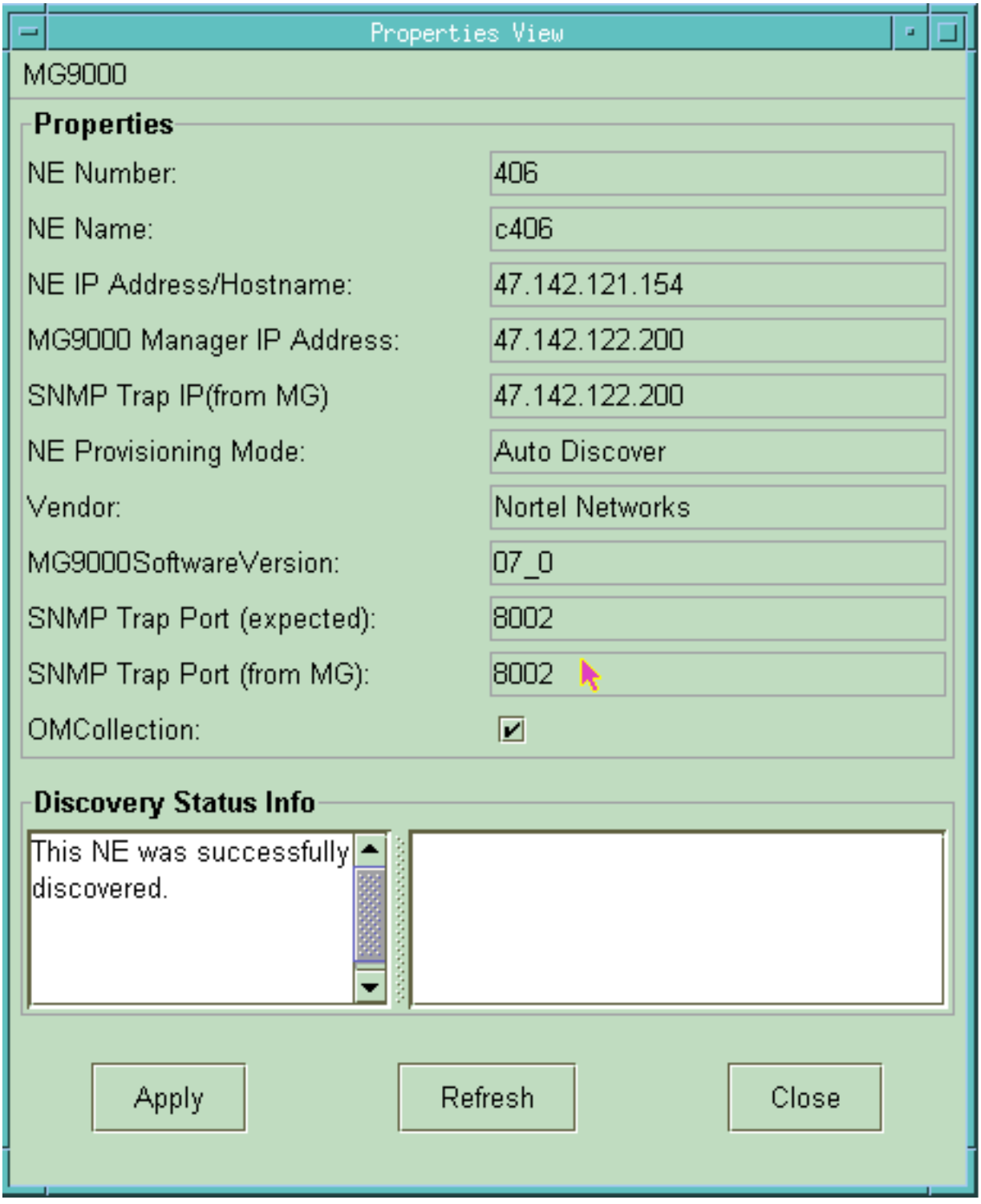
Figure 5 MG9K-EM "MG9000 Provisioning" GUI when "NE OMCollection" is checked



84.2.4 MG9K EM NE Properties view

In SN07, a new checkbox "NE OMCollection" is introduced in NE Properties GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

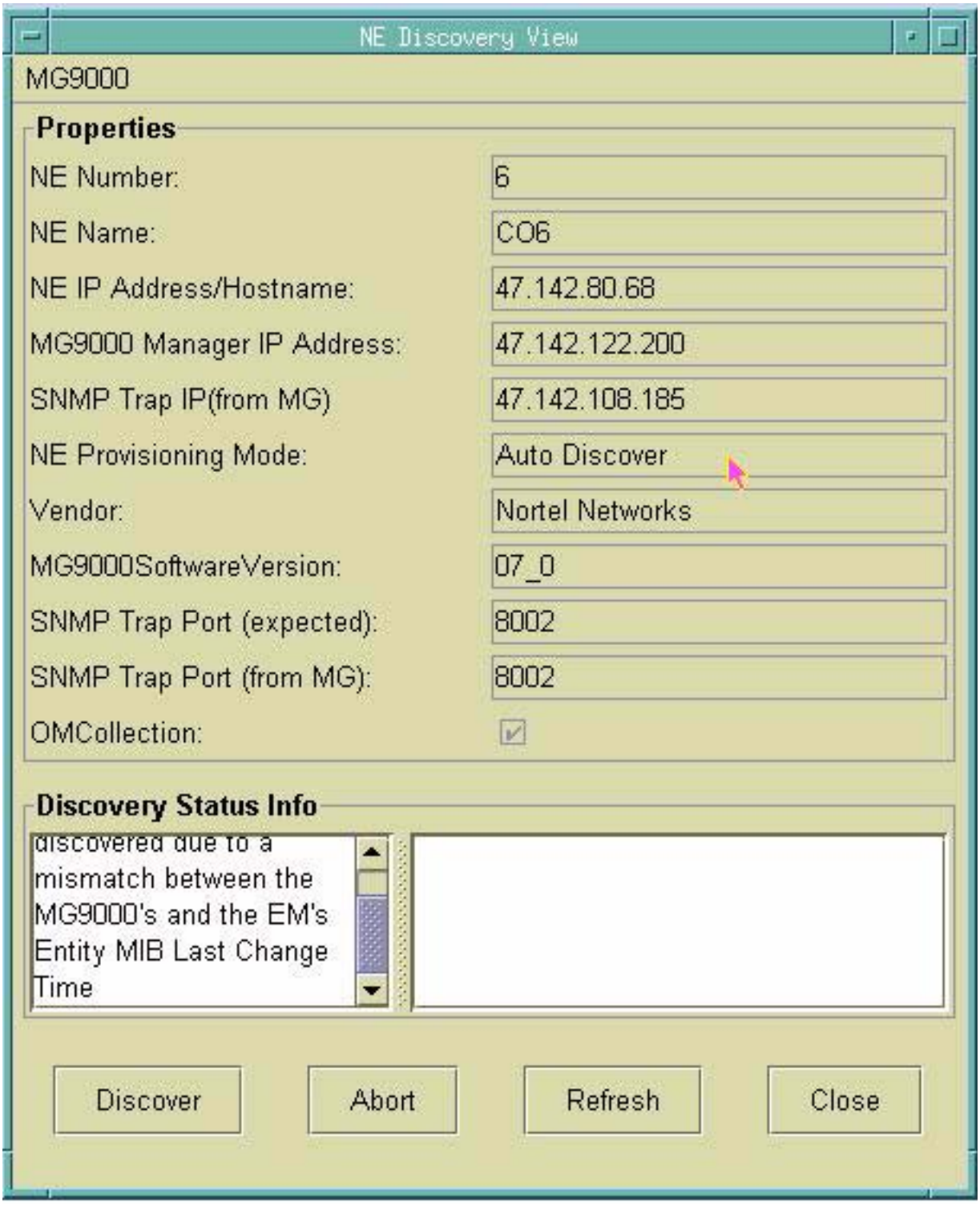
Figure 6 MG9K-EM “NE Properties” GUI when “NE Collection” is checked



84.2.5 MG9K EM NE Discovery view

In SN07, a new checkbox “NE OMCollection” is introduced in NE Discovery GUI. This is a read-only field. It indicates whether OM data collection is enabled or disabled.

Figure 7 MG9K-EM “NE Discovery” GUI when “NE Collection” is checked



84.2.6 MG9K EM NE OM Collector

Starting from SN07, OM Collector depends on MG9K EM as explained below.

- Before OM Collector could start collecting OM data for a NE, as explained in section 2.2.3, the NE has to be created in MG9KEM with “NE Collection” check box checked.

- OM Collector will either stop or restart collecting OM data based on the status of “NE OMCollection” checkbox of MG9KEM. As explained in sections 2.2.4 and 2.2.5, value of the checkbox “NE OMCollection” is modifiable in MG9KEM.

That means, OM Collector need to know IP address of the MG9KEM, with which it is associated. Operator can configure IP address of MG9KEM server through the script "/opt/nortel/omcltr_07/bin/OMCollector config".

84.3 Hardware Requirements or Dependencies

None

84.4 Software Requirements or Dependencies

This feature depends on MG9K changes for the deliverable #5, mentioned in section 2.2.

84.5 Limitations and restrictions

1. VMGs which are provisioned in SN05/SN06+ with non-zero Internal frame number, continue to exist as they are. i.e., they continue to exist with non-zero Internal frame number.
2. Frame location information is sent from MG9K-EM to SESM only at VMG provisioning time. So, any changes done to Frame location information from MG9K-EM after VMG is provisioned, is not sent to SESM. Frame location information present at XACore can be changed, even after VMG is provisioned. Any mismatch, which is introduced as result of such changes, is not audited or corrected.
3. A complete flow through provisioning is not supported for ABI VMGs Hence, for ABI VMGs, Craft-person need to manually enter Frame location information in XA-CORE table GWINV.

84.6 Interactions

This feature is an extension of the SN06.2 feature A00002704 and leverages the work of A00002704, to deliver the items 1 to 6 mentioned in section 2.2, which have impact on the end user.

84.7 Applicable customer facing sections

Indicate with an "X" the customer facing section(s) of the DDOC that apply to this functionality. Indicate with "N/A" the customer facing sections(s) of the DDOC that do not apply to this functionality. The designer(s) of this functionality must complete sections indicated.

Fault Management:

Logs	____X____
Alarms	____X____

Configuration:

Data Schema	____X____
User Interface	____X[1]____
Element Management	____X____
Security	____N/A____
Service Order	____N/A____
Office Parameters	____N/A____

Accounting (includes AMA billing)	____N/A____
Performance (includes operational measurements	____X____

84.8 Glossary

Term	Description
CSV	Comma separated values. One format of storing performance data
EM alarm	Alarm generated internally by MG9K EM. Ex; When communication from MG9K EM to MG9K goes down, MG9K-EM generates an alarm with specific problem "Comm Channel Down - Communication Lost to the NE".
Frame location information	It consists of frame type, floor position, row position, frame position, shelf position
Internal (logical) frame number	Frame number, which is unique within a MG9K

[1] Alarm browser GUI would show Frame location information.

Gateway alarm	Alarm reported from gateway.
Master frame	It has the master shelf.
NE	Network element
Office frame number	Frame number, which is unique within an office
OMC	OM Collector
OM data	Operational Measurement data. A.k.a performance data
MG9K frame line-up	MG9K frames are lined-up either left to right or right to left. When frames are lined-up left to right, new frames are positioned/added to right of existing frames, as MG9K grows and frames are numbered from left to right. That means, Master frame will be the left-most frame in the NE. When frames are lined-up right to left, new frames are positioned/added to left of existing frames, as MG9K grows and frames are numbered from right to left. That means, Master frame will be the right-most frame in the NE.
Subtending frame	It has the subtending shelves of a MG9K
VMG	Virtual Media Gateway is a logical representation of a gateway

84.9 References

- [DID] A00003531_MG9000_Frame_Location_DID.pdf V1.3
- A00003486 Gateway location information FN

85: Functional Description (FN): A00003560

85.1 Feature name and Feature ID

Patching SSPFS, CBM, and IEMS via the NPM

A00003560

Document Version: 1.1

85.2 Description

The Network Patch Manager is responsible for patching many Succession Network components previous to SN07. These components include:

GWC cards
MG9K-based cards
SESM
SAM21 EM
NPM
PSE
QCA
MG9K server
MG9K midtier
OM Collector

Beginning with this feature in SN07, the Network Patch Manager is used to patch additional components in Succession Networks as well as components in non-Succession configurations. These new components include the following:

CBM - Core Billing Manager
SSPFS platform
IEMS - Integrated Element Management System

85.2.1 NPM Installation and Configuration

Prior to SN07, the NPM is always installed on the SSPFS machine that contains the CS2000 Management load. Beginning with this feature in SN07, the NPM is delivered as part of the SSPFS platform and not the CS2000 Management load.

In existing customer sites where an NPM is moving from one physical box to another physical box, a migration process is required to ensure the new NPM contains any necessary previous data. This migration process includes the following:

- saving any customer-specific predefined reports that are stored in the NPM database
- saving all patch files from the golden directory
- movement of the data in the previous bullets from the old machine to the new machine
- re-datafilling of the predefined reports into the new NPM
- saving of the patch files in the golden directory on the new machine

In a given customer site, only one NPM should be installed. The SSPFS installation/upgrade/configuration scripts assist in identifying which SSPFS-based machine should have the NPM software installed. In general, the SSPFS-based machine that is to contain the IEMS application is the machine that should have the NPM installed. If an IEMS is not part of a customer site installation, the NPM should be installed on the same machine as the CBM application.

The various supported configurations are now discussed.

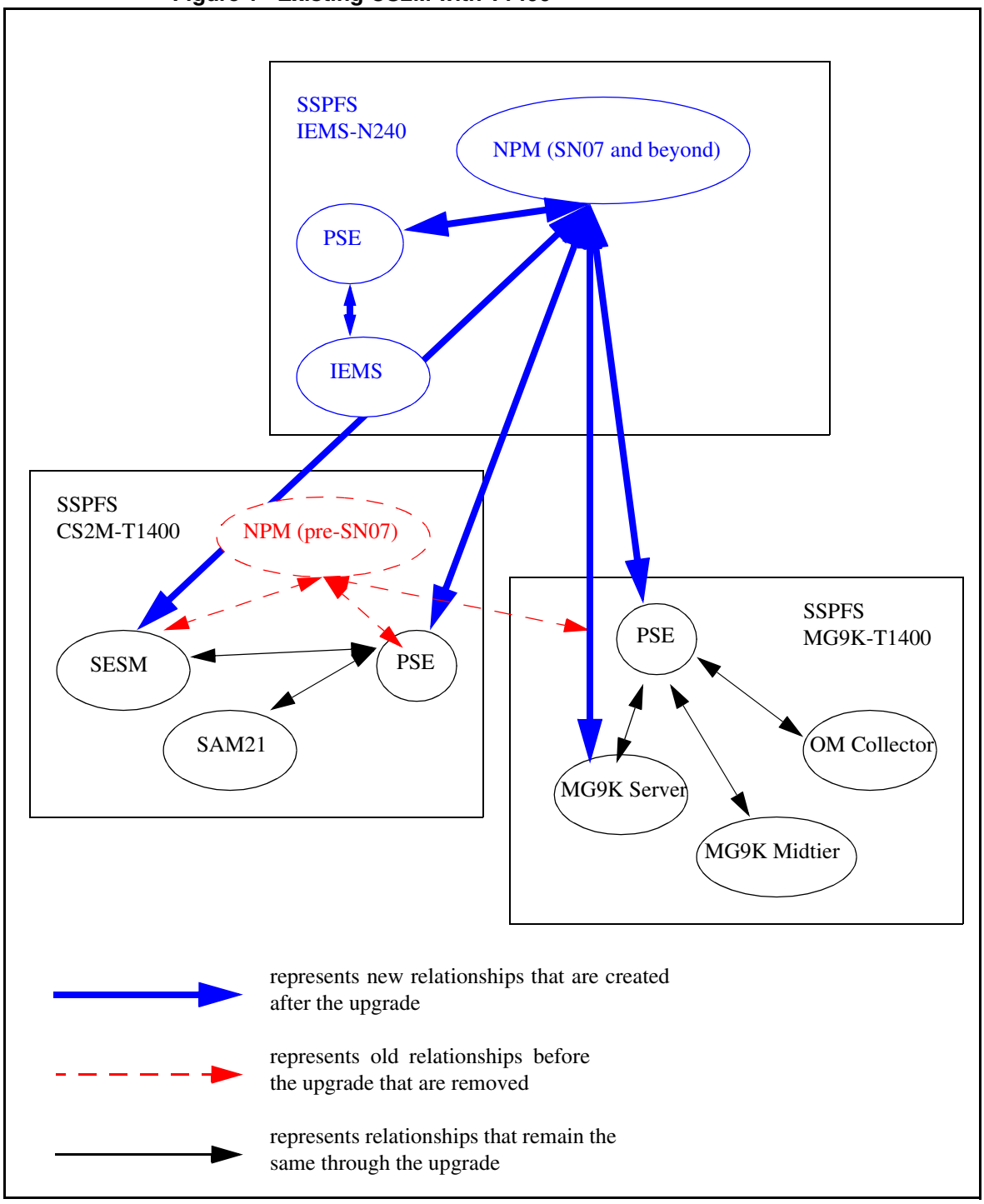
85.2.1.1 Existing CS2M on a T1400

In this configuration, an existing CS2000 customer site is being upgraded to SN07. The site has an existing T1400 SSPFS-based machine with NPM already installed and running with pre-SN07 software. Figure 1, "Existing CS2M with T1400" shows this site with a new N240 being installed that contains the IEMS and NPM running SN07. After the upgrade, the CS2M-based T1400 continues to run in the customer site (with SN07 CS2M software) without the NPM since it would be installed on the new N240 machine. In addition if MG9K EM components are present, these SSPFS-based machines continue to run on T1400(s) with the new SN07 software.

It should be noted in the figure that other patchable components may exist but are not shown to reduce the complexity of the diagram. In addition, the MG9K EM components running on 1 T1400 in the figure may run on separate T1400s. The components not listed in the figure may include:

- optional QCA application running on the T1400 that communicates with the PSE local to the T1400
- the CBM component being introduced in SN07 may be installed on the N240 along with the NPM and IEMS

Figure 1 Existing CS2M with T1400



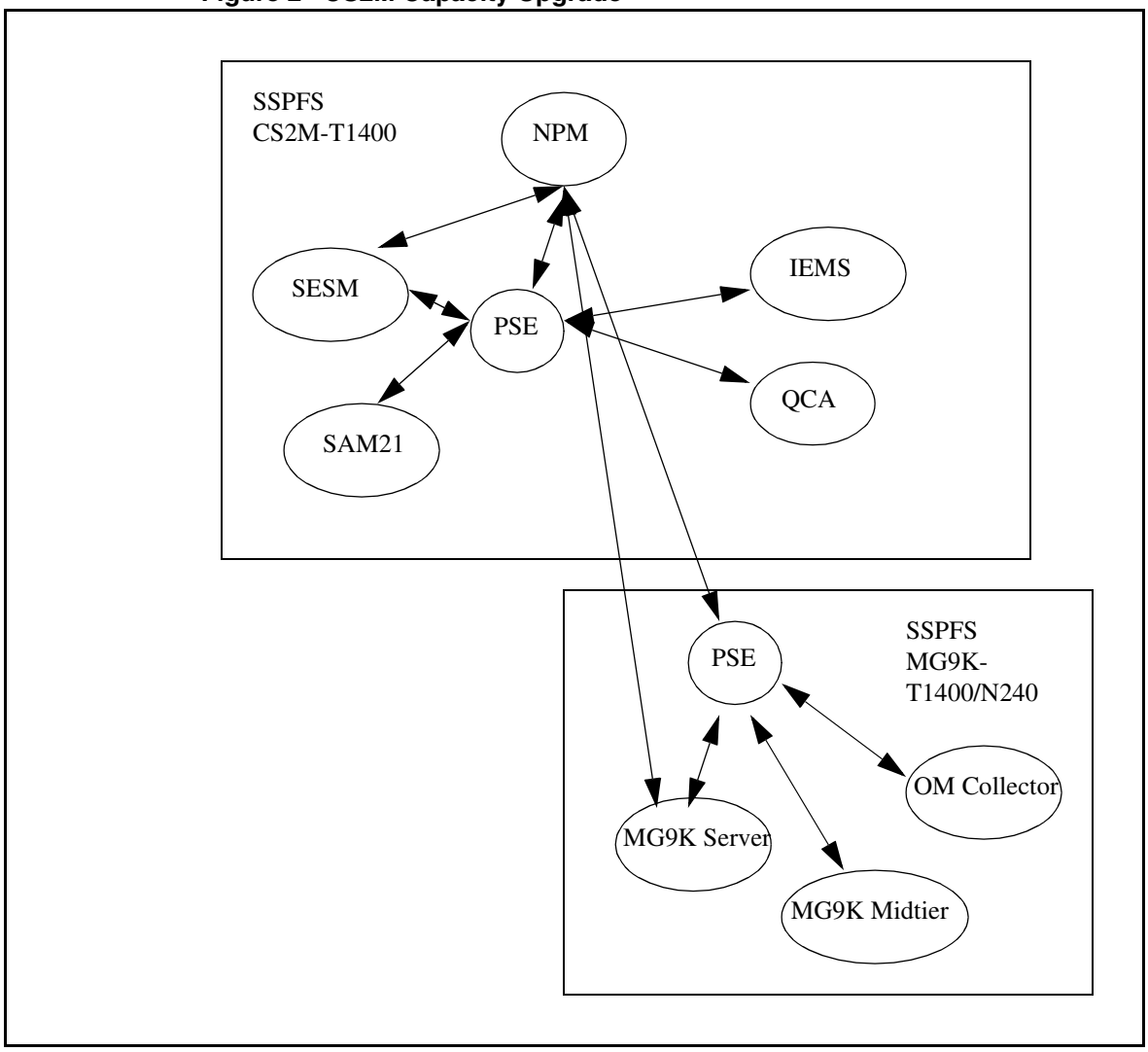
The following steps are required during the upgrade process in this configuration:

- the new N240 machine is commissioned with the SN07 versions of the IEMS and NPM installed on the machine
- the CS2M machine is upgraded to SN07, this process consists of the following:
  - — the PSE on the CS2M T1400 machine is configured to look at the CORBA name service on the new N240 machine
  - — the SESM application is upgraded, the EPM component within SESM now looks at the name service hostname associated with the local PSE to find the location of the NPM (this step ensures the GWCs associated with the EPM are registered with the new NPM)
  - — the NPM is not upgraded in the CS2M T1400 machine (i.e. effectively it is uninstalled)
- the MG9K machine (if present) is upgraded to SN07, this process consists of the following:
  - — the PSE on the MG9K-based T1400 machine(s) are configured to look at the CORBA name service on the new N240 machine
  - — the MG9K components are upgraded, the EPM component within the MG9K-server component now looks at the name service hostname associated with the local PSE to find the location of the NPM (this step ensures the MG9K-based cards associated with the EPM(s) are registered with the new NPM)

85.2.1.2 Existing CS2M gets a Capacity Upgrade

In this configuration, an existing CS2000 customer site has software that is being upgraded from pre-SN07 software to SN07 software and also has hardware that is being upgraded from a T1400 to an SN240. With this scenario, the IEMS component is loaded into the existing CS2M machine. Hence, there is only one place where the NPM can reside. Figure 2, "CS2M Capacity Upgrade" shows this configuration. Optionally shown in the figure is an MG9K-based machine that can run on a T1400 or N240 machine. Regardless of the number of MG9K-based machines or hardware, the NPM and PSEs are configured in the same way.

Figure 2 CS2M Capacity Upgrade



The following steps are required during the upgrade process in this configuration:

- the CS2M T1400 machine is upgraded to an N240 machine
- the SSPFS software on the N240 machine is upgraded to SN07
  - — SSPFS software is upgraded
  - — the PSE on this machine is upgraded to SN07 (since the NPM and PSE will coreside on this box, no configuration of a CORBA name service host is necessary on this machine)
  - — the old version of NPM is unloaded and the SN07 version is loaded
- IEMS is installed on the N240
- CBM is installed on the N240

- the remainder of the applications on the CS2M machine are upgraded to SN07
- the MG9K machine(s) (if present) are upgraded to SN07, from a patching perspective there are no modifications to the existing upgrade procedure

85.2.1.3 New CS2M Office gets an N240

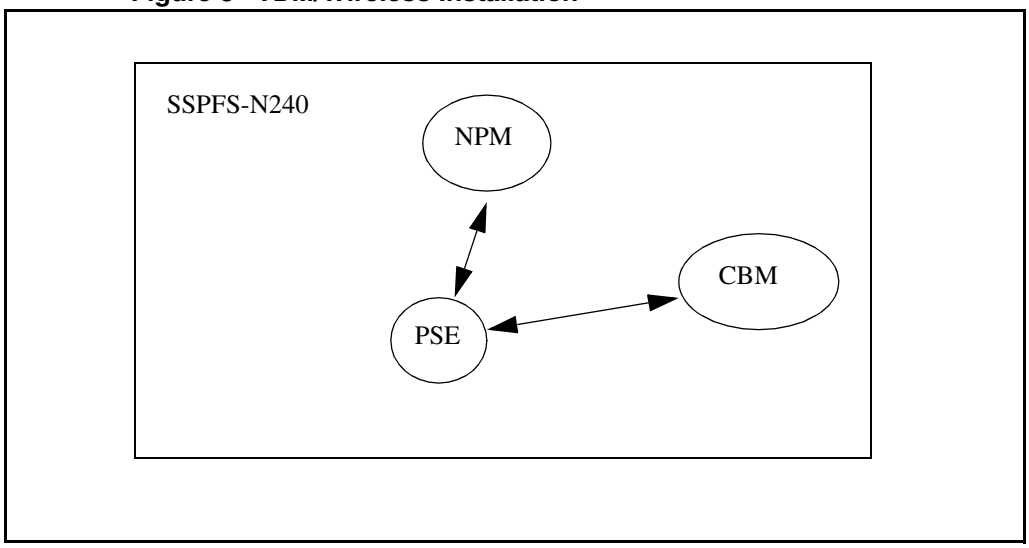
This scenario is similar to the configuration in figure 2. The only difference is this scenario is a ‘new install’ instead of an upgrade. The following steps are required during this ‘new install’ process:

- the SSPFS SN07 software on the N240 machine is installed
  - — SSPFS software is installed
  - — the SN07 PSE on this machine is installed (since the NPM and PSE will coreside on this box, no configuration of a CORBA name service host is necessary on this machine)
  - — the SN07 NPM is installed
- IEMS is installed on the N240
- CBM is installed on the N240
- the remainder of the applications on the CS2M machine are installed with SN07 software
- the MG9K machine(s) (if present) are installed with SN07 software, from a patching perspective there are no modifications to the existing installation procedure

85.2.1.4 TDM/Wireless

Beginning in SN07, existing TDM/wireless customers will be receiving an N240 SSPFS-based machine to handle CBM (SDM in the AIX-based configuration) instead of the SDM (Supernode Data Manager). Since there is only one SSPFS-based machine in this configuration, the NPM can only reside on this machine. In SN07 the process of receiving the new N240 machine is treated as a new install from a patching software perspective since the NPM and PSE components did not exist in this configuration prior to SN07. Figure 3, "TDM/Wireless Installation" shows this configuration.

Figure 3 TDM/Wireless Installation



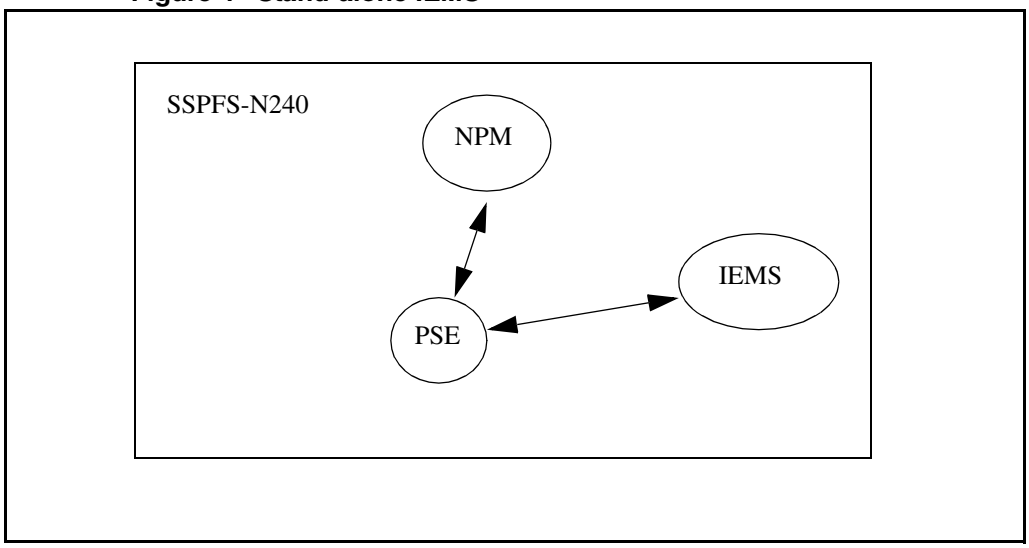
The following steps are required during this ‘new install’ process:

- the SSPFS SN07 software on the N240 machine is installed
  - SSPFS software is installed
  - the SN07 PSE on this machine is installed (since the NPM and PSE will coreside on this box, no configuration of a CORBA name service host is necessary on this machine)
  - the SN07 NPM is installed
- CBM is installed on the N240

85.2.1.5 Stand-alone IEMS

Beginning in SN07, a stand-alone IEMS configuration is supported. This configuration is similar to “85.2.1.4 TDM/Wireless” from a patching software perspective as it is a ‘new install’. Since there is only one SSPFS-based machine in this configuration, the NPM can only reside on this machine. Figure 4, "Stand-alone IEMS" shows this configuration.

Figure 4 Stand-alone IEMS



The following steps are required during this ‘new install’ process:

- the SSPFS SN07 software on the N240 machine is installed
  - — SSPFS software is installed
  - — the SN07 PSE on this machine is installed (since the NPM and PSE will coreside on this box, no configuration of a CORBA name service host is necessary on this machine)
  - — the SN07 NPM is installed
- IEMS is installed on the N240

85.2.2 Only One NPM

There should only be one NPM server installed in each site. This feature attempts to ensure only one NPM is installed via the following ways.

- SSPFS profiles
  No NPM should be installed on an MG9K-based machine. An NPM is preferred to be installed on the IEMS-based machine.
- verification of the PSE NS hostname when the NPM server is started
  When the PSE is configured, the configuration step asks for the hostname/ip address of the NPM server location. This feature modifies the NPM server to look at that configuration value. If the value is ever different from the local machine, the NPM fails to start.

While these steps help prevent more than one NPM from being installed, it is not a guarantee that it will prevent the scenario from occuring.

85.2.3 Patching Maintenance

When the new NPM patchable applications are installed (CBM, SSPFS, and IEMS), the NPM automatically becomes aware of the components. These

components appear in reports and the device list of the GUI. The following functions that exist for other targets in previous releases are now available for IEMS, CBM, and SSPFS.

- apply
- remove
- audit
- restart (IEMS only)
- set/report creation
- plans/automation
- alarms

85.2.3.1 IEMS

Similar to the existing OAM Java-based applications like SESM, SAM21EM, and MG9K EM components, the IEMS requires 2 steps for application and 2 steps for removal of patches.

application

- apply command from the NPM GUI or CLUI (sets patch to applied/ disabled)
- restart command from the NPM GUI or CLUI on IEMS (sets patch to applied/enabled)

removal

- remove command from the NPM GUI or CLUI (sets patch to removed/ enabled)
- restart command from the NPM GUI or CLUI on IEMS to disable the patch (sets patch to removed/disabled)

Beginning in SN06.2, the restart operation from the NPM GUI and CLUI can be automatically scheduled via NPM plans (autorestart). This capability is similar to the automatic application of patches.

85.2.3.2 SSPFS and CBM

Patches that are created and require application to the SSPFS and CBM components require one step from the NPM GUI or CLUI. Likewise for the removal operation. A single apply command or remove command from the NPM GUI or CLUI is sufficient for complete application or removal. If the associated application requires a restart or recreation of an existing process for application or removal, the ‘restart’ action is initiated during the single apply or remove request.

In some cases, an SSPFS or CBM patch may require additional action outside of the NPM GUI or CLUI for complete application or removal. In these cases, the patch is marked as non-autoappliable and contains special application instructions that describes the extra actions that are required.

For application of these patches, the patch appears as applied/disabled after the NPM apply command from the NPM GUI/CLUI. The extra actions described in the special application instructions automatically trigger the patch to become applied/enabled when the actions have been successfully completed. This behavior is also applicable for the remove scenario.

85.2.3.3 Full Matrix

Table 1, “Target/Command Matrix,” on page 821 shows a complete list of patchable applications/devices that are supported by the NPM in SN07. The table indicates the necessary commands required to fully apply or remove patches and whether automation is supported.

Table 1: Target/Command Matrix

	Full Application		Full Removal			
Target	Apply Cmd Required	Restart Cmd Required to enable	Remove Cmd Required	Restart Cmd Required to disable	autoapply supported	autorestart supported
MG9K Cards (OC3, SCI, SCO, ITP, ITX, DS1, ABI)	yes	no	yes	no	yes	n/a
GWC Cards	yes	no	yes	no	yes	n/a
SESM	yes	yes	yes	yes	yes	yes
SAM21 EM	yes	yes	yes	yes	yes	yes
NPM	yes	yes	yes	yes	yes	yes
PSE	yes	yes	yes	yes	yes	yes
QCA	yes	yes	yes	yes	yes	no

Table 1: Target/Command Matrix

	Full Application		Full Removal			
Target	Apply Cmd Required	Restart Cmd Required to enable	Remove Cmd Required	Restart Cmd Required to disable	autoapply supported	autorestart supported
MG9K server	yes	yes	yes	yes	yes	yes
MG9K midtier	yes	yes	yes	yes	yes	yes
OM Collector	yes	yes	yes	yes	yes	yes
IEMS	yes	yes	yes	yes	yes	yes
SSPFS	yes	no[a]	yes	no[a]	yes	n/a
CBM	yes	no[a]	yes	no[a]	yes	n/a

a. In some cases SSPFS or CBM patches may require reboot of applications or machines. These patches are marked as non-autoappliable and require human intervention.

85.2.4 Patch File Format Modifications

For the NPM to track different software with various behaviors, the patch file format is modified with this feature. While the specific details of the patch file format are not in this section, they can be found in the CN document associated with this feature.

85.2.5 Patch Calculation for CBM and SSPFS Patches

Prior to SN07, all NPM-based patching uses a loadname associated with a given device or application to perform patch calculation in determining what patches calculate for any given office. All previous SN07 patch types will continue to use the loadname for calculation purposes.

Beginning in SN07 with this feature, CBM and SSPFS patches that are tracked by the NPM use a new record in addition to the loadname. A functional component record (fc) is introduced into the patch file and the NPM database. This new record is tracked against CBM/SSPFS patches and CBM/SSPFS applications.

The NPM ‘getpatch’ command and ‘apply’ command are updated with this feature to check for the presence of functional component records in a patch file. If these records are present, the records are compared against the the fc’s associated with the devices in the office in addition to the loadname. Both the loadname and functional component records must match for the given patch to calculate for the office.

85.2.6 QCA Patches with Autorestart=”n”

The optional QCA application became patchable via the NPM beginning in SN06.2. With this feature and the patch file format modifications, all QCA patches have the autorestart flag set to ‘n’ by default. This modification is necessary to ensure that the QCA application does not lose service by virtue of an NPM automated task triggering the action. As the QCA application tracks critical customer data, the prevention of unforseen data is paramount.

85.3 Applicable customer facing sections

Fault Management

Not applicable	_X____
Logs	_N/A__
Alarms	_N/A__

Configuration

Not applicable	_____
Data Schema/MIBs	_X____
User Interface	_X____
GUI	__N/A_
Element Management	__N/A_
Security	_N/A__
Service Order	_N/A__
Office Parameters	_N/A__
SOC	_N/A__
Upgrades impact	__X___

Accounting (includes AMA billing)_____

Not Applicable	__X___
Billing changes	_____

Performance _____

Not Applicable	__X___
Operational Measurements	_____
Performance Measurements	_____

85.4 Hardware Requirements or Dependencies

None.

85.5 Software Requirements or Dependencies

None.

85.6 Limitations and restrictions

Please refer to “85.2.2 Only One NPM” on page 819 for limitations on preventing more than one NPM being installed in a site.

85.7 Interactions

A00003615 - SSPFS Patching
A00002133 - CBM Patching

86: Functional Description (FN): A00003562

86.1 Feature name

SAM21 Element Manager (EM) support for CICM

86.2 Description

The SAM21 Element Manager now allows the user to:

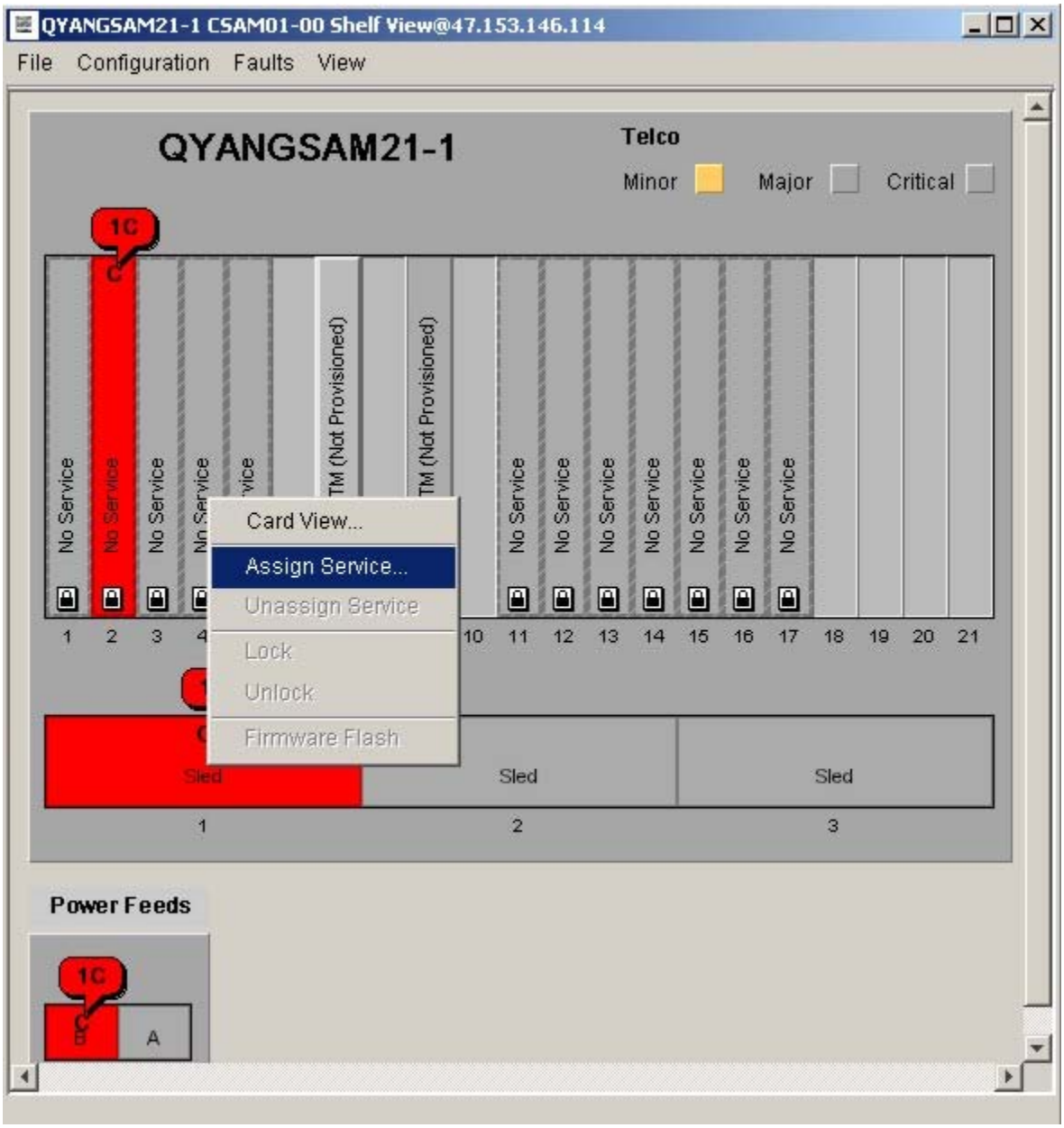
- Provision CentrexIP Client Manager application(also known as “CICM”) on a given MCPN5385 card
- Provision CICM Element Manager application(also known as “CICM-EM”) on a given MCPN5385 card

The SAM21 defines new provisioning panels for the new CICM and CICM-EM service respectively.

86.2.1 Provision CICM Service On a MCPN5385 card

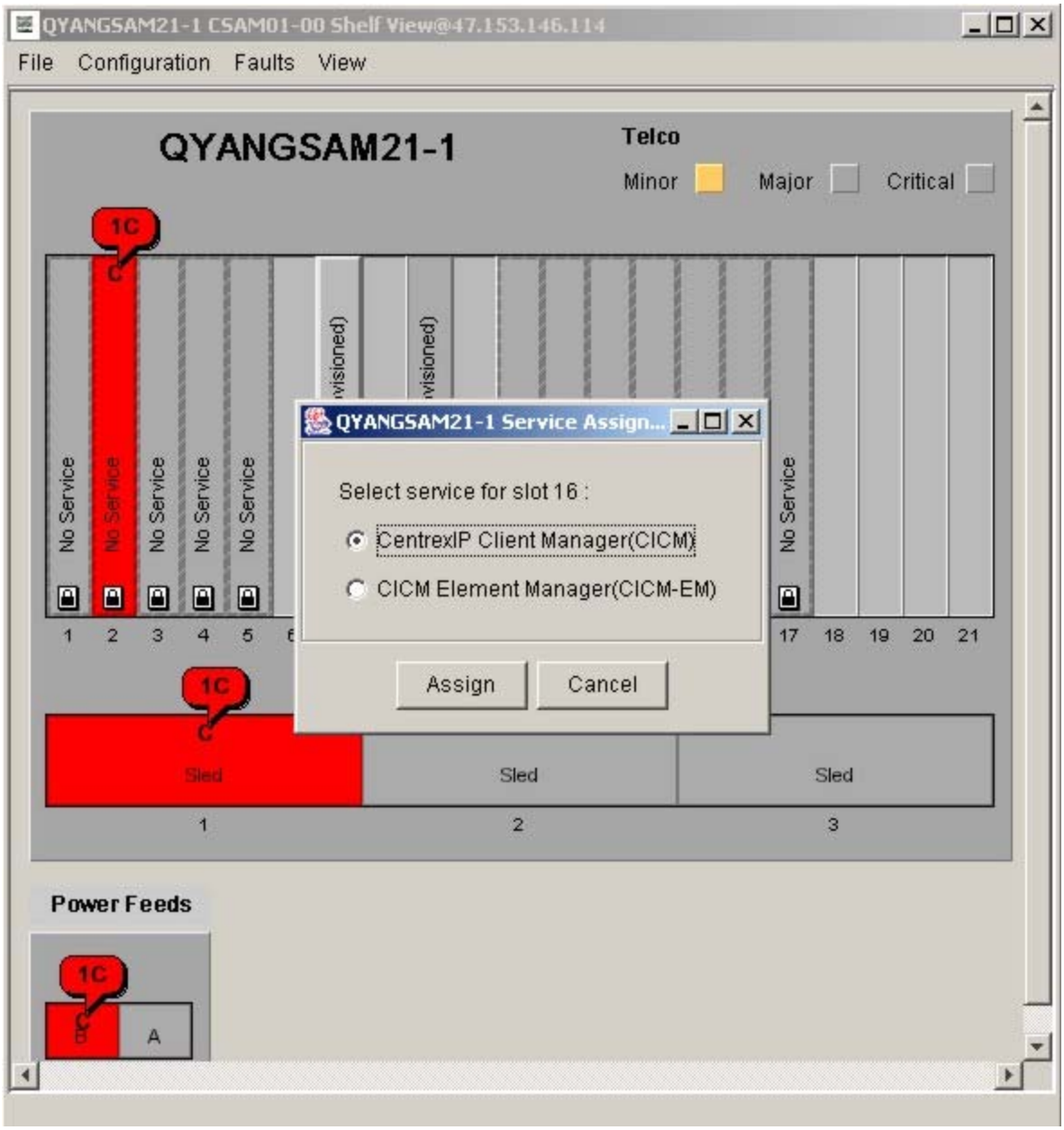
86.2.1.1 Assign Service

The SAM21 EM mechanism to provision service on a card has not changed. When displaying the shelf view, the user can right click on a card to view the Card Popup Menu. If the card currently is not assigned a service, the user can select “Assign Service ...” from this menu.



When the user selects “Assign Service...”, the SAM21 EM displays the Service Assignment popup window. Based on the card’s hardware (model type and memory), the SAM21 EM determines the set of services that can be assigned to the card and allows the user to choose one of them.

The CICM service can be assigned to a MCPN5385 card.

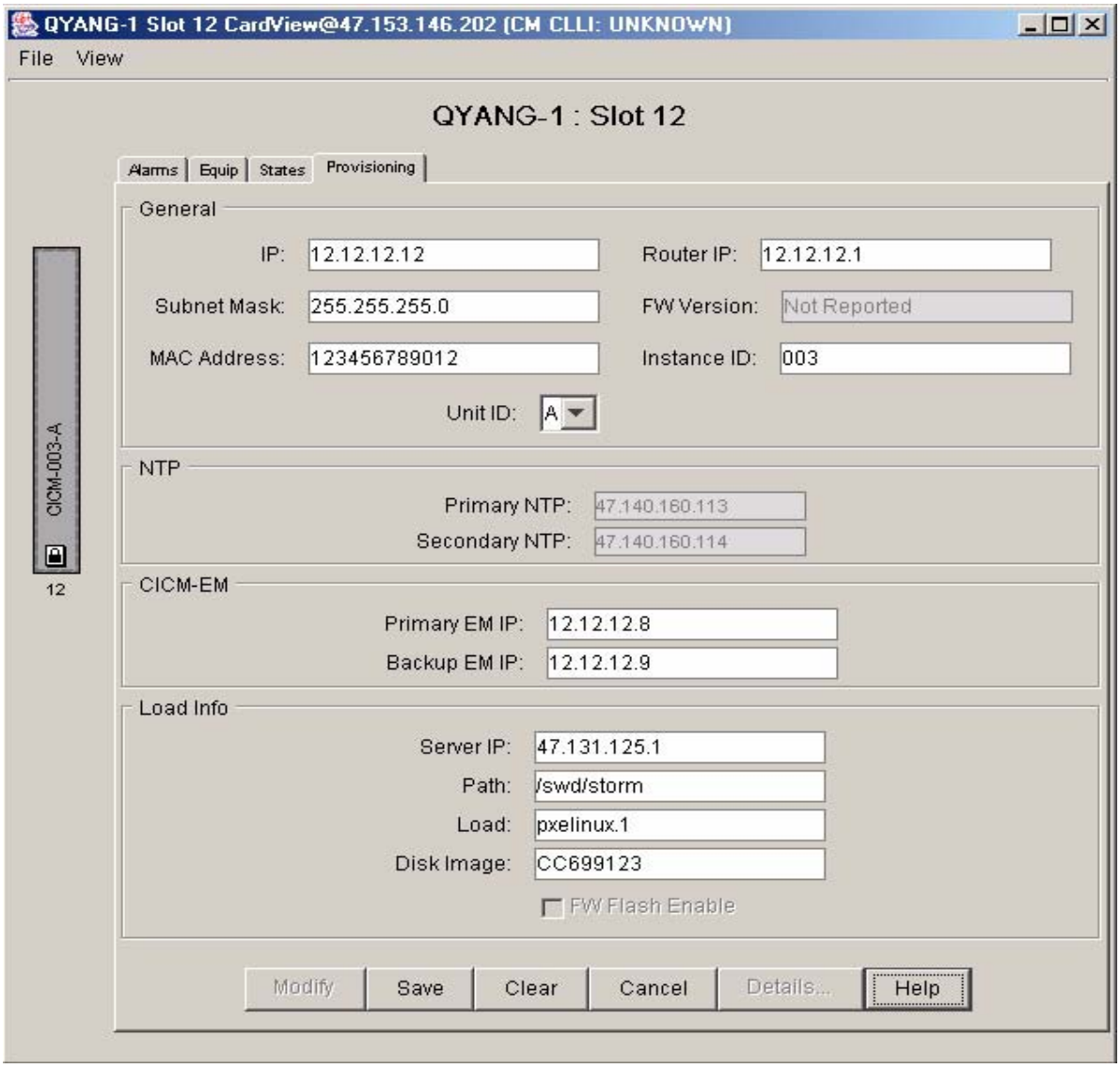


When the user selects the listed “CICM” service and then clicks “Assign”, the SAM21 EM displays a CICM service provisioning panel.

86.2.1.2 CICM Provisioning Panel

The CICM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM Provisioning Panel follows.

- **IP** : The IP address of the MCPN5385 card.
- **Router IP**: The IP address of the card's router.
- **Subnet Mask** : The card's subnet mask.
- ***FW Version*** : The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address**: The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID** : The instance integer identifier of the CICM card, and applies to both CICM and CICM-EM.
- **UNIT ID**: 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- ***Primary NTP***: The primary NTP server IP address provisioned for NE.
- ***Secondary NTP***: The secondary NTP server IP address provisioned for NE.
- (Load Info) **Server IP** : The IP address of the server (SDM) containing the CICM software load.
- (Load Info) **Path** : The server's directory that contains the CICM software load.
- (Load Info) **Load** : The file name of the CICM Linux bootstrap, distributed with the boot server.
- (Load Info) **Disk Image**: The file name of the CICM software load, distributed with the boot server.
- ***FW Flash Enable*** : Check this box to enable firmware flash on the card. Now Disabled.
- (CICM-EM)**Primary EM IP**: The IP address of the primary CICM-EM, for CICM only.
- (CICM-EM)**Backup EM IP**: The IP address of the backup CICM-EM, for CICM only.



86.2.1.3 Provisioning Rules

Two CICM/CICM-EM cards(card A and B) form a pair to provide redundancy. When provisioning a mated pair of CICM cards, the user can provision the cards in either order. For example, “CICM-110-A” and “CICM-110-B” form a CICM pair.

There is no existing relationship between the IP addresses of the CICM/CICM-EM pair. And there are no active and inactive IP addresses(like the GWC) for CICM card.

Some provision information, including load info, subnet, router, and EM address, should be the same between the CICM/CICM-EM pair. But it is not mandatory. If the craftsperson provides different datafill, the SAM21 EM will prompt a warning message for confirmation.

The CICM/CICM-EM Provisioning Panel verifies the following provisioning rules:

- At most two CICM/CICM-EM cards can be provisioned with the same instance ID, each CICM/CICM-EM pair has a unique instance ID.
- Each MAC address of a CICM/CICM-EM card must be unique among all the cards on SAM21 shelf.

When the user changes the datafill for an existing CICM card, the SAM21 EM performs the change and then displays the following message to the user: "The datafill for this CICM card has been changed. Please ensure that the card's mate uses the same datafill."

86.2.1.4 Maintenance Behavior

This section considers the behavior the user should see when the user attempts a maintenance action on a card provisioned with the CICM service.

- If the user attempts to lock the inactive CICM card, the SAM21 EM immediately attempts to lock the card.
- If the user attempts to lock the active CICM card, the SAM21 EM client displays the following message: "WARNING: This is the active CICM unit. Locking the active unit will cause a service outage. Contact next level NT support before continuing. Do you wish to proceed with the lock?" If the user clicks "Yes", then the SAM21 EM immediately attempts to lock the card.
- If the user attempts to unassign service to an CICM card, the SAM21 EM client displays the following message: "WARNING: Unassigning service to the card in slot x decommissions one of the processor units of CICM node. Do you wish to proceed?". If the user clicks "Yes", then the SAM21 EM unassigns service.

86.2.1.5 Card Replacement

Firstly the user removes a CICM/CICM-EM card from SAM21 EM shelf. Then a card is inserted into the same slot, it will be auto-provisioned with the same provisioning data as the previous card in that slot, so the MAC address will be the old MAC.

Several scenarios are described here:

- If the craftsperson reseated the same card, he needn't to take further action.

- If the craftsperson replaces the card with a different one, then he needs to reprovision its MAC address. If the craftsperson doesn't reprovision the MAC address, the card will fail to boot.
- If the craftsperson exchanges two cards in the same shelf or from different shelves, for example, card A in slot 1, card B in slot 2. After exchange, card A is in slot 2, card B is in slot 1. Card A will be auto-provisioned as card B, card B auto-provisioned as card A. If the user does not reprovision them accordingly, the two cards will not work properly after booted.

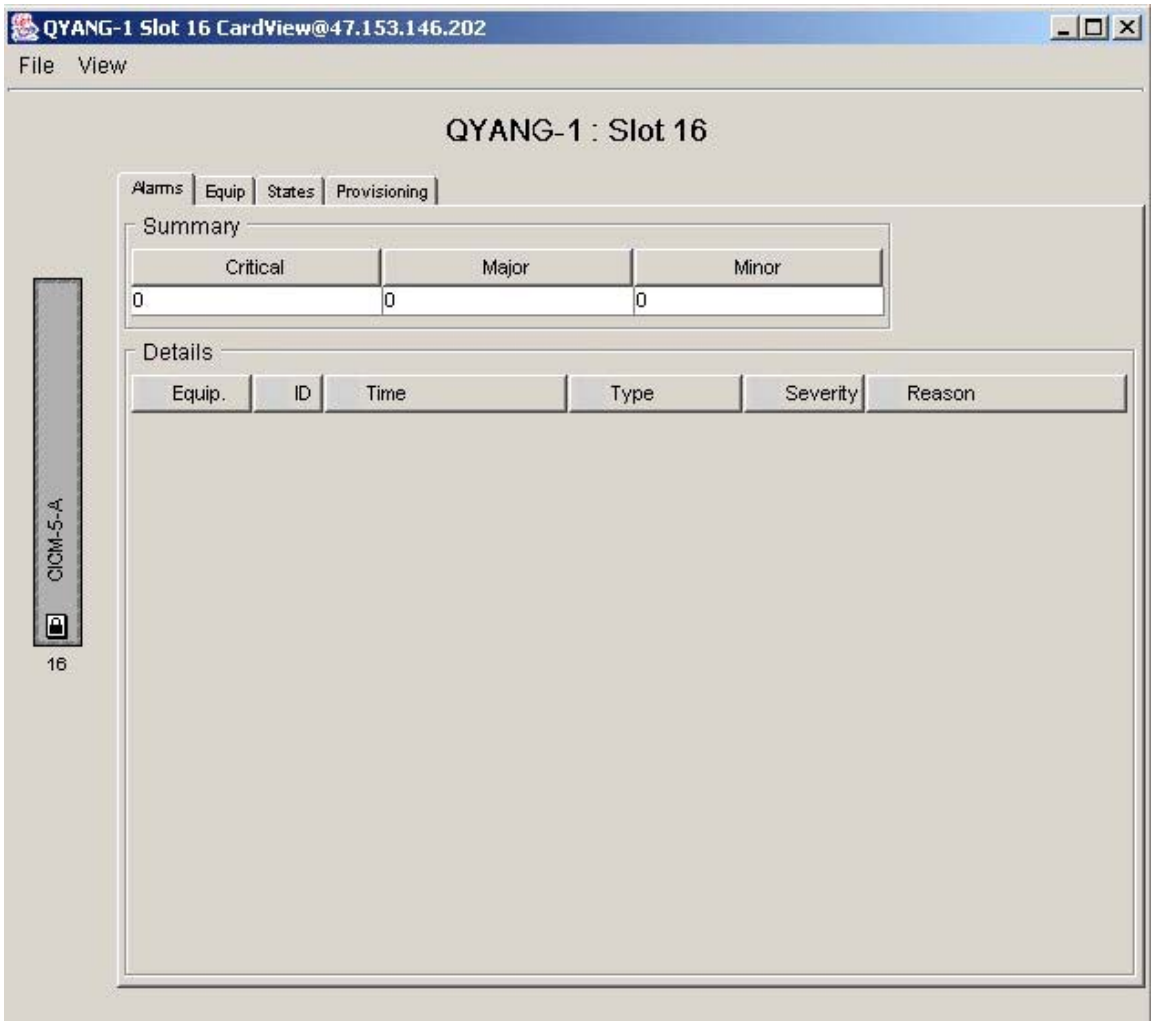
The craftsperson must reprovision the MAC address after card replacement. It is recommended that when replace the card with a different one the user unassigns service from CICM card before removal.

If the craftsperson wants to reinsert a CICM card into a different slot, he must reprovision its MAC address to a dummy one, such as "aaaaaaaaaaaa" before removal, then he can insert it into another slot. Otherwise, he will get an error message stating that the mac address has been reserved by the previous slot. It is recommended that when move the card to another slot the user unassigns service before removal.

86.2.1.6 Card View

Out-of-Service Diagnostics (OOS Diags) for the CICM hardware is not supported in SN07. So the diagnostics tab will not appear on CICM card view.

A picture of the CICM Card View follows.



86.2.1.7 Popup Menu for CICM card

Firmware flash for the CICM hardware is not supported in SN07. When the user right-clicks on the CICM card item on the shelf view, a popup menu will appear, but the “firmware flash” menu item is disabled.

A picture of the CICM Card popup menu follows.

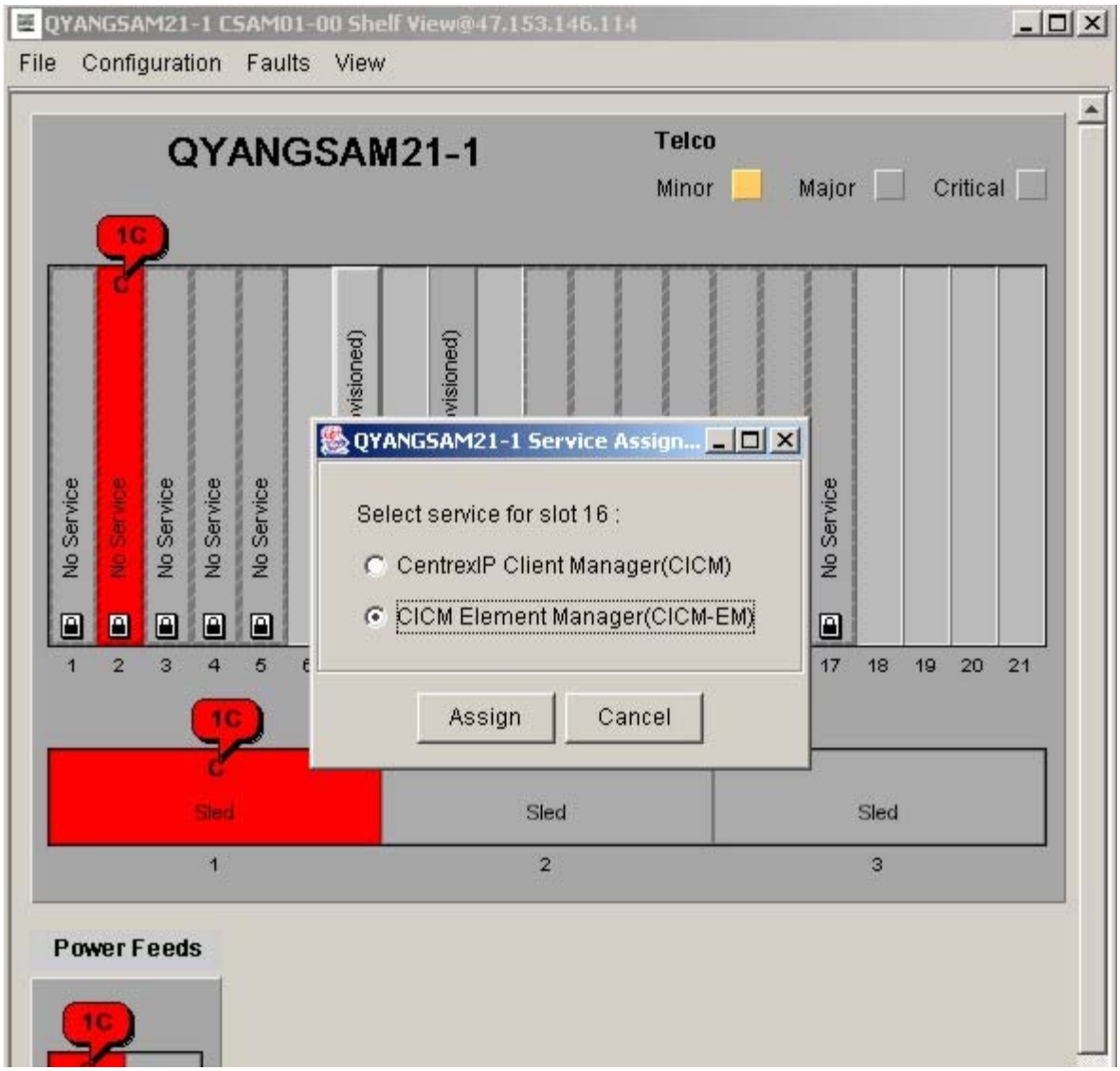
86.2.2 Provision CICM-EM Service On a MCPN5385 card

The CICM-EM is different from CICM card on its provisioning panel. The other aspects, such as maintenance, provisioning rules, etc., is the same as CICM card.

86.2.2.1 Assign Service

When the user selects “Assign Service...” on a MCPN5385 card, the SAM21 EM displays the Service Assignment popup window.

The CICM-EM service can be assigned to a MCPN5385 card.



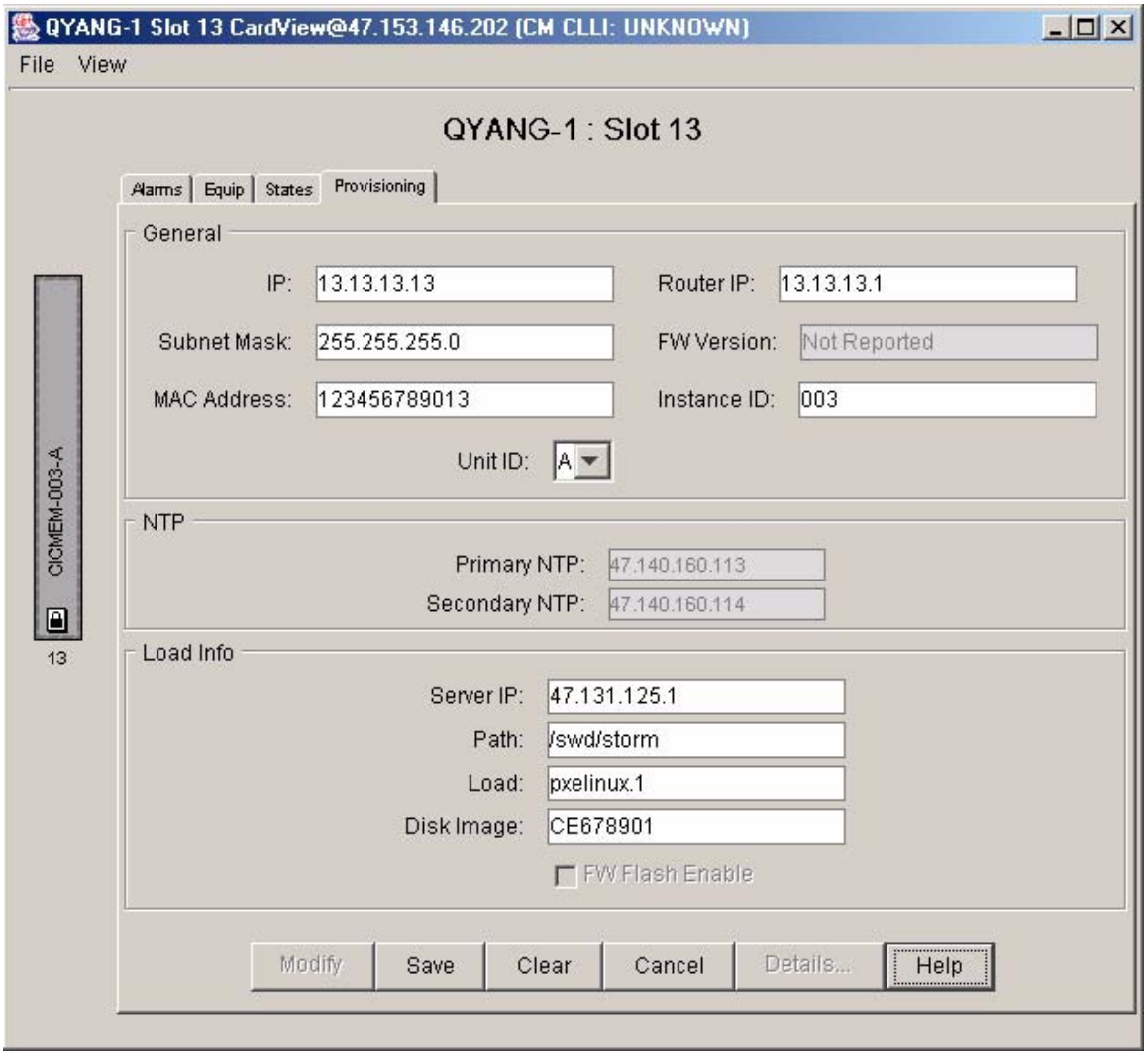
When the user selects the listed “CICM-EM” service and then clicks “Assign”, the SAM21 EM displays a CICM-EM service provisioning panel.

86.2.2.2 CICM-EM Provisioning Panel

The CICM-EM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM-EM Provisioning Panel follows.

- **IP** : The IP address of the MCPN5385 card.
- **Router IP**: The IP address of the card’s router.
- **Subnet Mask** : The card’s subnet mask.

- ***FW Version*** : The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address**: The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID** : The instance integer identifier of the CICM-EM card
- **UNIT ID**: 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- ***Primary NTP***: The primary NTP server IP address provisioned for NE.
- ***Secondary NTP***: The secondary NTP server IP address provisioned for NE.
- (Load Info) **Server IP** : The IP address of the server (SDM) containing the CICM-EM software load.
- (Load Info) **Path** : The server's directory that contains the CICM-EM software load.
- (Load Info) **Load** : The file name of the CICM-EM Linux bootstrap, distributed with the boot server.
- (Load Info) **Disk Image**: The file name of the CICM-EM software load, distributed with the boot server.
- ***FW Flash Enable*** : Check this box to enable firmware flash on the card. Now not supported.



Glossary

Acronym	Definition
EM	Element Manager
CICM	CentrexIP Client Manager
CICM-EM	CentrexIP Client Manager's Element Manager
SAM	Service Application Module
SC	Shelf Controller
SDM	Succession Data Manager

SSPFS	Succession Server Platform Foundation Software
GWC	Gateway Controller

87: Functional Description (FN): A00003567

87.1 Feature name

MG9000 Element Manager support for ABI ESA.

87.2 Description

In SN07, ESA capability will be introduced for ABI lines. ABI ESA provides the ability to support basic XPM calls within the MG9000. The MG9000 ABI cards will terminate CSide links of the extending XPMs and give them ESA capability if the MG9000 is out of communication with its assigned Gateway Controller (GWC).

The element manager will build on existing ITP ESA functionality for retrieving the ESA translation data from the core and pushing it to the MG9000. Data common to ITP and ABI VMGs will be handled as in SN06.2. Additionally , new data specific to ABI cards will be retrieved from the core and sent to the MG9000. This data will include, node, BNV and term type entries. This new data will allow the MG9000 to support the associated call processing features for ABI while in ESA mode.

As in SN06.2, this feature provide the following:

- Ability to retrieve the ESA data organized on a VMG basis from the core. This data will be retrieved through the SDM platform on a 24 hour basis. This data will also be retrievable from the SDM on a manual basis. Another manual command on the core will have to be used to generate the core ESA data, the MG9000 EM will not be able to invoke the core's ESA data build.
- The ability to push the required ESA data down to the MG9000 by formatting an XML data file and sending it via FTP to the associated VMGs ABI card using a floating IP address.
- Upgrades of ESA data.

Additionally, this feature will add support for secure FTP for the data transfer between the EM and the MG9000. Currently this transfer occurs over standard non-secure FTP. Functionality will be added to :

- Provide a means to set a password and/or username . This is currently proposed to be via a gui accessible via the EM server.(details TBD)
- Allow data transfer to and from the MG to take place via secure FTP. This change will be transparent to the user. Secure FTP will be used for the OM Collector utility and ESA data ftp to the MG9000.

87.3 Hardware Requirements or Dependencies

No additional ESA requirements are needed for this feature besides the standard CS2000 hardware, the MG9000 EM and the MG9000 Gateway.

87.4 Software Requirements or Dependencies

This feature is providing ABI ESA support capability for the MG9000 EM, as well as secure interface support. It has dependences on the following features:

- A00002380: ESA for ABI: MG9000 , XPM and CM
- A00003737 - LCI Remote Access and Security

87.5 Limitations and restrictions

- The ESA data from the core will be downloaded to the MG9000 only once every 24 hours. This is the same manner in which the core handles loading the RSC with ESA data.
- The MG9000 EM will not allow the modification of any ESA data retrieved from the core.
- The MG9000 EM will not be providing a ESATRVR test tool. This test tool will be supplied by the core.
- The MG9000 EM will provide a mechanism to manually pull the latest ESA data from the Core. This mechanism will not push the ESA data down to the MG9000. The craftsperson will have to manually push the ESA data down to the MG9000 for each VMG. This is to prevent overloading the MG9000 with new data. Also, this mechanize will only work provided that the craftsperson has used the Core command to generate the latest Core xml data file for the EM to retrieve, the EM does not have the ability to invoke this Core command.

87.6 Interactions

N/A

87.7 Applicable customer facing sections

Fault Management

Logs	_X___
Alarms	_X___

Configuration

Data Schema	_____
User Interface	_____
Element Management	_X___

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

87.8 Glossary

Term	Description
XPM	Ex Peripheral Module
EM	Element Manager
ESA	Emergency Stand Alone
GUI	Graphical User Interface
GWC	Gateway Controller
MG9000	Media Gateway 9000
MIB	Managed Information Base
SNMP	Simple Network Management Protocol
VMG	Virtual Media Gateway

88: Functional Description (FN): A00003568

88.1 Introduction

Nortel Networks is expanding its Emergency Call Services (ECS) to handle mobility of Internet Protocol (IP) telephony clients in a Voice over IP (VoIP) Enterprise environment. To provide this capability, enhancements to existing network components are required.

88.1.1 Scope

This document covers the Centrex IP Client Manager (CICM) ECS Location Identification reporting solution. The Location Identification information may also be used for purposes other than ECS.

This functionality is not applicable to the Time Division Multiplexing (TDM) CICM product.

88.1.2 Intended Release

SN07.

88.2 Functional Description

88.2.1 Description

For fixed lines, either in a traditional TDM network or a line connected to an analogue line gateway, the location of the line, for Emergency Call Services (ECS), can be determined using the Calling Line Identity (CLI). Information from region's telecommunications providers would be required to associate a CLI with a location. As the lines are of fixed location the ECS call routing is statically configured as well.

For CICM telephony clients the location of a user is not fixed. Unistim terminals, in an Enterprise, connecting to the Call Server 2000 (CS2K) via the CICM are not statically configured against a particular node in the network topology and their physical location may be anywhere in the Enterprise.

We have implemented a solution where the location information is configured in, and provided by, the Dynamic Host Configuration Protocol (DHCP) server.

When the CICM telephony client boots-up it request can request DHCP options from the DHCP server, this includes Location Identification information options. If available, the DHCP server will return the location information to the set. The CICM gateway will request the location information from the CICM telephony client when a user logins in from the client. The CICM gateway reports the location information, via H.248, to the GWC. If configured, an application running on the Gateway Controller (GWC) re-packages the information and reports it to a Location Recipient application.

The solution also supports the reporting of user defined location identification. This is required for CICM telephony soft clients on networks with DHCP servers that do not support the new location identification DHCP options.

The Location Recipient is outside the scope of this activity.

This solution reports the necessary information to support the Enterprise ECS solution. This solution uses a Location Information Server (LIS) to provide the physical location information. The ECS correlates the LIS information with the client information using IP addresses and MAC address. Please refer to reference [3] for more details.

The mechanism for reporting CICM telephony client location information can also be employed to report the client's location, unique network id (unid), within the network topology. This is required for location/network based policy services:

- Correctly inserting the media portal to traverse NAT devices
- Admissions control

88.2.1.1 Reference Network

Figure 1 CICM Carrier ECS solution reference network shows a example network configuration. It shows an enterprise with a large central campus and several locations.

Table 1 describes each of the locations shown, how they are connected to the carrier network and the DHCP capabilities provided on site.

Table 1 Network Locations

Site	Description	Connectivity to carrier	DHCP capabilities
A1	Central campus	Direct connection to carrier network via NAT.	On site DHCP server supporting multiple scopes and vendor options.

A2	Secondary campus	Via limited bandwidth link to central campus.	On site DHCP server supporting multiple scopes and vendor options.
A3	Satellite office	Via limited bandwidth link to secondary campus.	DHCP is relayed to server on secondary campus
A4	Remote branch office	Hardware VPN device provides access to central campus over a limited bandwidth link into the internet.	VPN device provides DHCP for site – no support for vendor options.
A5	Home user	Dialup or software VPN over the internet to enterprise RAS/ VPN.	None – RAS/VPN provides IP address.

The distinction between sites A4 and A5 is that site A4 is a “known” location, but A5 is a site that is being used for temporary access to the enterprise (e.g. home or hotel).

The DHCP servers in the enterprise are configured with the Location and UNID for each scope it supports. E.g.; Consider a CICM telephony client on the ground floor in the Central Campus building. The DHCP server is configured with the location of CEN GF and UNID of 31 for this scope. The CICM telephony client may request the DHCP vendor option X to retrieve the configured location and unid.

Note: option X refers to the IETF GEOPRIV working group civil and geospatial location identification DHCP options. Please refer to references [1] and [2].

Figure 1 CICM Carrier ECS solution reference network also shows the ‘default’ location identification information configured on the CICM. This is configured against a network domain profile. If a user logs in from CICM telephony client that cannot provide the location identification information, e.g. from site A4 or A5, the default location identification information is used for the client.

88.2.1.1.1 Enterprise ECS solution

For completeness, a description of the Enterprise ECS solution will be outlined and how the CICM ECS Location Identification reporting functionality introduced by this activity meets it’s requirements.

Please refer to reference [3].

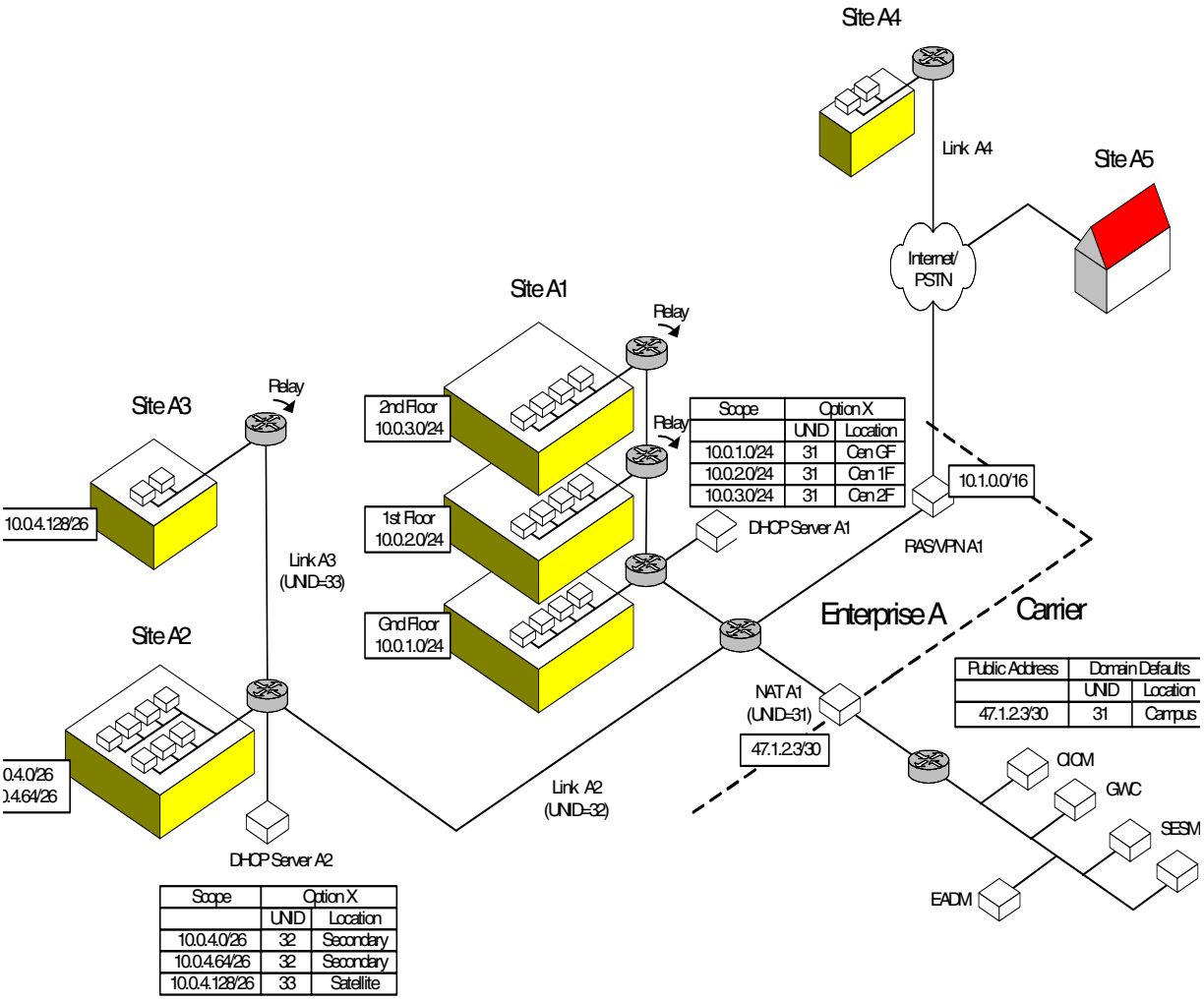
Figure 1 and Figure 2 Enterprise ECS solution reference network gives an example of the network configuration for the Enterprise ECS solution.

In the Enterprise ECS solution the Location Identification information is not configured as options in the DHCP servers. Instead the Location Information Service (LIS) gathers etherswitch/port-to-IP/MAC address associations for all devices connected to the network. The LIS performs this function by gathering information from routers and etherswitches. The LIS forwards the information onto the Emergency Application/Data Manager (EADM).

The EADM determines how emergency calls from telephony clients should be handled and sends this information to the Call Server. To accomplish this, the EADM correlates data from the LIS and the telephony client controller and uses its own network topology data to determine what emergency call handling information to send to the Call Server. In addition, the EADM handles Emergency Response Location (ERL) management and Automatic Location Identification (ALI) entry updates to the ALI Database.

In the CICM ECS Location Identification solution the EADM receives the Location Identification information the gateway controller, e.g. the GWC, not the telephony client controller, e.g. the CICM. Included in the Location Identification information reported by the GWC to the EADM are the telephony client's public IP address, private IP address, MAC address and a way to uniquely identity the client on the Call Server. The EADM correlates this information with the information from the LIS. The EADM can then update the call server with emergency call routing for the telephony client and decide whether to use the Location Identification information reported by the GWC or use Location Identification information from it's own database

Figure 1 CICM Carrier ECS solution reference network

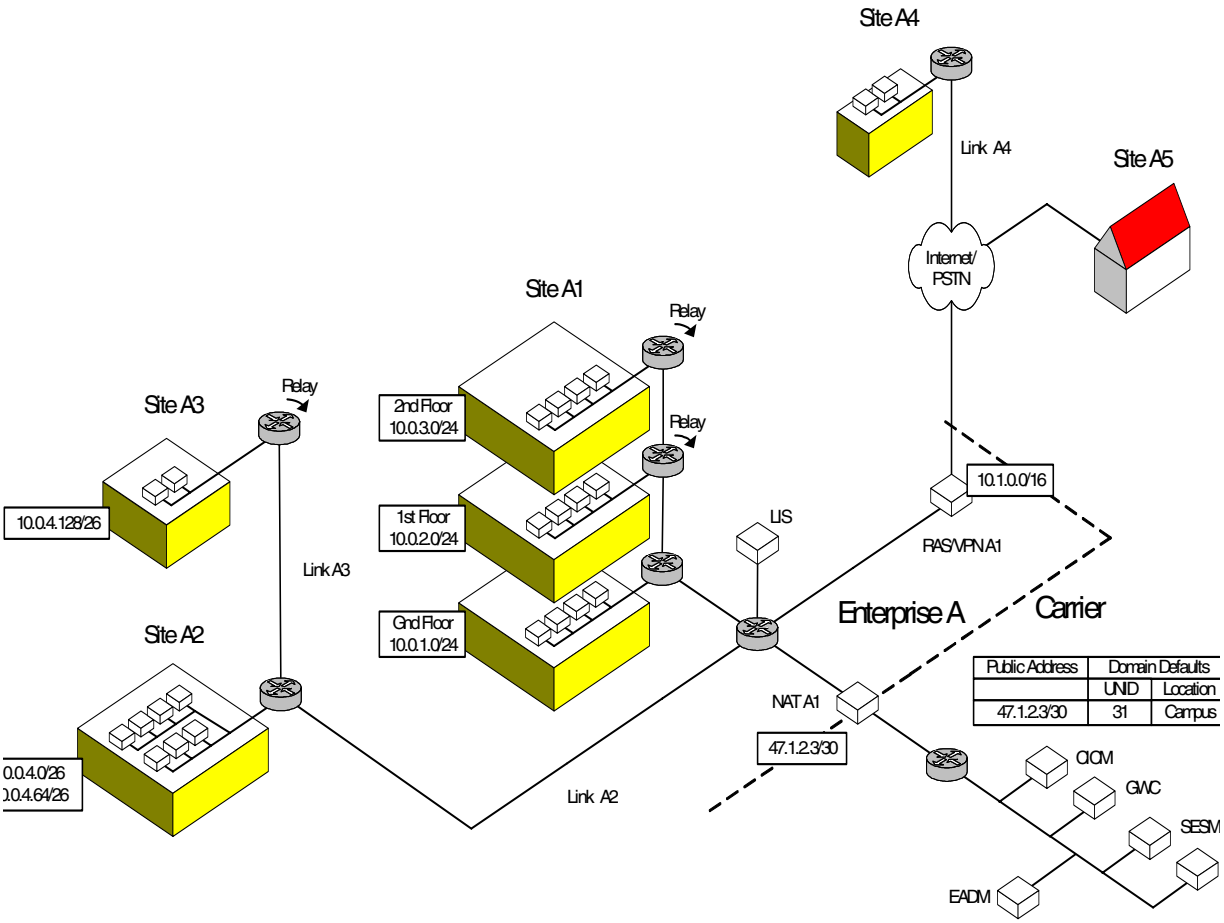


Scope	Option X	
	UNID	Location
10.0.1.0/24	31	Gen GF
10.0.2.0/24	31	Gen 1F
10.0.3.0/24	31	Gen 2F

Public Address	Domain Defaults	
	UNID	Location
47.1.2.3/30	31	Campus

Scope	Option X	
	UNID	Location
10.0.4.0/26	32	Secondary
10.0.4.64/26	32	Secondary
10.0.4.128/26	33	Satellite

Figure 2 Enterprise ECS solution reference network



88.2.1.2 Operation overview

The CICM ECS Location Identification solution allows location identification information to be configured at the network level and reported through the network, ultimately being reported to an ECS application. Each component can process the information as required, e.g. the GWC uses the UNID in call processing for NAT traversal.

Figure 3 and Figure 4 show how the Location Identification information is requested and reported through the network when a user logs in to a CICM telephony client.

When a CICM telephony client starts-up it requires the following pieces of information:

- It’s own IP address
- The CICM server settings; IP address, connection retries, server action

For flexibility the CICM telephony client can obtain this information from the DHCP server at start-up. The IP address is obtained as part of the standard DHCP Discover and the CICM server settings are obtained by requesting vendor and site specific options.

The Nortel CICM configuration DHCP option (Nortel-i2004-A) has been extended to include the name of the middle-box that the CICM telephony client gains network connectivity through. The middle-box id is eventually reported northbound and used by the Internet transparency functionality.

The CICM telephony client requests the Nortel Location Identification options from the DHCP Server. The DHCP Server may have none or only some of the options configured. Only the configured Location Identification options will be returned by the DHCP Server to the CICM telephony client.

Please refer to section 2.1.3.1 DHCP for more DHCP configuration details.

When the CICM telephony client registers with the CICM server, the CICM requests the CICM telephony client’s MAC address and middle-box name (Unique Network Identifier).

When a user logs into a CICM telephony client the CICM requests the location information from the CICM telephony client.

In the case of the CICM telephony soft client the user can define the location identification as part of the login interface.

If a Location Identification options is requested by the CICM but not made available by the DHCP Server the CICM telephony client will respond to the CICM with the appropriate Unistim command containing no information.

Once all of the Location Identification information has been collected from the CICM telephony client the CICM registers the successful user login with the GWC via a H.248 location change event of the terminal location package.

The GWC uses this event to trigger an audit of the H.248 location identification package for the termination, to collect the Location Identification information.

The CICM responds to the audit with an H.248 audit message for the termination containing all the available Location Identification information.

The GWC uses the Unique Network Id for call processing and so stores the value internally. The GWC uses the Location Identification information received from CICM for the termination to build a Location Add XML structure to send to the Location Recipient application.

The Location Add XML structure is sent to the Location Recipient application over a TCP/IP connection that the GWC maintains.

More details about the interfaces between the network components involved is given in section 1.1.2.1.3 Interface

Figure 3 Propagation of Location Identification information during user registration (Client to CICM

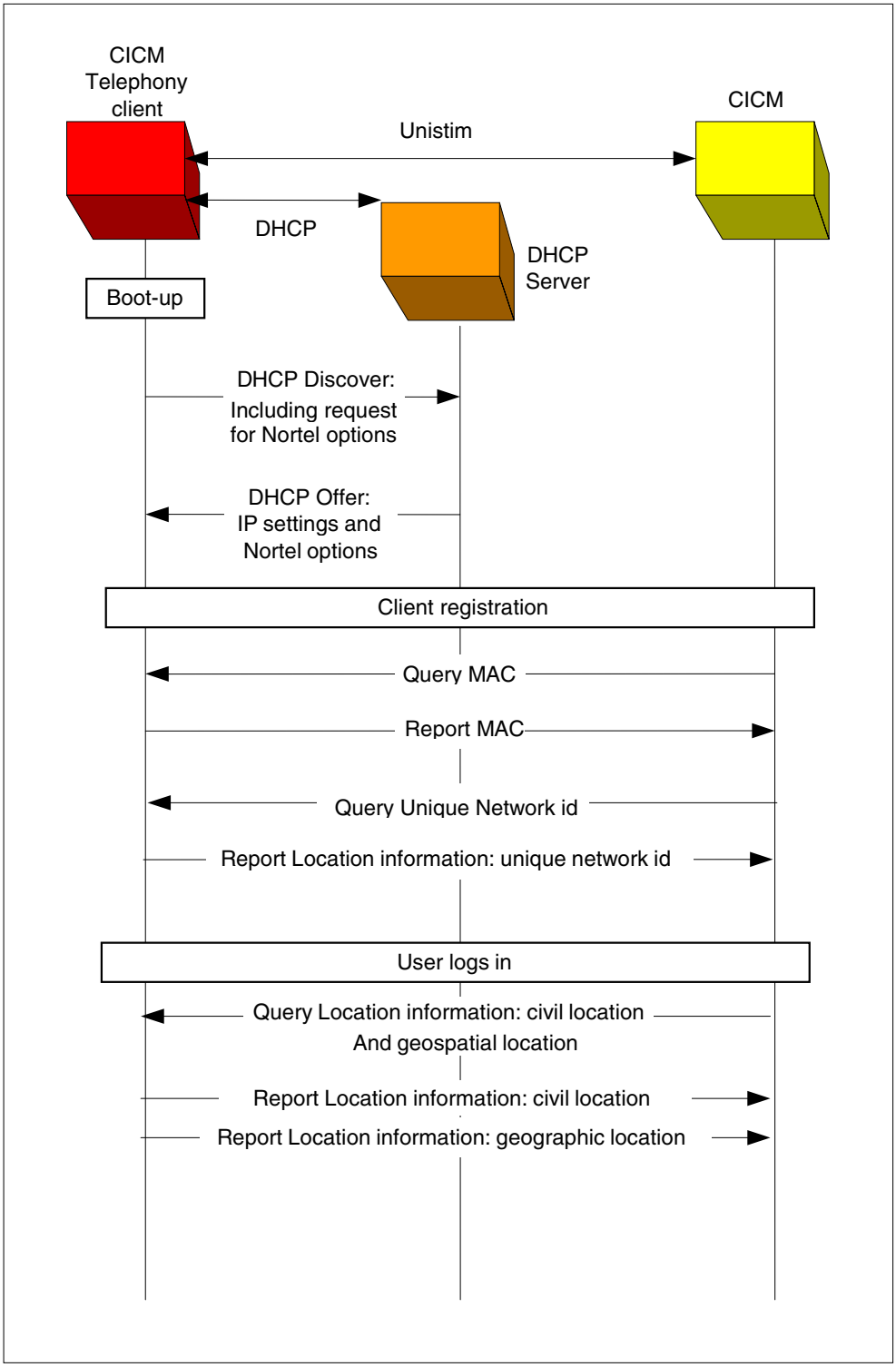
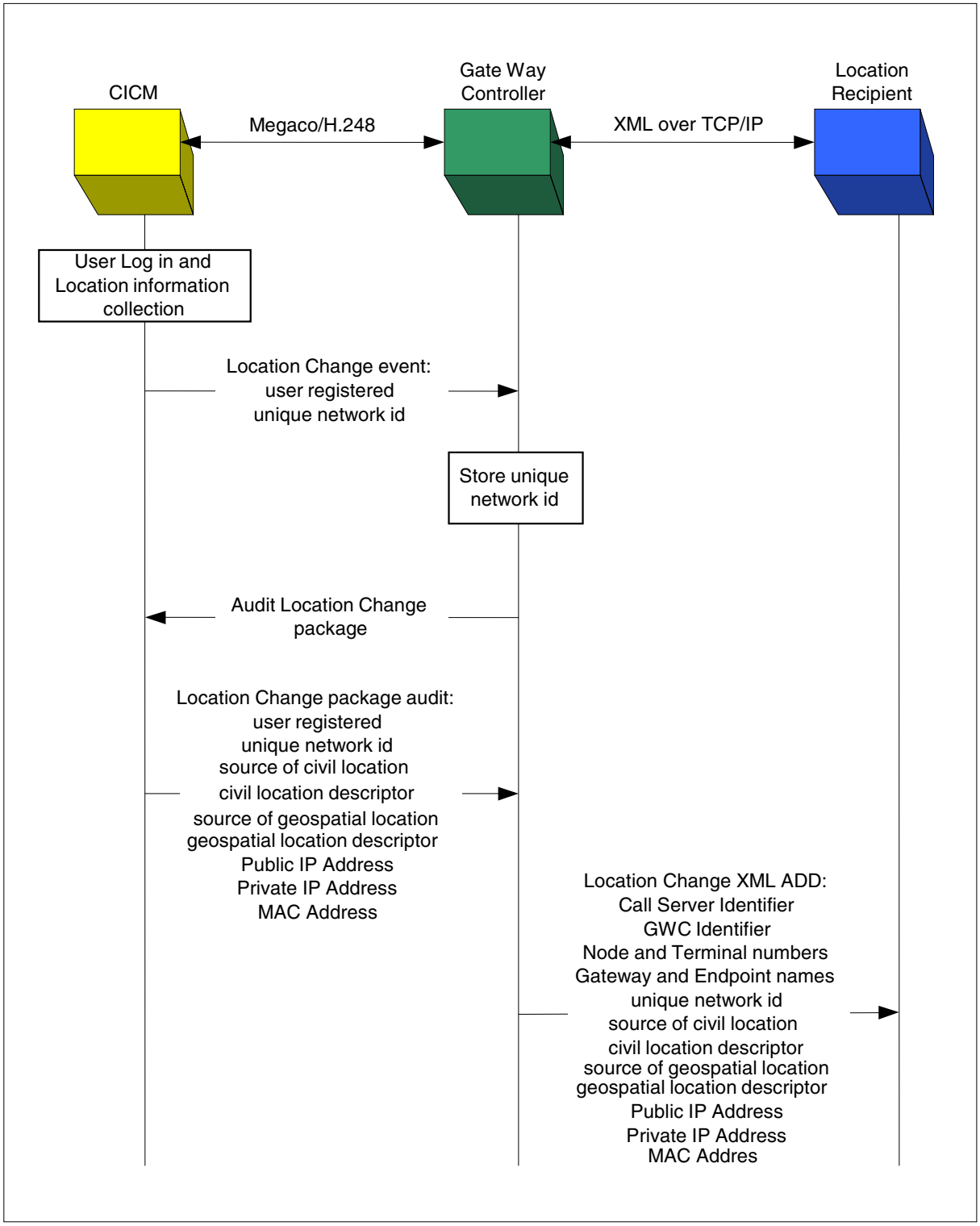

CICM
Telephony
client
Unistim
CICM
DHCP
DHCP
Server
Boot-up
DHCP Discover:
Including request
for Nortel options
DHCP Offer:
IP settings and
Nortel options
Client registration
Query MAC
Report MAC
Query Unique Network id
Report Location information: unique network id
User logs in
Query Location information: civil location
And geospatial location
Report Location information: civil location
Report Location information: geographic location

Figure 4 Propagation of Location Identification information during user registration (Client to Location Recipient)

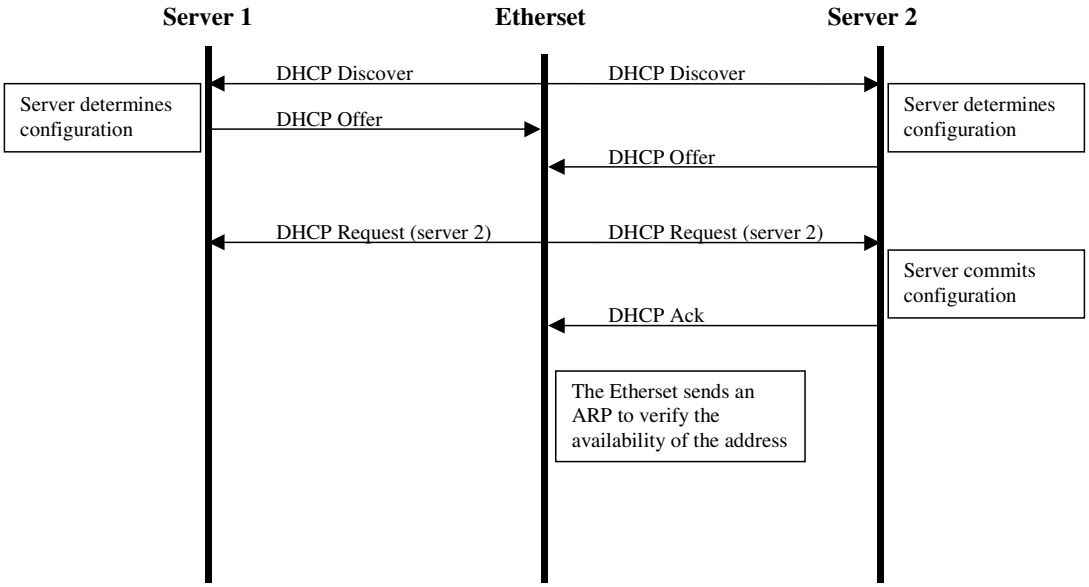


88.2.1.3 Interfaces

The following sections describe how the location identification information is reported from the CICM telephony client through the network.

88.2.1.3.1 DHCP A

CICM telephony client can obtain Nortel-specific configuration information from DHCP server; this includes the Location Identification information. The information is carried by DHCP options in DHCP OFFER message and DHCP ACK message.



1 Nortel specific configuration

5 DHCP vender-specific options (128, 144, 157, 191, and 251) and 5 DHCP site-specific options (128, 144, 157, 191, and 251) can be used to carry Nortel-specific configuration information:

- Nortel-i2004-A
- VLAN-A

12 DHCP vender-specific options (128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, and 251) and 12 DHCP site-specific options (128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, and 251) can be used to carry Nortel-specific configuration information:

- Nortel-Geo-Civil-A

- Nortel-Geo-Spatial-A

The options are listed (starting from highest priority) below. Higher priority option can overwrite lower priority option if they carry the same information.

- Vender-specific option 128 (highest priority)
- Vender-specific option 131
- Vender-specific option 144
- Vender-specific option 157
- Vender-specific option 188
- Vender-specific option 191
- Vender-specific option 205
- Vender-specific option 219
- Vender-specific option 223
- Vender-specific option 232
- Vender-specific option 247
- Vender-specific option 251
- Site-specific option 128
- Site-specific option 131
- Site-specific option 144
- Site -specific option 157
- Site -specific option 188
- Site -specific option 191
- Site -specific option 205
- Site -specific option 219
- Site -specific option 223
- Site -specific option 232
- Site -specific option 247
- Site -specific option 251 (lowest priority)

At the beginning of the options, a unique identifier identifies the format of the possible Nortel options. The current defined formats are:

Identifier	Comment
“Nortel-i2004-A”	Carrying call server information and Net6 server information
“VLAN-A”	Carrying VLAN information

“Nortel-Geo-Civil-A”	Carrying civil location information
“Nortel-Geo-Spatial-A”	Carrying geospatial location information

2 Nortel-i2004-A option

To facilitate the Internet Transparency functionality for CICM telephony clients, the name of the middle-box (unique network id (UNID)) that the CICM telephony client gains network connectivity through can be configured in the DHCP server.

The Nortel UNID has been added to the Nortel-i2004-A option.

The DHCP option format is:

Type (1 octet):

5 choices are 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, and 251).

Providing a choice of five types allows the IP telephone to work in environments where the initial choice already is used for other purpose.

Length (1 octet):

Variable - depends on message content.

Data (length octets):

- ASCII based
- format

```
Nortel-i2004-
A,iii.jjj.kkk.lll:pppp,aaa,rrr;iii.jjj.kkk.lll:pppp
,aaa,rrr;bbb.ccc.ddd.eee:fffff;nnnnnnnnnnnn.
```

WHERE:

"Nortel-i2004-A" - identifies this as the Nortel option

"," - is used to separate fields

";" - is used to separate servers’ info

"." - is used to signal end of structure

"iii.jjj.kkk.lll:ppppp" - ASCII encoded decimal

- Identifies IP address and port number for server.
- The 1st one identifies the primary server.
- The 2nd one identifies the secondary server.

"aaa"- identifies Action for server (ASCII encoded decimal, range 0..255)

"rrr" - identifies retry count for server (ASCII encoded decimal, range 0..255)

"bbb.ccc.ddd.eee:fffff" - ASCII encoded decimal.

- Identifies IP address and port number for Net6 server.
- This part is optional.

"nnnnnnnnnn" - identifies Unique Network Identification (UNID)

- ASCII based character string, up to 32 bytes long
- Character **';'** is not allowed.

This string may be NULL terminated although the NULL is not required for parsing.

Notes:

- "aaa" and "rrr" are ASCII encoded decimal numbers with a range of 0..255. They identify the "Action Code" and "Retry Count", respectively, for the associated TPS server. Internally to i200x they will be stored as 1 octet (0x00..0xFF). Note that these fields must be no more than 3 digits long.
- First server is always considered "Primary", second server always considered "Secondary".
- If only one server is required, terminate primary TPS sequence immediately with "." instead of ";" e.g. "Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr."
- If Net6 server ("bbb.ccc.ddd.eee:fffff") and/or UNID ("nnnnnnnnnn") are required, the secondary server need to be specified.
- Action code values:
  0 reserved
  1 UNIStim Hello (currently only this type is a valid choice)
  2..255- reserved
- "iii.jjj.kkk.lll" and "bbb.ccc.ddd.eee" are ASCII encoded, decimal numbers representing the IP address of the server. They do not need to be 3 digits long as the "." and ":" delimiters will guarantee parsing. For example, '001', '01' and '1' would all be parsed correctly and interpreted as value 0x01 internal to the i200x. Note that these fields must be no more than 3 digits long each.
- "ppppp" and "fffff" are the port number in ASCII encoded decimal. It does not need to be 5 digits long as the ":" and "," delimiters will guarantee parsing. For example, '05001', '5001', '1', '00001' etc. would all be parsed correctly and accepted as correct. The valid range is 0..65535 (stored

internally in i200x as hexadecimal in range 0..0xFFFF). Note that this field must be no more than 5 digits long.

- In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021 and 21 are all parsed and interpreted as decimal 21.
- "**;nnnnnnnnnn**" is optional.
- When "**;nnnnnnnnnn**" does not exist, "**;bbb.ccc.ddd.eee:fffff**" is optional.
- When "**;nnnnnnnnnn**" exists, "**bbb.ccc.ddd.eee:fffff**" is not optional, it should be set as "**0.0.0.0:0**" when Net6 is not need to be set.
- The following settings are possible valid settings:

Nortel-i2004-A,iii.jjj.kkk.lll:pppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr;bbb.ccc.ddd.eee:fffff;nnnnnnnnnn.

Nortel-i2004-A,iii.jjj.kkk.lll:pppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr;0.0.0.0:0;nnnnnnnnnn.

Nortel-i2004-A,iii.jjj.kkk.lll:pppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr;bbb.ccc.ddd.eee:fffff.

Nortel-i2004-A,iii.jjj.kkk.lll:pppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.

Nortel-i2004-A,iii.jjj.kkk.lll:pppp,aaa,rrr.

The UNID has two valid formats:

- A middlebox name, and must match one of the IP-VPNs (virtual NATs) provisioned in the GWC EM.
- A middlebox id, this is identified by a '#' followed by a numeric value.

Example valid Nortel-i2004-A DHCP options;

No middlebox name/id configured:

```
Nortel-i2004-
A,11.12.13.14:15,1,6;11.12.13.15:15,1,6.
```

Middlebox name configured:

```
Nortel-i2004-
A,11.12.13.14:15,1,6;11.12.13.15:15,1,6;;middlebox-
1.
```

Middlebox id configured:

```
Nortel-i2004-
A,11.12.13.14:15,1,6;11.12.13.15:15,1,6;;#12345.
```

Note: configuring the UNID in the Nortel-i2004-A DHCP option will affect the operation of the GWC ITA/VCAC functionality. I.e. if the CICM telephony clients reports a UNID (middlebox name/id) to the CICM then this will be used in preference to the middlebox name/id associated with the Network Profile.

3 Location information DHCP options

Our goal is to implement standard DHCP location options. This is achieved by implementing the IETF GEOPRIV working group DHCP options for civil and geospatial location identification. Please refer to references [1] and [2].

At the time of developing this feature the IETF GEOPRIV working group have not finalised the DHCP option numbers for the civil and geospatial location options. Therefore Nortel specific option headers replaced the single byte DHCP option number specified in the GEOPRIV DHCP options. The location information in the option complies to the GEOPRIV specification.

3a Nortel-Geo-Spatial-A option

The DHCP option format is:

Type (1 octet):
12 possible choices are 0x80, 0x83, 0x90, 0x9d, 0xbc, 0xbf, 0xcd, 0xdb, 0xdf, 0xe8, 0xf7, 0xfb (128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, and 251).

Providing a choice of five types allows the IP phone to work in environments where the initial choice may already be in use by a different vendor.

Length (1 octet):
The value is variable depending on message content.

Data (length octets):
ASCII based

The format is:

```
"Nortel-Geo-Spatial-A,xxxxxx"
```

where,

Nortel-Geo-Spatial-A" is the unique identifier for Nortel geographic location option. xxxxxx is binary-based GEOPRIV geospatial option, less the DHCP option number byte. Fixed length of 17 bytes.

The data for the Nortel-Geo-Spatial-A DHCP option can be derived in two ways:

1. Configure the spatial location against a network profile or network location on the CICM EM network page. This will provide the whole Nortel-Geo-Spatial -A DHCP option that can be used in the DHCP server. One the data has been copied the spatial location can be deleted from the network profile or network location.
2. Use the IETF GEOPRIV working group internet draft for the geospatial DHCP option. Please see reference XX.

3b Nortel-Geo-Civil-A option

GEOPRIV civil data has a 1 byte length indicator; this means that the civil location data can be up to 255-bytes long. Including the Nortel header this causes a GEORPIV civil data option to be longer than the maximum DHCP option length of 255 bytes. Therefore the option may require fragmenting over more than one DHCP option so a fragment ID has been included.

Only fragment id's of 0 and 1 will be used and this will only be in the case that the civil location option is greater than 230 bytes. However, provision has been made within the Nortel-Geo-Civil-A fragmentation operation for more than two fragments to allow future expansion.

The DHCP option format is:

Type (1 octet):
12 possible choices are 0x80, 0x83, 0x90, 0x9d, 0xbc, 0xbf, 0xcd, 0xdb, 0xdf, 0xe8, 0xf7, 0xfb (128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, and 251).

Providing a choice of five types allows the IP phone to work in environments where the initial choice may already be in use by a different vendor.

Length (1 octet):
The value is variable depending on message content.

Data (length octets):
ASCII based

The format is:

```
"Nortel-Geo-Civil-A,i,xxxxxx"
```

where

Nortel-Geo-Civil-A" is the unique identifier for Nortel geographic civil location. i is the fragment identifier for multiple fragmented data. xxxxxx is the GEOPRIV civil DHCP option, less the DHCP option number byte. The maximum size is 230 bytes.

Notes:

"i" is ASCII encoded decimal numbers with a range of 0..4. It identifies the fragment number for multiple-fragmented civil data. If civil data appear in different Nortel-specific options and the fragment IDs are not unique, the higher priority option will overwrite the lower priority option.

Fragments of geo data can be placed in any of the 12 Nortel-specific options. They don't need to follow sequence. However, fragment ID should continue from 0 to n. For example, if fragment 0, 1, 3, and 4 are supplied, only fragment 0 and 1 are accepted.

The data for the Nortel-Geo-Civil-A DHCP option can be derived in two ways:

3. Configure the civil location against a network profile or network location on the CICM EM network page. This will provide the whole Nortel-Geo-Civil-A DHCP option that can be used in the DHCP server. One the data has been copied the civil location can be deleted from the network profile or network location.
4. Use the IETF GEOPRIV working group internet draft for the civil DHCP option. Please see reference XX.

4 I200x DHCP configurations

The i200x has three levels DHCP configuration:

- Off – the client IP address and CICM server information is configured in the client.
- On / Partial – the client IP address is obtained from DHCP and the CICM server information is configured in the client
- On / Full – the client IP address is obtained from DHCP and the CICM server information is configured in the client

When DHCP configuration is Off the UNID, civil location and geospatial location are not obtained from the DHCP server.

When Partial DHCP configuration is used the civil location and geospatial location can be obtained from the DHCP server, but the UNID is not. This is because the UNID is configured as part of the CICM server information which is configured in the client.

When Full DHCP configuration is used the UNID, civil location and geospatial location can be obtained from the DHCP server.

5 M6350 softclient DHCP configurations

The M6350 softclient has two levels DHCP configuration controlled by the 'Automatic Server Selection' check-box on the Server Settings window of the M6350 Configuration Wizard.

- Unchecked – Automatic Server Selection disabled, the CICM server information is configured in the Server Settings window of the M6350 Configuration Wizard.
- Checked – Automatic Server Selection enabled, the CICM server information is obtained from DHCP.

The softclient will always attempt to obtain the UNID, civil location and spatial location from the DHCP server whether Automatic Server Selection is enabled or disabled.

Note: When deleting Civil and Spatial options from the DHCP server the client side will not reflect the changes immediately. The DHCP client contains a DHCP caching mechanism when known DHCP options are not returned from the server. i.e. if an option has been requested and obtained from the DHCP server once it will be cached and used if a subsequent query does not return data for the said option number. If it is required to have the deletion of the option immediately updated on the client side the following mechanism should be used. Instead of deleting the Civil and Spatial Nortel options, simply provide no data for the option. I.e. place 0 into the binary array of the civil and/or spatial options. This will result in overriding the cached data on the client side.

Note: It can take several minutes for changes in the DHCP options to be picked up by the softclient. This is because of the DHCP client contains a DHCP caching mechanism.

88.2.1.3.2 Unistim

Unistim (Unified Networks IP Stimulus) is a Nortel Networks defined protocol for Internet Terminals (IP phones) used for VoIP (Voice over Internet Protocol) telephony services.

The information required for the ECS location identification solutions is:

- Public IP Address
- Private IP Address
- MAC Address
- Civil Location description
- Geospatial Location description
- Unique Network Id

The Public and Private IP Addresses are required for the CICM to manage a telephony client and so are already reported to the CICM prior to this activity.

This activity implemented Unistim commands to request and report the following client information.

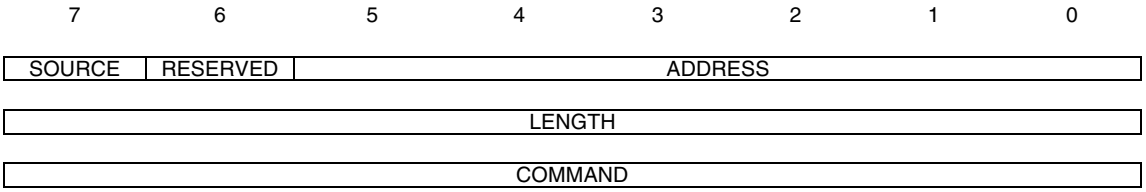
- MAC Address
- Civil Location description
- Geographic Location description
- Unique Network Id

1 Requesting the MAC Address

A CICM telephony client's MAC address is necessary as it is essential to the Enterprise ECS solution, e.g. the MAC address will be used to tie the output of the GWC to the output of the LIS.

The Query MAC Address is introduced as a NI to IT command for the Basic Manager.

Figure 5 Query MAC Address (10 XX)



1st Byte; Command header:

- Source = 0 (originated by NI)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = 0x03 (3 bytes)

3rd Byte; Command contents:

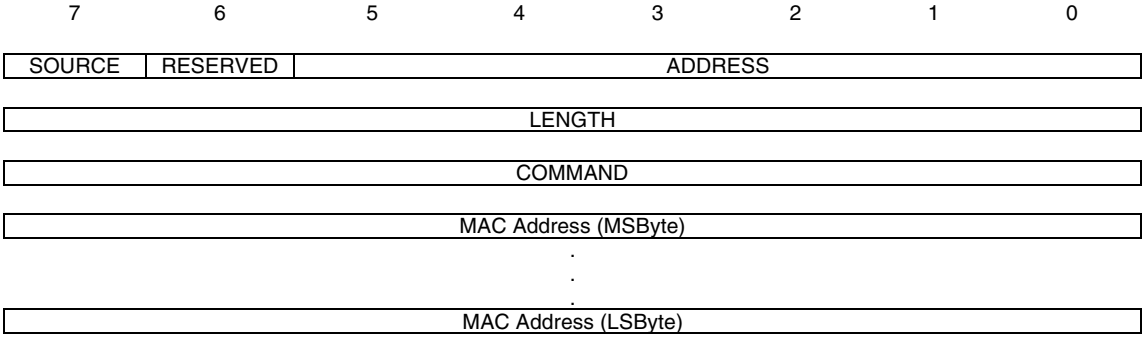
- Command = 0x10 (Query MAC address)

2 Reporting the MAC Address

The CICM telephony client responds to the 'query MAC' command with a 'MAC information report' command containing the clients MAC address. This is a new 'IT to NI' command for the Basic Manager.

An i200x responds with the sets MAC address. A M6350 softclient responds with the MAC address of the host adapter being used.

Figure 6 MAC Information report (11 XX XX XX .. XX)



1st Byte ; Command header:

- Source = 1 (originated by IT)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = 0x09 (9-Bytes, 3-Byte header + 6-Byte MAC address)

3rd Byte; Command contents:

- Command = 0x11 (MAC Address report)

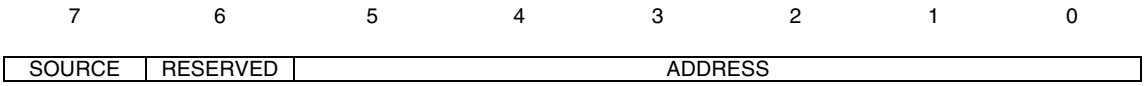
4th Byte; Command contents: MAC Address (MSByte)

9th Byte; Command contents: MAC Address (LSByte)

3 Requesting the Location Identification information

To request the Location Identification information from the telephony client the CICM sends a new Unistim ‘query location’ command. Within the command the CICM can specify which location identification parameters are required, i.e. unique network id, civil location description and geospatial location description. The Query Location Unistim command is a new ‘NI to IT’ command for the Basic Manager.

Figure 7 Query Location (0F XX)



LENGTH							
COMMAND							
RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	GLOC	LOC	UNID

1st Byte ; Command header:

- Source = 0 (originated by NI)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = 0x04 (4 bytes)

3rd Byte; Command contents:

- Command = 0x0F (Query Location)

4th Byte; Command contents: indicates which information is being requested

- UNID = 1 if Unique Network Id is required, otherwise UNID = 0
- LOC = 1 if Location descriptor is required, otherwise LOC = 0
- GLOC = 1 if the Geographical Location descriptor is required, otherwise GLOC = 0

4 Reporting the Location Identification information

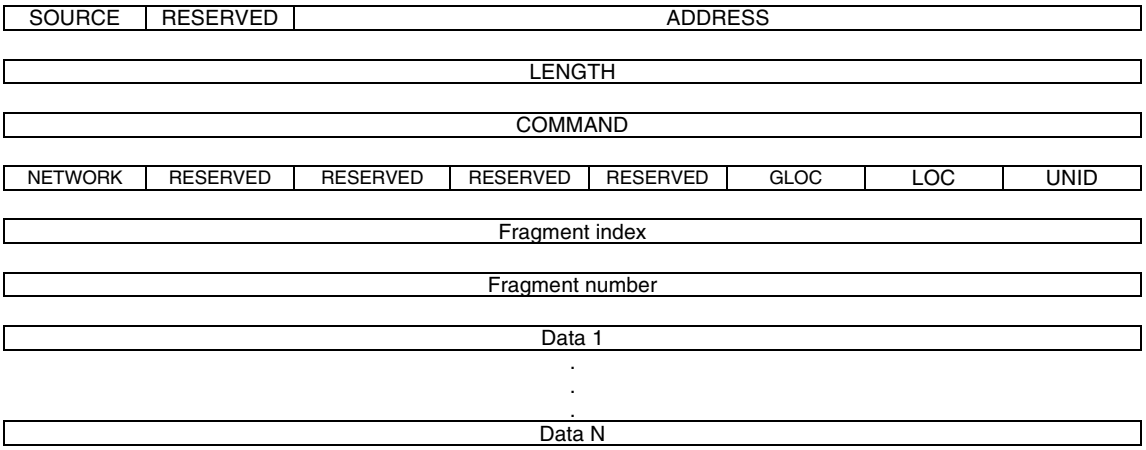
The CICM telephony client responds to the ‘query location’ command with a separate ‘location information report’ command for each requested parameter. This command includes fields for the parameter id, length and value.

The civil location descriptor may too large to fit into a single Unistim command, maximum length is 255-bytes, therefore the ‘location information report’ message supports fragmentation. In the case where the location descriptor is larger than the maximum size to fit into a single Unistim ‘Location Information report’ command the telephony client will fragment the location descriptor and the CICM will rebuild the location descriptor.

The Location Information report Unistim command is a new ‘IT to NI’ command for the Basic Manager.

Figure 8 Location Information report (10 XX XX XX .. XX)

7	6	5	4	3	2	1	0



1st Byte ; Command header:

- Source = 1 (originated by IT)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = variable

3rd Byte; Command contents:

- Command = 0x10 (Location Information report)

4th Byte; Command contents: indicates which information is being report, either:

- UNID = 1 if Unique Network Id is reporting in this command; LOC and GLOC must equal 0
- LOC = 1 if Location descriptor is reporting in this command; UNID and GLOC must equal 0
- GLOC = 1 if geospatial location descriptor is reporting in this command; UNID and LOC must equal 0
- NETWORK = 1 if the location information is provided by the network. If NETWORK = 0, the location information has been provided by the user.

  Note: Note: For the UNID, NETWORK must always be 1.

  Note: Note: Location Identification information reported by an i200x etherset will always have NETWORK equal to 1.

Note: Note: NETWORK can only equal to 0 for the Location Identification information reported by the M6350 soft client when the user specifies the location information manually.

5th Byte; Command contents:

- Fragment index – the index of the command within the fragmented command

6th Byte; Command contents:

- Fragment Number – the total number of fragments required to report the location identification data.

7th Byte; Command contents:

- Data 1 – first byte of the Location Information data.

Nth Byte; Command contents

- Data N – last byte of the Location Information data.

If a parameter is requested but not available, e.g. was not provided by the DHCP server, then the terminal responds with a 'location information report' message for the parameter specifying a Length of 6, i.e. the Unistim Location Information report command header with no data.

88.2.1.3.3 H.248

Prior to this activity, the location change event of the terminal location H.248 package was implemented to report the Unique Network ID (UNID) for the CICM telephony client from the CICM to the GWC. This event is reported after a user has successfully logged into a client. The reported Unique Network ID is used for network policy services. This event and operation is maintained by this activity. The location change event is used to trigger an audit of the Terminal State Descriptor, which contains the Location Identification package.

Please refer to Appendix A: H.248 Location Identification package description for more details of the Location Identification H.248 package.

The location change event contains two parameters:

- reg, a Boolean used to indicate whether the termination is being registered to, or un-registered from, the unique network id (locid).
- locid, a String used to represent the unique network id (locid)

When a user logs in to a CICM telephony client the CICM sends a location change event with reg=TRUE and the locid.

When a user logs out from a CICM telephony client the CICM sends a location change event with reg=FALSE.

88.2.1.3.4 Northbound to Location Recipient

The GWC collects the CICM ECS Location Identification information from the CICMs that it controls. The Location Identification information is immediately sent to the Location Recipient. The Location Identification information is reported by the GWC to the Location Recipient in a proprietary XML format. The XML structure is generated from the location information received in the H.248 TermState audit message and termination/endpoint information held in the GWC.

The information required by the Location Recipient is given in Table 2 Location Identification parameters.

Table 2 Location Identification parameters

Parameter	XML tag	Description	Format	Example
Call Server Identifier	csid (attribute of locid element)	Used to identify the Call Server that provides call processing for the CICM telephony client	String	CS2K_LONDON
GWC Identifier	gwcid (attribute of locid element)	Used to identify the Gateway Controller that provides call processing and management for the CICM telephony client	String	GWC-1
Node number	node (attribute of terminal element)	The number the Call Server uses to uniquely identify the CICM node.	Numeric	4
Terminal number	term (attribute of terminal element)	The number the Call Server uses to uniquely identify the CICM telephony client on the node.	Numeric	1
Gateway name	gw (attribute of terminal element)	The name of the gateway, used in the GWC and GWC-EM	String	cicm-1
Endpoint name	ep (attribute of terminal element)	The name of the endpoint on the gateway, used in the GWC and GWC-EM.	Numeric	tp/0/0001
Unique Network ID	unid	Uniquely identifies the middle-box, NAT or LBL that CICM telephony client network is behind.	Numeric	45
Public IP Address	pubip	The public IP address of the CICM telephony client	String	
Private IP Address	privip	The private IP address of the CICM telephony client	String	
MAC Address	mac	The MAC address of the CICM telephony client	String	
Source of Geospatial Location Information	geosrc	Whether the geospatial location descriptor was provided by the Network, e.g. DHCP Server, or by the User, e.g. the M6350 CICM softclient	String	network
Geographic Location Descriptor	geo	The geospatial location of the CICM telephony client. In the GEOPRIV geospatial DHCP option format, not include the single byte option number at the start.	String	
Source of Civil Location Information	civilsrc	Whether the civil location descriptor was provided by the Network, e.g. DHCP Server, or by the User, e.g. the M6350 CICM softclient	String	user
Civil Location Descriptor	civil	The civil location of the CICM telephony client. In the GEOPRIV civil DHCP option format, not include the single byte option number at the start.	String	

The XML schema is provided in Appendix C: Location Identification reporting XML schema.

1 XML messages

Several XML messages are required to support the reporting of location identification data to the location recipient and to maintain the integrity of the data in the location recipient.

1a New Location identification data (add)

When the GWC receives location identification data from the CICM for a newly registered termination it creates an ‘add’ XML structure and sends it to the location recipient.

The H.248 Location Identification package audit from the CICM does not identify if this is the first time the location identification information is being reported for the termination; therefore the GWC uses an internal flag to indicate whether the location identification information has been successfully reported to the Location Recipient. If the flag is false, an ‘add’ XML message is sent to the Location Recipient containing the Location identification information.

The internal GWC per termination ‘location identification’ flag is set when the add XML message is successfully sent to the Location Recipient.

An example ‘add’ XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>
<locid csid=”CS2K_LONDON” gwcid=”GWC-1”>
   <add>
      <terminal node=”4” term=”1” gw=”cicm-1” ep=”tp/0/0001”>
         <unid>45</unid>
         <pubip>47.165.168.100:2000</pubip>
         <privip>10.0.1.16:5000</privip>
         <mac>0E184F93AC01</macc>
         <geosrc>network</geosrc>
         <geo>xxxxxxxxxxxx</geo>
         <civilsrc>network</civilsrc>
         <civil>xxxxxxxxxxxxxxxxxxxxxxxx</civil>
      </terminal>
   </add>
</locid>
```

1b Changed Location identification data (change)

If the GWC receives location identification data from the CICM for a termination that has already successfully reported location identification to the

Location Recipient, the GWC generates a ‘change’ XML structure and sends it to the location recipient.

An example ‘change’ XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>
<locid csid=”CS2K_LONDON” gwcid=”GWC-1”>
   <change>
      <terminal node=”4” term=”1” gw=”cicm-1” ep=”tp/0/0001”>
         <unid>45</unid>
         <pubip>47.165.168.100:2000</pubip>
         <privip>10.0.1.16:5000</privip>
         <mac>0E184F93AC01</macc>
         <geosrc>network</geosrc>
         <geo>xxxxxxxxxxxx</geo>
         <civilsrc>network</civilsrc>
         <civil>xxxxxxxxxxxxxxxxxxxxxxxx</civil>
      </terminal>
   </change>
</locid>
```

1c Remove Location Identification data (remove)
When a user logs out of a CICM telephony client the location identification information is no longer required or reliable. The CICM reports the user log out in a H.248 location change event. When the GWC receives this event it resets the stored unique network id and sends a ‘remove’ XML structure to the location recipient to indicate that the location identification information for the termination/endpoint is no longer valid.

An example ‘remove’ XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>?>
<locid csid=”CS2K_LONDON” gwcid=”GWC-1”>
   <remove >
      <terminal node=”4” term=”1” gw=”cicm-1” ep=”tp/0/0001”>
      </terminal>
   </remove >
</locid>
```

The internal GWC ‘location identification’ flag is reset so that any subsequent location identification information received from the CICM is treated as new information.

1d Synchronize Location Identification data (SYNC)

The location recipient sends this message when it requires the location data to be synchronized.

An example SYNC XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>?>
   <locid >
      <sync/>
   </locid >
```

On receipt of the synchronize message the GWC recovers the Location Identification information for every termination by auditing the Location Identification package for every registered CICM telephony client termination. For unregistered endpoints a ‘remove’ XML message will be sent to the location recipient.

1e Connection Keep-alive (keepalive)

The TCP/IP connection established by the GWC has a time-out, e.g. if no data is sent over the connection for 2 hours the GWC drops the connection. To prevent the connection from being dropped due to this timeout a timer is used. If the timer reaches a predefined time, e.g. 1 hour, the GWC sends a ‘keepalive’ XML structure to the Location Recipient to keep the connection alive. The timer is reset each time data is sent on the connection. The location recipient will ignore the ‘keepalive’ XML structure.

An example ‘keepalive’ XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>?>
   <locid csid=”CS2K_LONDON” gwcid=”GWC-1”>>
      <keepalive/>
   </locid>
```

1f Connection status message (status)

The location recipient sends this message to check that the connection is still active.

An example ‘status’ XML structure:

```
<?xml version='1.0' encoding="UTF-8"?>?>
   <locid>
      <status />
   </locid >
```

The ‘status’ message will be ignored by the Location Identification application on the GWC.

88.2.1.3.5 SNMP

A new SNMP MIB has been introduced to send the Location Identification configuration from the GWC Element Manger to the GWC. Please refer to Appendix B: GWC-LOCATION-CHANGE-REPORTING-MIB.

88.2.1.4 Feature Configuration and Activation

There are several places within the Call Server network that require configuring to enable the CICM ECS Location Identification functionality.

88.2.1.4.1 DHCP Server

The DHCP Server must be configured with the DHCP options for the GEOPRIV civil location identification, GEOPRIV geospatial location identification and unique network id.

Please refer to section 1.2.1.3.1 DHCP.

88.2.1.4.2 CICM telephony clients

1 Ethersets (i200x)

The Etherset (i200x) must be configured to use full DHCP configuration to support the reporting of the UNID, civil and geospatial location Identification.

The Etherset (i200x) must be configured to use partial DHCP configuration to support the reporting of the civil and geospatial location Identification. The reporting of the UNID is not supported when using partial DHCP configuration.

If the Etherset (i200x) is configured not to use DHCP configuration reporting of the UNID, civil and geospatial location Identification is not supported.

The i200x requires phase 2 firmware level D41 and above.

2 Soft client (M6350)

The M6350 softclient has been modified to provide the user with an interface to specify their civil and geospatial location description when logging in.

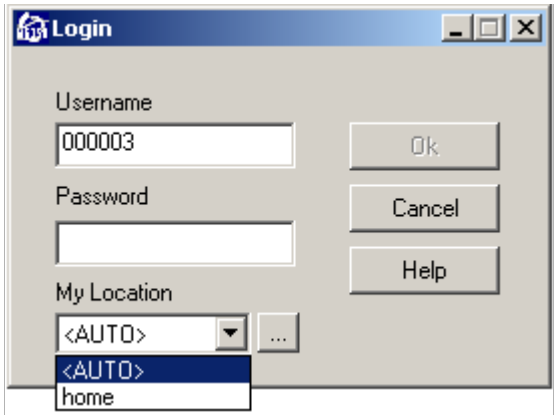
The M6350 CICM softclient has also been modified to allow the user to specify automatic server selection. If this is selected the M6350 softclient retrieves the CICM and Location Identification options from the DHCP server. Meaning that the user is not required to specify the server address.

The CICM telephony softclient must be at release 7.

2a Entering location description

The user log in process has been changed so that the user is prompted to choose a location description. An example is given in Figure 9 CICM Soft client login GUI.

Figure 9 CICM Soft client login GUI

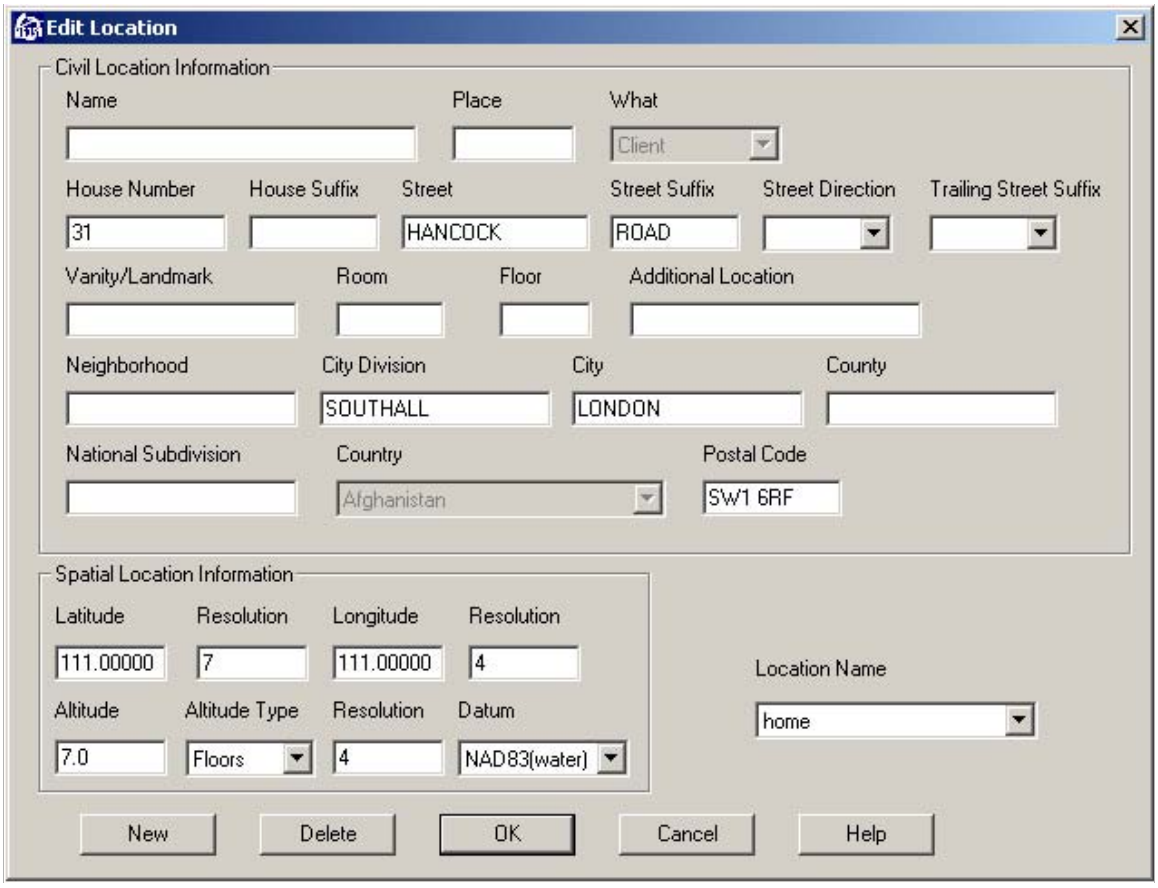


The <AUTO> location is provided if a location, civil and/or geospatial, is provided by the DHCP server.

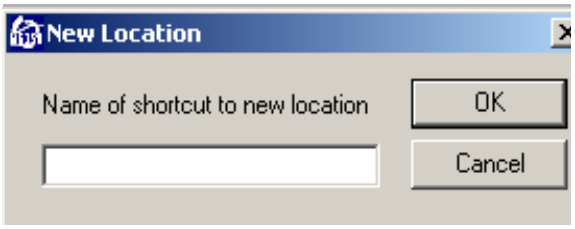
The GUI may provide a list of previously entered locations, which a user can choose from, or enter a new location. The "…" button opens the "Edit Location" window for viewing and editing location details. The existing locations can be viewed and edited in the "Edit Location" window. The <AUTO> location can only be viewed in the "Edit Location" window. New locations are entered in the "Edit Location" window.

An example is given in Figure 10 CICM M6350 Soft client Edit.

Figure 10 Figure 10 CICM M6350 Soft client Edit Location window



The “New” button is used to enter new location details. When “New” is pressed the following windowed is opened. The new location name is specified here.



Entering the location name, which can not be a name used before, and pressing “OK” causes the fields in the existing “edit location” window to be cleared and the new location details can be entered.

When entering location details only the relevant fields need to be modified, e.g. unnecessary fields can be left blank.

Note: Note: if all the fields of the civil or spatial location are left blank then the respective location information parameter is not generated. E.g. If the user know their civil location details but not the spatial location details then they should leave all the spatial fields blank and the client will not generate a spatial location.

The “Delete” button deletes the location currently being viewed.

The “OK” button closes the “edit location” window saving any changes.

The “Cancel” button closes the “edit location” window discarding any changes.

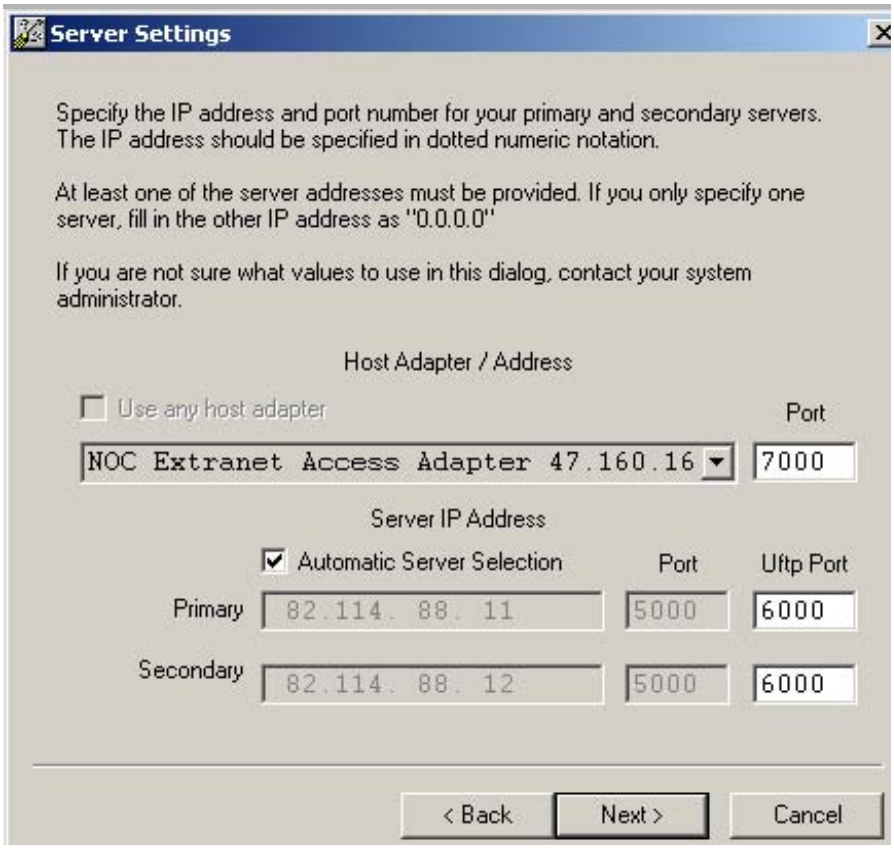
The “Help” button opens the “edit location” help window.

2b Enabling automatic server selection

An existing part of the M6350 softclient “Configuration wizard” is the ‘Server settings’ window. In this window the user specifies the CICM server settings to use. Prior to this activity only manual server selection was available, requiring the user to enter the address of the CICM server. A new option has been provided which allows the user to choose ‘automatic server selection’. When ‘automatic server selection” is enabled the Server settings fields are greyed out as the server settings are obtained from DHCP.

An example is shown in Figure 11 CICM Soft client server settings GUI.

Figure 11 Figure 11 CICM Soft client server settings GUI



Choosing ‘automatic server selection’ means that the server settings are obtained from the DHCP server when the M6350 softclient is started. Please refer to section 1.2.1.3.1 (2) Nortel-i2004-A option for more details.

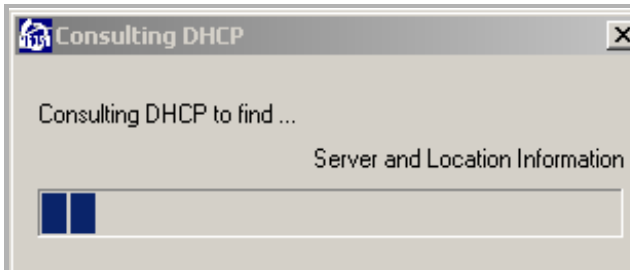
It is suggested that the location details provide by the DHCP server and made available to the user as the <AUTO> location be used, however the user can view the location details and decided whether they wish to use the <AUTO> location or not.

When reporting the civil and geospatial location description to the CICM the M6350 softclient indicates whether the information was provided by the network or user defined. This is because the ECS system may consider a network provided location descriptor more reliable.

2c Starting the M6350 Softclient

Starting the M6350 softclient has not been changed by this feature other than when the M6350 softclient is started a window is opened indicating that a DHCP request is being performed.

If “automatic server selection” is not enabled only the location DHCP options are used from the DHCP server. If “automatic server selection” is enabled the server settings and location DHCP options are used from the DHCP server. Example dialog display when starting the M6350 softclient:



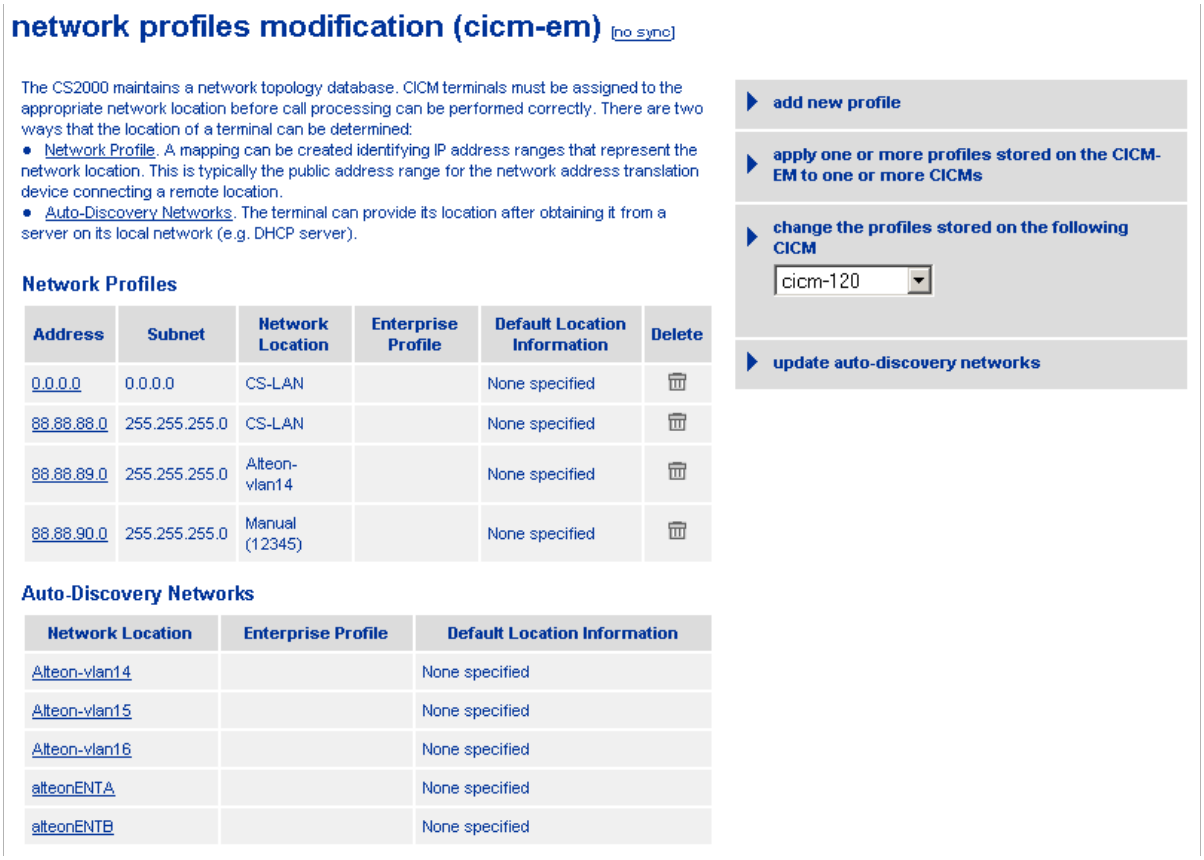
88.2.1.4.3 CICM Element Manager

On the ‘network’ page of the CICM Element Manager the operator has the option to configure a default civil location and default geospatial location against ‘Network Profiles’ and ‘Network Locations’.

One the ‘terminals’ page the operator can view the current location details of a terminal.

1 Network page

The network page of the CICM EM allows profiles to be configured for different enterprises, ranges of IP Addresses. To facilitate ITA a Network Location can be associated with a Network Profile. This Network Location is the default middlebox to use if the client does not provide a middlebox.



In SN06.2 a CICM Network Profile was solely used to associate an Enterprise to a Network Location (middlebox). When a user logs into a CICM telephony client in the Enterprise the middlebox id was derived from the ‘network location’ of the ‘network profile’ and reported to the GWC for call processing purposes.

This process has been superseded in SN07 as CICM telephony clients can now report the middlebox name/id to the CICM. However, the association of Network Profiles to Network Locations has been retained for backwards compatibility, i.e. scenarios when the client does not report the middlebox name/id.

This could be because phase 1 i200x’s firmware does not support the reporting of the middlebox name/id, or when the middlebox name/id is not available in the Nortel-i2004-A DHCP option.

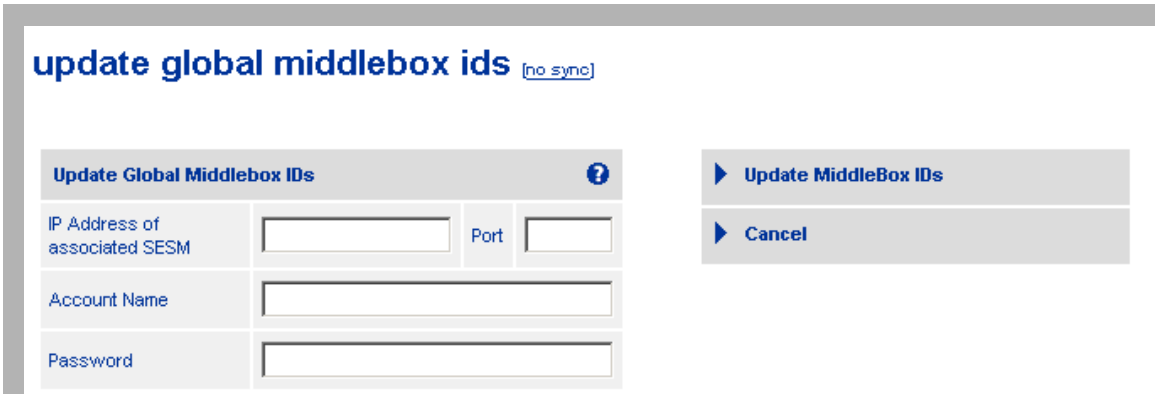
The ‘network location’ can take one of three forms:

- CS-LAN – This is the default Network Location. If this value is used all the clients in the Network Profile are considered to be within the Call Server LAN and therefore ITA is not required Middlebox id of 0.

- An Auto-Discovery Network – These are configured in SESM as IP-VPNs (virtual NATs). The names and id are downloaded from the SESM before they can be used.
- A Manually Defined Limited Bandwidth Link (LBL) – This is when the Enterprise is behind a LBL. The middlebox id must be retrieved manually from the SESM.

1a Auto-Discovery Networks

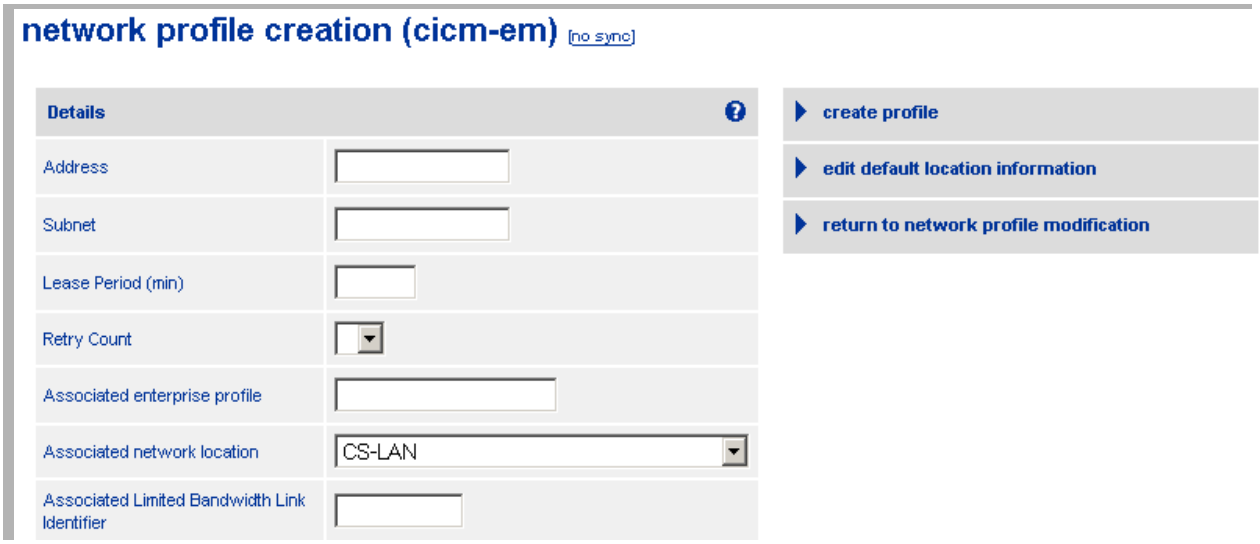
To be able to associate a IP-VPNs (virtual NATs) with a Network Profile they first must be downloaded from the GWC EM. This is achieved by selecting the 'update auto-discovery networks' option on the CICM EM network page. This opens the following page:



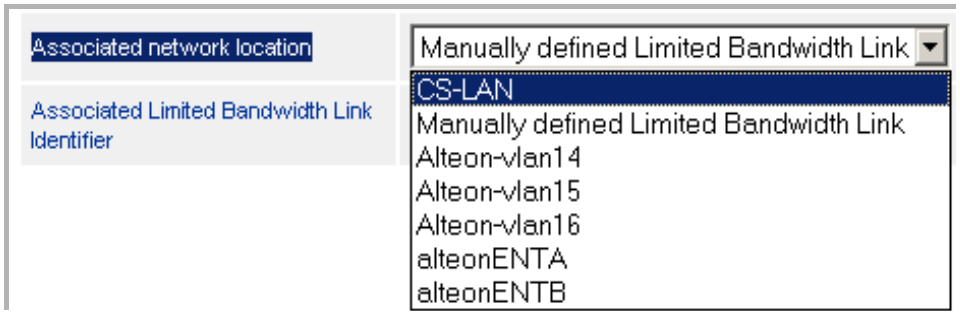
The SESM/GWC EM OSSGate IP Address, Port number, Account name and password should be entered and 'Update MiddleBox Ids' selected. This retrieves the list of IP-VPNs (virtual NATs) from the GWC EM and adds them to the Auto-Discovery Networks List on the CICM EM network page (see above).

1b Configuring a new Network Profile

To configure a Network profile select the 'add new profile' option on the CICM EM network page. This opens the following page:



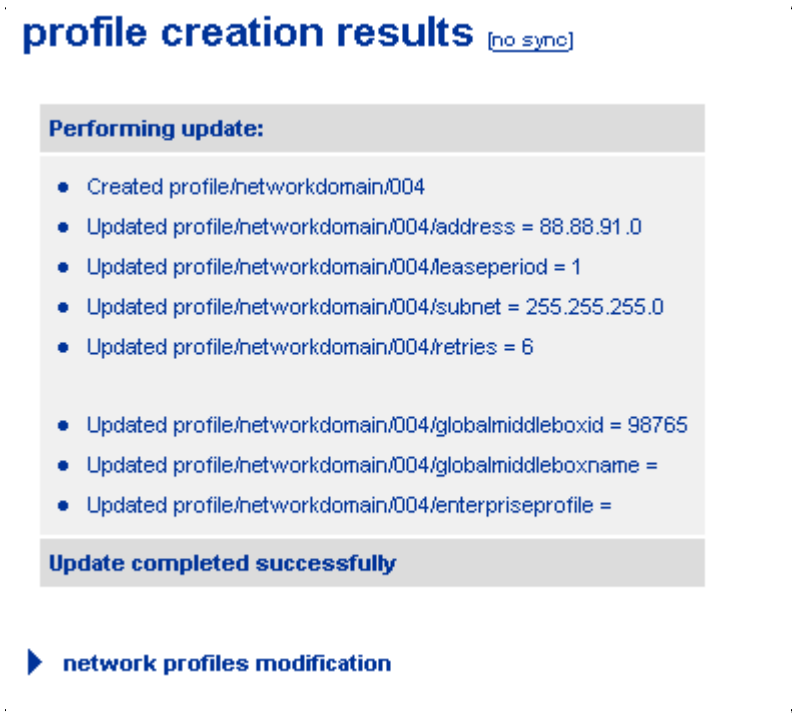
Configure the fields as required. If the clients reside in the CS-LAN leave CS-LAN selected in the 'Associated network location' drop-down menu. Otherwise, select a Auto-Discovery Network or 'Manually Defined Limited Bandwidth Link'. See example below.



If 'Manually defined Limited Bandwidth Link' is selected the 'Limited Bandwidth Link Identifier' must be configured in field 'Manually defined Limited Bandwidth Link'.

If CS-LAN or an Auto-Discovery Network is selected field 'Associated Limited Bandwidth Link Identifier' does not need a value, any value will be ignored unless 'Manually defined Limited Bandwidth Link' is selected.

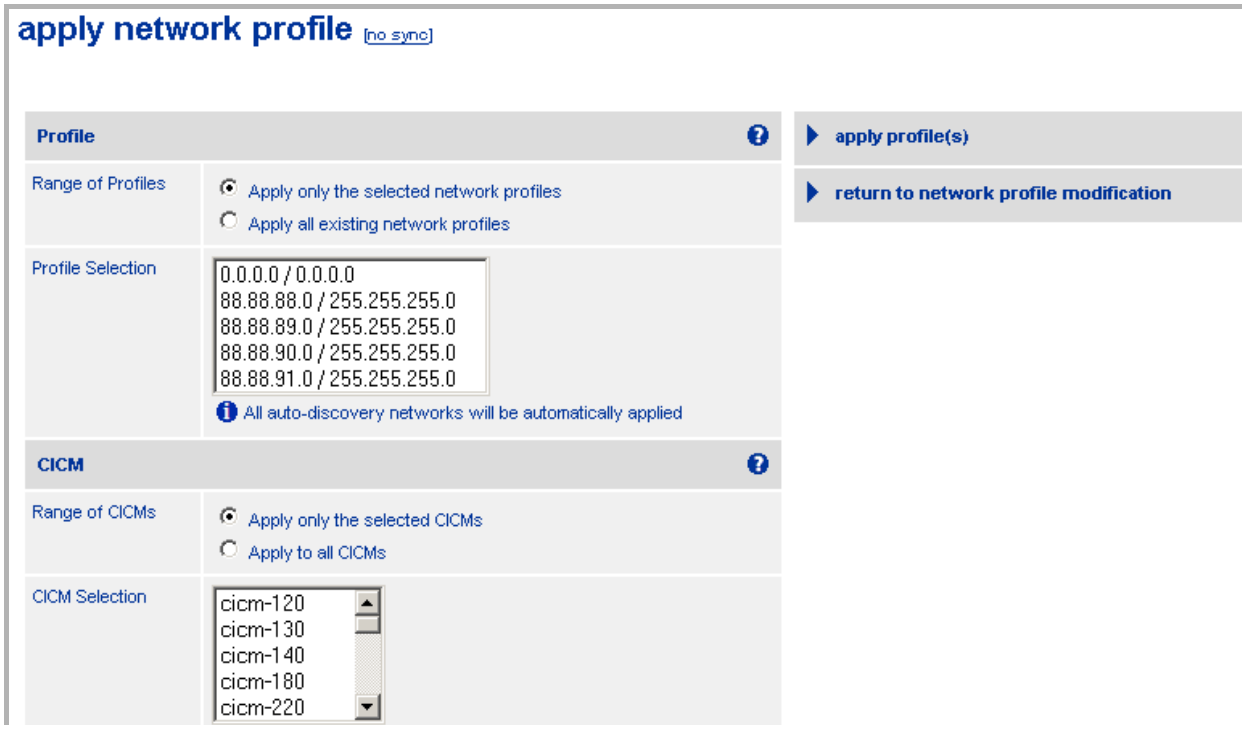
Once the new Network Profile fields have been configure select 'create profile' to save the new Network Profile. A results page shows what actions have been performed.



Select ‘network profiles modification’ to return to the CICM EM network page, where the new Network Profile is displayed.

1c Modifying an existing Network Profile
To modify an existing Network profile select the Network Profile's address, which is a hyperlink. This opens the Network Profile page for the selected Network Profile. The fields can be modified and the changes saved by selecting 'save your changes to this profile'.

1d Applying Network Profiles to a CICM gateway
The changes to the Network Profile page must be applied to the CICM gateway before they take affect. This is achieved by selecting 'apply one or more profiles stored on the CICM-EM to one or more CICMs'. This opens the following page:



The Profiles to apply are selected, alternatively all the profiles are selected. The CICMs to apply the Profiles to are selected, alternatively all the CICMs the CICM EM knows about are selected. Select 'apply profile(s)' to apply the profiles to the CICM. The results of the apply are displayed on a new page.

Note: The Auto Discovery Networks MUST be applied to the CICM before they take affect. All the Auto Discovery Networks are always applied to a CICM when a Network Profile is applied.

2 Default Location Information

Default Location Information can be configured against Network Profiles and Network Locations.

The configured Default Location Information will be used if the terminal does not report the location information. The civil and spatial location information is considered separately, e.g. if a terminal reports only civil location information the spatial location information will be taken from the Network Profile or Network Location, and vice versa if the terminal reports only the spatial location information.

The Default Location Information configured against the Network Profile takes precedence over the Default Location Information configured against the Network Location.

Default Location Information can only be configured against Auto-Discovery Network Locations. Default Location Information can not be configured against the CS-LAN or Manually Defined Limited Bandwidth Link Network Locations.

If a terminal reports an Auto-Discovery Network Location as the middlebox name and this matches one of the Auto-Discovery Network Locations then this will be used instead of the Network Location configured against the Network Profile. The Default Location Information configured against the Auto-Discovery Network Location will be used if the terminal does not report Location Information or the Network Profile does not have Default Location Information Configured.

Table 3 Use of Default Location Identification shows example scenarios of how the Default Location Information configured against the Network Profile and Network Location are used. Table 3 Use of Default Location Identification is intended to give example of the operation and is not a complete list of scenarios.

Table 3 Use of Default Location Identification

Information reported by terminal			Network Profile			Network Location		Information reported for terminal (from)		
UNID	Civil Location	Spatial Location	Network Location type	Civil Location	Spatial Location	Civil Location	Spatial Location	UNID	Civil Location	Spatial Location
No	No	No	CS-LAN	No	No	N/A	N/A	CS-LAN	None	None
No	No	No	Manual LBL	No	No	N/A	N/A	LBL Id	None	None
No	No	No	Auto-Discovery	No	No	No	No	Auto-Discovery	None	None
No	No	No	CS-LAN	Yes	No	N/A	N/A	CS-LAN	Network Profile	None
No	No	No	Manual LBL	No	Yes	N/A	N/A	LBL Id	None	Network Profile
No	No	No	Auto-Discovery	Yes	Yes	No	No	Auto-Discovery	Network Profile	Network Profile
No	No	No	Auto-Discovery	No	No	Yes	Yes	Auto-Discovery	Network Location	Network Location
No	No	No	Auto-Discovery	Yes	Yes	Yes	Yes	Auto-Discovery	Network Profile	Network Profile
No	No	No	Auto-Discovery	Yes	No	Yes	Yes	Auto-Discovery	Network Profile	Network Location
Auto-Discovery	No	No	N/A	No	Yes	Yes	Yes	Reported by terminal	Network Location	Network Profile
Auto-Discovery	Yes	No	N/A	No	Yes	Yes	Yes	Reported by terminal	Reported by terminal	Network Profile
Auto-Discovery	Yes	Yes	N/A	No	Yes	Yes	Yes	Reported by terminal	Reported by terminal	Reported by terminal
Manual LBL	No	No	N/A	No	Yes	N/A	N/A	Reported by terminal	None	Network Profile
Manual LBL	Yes	No	N/A	No	Yes	N/A	N/A	Reported by terminal	Reported by terminal	Network Profile
Manual LBL	Yes	Yes	N/A	No	Yes	N/A	N/A	Reported by terminal	Reported by terminal	Reported by terminal

2a Configuring Default Location Information against a Network Profile
Default Location Information for a Network Profile can be configured on the Network Profile Creation page or modified on the Network Profile Page, please see sections 1.2.1.4.3(1b) Configuring a new Network Profile and 1.2.1.4.3.(1c) Modifying an existing Network Profile respectively on how to get to these pages.

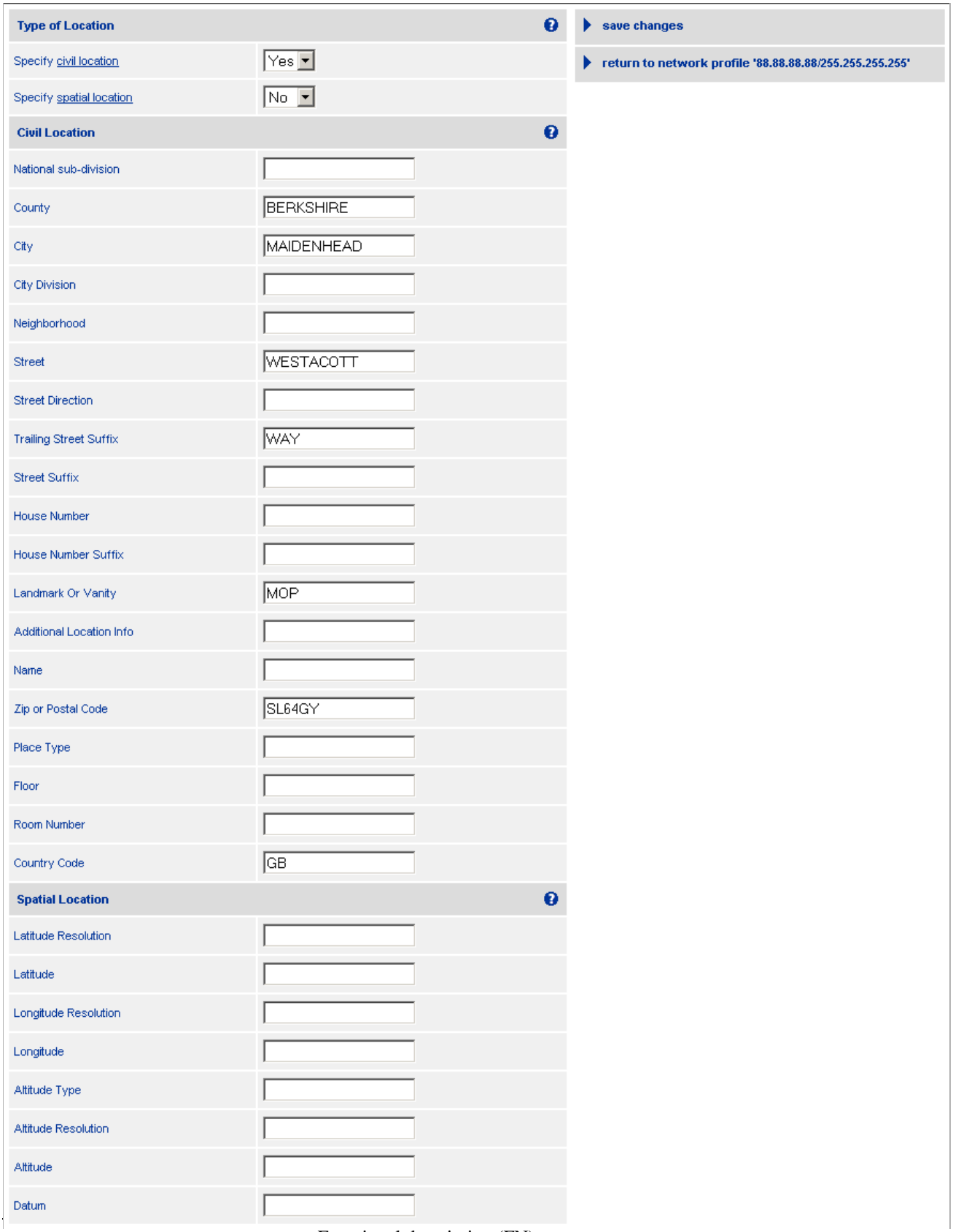
When a Default Location Information is configured for a Network Profile it is displayed when viewing the Network Profile. A textual representation of the Default Location Information is displayed, as well as the Default Location Information formatted as the Nortel-Geo-Civil-A DHCP option for the civil location and the Nortel-Geo-Spatial-A DHCP option for the spatial location.

Once on the page select ‘edit default location information’, on the right at the top, to open the ‘edit default location information’ page for the Network Profile. If the Network Profile already has Default Location Information configured this is displayed.

Default Location information configuration help is displayed by selecting the (?) in the section header.

The general rules for configuring the default location information are as follows:

- Civil Location – all fields other than the Country Code are optional. The Country code must be two letters and a valid ISO-3166 Country Code, the list of Country Codes is provided in the help.
- Spatial Location – the fields must contain numeric characters, other than '-' for negative values and '.' for fractions. The values must be within the specific ranges, which are provided in the help.



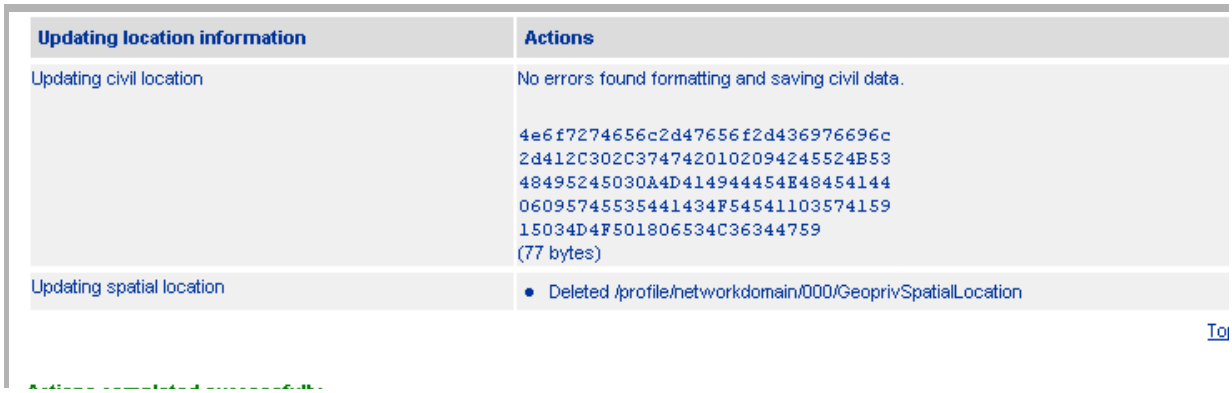
Type of Location	
Specify civil location	Yes
Specify spatial location	No

Civil Location	
National sub-division	
County	BERKSHIRE
City	MAIDENHEAD
City Division	
Neighborhood	
Street	WESTACOTT
Street Direction	
Trailing Street Suffix	WAY
Street Suffix	
House Number	
House Number Suffix	
Landmark Or Vanity	MOP
Additional Location Info	
Name	
Zip or Postal Code	SL64GY
Place Type	
Floor	
Room Number	
Country Code	GB

Spatial Location	
Latitude Resolution	
Latitude	
Longitude Resolution	
Longitude	
Altitude Type	
Altitude Resolution	
Altitude	
Datum	

Functional description (FN)

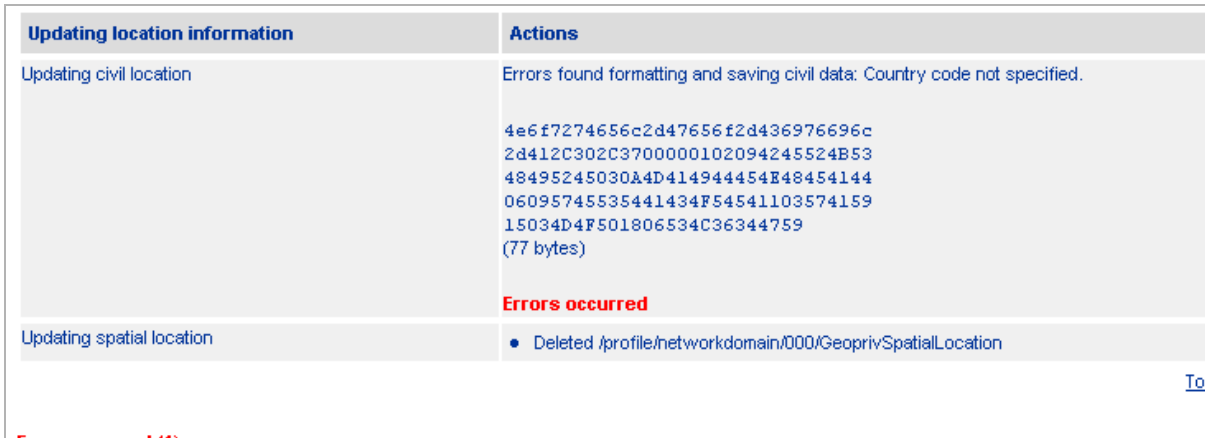
Once the Default Location Information has been configure, or modified, select ‘save changes’ to save the Default Location Information to the Network Profile. The ‘updating location information’ page reports the outcome of the ‘save changes’, e.g.



Updating location information	Actions
Updating civil location	No errors found formatting and saving civil data. 4e6f7274656c2d47656f2d436976696c 2d412C302C3747420102094245524B53 48495245030A4D414944454E48454144 0609574553544143 4F54541103574159 15034D4F501806534C36344759 (77 bytes)
Updating spatial location	• Deleted /profile/networkdomain/000/GeoprivSpatialLocation

To

The page reports whether errors were found while formatting and saving the default location information. If no errors were found the outcome “No errors found formatting and saving civil data.” and “No errors found formatting and saving spatial data.” for the civil and spatial locations respectively is reported. If errors are found they are listed and the total number of errors found is reported. E.g. For the case when the country code (mandatory field) has not been specified.



Updating location information	Actions
Updating civil location	Errors found formatting and saving civil data: Country code not specified. 4e6f7274656c2d47656f2d436976696c 2d412C302C3700000102094245524B53 48495245030A4D414944454E48454144 0609574553544143 4F54541103574159 15034D4F501806534C36344759 (77 bytes) **Errors occurred**
Updating spatial location	• Deleted /profile/networkdomain/000/GeoprivSpatialLocation

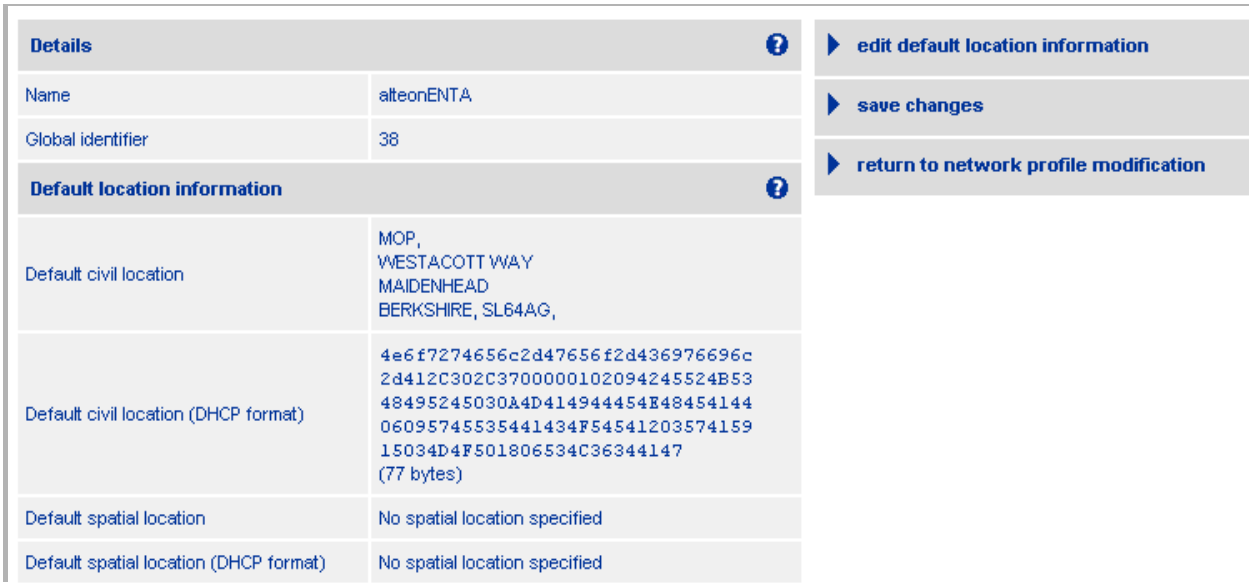
To

Even if errors are found a best effort is made format and save the default location information, it is the responsibility of the operator to re-edit the default location data to rectify the errors found.

Note: Changes to the Default Location Information for a Network Profile must be applied to the CICM gateway before they will take affect. Please see section 1.2.1.4.3(1d) Applying Network Profiles to a CICM gateway.

2b Configuring Default Location Information against a Network Location
Default Location Information for a Network Location can be configured on the 'auto-discovery network' page for an Auto-Discovery Network Location. To get to this page select the Network Location from the Auto-Discovery Networks list on the Networks page. An example is shown in section 1.2.1.4.3(1) Network page.

When a Default Location Information is configured for a Network Location it is displayed on the 'auto-discovery network' page. A textual representation of the Default Location Information is displayed, as well as the Default Location Information formatted as the Nortel-Geo-Civil-A DHCP option for the civil location and the Nortel-Geo-Spatial-A DHCP option for the spatial location.



Once on the page select 'edit default location information', on the right at the top, to open the 'edit default location information' page for the Network Location. If the Network Location already has Default Location Information configured this is displayed.

Please refer to section 1.2.1.4.3(2a) Configuring Default Location Information against a Network Profile for detail configuring the Default Location Information fields.

3 Terminal Page

The current location details of a terminal can be viewed in the Networking Information section of the terminal page.

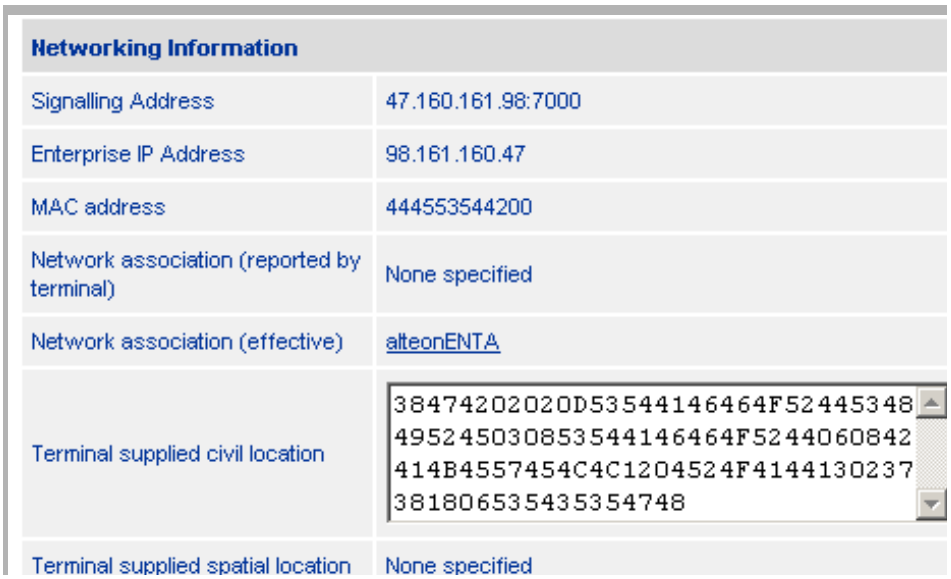


Table 4 Description of Network Information fields on terminal page

Name	Description	Comments
Signaling Address	Public IP Address of terminal signalling network interface	
Enterprise IP Address	Private IP Address of terminal	
MAC Address	MAC Address of terminal signalling network interface	
Network association (reported by terminal)	The middlebox name/id reported by the terminal.	
Network association (effective)	The middlebox name/id reported to the GWC for the terminal.	If this is an auto-discovered middlebox name, this is a hyperlink to the auto-discovery network page for the Network location.
Terminal supplied civil location	The civil location (bytes) reported by the terminal.	Does not contain the civil location taken from the Network Profile or Network Location.
Terminal supplied spatial location	The spatial location (bytes) reported by the terminal.	Does not contain the spatial location taken from the Network Profile or Network Location.

The Network Information on the terminal page is historic, e.g. it is not updated when a user logs out of the terminal and is only updated when a user logs into the terminal.

88.2.1.4.4 GWC Element Manager

The CICM ECS Location Identification functionality on the GWC is activated via the GWC Element Manager GUI.

1 Configuring the Location Recipient

The destination for the Location Identification information, e.g. the Location Recipient, is configured in the GWC Element Manager. The Location Recipient is configured in the Location Recipient tab of the Network Devices section of the Network panel. The default value for the Location Recipient DNS, IP Address and Port number is <not configured>. Please see Figure 12, GWC Element Manager Network Panel, that follows.

To configure the Location Recipient press the change button. This opens to 'Change Add Location Recipient' window. Please refer to "Change Location Recipient window" on page 888.

Figure 12 GWC Element Manager Network Panel

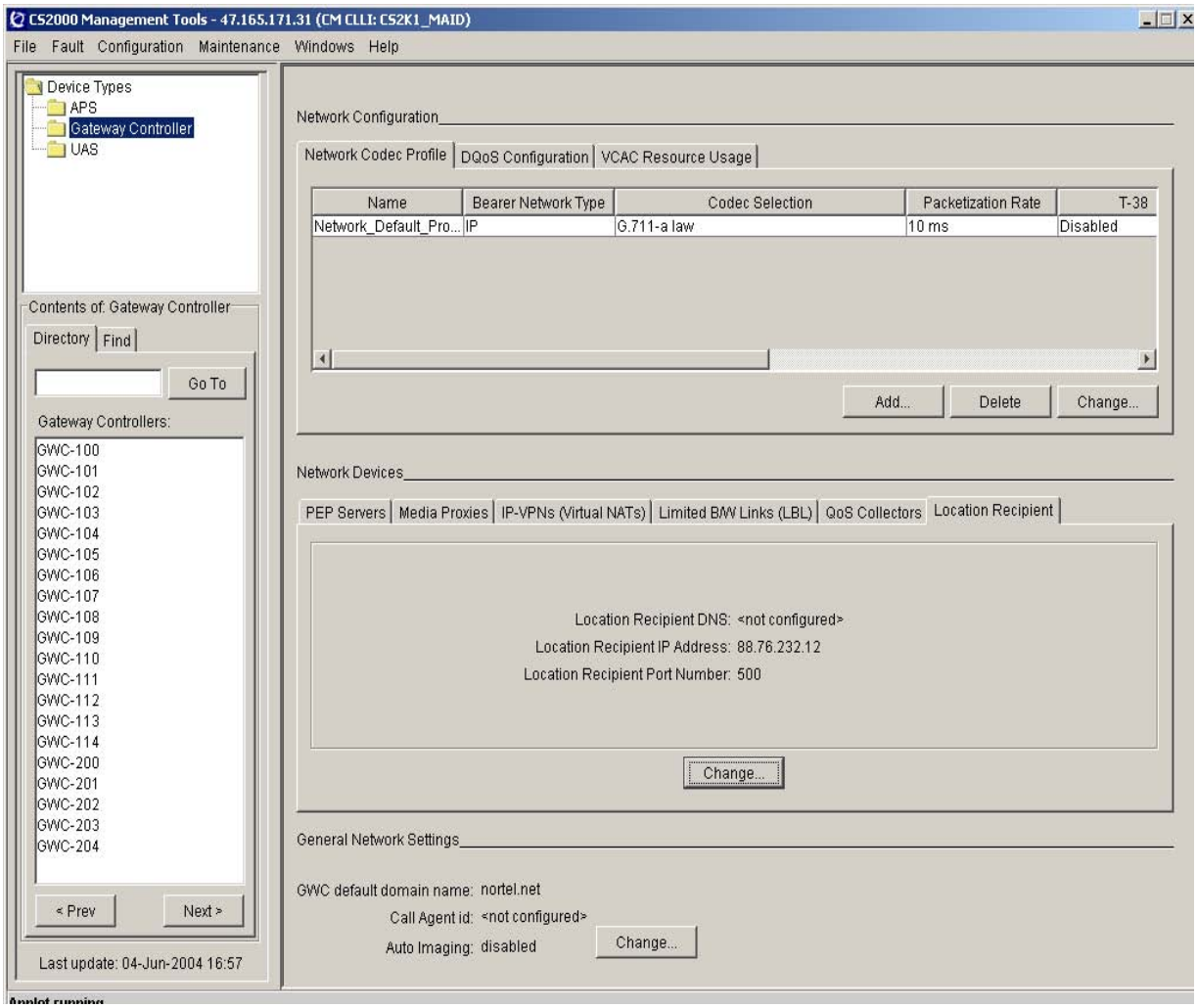
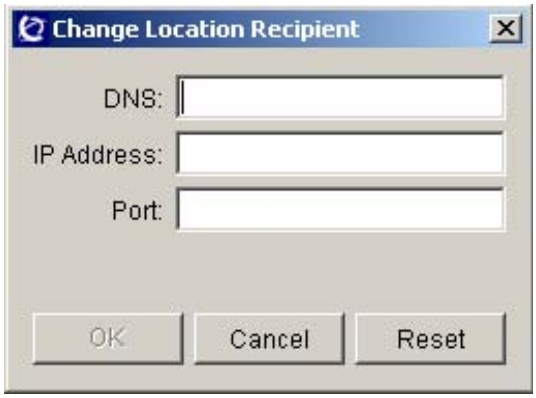


Figure 13 Change Location Recipient window



Each field has a Change Location Recipient window has *tip-text*.

The format of the DNS is any valid DNS character string that does not contain spaces. The format of the IP Address is <0-255>.<0-255>.<0-255>.<0-255>. The format of the port is any number in the range 0 to 65535, the Change Location Recipient window will only allow the user to enter data is the correct format.

Once the data has been entered the OK button is pressed to submit the data.

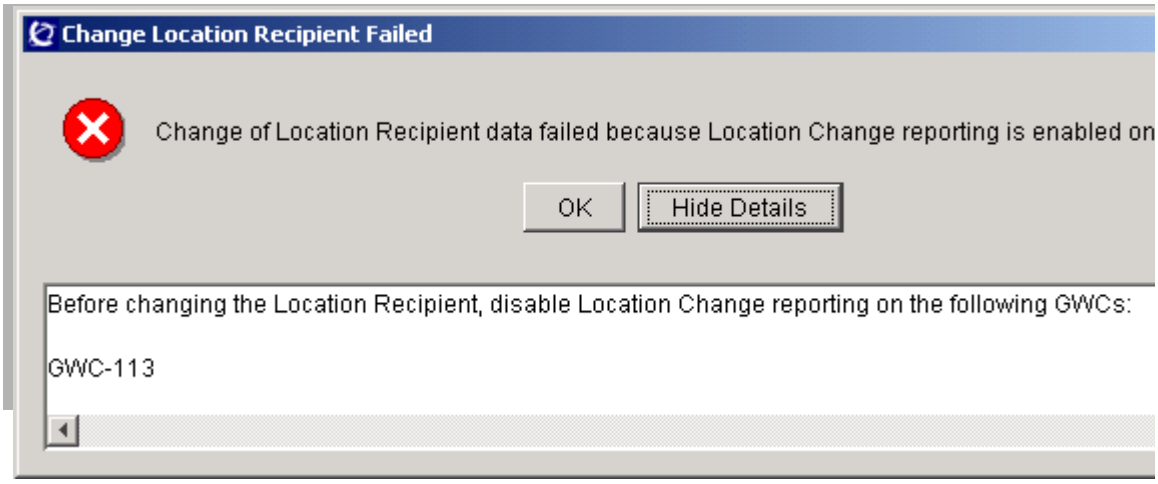
An error dialog is displayed if an incorrect value is entered in any of the fields. To allow either, or both, the DNS and IP Address to be configured, *blank* is considered a valid entry.

The following configuration combinations are acceptable:

- DNS, IP Address and Port Number – the GWC will use the DNS in preference to the IP Address. If the DNS look-up is not successful the connection will be attempted with the IP Address.
- DNS and Port Number – the IP Address takes the value <not configured>
- IP Address and Port Number – the DNS takes the value <not configured>

The Location Recipient values cannot be changed if the Location Recipient is associated with a GWC. Figure 14 Change Location Recipient failure window gives an example of the error message.

Figure 14 Change Location Recipient failure window



To unconfigure the Location Recipient the change button is pressed, then in the Change Location Recipient window the reset button is used to enter the default values, e.g. <not configured>, and OK is pressed to submit the data.

2 Activating the Location Change reporting on the GWC

The Location Change reporting from a GWC to the Location Recipient is activated via a checkbox in the GWC controller-provisioning panel. Please refer to Figure 15 GWC Controller provisioning panel.

The checkbox is only available for 'large line gateway' GWC profiles.

The checkbox cannot be checked if a Location Recipient has not been configured. Please refer to Figure 16 Location Change reporting checkbox error for an example of the error message.

When the checkbox is check the GWC Element Manager sends the Location Recipient configuration values to the GWC via SNMP. A 'status' parameter is also sent to the GWC, this has the value 'enabled'.

When the checkbox is unchecked the GWC Element Manager sends the 'status' parameter to the GWC, this has the value 'disabled'.

If the GWC is performing 'Device Recovery' Location Recipient configuration can not be transferred to the GWC via SNMP. Figure 17 GWC Device Recovery error shows the error dialog that will be displayed.

Figure 15 GWC Controller provisioning panel

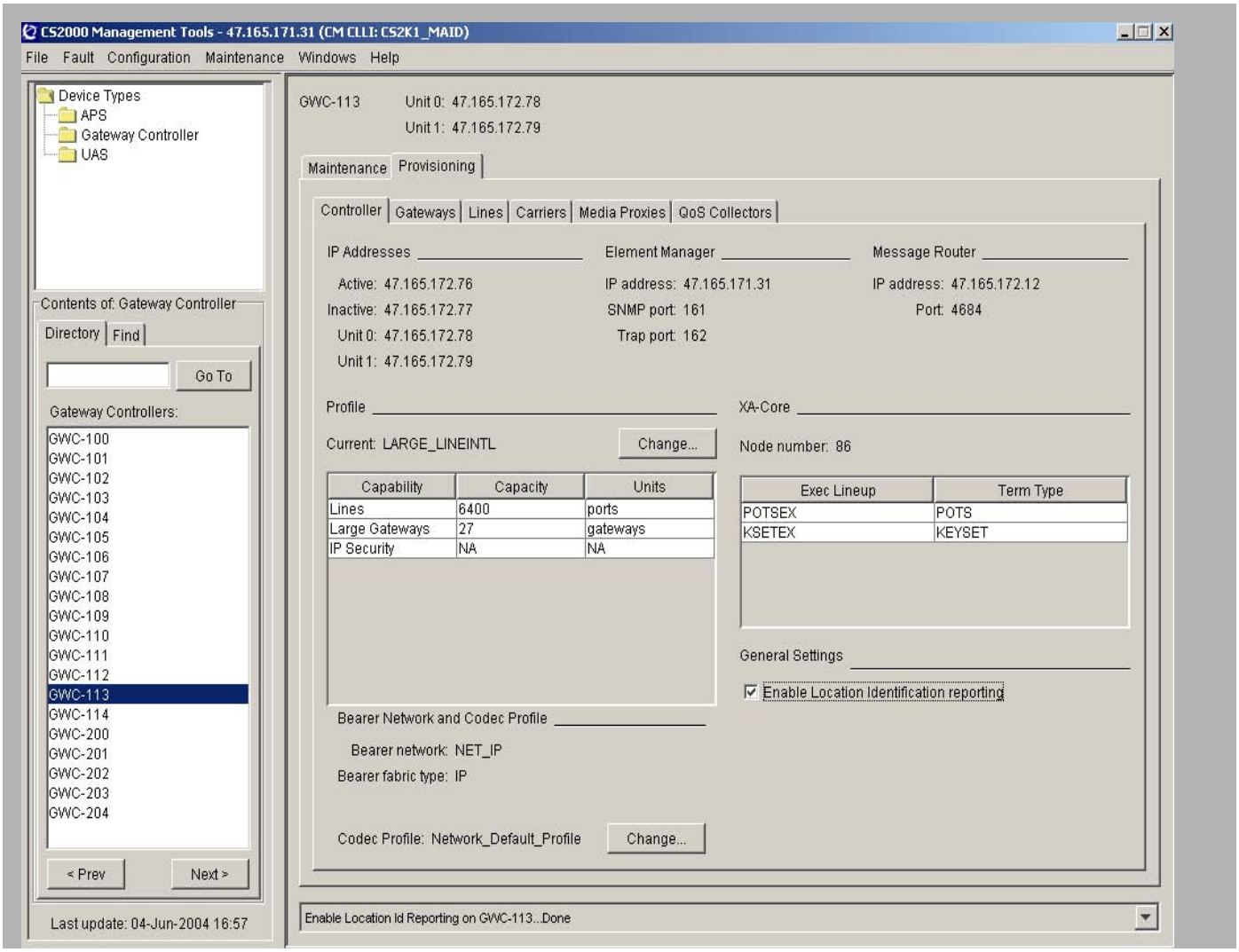


Figure 16 Location Change reporting checkbox error

Figure 17 GWC Device Recovery error

88.2.1.5 GWC Location Identification reporting application operation

This section describes the operation of the Location Identification reporting application on the GWC. The application is responsible for:

- Interfacing with the H.248 application, this includes:
  a. Notification on receiving a H.248 terminal location package location change event for a termination.
  b. Sending an audit request on the H.248 location identification package for a termination.
  c. Notification on receiving a H.248 location identification package audit.
- Queuing Location Identification information to be sent to the Location Recipient.
- Recovery and auditing of Location Identification information.
- Establishing and maintaining the TCP/IP connection to the Location Recipient.

The Location Identification reporting is enabled for a GWC in the GWC Element Manager, please refer to section 1.2.1.4.4 GWC Element Manager.

The GWC Element Manager enables Location Identification reporting on the GWC via SNMP.

When the Location Identification reporting application is enabled it does the following:

- Initialises the queue, recovery and audit mechanisms
- Establishes a TCP/IP connect to the configured Location Recipient

Once the Location Identification reporting application has been initialised it can:

- Accept notifications from the H.248 application
- Send audit requests to H.248 application
- Accept XML from the Location Recipient TCP/IP connection
- Send XML structures to the Location Recipient TCP/IP connection

The operation of the GWC Location Identification reporting application for an initial user login is described in section 1.2.1.2 Operation overview.

If the TCP/IP connect cannot be established to the Location Recipient the Location Identification reporting application queues the Location Identification information to be sent. Once the connection is established the queued Location Identification information is processed and sent to t he Location Recipient.

If the queue overflows, the recovery indicator is set for the termination. The Location Identification reporting application regularly audits the recovery indicators for all terminations. If the audit detects a set recovery indicator for a termination it initiates an audit of the H.248 Location Identification package for the termination.

While the TCP/IP connection is not established the Location Identification reporting applications does not use the Location identification information audit/recovery procedures.

The GWC Location Identification reporting applications operates until instructed to stop by the GWC Element Manager.

88.2.1.6 CICM Middle-box Id reporting operation Internet Transparency and VCAC

This activity has changed the way that middleboxes are configured in the CICM EM and introduced a new method to allow the CICM terminal to report the middlebox name/id.

Internet transparency (ITA) was originally introduced in SN06; The Internet Transparency Application Agent is required by telephone service providers with customers that are either using low bandwidth links or protecting their networks with uncontrolled NA(P)Ts. Prior to SN06, the CS2000 GWC did not have the ability to handle calls involving media gateways behind NA(P)Ts. These NA(P)Ts separate two networks with different IP address space - such as a private enterprise network and common address realm. The ITA introduces the ability to dynamically allocate NA(P)T binds through the use of a Media Proxy, so endpoints behind NA(P)T boxes remain reachable on a per-call basis.

In SN06.2 ITA was extended to CICM gateways, however because the CICM it is more of a signalling proxy rather than a media gateway, it does not require

an association with any single middlebox; it can support terminals from behind a number of middleboxes. Therefore a means to associate terminals with middleboxes was introduced. This was achieved by using Network Profiles; a middlebox id can be specified for an Enterprise, range of IP addresses, in the CICM Element Manager (EM). When a user logs into a CICM telephony client from within Enterprise, the middlebox id is reported to the GWC in Megaco/H.248 messaging. The GWC ITA agent then uses the middlebox id to determine whether a media portal should be introduced.

In SN07 due to this activity the provisioning of the Network Profile middlebox id has been changed. The middlebox name or id can be obtained by the CICM telephony client from DHCP and provided to the CICM gateway on registration. If the middlebox name or id is not provided by the CICM telephony client the middlebox id in the network profile is used.

The provisioning of the Network Profiles has been modified. The user can now download a list of IP-VPNs (virtual NATs) from the GWC EM, and associate one of the downloaded 'Auto-Discovery Networks' as the 'Network Location' for the Network Profile. Alternatively, the user can manually associate a 'Limited Bandwidth Link', configured in the GWC EM, using its Global Id, obtained from the GWC EM.

The middlebox name provisioned in DHCP and reported by the CICM telephony client must match one of the 'Auto-Discovery Networks' downloaded from the GWC EM so that the 'unique global id' can be determined and reported to the GWC.

If the middlebox name provisioned in DHCP and reported by the CICM telephony client does not match one of the 'Auto-Discovery Networks' downloaded from the GWC EM, the middlebox is taken from the appropriate Network Profile, and it's 'unique global id' is be determined and reported to the GWC.

The middlebox id can be provisioned in DHCP; it must be in the format #<number>, e.g. #12345. The # indicates that this is a middlebox id rather than middlebox name. The middlebox id does not have to match one of the 'Auto-Discovery Networks' downloaded from the GWC EM. The middlebox id is reported to the GWC.

The following diagrams show several CICM telephony clients registering with a CICM gateway and the expected operation.

88.2.2 Hardware requirements

None.

88.2.3 Software Requirements or Dependencies

SESM must be at release 7.

GWC must be at release 7.

CICM must be at release 7.

CICM EM must be at release 7.

CICM soft client must be at release 7.

Minimum phase 2 i200x firmware release is Phase2_rel_3_43 (0604D43).

88.2.4 Limitations and restrictions

Phase 1 i200x firmware does not support the new UNID extension to the Nortel-i2004-A DHCP option therefore the middlebox id reported for the terminal will also be taken from the Network Profile.

Phase 1 i200x firmware does not support the new Nortel-Geo-Civil-A and Nortel-Geo-Spatial -A DHCP options therefore the civil and spatial locations reported for the terminal will also be taken from the Network Profile (if Default Location Information configured) or the Network Location (if Default Location Information configured).

A Default Location can not be configured for a ‘Manually Defined LBL’. Default Locations can only be configured for Network Profiles and Auto-Discovered Network Locations.

It is possible that the Call Agent Id (CAID) on the GWC EM is changed; this will result in all the global middlebox id’s of NATs and LBLs being changed. If the CAID is changed then the NATs must be auto-discovered again in the CICM EM and applied to the CICMs, and any ‘Manually Defined LBLs’ configured against Network Profiles must be changed, and the Network Profiles applied to the CICMs.

88.2.5 Interactions

None.

88.2.6 Logs (LG)

None.

88.2.7 Data schema (DS)

Table 5 MIB entries

MIB name (registry key etc)	**MIB version** (from/to)	**New, Modified, Deleted**	**Description** (including backwards compatibility)
gwcLocationChangeReportingMIB	1	New	See Appendix B: GWC-LOCATION-CHANGE-REPORTING-MIB

88.2.8 Operating system parameters (OP)

None.

88.2.9 Alarms (AL)

Table 6 alarm signals

Alarm condition	Alarm signal	NEW/CHANGED/ DELETED/ RELOCATED
Unable to esatablish a connection to Location Recipient.	GWC 314	NEW

Example:

```
CS2K1 *** GWC314 JUN30 11:02:37 0586 TBL GWC Fault

Location: GWC-213-UNIT-0

NotificationID: 3

State: Raise

Category: Processing Error

Cause: Communications subsystem failure

Time: Jun 30 11:09:58 2004

Component Id: GWC=GWC-213-UNIT-0;Version=GI070BO;Unit=unit_0;Software=LocIdRep

Specific Problem: Location Id Reporting connection <88.53.45.223> has failed -
attempting recover

Description: Location Id Reporting connection failure
```

88.2.10 Software optionality control (SOC)

None.

88.2.11 Table Licensing

None.

88.2.12 Glossary

Term	Description
CICM	Centrex IP Client Manager
CLI	Calling Line Idenifier
CS2K	Call Server 2000
DHCP	Dynamic Host Configuration Protocol
EADM	Emergency Application & Data Manager
ECS	Emergency Call Services
FN	Functional Description
GEOPRIV	Geographic Location/Privacy
GWC	Gateway Controller
IEFT	Internet Engineering Task Force
IP	Internet Protocol
IT	Internet Terminal
LIS	Location Information Server

NAT	Network Address Translator
NI	Network Intelligence
MAC	Media Access Control
Megaco/H.248	Media Gateway Control
RAS	Remote Access Services
SN07	Succession software release 7
TDM	Time Division Multiplexing
UNID	Unique Network Identifier
Unistim	Unified Networks IP Stimulus Protocol
VoIP	Voice over IP
VPN	Virtual Private Network

88.2.13 References

1. draft-ietf-geopriv-dhcp-lci-option-03.txt, June 8, 2004 - http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-civil-00.txt
2. draft-ietf-geopriv-dhcp-civil-02.txt, March 20, 2004 - http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-civil-02.txt
3. Enterprise Emergency Call Service Architecture Specification - http://livelink-ott.ca.nortel.com/livelink/livelink.exe/5146119/E911_Architecture_Spec.doc?func=doc.Fetch&nodeid=5146119

88.2.14 Appendices

88.2.14.1 Appendix A: H.248 Location Identification package description

88.2.14.1.1 H.248.x Location Identification Reporting Package

88.2.14.1.2 Summary

This document defines a package that provides Termination Location Identification reporting for H.248.

88.2.14.1.3 Scope

This document defines a package that provides Termination Location Identification reporting for H.248. The support of this package is optional.

88.2.14.1.4 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

ITU-T Recommendation H.248.1 (05/2002), Gateway Control Protocol

- Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information
- Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses

88.2.14.1.5 Definitions -

88.2.14.1.6 Abbreviations

- MG Media Gateway
- MGC Media Gateway Controller

88.2.14.1.7 Location Identification reporting Package

PackageID: locId
Version: 1
Extends: tl

This package defines Termination Location Identification reporting for IP Terminals.

1 Properties

1a Unique Network Id
PropertyID: locid (0x0001)
Description: Reports the Unique Network Id (middle-box id) of an IP Terminal for location identification purposes. This is the unique global id assigned to a middle-box when it is configured in 'CS2000 Management Tools'.

Type: String
Possible Values: Any value of meaning between the MG and MGC. Default value is an empty String.
Defined In: Termination State Descriptor
Characteristics: Read only.

1b Public IP Address
PropertyID: pubAddr (0x0002)
Description: Reports the public IP address of an IP Terminal for location identification purposes.

Type: Octet String
Possible Values: Default value is an empty String. If the civil location (loc) or geospatial location (gloc) properties are present then this property must contain a non-default value.

Defined In: Termination State Descriptor
Characteristics: Read only

1c Private IP Address
PropertyID: privAddr (0x0003)
Description: Reports the private IP address of an IP Terminal for location identification purposes.

Type: Octet String
Possible Values: Default value is an empty String. If the civil location (loc) or geospatial location (gloc) properties are present then this property must contain a non-default value.
Defined In: Termination State Descriptor
Characteristics: Read only

1d MAC Address
PropertyID: macAddr (0x0004)
Description: Reports the MAC address of an IP Terminal for location identification purposes.

Type: Octet String.
Possible Values: MAC address encoded in hex. Default value is an empty String. If the civil location (loc) or geospatial location (gloc) properties are present then this property must contain a non-default value.
Defined In: Termination State Descriptor
Characteristics: Read only

1e Source of Geospatial Location information
PropertyID: glocsrc (0x0005)

Description: Identifies whether the network or the user provided the geospatial civil location information.

Type: Enumeration

Possible Values: Not Applicable (0x0001), Network (0x0002), User (0x0003). Default value is 0x0001. If the geospatial location (gloc) property is present then this property must contain a non-default value.

Defined In: Termination State Descriptor

Characteristics: Read only

1f Geospatial Location

PropertyID: gloc (0x0006)

Description: Reports the geospatial location of an IP Terminal.

Type: Octet String

Possible Values: Format specified in the IETF GEOPRIV working group geospatial location Internet draft (defined above). Default value is an empty String.

Defined In: Termination State Descriptor

Characteristics: Read only

1g Source of Civil Location information
PropertyID: locsrc (0x0007)

Description: Identifies whether the network or the user provided the civil location information.

Type: Enumeration

Possible Values: Not Applicable (0x0001), Network (0x0002), User (0x0003). Default value is 0x0001. If the civil location (loc) property is present then this property must contain a non-default value.

Defined In: Termination State Descriptor

Characteristics: Read only

1h Civil Location
PropertyID: loc (0x0008)

Description: Reports the civil location of an IP Terminal.

Type: String

Possible Values: Format specified in the IETF GEOPRIV working group civil location Internet draft (defined above). Default value is an empty String.

Defined In: Termination State Descriptor

Characteristics: Read only

2 Events

None.

88.2.14.1.8 Signals
None.

88.2.14.1.9 Statistics
None

88.2.14.1.10 Procedures
These are the procedures!

88.2.14.2 Appendix B: GWC-LOCATION-CHANGE-REPORTING-MIB

```
-- DMS Call Server GateWay Controller Location Change Reporting MIB

GWC-LOCATION-CHANGE-REPORTING-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress
            FROM SNMPv2-SMI
        DisplayString, RowStatus
            FROM SNMPv2-TC;



--
-- Define the location of this MIB within the MIB tree
--

nortel   OBJECT IDENTIFIER ::= { enterprises 562 }
voip     OBJECT IDENTIFIER ::= { nortel 28 }
ptn              OBJECT IDENTIFIER ::= { voip 0 }
serviceControl  OBJECT IDENTIFIER ::= { ptn 1 }
legacyCallServerOBJECT IDENTIFIER ::= { serviceControl 4 }
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }

--
-- Define the elements in the GWC Location Change Reporting MIB
--

gwcLocationChangeReportingMIB MODULE-IDENTITY
```

```
      LAST-UPDATED "200210090000Z"   -- October 9, 2003
      ORGANIZATION "Nortel DMS Call Server"
      CONTACT-INFO "David Johnson
                Nortel Networks Inc.
                Maidenhead Office Park, Westacott Way
               Maidenhead, BERKS, UK, SL6 3QH
                Phone: 01628 431218
                email: davidjoh@nortelnetworks.com"
      DESCRIPTION  "The MIB module defines information about
                the Location Change Reporting
                     data provisioning supported
               by the GateWay Controller (GWC)."

  ::= { lcsGateWayController 24 }

locationChangeReportingStatus OBJECT-TYPE
         SYNTAX        INTEGER{
                       disable (0),
                       enable  (1)
                     }
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
         "A boolean value indicating whether Location Change Reporting
          is enabled or disabled on a per GWC base. By default, Location
     Change Reporting is disabled."
        DEFVAL { 0 }
        ::= { gwcLocationChangeReportingMIB 1 }

locationChangeReportingPort OBJECT-TYPE
   SYNTAX Integer32(0..65535)
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
       "Location Change Reporting Location Recipient Port, the range
           is from 1024 to 65535."
   DEFVAL { 0 }
   ::= { gwcLocationChangeReportingMIB 2 }
```

```
locationChangeReportingIpAddress OBJECT-TYPE
   SYNTAX IpAddress
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
       "Location Change Reporting Location Recipient IpAddress."
   DEFVAL { '00000000'h }
   ::= { gwcLocationChangeReportingMIB 3 }

locationChangeReportingErrorMessage OBJECT-TYPE
   SYNTAX DisplayString (SIZE(1..128))
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
           "Error Message holds a descriptive error message
            in case of an snmp failure of the last operation."
   ::= { gwcLocationChangeReportingMIB 4 }

locationChangeReportingErrorType OBJECT-TYPE
    SYNTAX INTEGER { information    (0),
                     warning    (1),
                     error    (2) }
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
           "This value contains the type of error that occurred on
             the last SET failure on any variable in the gateWayTable.
             The combination of this type and the error message give
             the manager enough information to process the failure."
      ::= { gwcLocationChangeReportingMIB 5 }

END
```

88.2.14.3 Appendix C: Location Identification reporting XML schema

```
<!-- Nortel Networks Location Identification XML schema (file NNLocId.xsd)-->
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<xsd:element name='locid' type='locidtype'/>
```

```
<xsd:complexType name='locidtype'>
    <!-- moved below -->
    <xsd:choice>
        <xsd:element name='add'       type='infotype'/>
        <xsd:element name='change'    type='infotype'/>
        <xsd:element name='remove'    type='infotype'/>
        <xsd:element name='keepalive'/>
        <xsd:element name='sync'/>
        <xsd:element name='status'/>
    </xsd:choice>
     <xsd:attribute name='csid'        type='xsd:string'/>
    <xsd:attribute name='gwcid'       type='xsd:string'/>
</xsd:complexType>

<xsd:complexType name='infotype'>
   <xsd:sequence>
    <xsd:element  name='terminal' type='termtype'/>
   </xsd:sequence>
</xsd:complexType>

<xsd:complexType name='termtype'>
    <!-- Moved below -->
    <xsd:sequence>
        <xsd:element name='unid' type='xsd:integer' minOccurs="0"/>
        <xsd:group   ref='addressinfo'/>
        <xsd:group   ref='geoinfo' minOccurs="0"/>
        <xsd:group   ref='civilinfo' minOccurs="0"/>
    </xsd:sequence>
   <xsd:attribute name='node'  type='xsd:string' use='required'/>
    <xsd:attribute name='term' type='xsd:string' use='required'/>
    <xsd:attribute name='gw' type='xsd:string' use='required'/>
    <xsd:attribute name='ep' type='xsd:string' use='required'/>
</xsd:complexType>

<xsd:group name='civilinfo'>
    <xsd:sequence>
        <xsd:element name='civilsrc' type='xsd:string'/>
```

```
        <xsd:element name='civil' type='xsd:string'/>
    </xsd:sequence>
</xsd:group>

<xsd:group name='geoinfo'>
    <xsd:sequence>
        <xsd:element name='geosrc' type='xsd:string'/>
        <xsd:element name='geo' type='xsd:string'/>
    </xsd:sequence>
</xsd:group>

<xsd:group name='addressinfo'>
    <xsd:sequence>
        <xsd:element name='pubip' type='xsd:string' minOccurs="0"/>
        <xsd:element name='privip' type='xsd:string' minOccurs="0"/>
        <xsd:element name='mac' type='xsd:string' minOccurs="0"/>
    </xsd:sequence>
</xsd:group>

</xsd:schema>
```

89: Functional Description (FN) A00003571

89.1 Feature name

MG9000 Cards Support A00003571 (ITP, ITX, ABI, SCO)

89.2 Description

This activity supports the release of the following PECCODEs for ITP, ITX, ABI and SCO cards in the MG9000EM:

- Internet Telephony Processor (ITP): NTNY30CA (IP & AAL1 modes)
- Internet Telephony Extender (ITX): NTNY41BA
- Super Core OC3 (SCO): NTNY45CA
- Access Bridging Interface (ABI): NTNY43BA (IP & AAL1 modes)

The user interface for the ITP, ITX, SCO and ABI are not impacted by this feature.

The new VMG of type ABI-IP is added to the VMG provisioning creation. The areas for ‘Silence Suppression (VoIP)’ and ‘QoS Threshold (VoIP Only)’ will be un-gray for this new VMG type (same configuration rules as the current ITP-IP VMG type).

A new field ‘Bearer Address’ will be added in the GW Config pannel. This field will be editable for ABI-IP Vmg type and it will be gray out for all other VMG types but it will display the same IP address use in the CIPOA Address field.

The ‘CIPOA Address’ label will be renamed ‘Signalling Address’.

The OVLD alarm and logs format are used to report the failures of the ‘Stream Control Transmission Protocol’ (SCTP) reported by the ABI.

The MG9000 is reporting SCTP Operational measurementes via a OM collector interface (please refer to A00003767 ‘IP ABI PPVM ROBUSTNESS & MSG LOSS’ for more infromation on OM fields an data collected).

89.3 Hardware Requirements or Dependencies

This activity supports the following new card releases:

— Internet Telephony Processor (ITP): NTNY30CA (IP & AAL1 modes)

— Internet Telephony Extender (ITX): NTNY41BA

— Super Core OC3 (SCO): NTNY45CA

— Access Bridging Interface (ABI): NTNY43BA (IP & AAL1 modes)

89.4 Software Requirements or Dependencies

This activity is released in SN07 MG9000 Element manager and has the correspondent SN07 MG9000 gateway release features:

— A00004109: CALLP CHANGES TO SUPPORT NEW ITP

— A00003767: IP ABI PPVM ROBUSTNESS & MSG LOSS

— A00003729: IP ABI CALLP AND CONNECTIONS

89.5 Limitations and restrictions

The new release of ITP and ABI cards are ONLY supported in the SN07 or higher release for MG9000EM and MG9000.

Due to the change of MIBs the fields in the ‘Silence Suppression (VoIP Only)’ area: Voice *Activity Detection Mode* and *Confort Noise Generator Mode,* for upgrades to SN07 the values VAD and CNG in the MG9000EM will be downloaded to the GW after the NE audit has completed. Before the audit is executed the GW will have the defaults values.

89.6 Interactions

None

89.7 Applicable customer facing sections

Fault Management	
Logs	___X__
Alarms	___X__
Configuration	
Data Schema	_____
User Interface	_____
Element Management	___X__
Security	_____
Service Order	_____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

89.8 Glossary

Term	Description
New term	Definition

90: Functional Description (FN) A00003576

90.1 Feature name

SN07: Trunk Security

90.2 Description

This feature enables the IP Security (IPSec) capability for the following GWC trunking profiles:

— TRUNKNA

— TRUNKINTL

The IPSec provisioning GUI is modified/enhanced as follows::

— in the “IPSec Profile” panel, the “SA renew thresh” field (which was previously expressed as a percentage of SA lifetime) is changed to “Grace Period (seconds)”.

— a “Comment” field is added to the “Connection Policy” panel. When a connection policy is added, the user can enter descriptive comments in the “Comment” field. These descriptive comments provide an extra level of detail or history regarding that specific connection policy.

— the option to enter the Kerberos service key in hexadecimal format, as well as the currently supported PEM format.

— showing (1) the Kerberos panel and (2) the "KERBEROS" option in the “IPSec Profile” panel “Key Negotiation” field, only if the Kerberos capability is included for that GWC profile.

The IPSec portion of the Gateway Controller on-line help panels are enabled.

90.3 Hardware Requirements or Dependencies

Not applicable.

90.4 Software Requirements or Dependencies

Not applicable.

90.5 Limitations and restrictions

Not applicable.

90.6 Interactions

Not applicable.

90.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

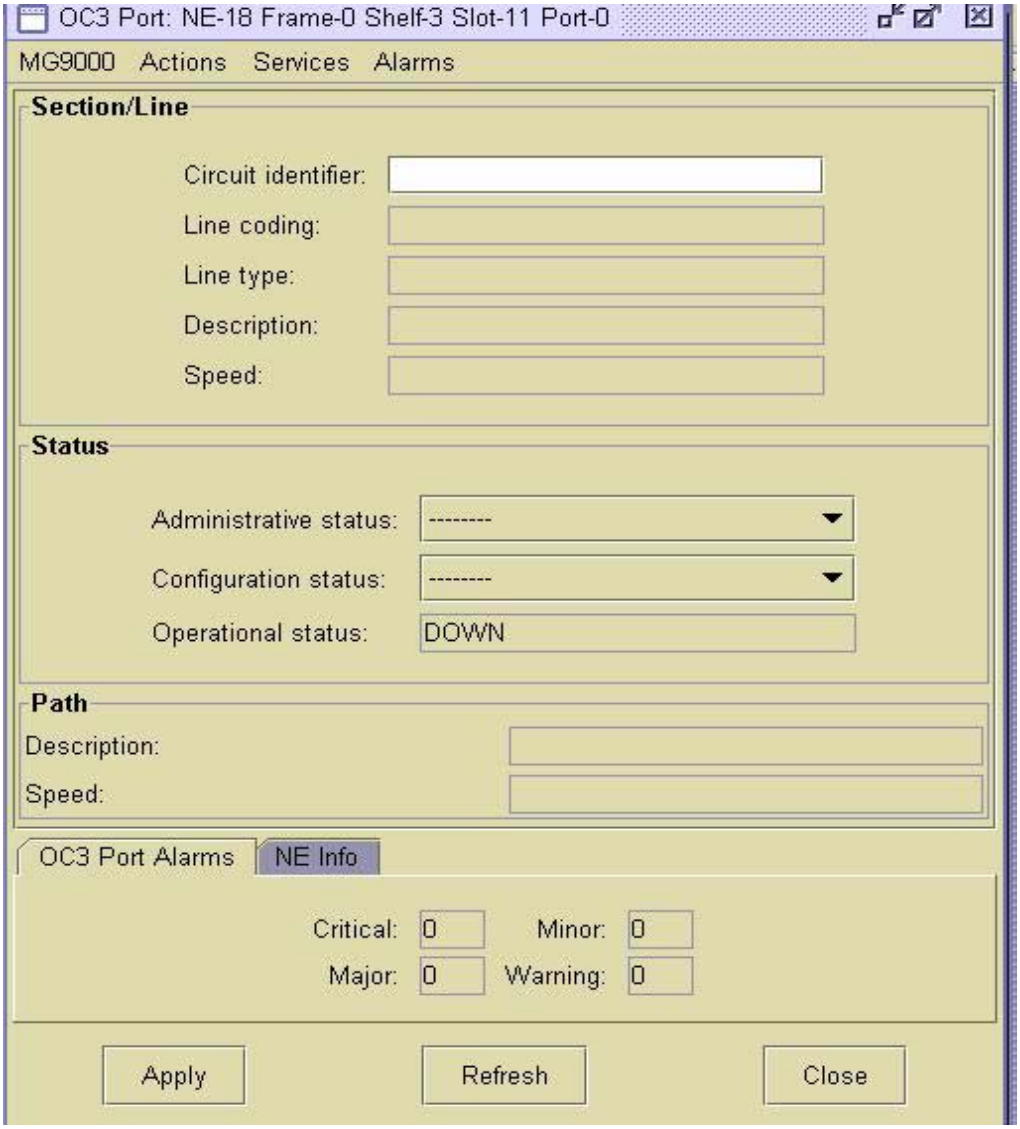
90.8 Glossary

Term	Description
GWC	Gateway Controller
IPSEC	IP Security
SA	Security Association
PEM	Base 64
SESM	Succession Element Sub-Element Manager
TRUNKINTL	International Trunk (*GWC profile*)
TRUNKNA	North American Trunk (*GWC profile*)

91: Functional Description (FN) A00003591

91.1 Feature name

ActId A00003591 MG9000 OC3 Channelization support from EM.



a. Refer to Actid A00003604 MG9000-OC3 Carrier OAM&P for channelized OC3 carrier.

91.2 Description

This feature enables the user to view and modify (only the administrative and configuration status can be modified) the channelized carrier(OC3) configuration . This document discusses the changes in EM for this feature from user perspective.

91.3 Hardware Requirements or Dependencies

No new requirements. This product runs on the same hardware as the existing MG9k Element Manager application.

91.4 Software Requirements or Dependencies

No new requirements. This activity is packaged with the existing MG9k EM software application.

This feature will be shipped as part of the SN07 stream for the MG9k EM.

91.5 Limitations and restrictions

None

91.6 Interactions

This feature introduces new screens and modifications to the existing GUI

91.6.1 Carrier configuration Display

The screen remains unchanged for concatenated sonet and SDH carrier. Figure 1 shows the carrier configuration details for the concatenated sonet carrier

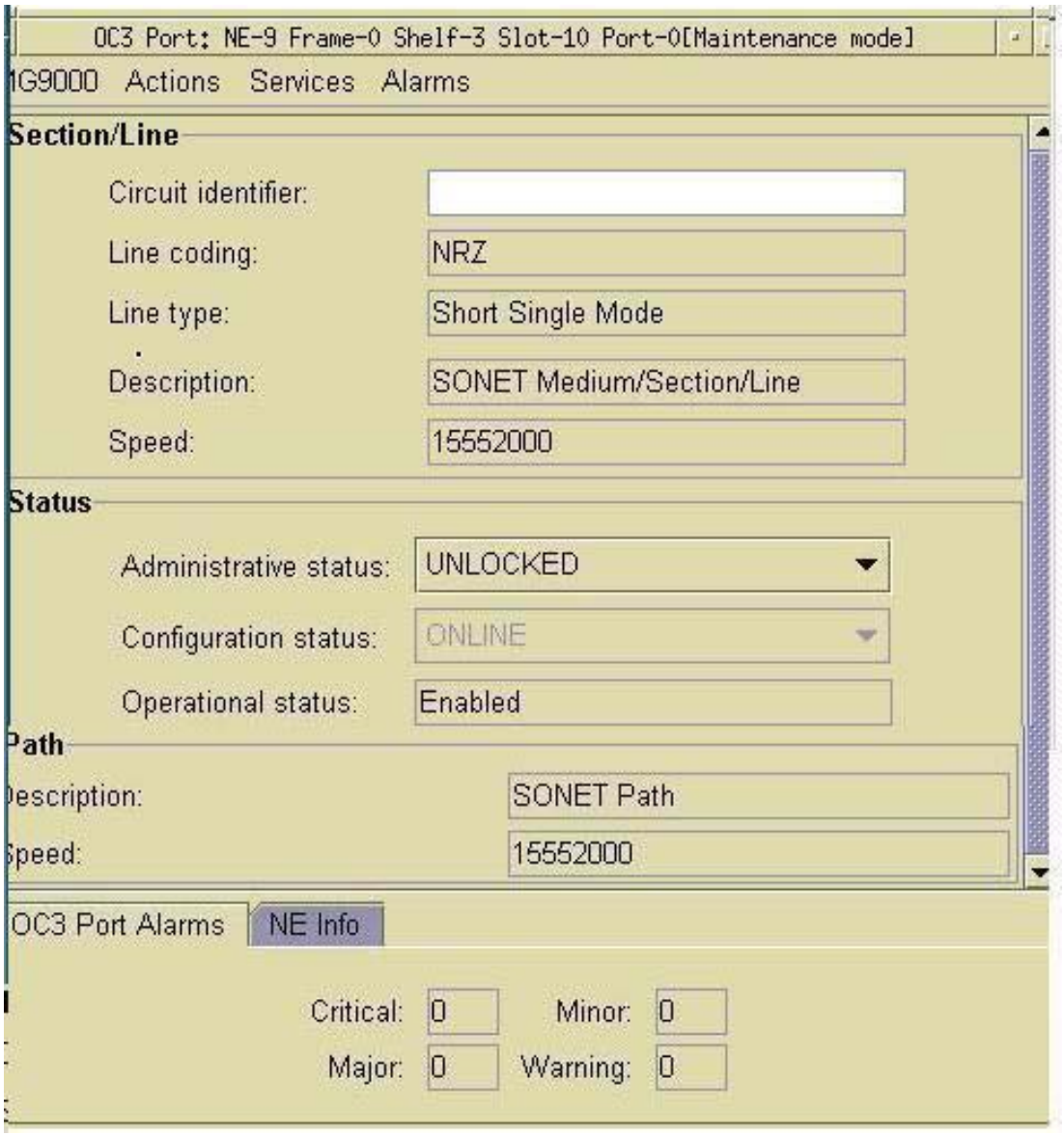


Figure 1 : OC3c Carrier details

If the carrier is in 'channelized mode', clicking on the OC3 Port icon in the OC3 card view will display the screen as shown in the figure 2. This new screen shows totally three icons for STS1 path details. By default OC3 section/ Line description/status is displayed in a tab as shown in figure 2. Double clicking on the STS1 path will display STS1 path information and its status as shown in the figure 3.The user will be able to lock/unlock and online/offline the OC3 section/Line and all the 3 STS1 paths individually.

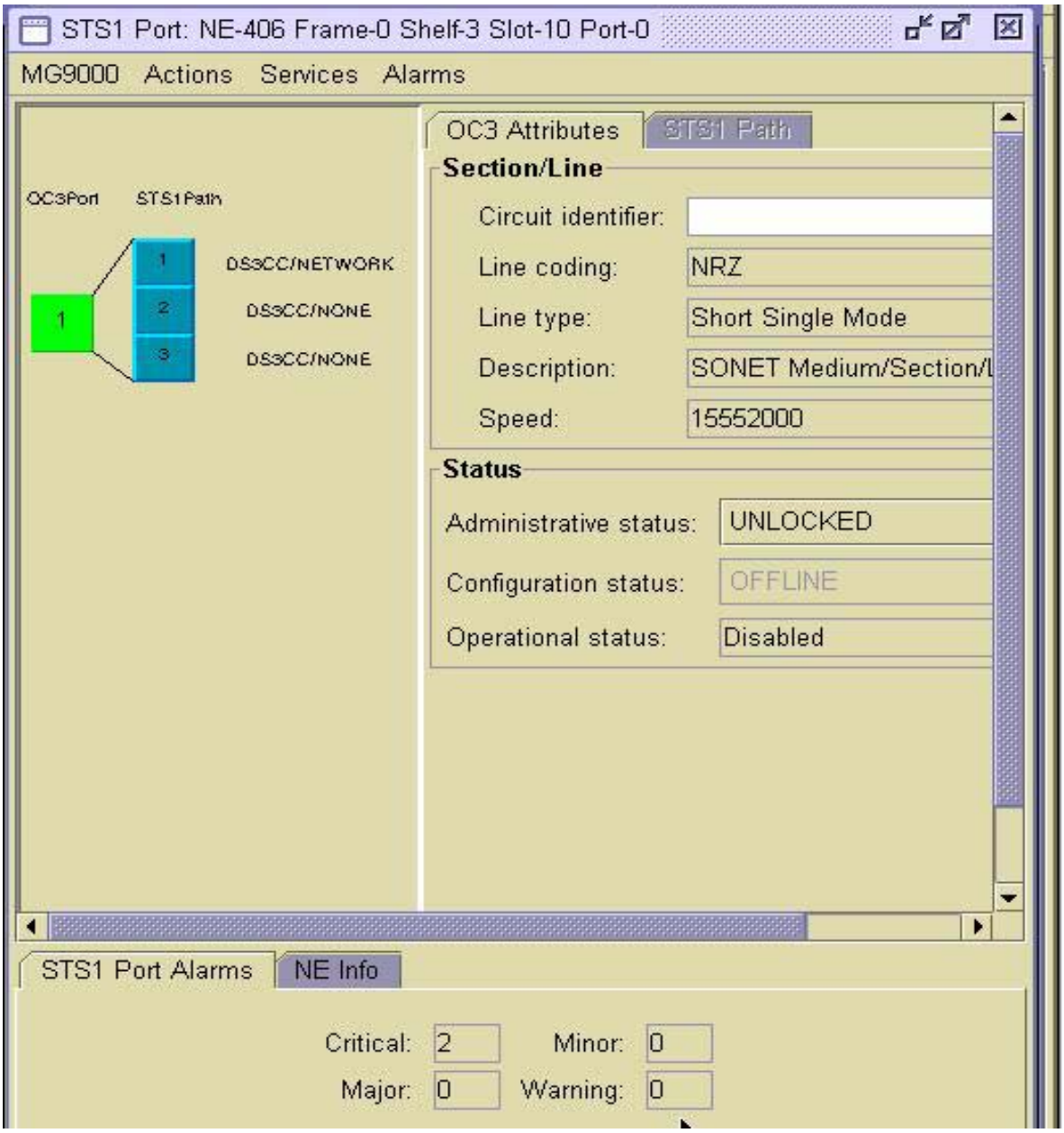


Figure 2 : Section/Line Configuration details for channelized carrier

The label next to the STS1 paths help the user to identify the network carrier and the payload on the paths. The payloads can be STS1, DS3CC and DS3PLCP. If the payload is DS3PLCP, f or network carrier the label would be DS3PLCP/NETWORK and for inactive carrier it would be DS3PLCP/NONE.

The OC3 Section/Line can be locked only after locking all the 3 STS1 paths.When the user tries to lock OC3Section/Line, a warning message “The Network Path should be locked before locking OC3 Section/Line. Are you sure the network path is locked?” will be popped up to the user. If the network path is not locked, the user can cancel OC3Section/Line lock request and lock the network path, then attempt locking OC3Section/Line

For unlocking Network Carrier, the OC3 Section/Line should be unlocked first. When the user tries to unlock the network path, a warning message ”The OC3Section/Line should be unlocked before unlocking the network path. Are you sure the OC3Section/Line is unlocked?” will be displayed to the user. If the OC3Section/Line is not unlocked, the user can cancel network path unlock request and unlock theOC3Section/Line, then attempt unlocking network path

A non-network carrier can not be unlocked.

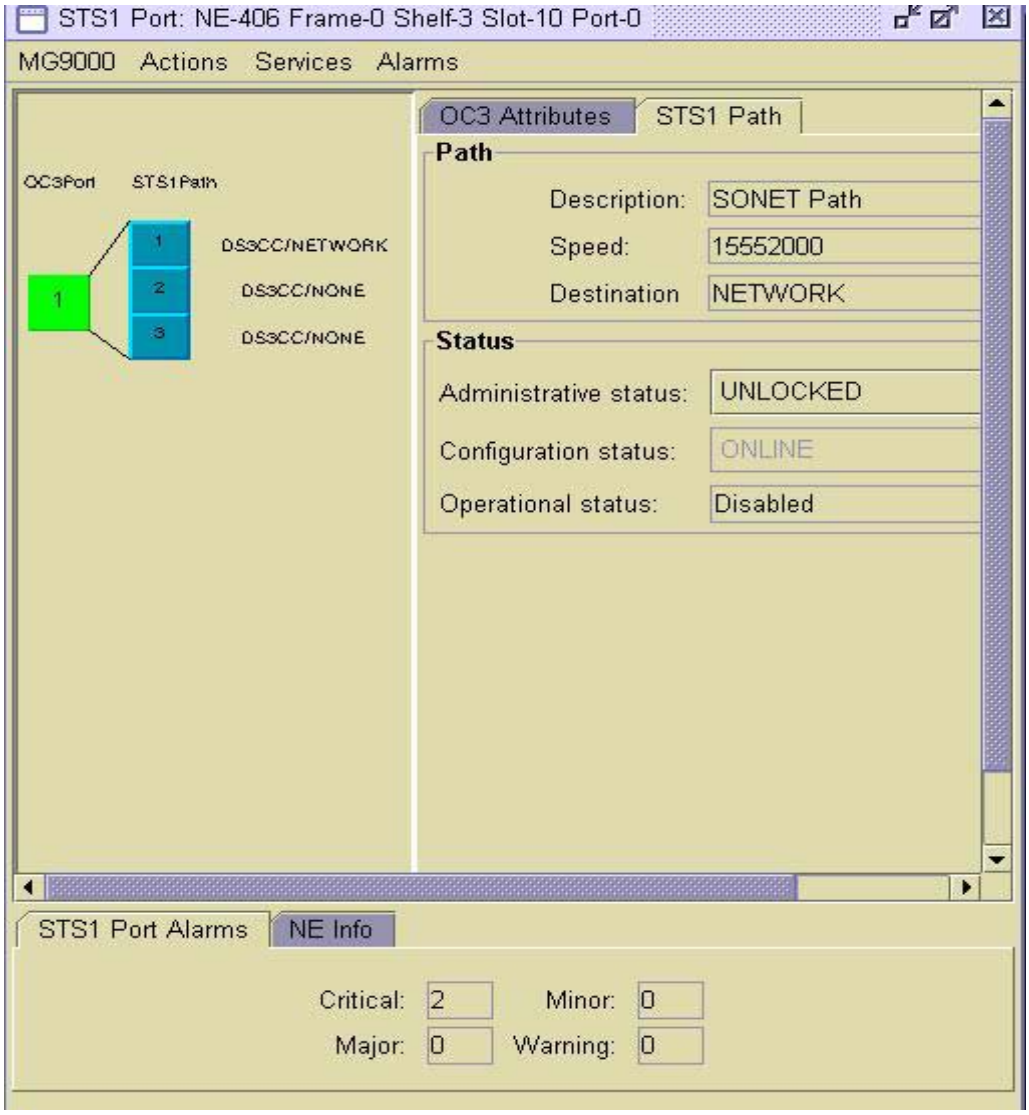


Figure 3 :STS1 path description and status

Figure 4 Default screen if the carrier is not provisioned.

91.6.2 Performance Parameters

If the carrier is configured in concatenated mode (Sonet or SDH), there is no change in the performance parameter screen.

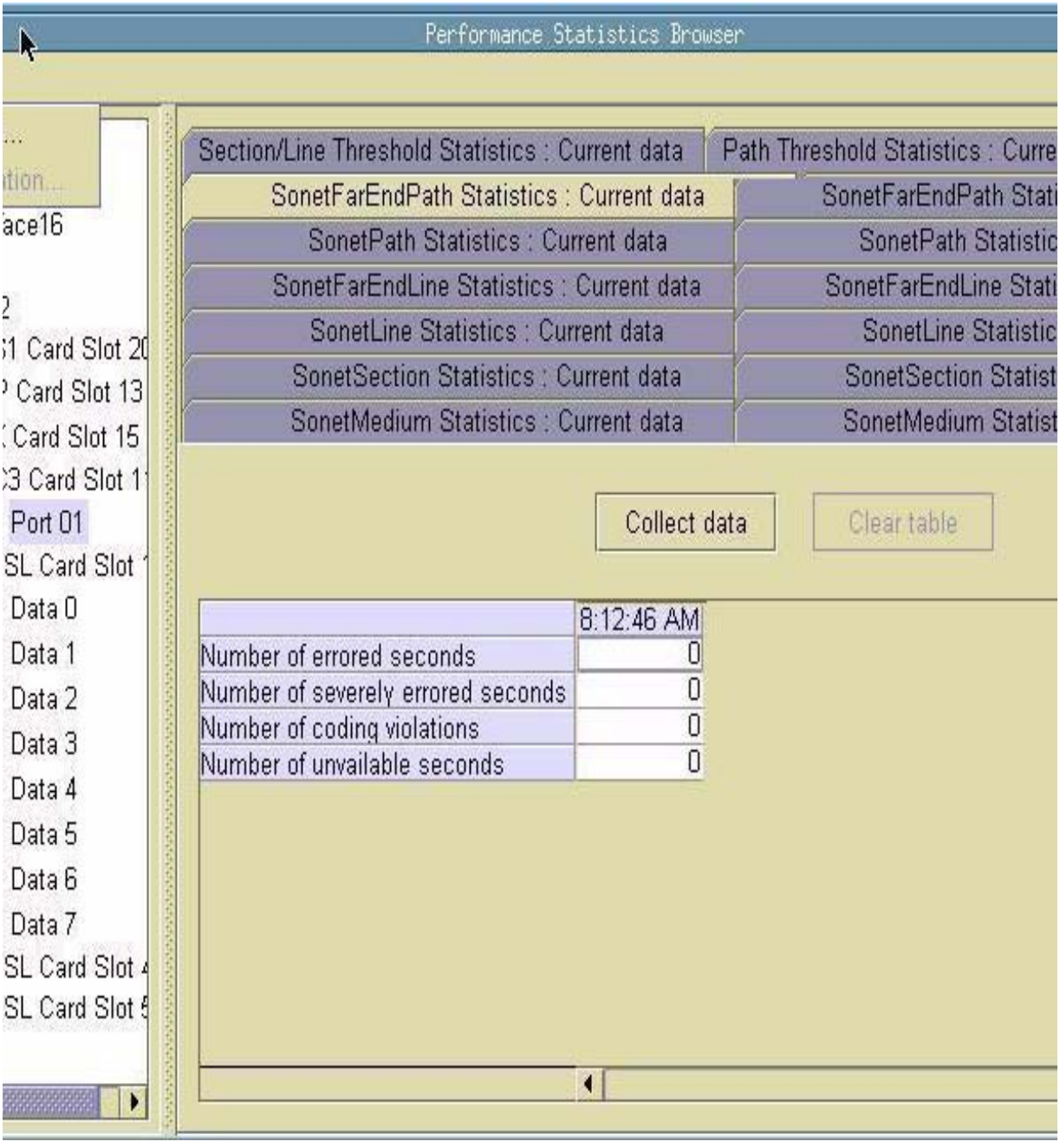


Figure 5: OC3 section/Line , STS3 path peformance parameters

If the carrier is in channelized mode, clicking on OC3 port will display OC3 section/Line information. Three STS1 subnodes will be displayed below Port for STS1 information. Clicking on each of STS1 will display its path performance details. DS3 path performance parameters will be displayed if DS3 is payload is supported on STS1.If the payload is STS1 the nodes label will be STS1-0x and if DS3 payload is selected on the STS1 path the nodes label will be STS1-DS3-0x.

The OC3 channelization feature supports new DS3 - Mibs. The DS3 statistics will be displayed in the performance browser only when the payload selected is DS3Clearchannel(DS3CC) or DS3PLCP for a channelized carrier

The new PMs are DS3Path(Current and history data) and DS3FarEndPath(Current and History data).

The DS3Path PM has the following data

"P - bit number of errored seconds,P - bit number of severely errored seconds,Severely errored seconds,Number of unavailable seconds,P - bit number of coding violations,C - bit number of coding violations, C - bit number of errored seconds,C - bit number of severely errored seconds " .

The DS3FarEndPath PM has

"Number of errored seconds,Number of severely errored seconds,Number of coding violations and Number of unvailable seconds".

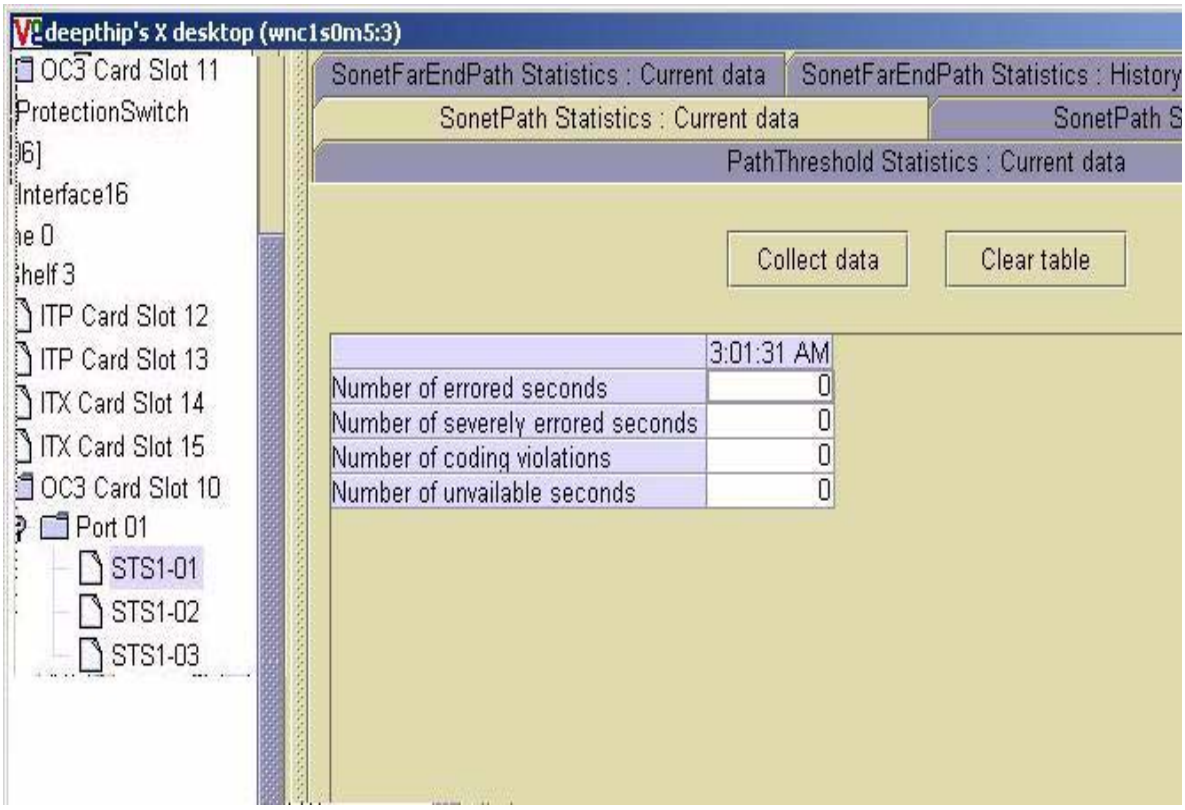


Figure 6 : STS1 Path performance parameters

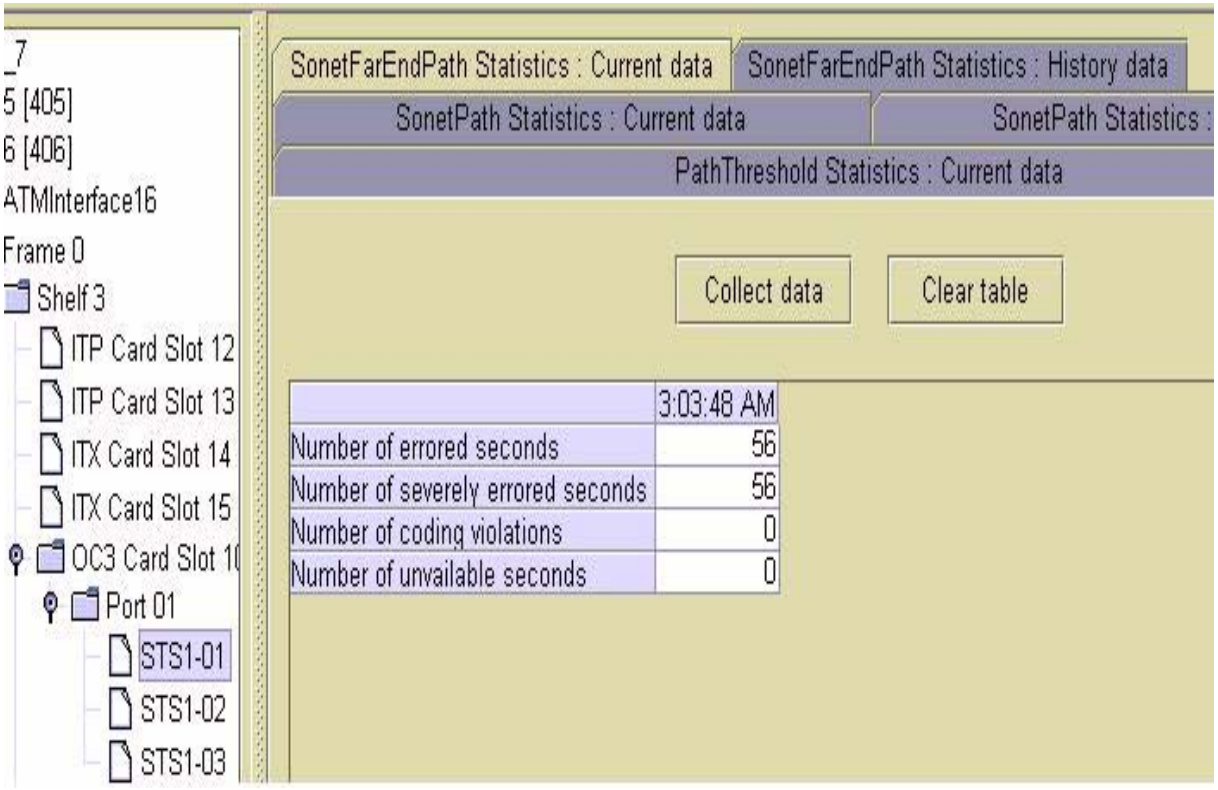


Figure 7. STS1FarEndPath Statistics

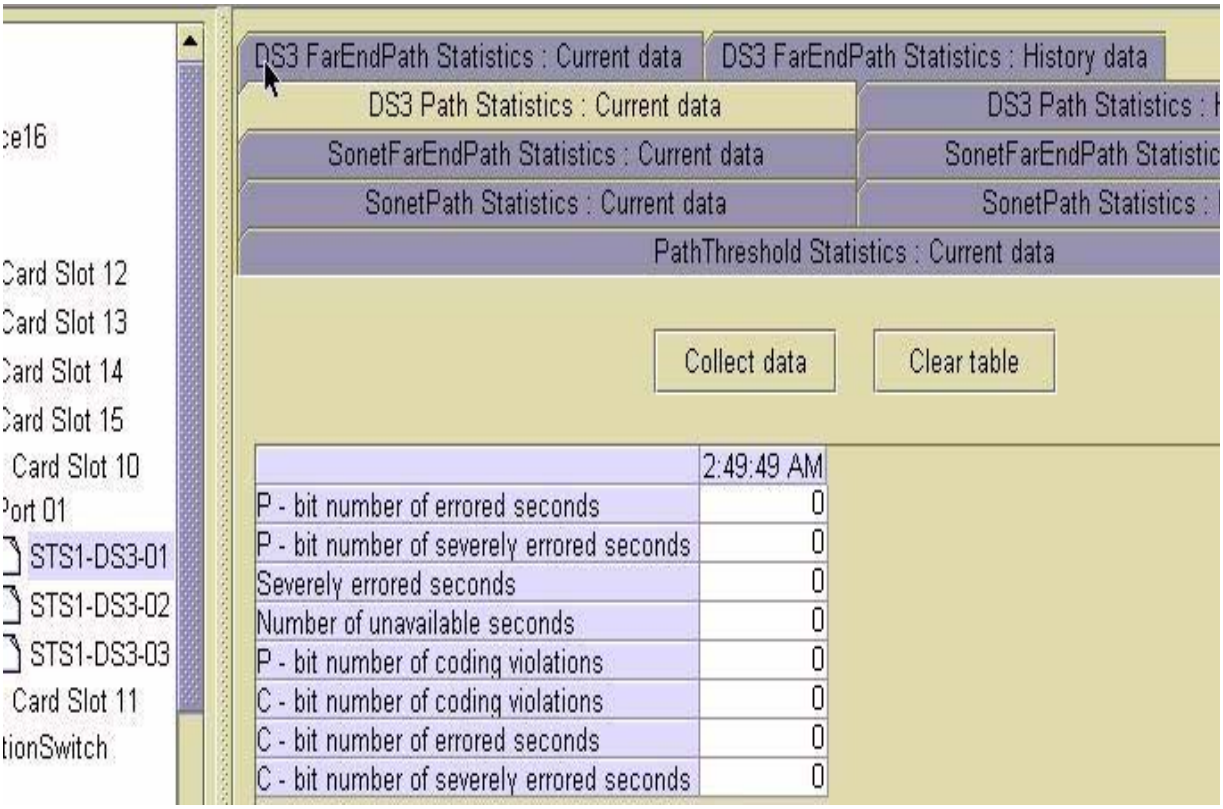


Figure 8: DS3 Path Performance parameters

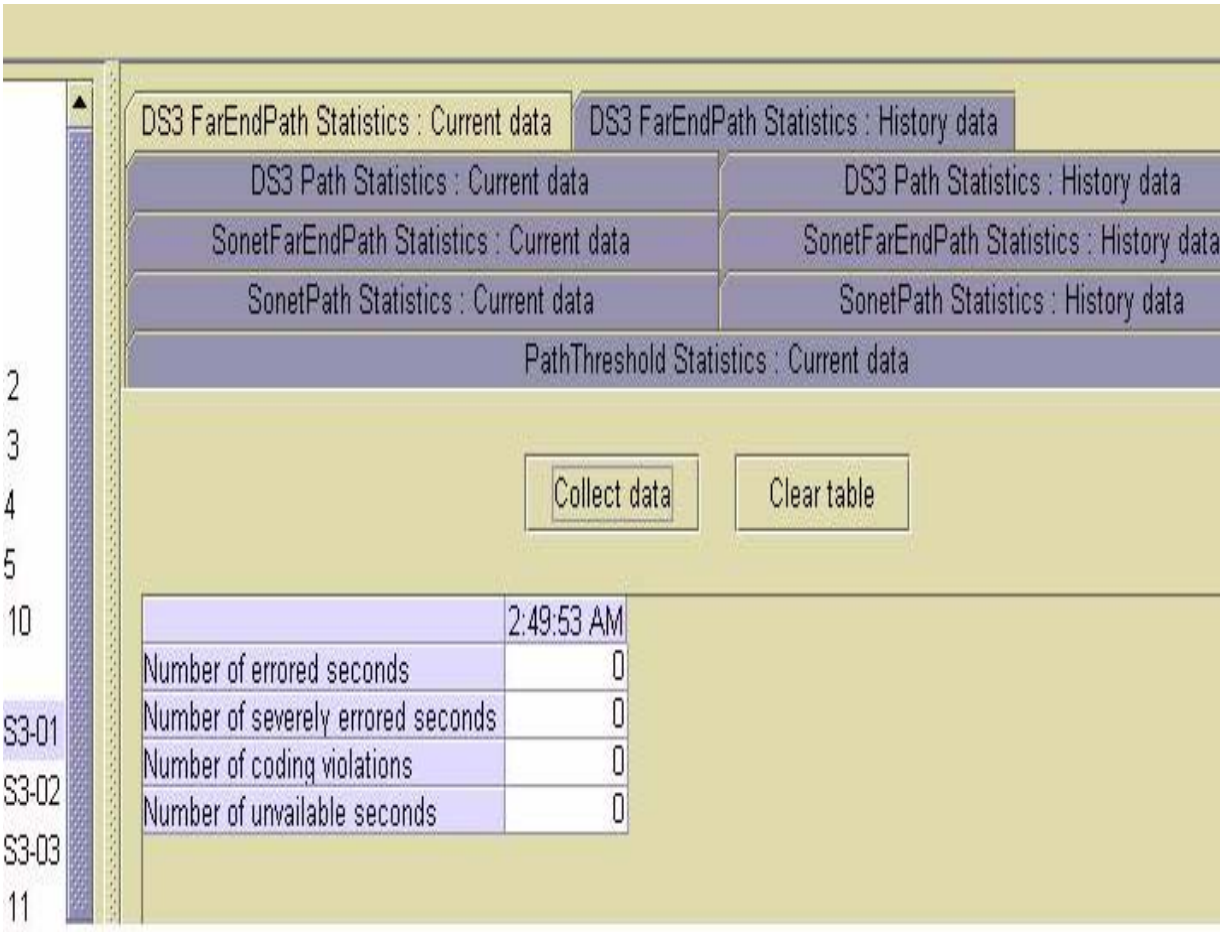


Figure 9: DS3 FarEndPath performance parameters

91.6.3 STS1 and DS3 alarms

From the user perspective, the alarm display will not change.The alarms will be raised for both STS1 path and DS3 payload.Now the STS1 path and DS3 alarms will be included in the OC3 port alarm count.The DS3 alarms to expect at EM will be LOF,RAI and AIS. The alarm description will let the user know whether the alarm belongs to DS3 or STS1.

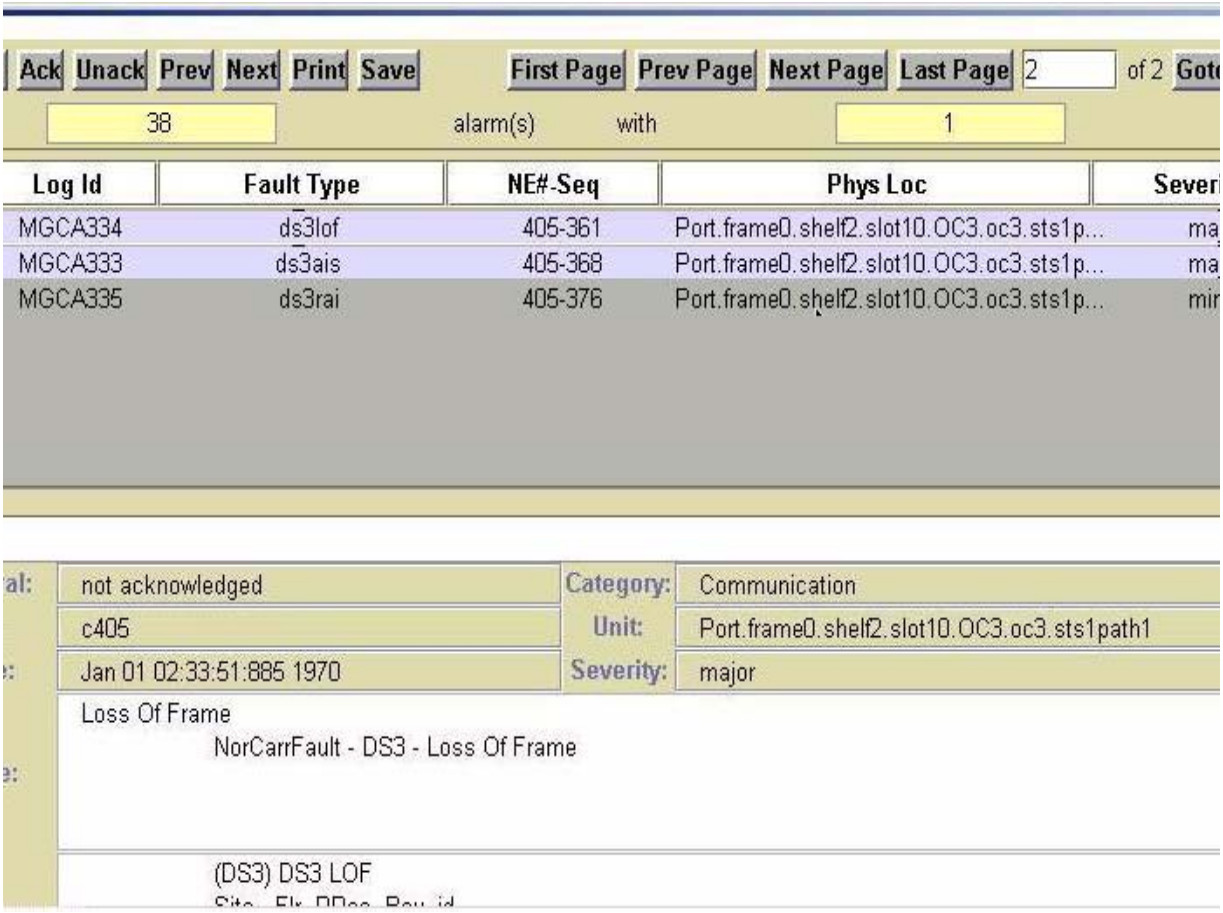


Figure 10: DS3 Alarm information

91.6.4 Upgrade and Downgrade

The user should not try downgrading the MG9K when the carrier is channelized The MG9K in SN07 has new hardware to support channelization, so SN06.2 and below load should not be used on this MG9k. If a SN06.2 MG9K has to be upgraded to SN07, it should have the new hardware.

91.7 Error scenarios

The SNMP set errors will be handled.

91.8 Glossary

STS1 Synchronous Transport Signal Level 1

STS3	Synchronous Transport Signal Level 3
EM	Element Manager
DS3	Digital Signal Type 3
OC3c	Concatenated carrier
OC3	Channelized carrier.
LOF	Loss Of Frame
RAI	Remote Alarm Indication
AIS	Alarm Indication Signal

91.9 Applicable customer facing sections

Fault Management	
Logs	__X__
Alarms	__X____
Configuration	
Data Schema	__X___
User Interface	__X___
Element Management	__X___
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	___X__

92: Functional Description (FN): A00003604

92.1 Feature name

OC3 Channelized Support.

92.2 Description

This new feature will allow the user to provision the carrier (only for SONET and not for SDH) in “Channelized” mode in addition to the previously existing functionality.

92.3 Carrier Provisioning Page

This page is used by the user for provisioning the carrier. It is invoked by selecting the DCC card and clicking on the “Carrier à Provisioning” option listed in the Menu. A message “Please select Signal Type and Payload Width for Provisioning the carrier” is displayed to the user.

This page is divided in two sections. Section one contains “Signal Type”, “Payload Width”, “Host Name”, “Line Coding”, “Line Type”, “Query” button and “Submit” button. And the second section contains the details about the STS1 paths.

Initially, the page comes up with only the first section. Only the “Signal Type” field in this section is enabled. Figure 1and Figure 2 show the Carrier Provisioning page with only the first section. Figure 3shows the Carrier Provisioning page with both the sections.

The “Query” button remains enabled always.

92.3.1 SDH Signal Type

If the user selects SDH as the “Signal Type”, the “Payload Width” will contain only STM1 value. The user in this case has to only give a proper “Host Name” and click on the “SUBMIT” button. For this case the second section will not be shown to the user.

Figure 1 shows the screen shot when SDH is selected as “Signal Type”.

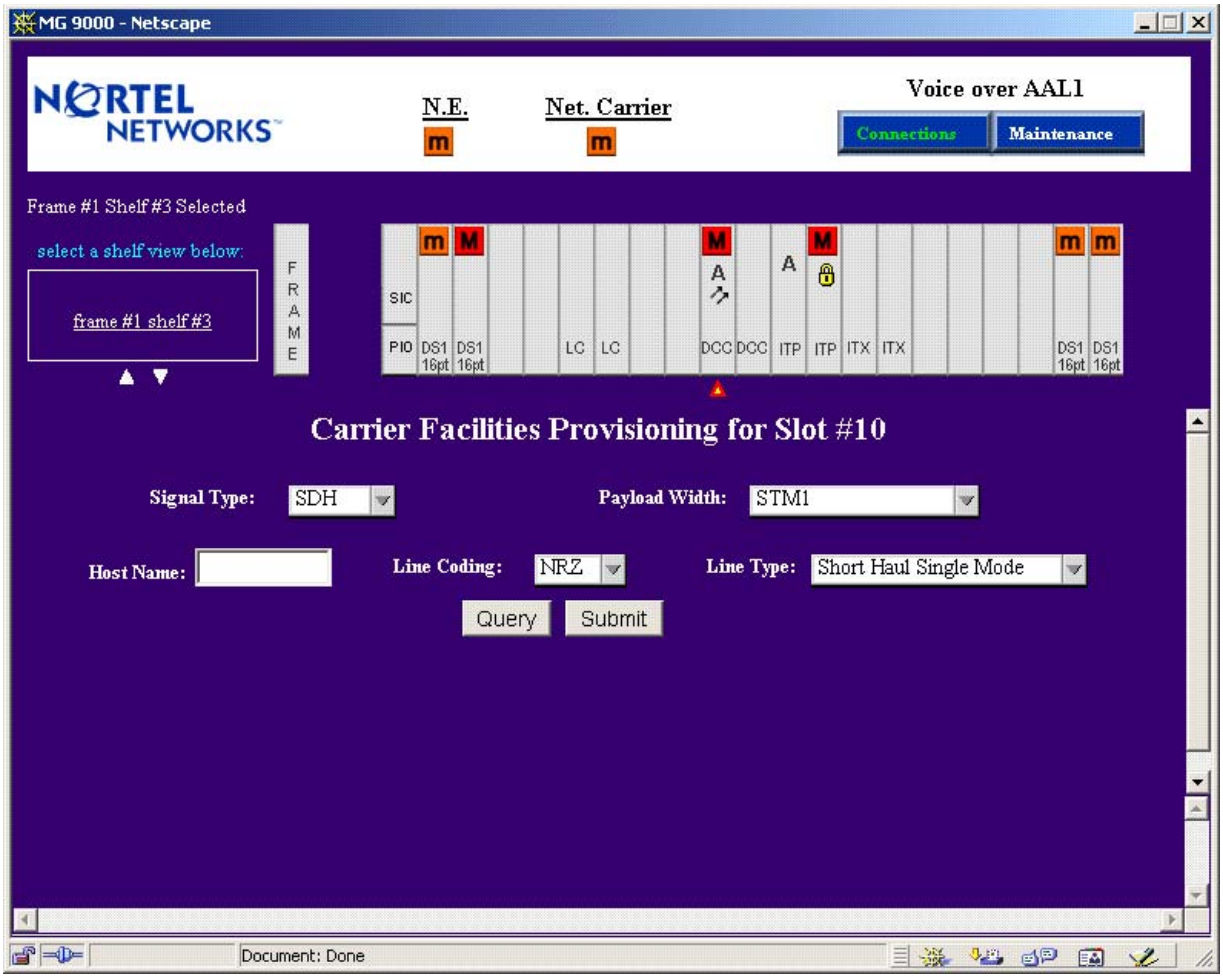


Figure 1 Carrier Provisioning Screen having "Signal Type" as "SDH"

92.3.1.1 SONET Signal Type

If the user selects SONET as the "Signal Type", the "Payload Width" list box will be enabled with "-------" as the default value and "OC3 Concatenated", "OC3" the other values.

92.3.1.1.1 OC3 Concatenated Payload Width

On selecting "OC3 Concatenated", the user has to only give a proper "Host Name" and click on the "SUBMIT" button. For this case the second section will not be shown to the user. Figure 2 shows the screen shot when "OC3 Concatenated" is selected as the "Payload Width".

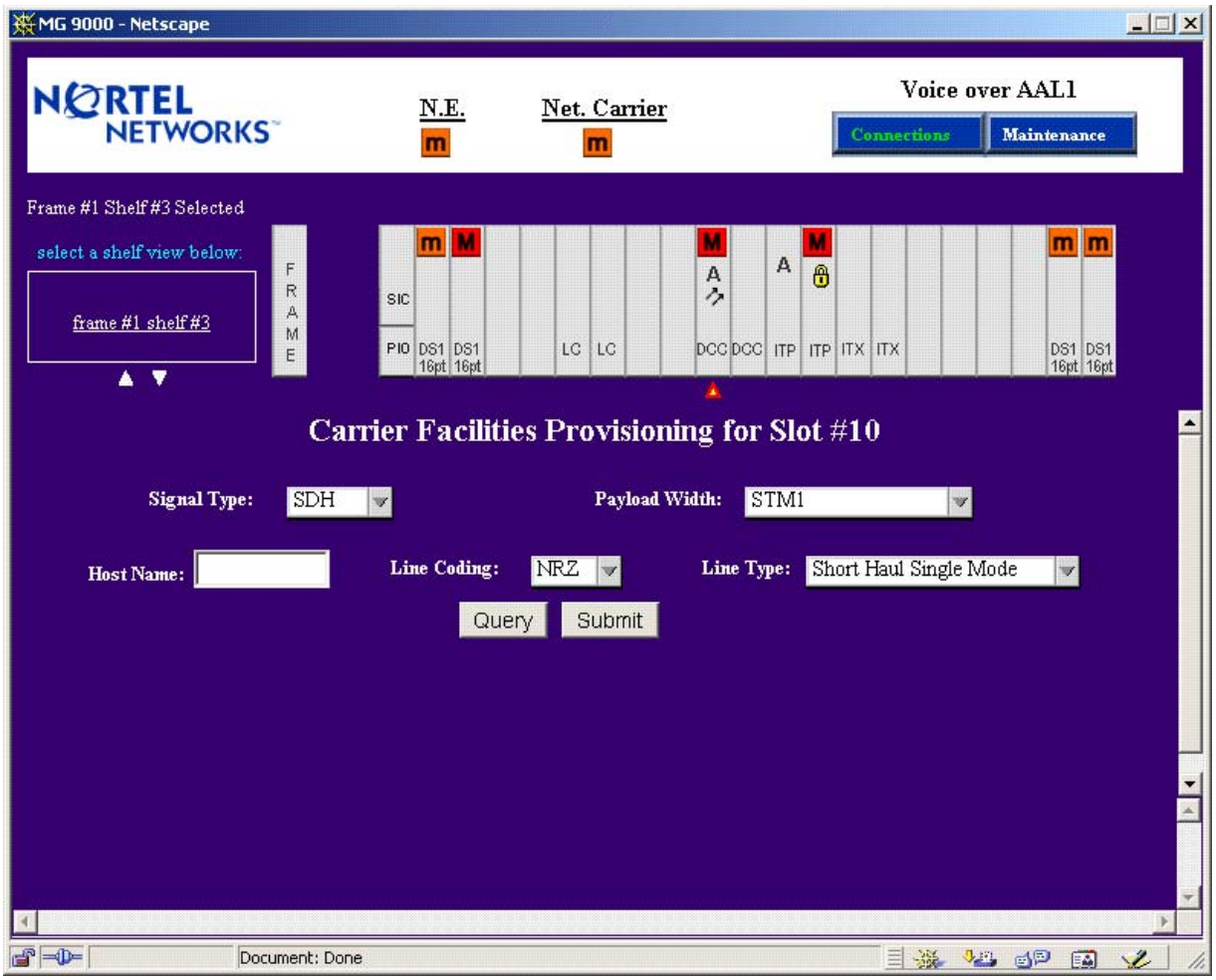


Figure 2 Carrier Provision Screen having "Payload Width" as "OC3 Concatenated"

92.3.1.1.2 OC3 Payload Width

On selecting "OC3" as the "Payload Width", the second section is shown to the user. The "SUBMIT" button of the first section still remains disabled only on IE5.5. For the other browsers, click on this SUBMIT button gives a message saying – 'Submit the path details by clicking the submit button against the path'.

The STS1-1 path of the second section will have the default values of "Payload" and "Destination" as "Ds3clearChannel" and "NETWORK" respectively. The other STS1 paths will have the default values of "Payload" and "Destination" as "Ds3ClearChannel" and "NONE" respectively.

After entering a valid "Host Name", the user has to click on any one of the "SUBMIT" buttons in second section.

If the LCI user selects “sts1” option under the “Payload” list box and clicks on the corresponding “SUMBIT” button, then the carrier will not carry any DS3 Payload though it will be configured in “OC3” mode.

If the user wishes to designate another STS1 path as "Network", then the existing "Network" STS1 path must be changed to "None". After this, the user may choose a different "Network" carrier. An error message “Only one STS1 Path may be designated as a Network carrier” is displayed for this case. Figure 3 shows the screen shot when OC3 is selected as “Payload Width”.

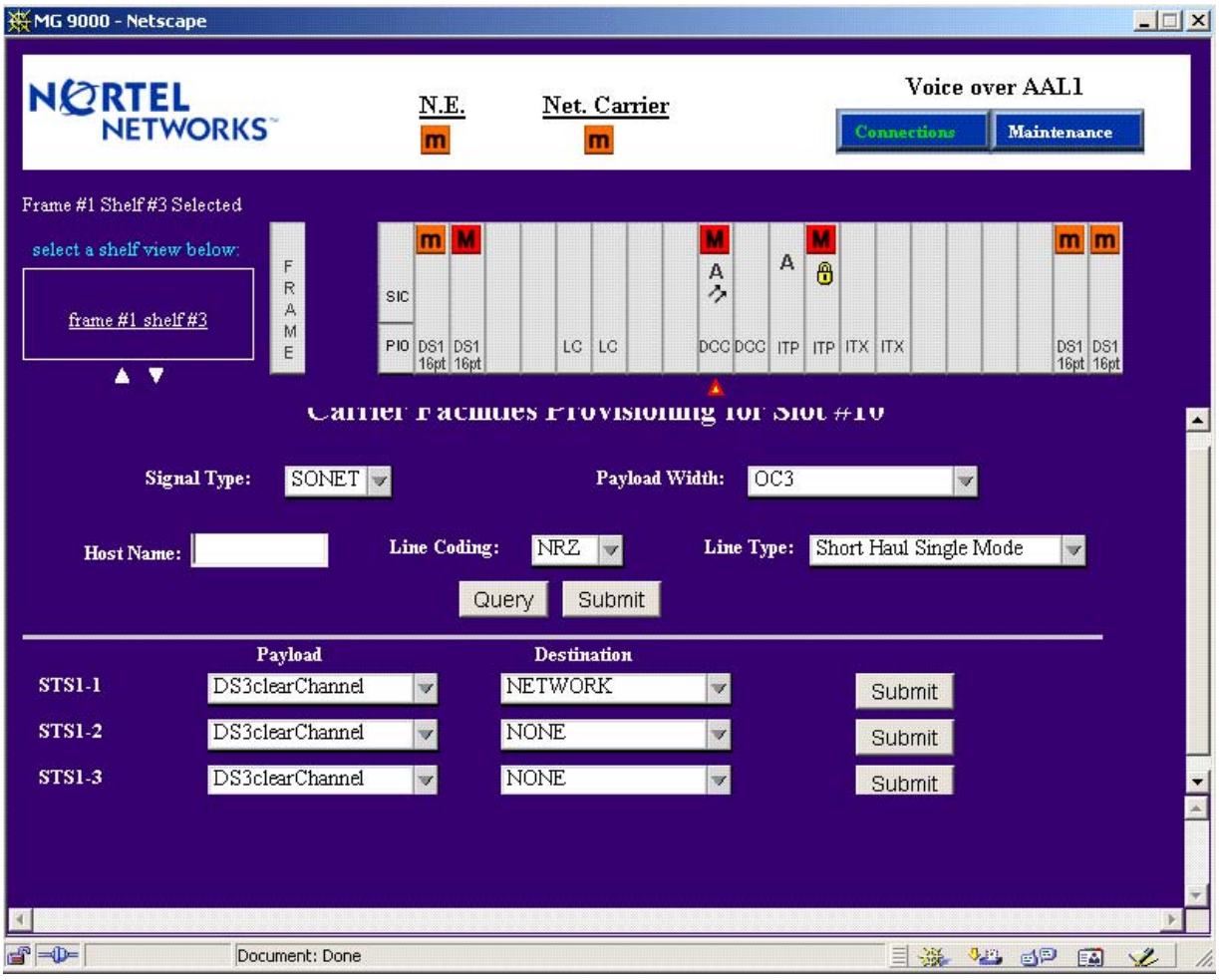


Figure 3 Carrier Provision Screen having “Payload Width” as “OC3”

92.3.2 Carrier Controls Page

This page is used by the user for locking/unlocking the carrier. It is invoked by selecting the DCC card and clicking on the “Carrier à Controls” option listed in the Menu.

92.3.2.1 Carrier provisioned in “SDH” and “OC3 Concatenated” mode

In this case, the old “Carrier Controls” page is displayed to the user as shown in Figure 4. There is no change in the behavior of this page.

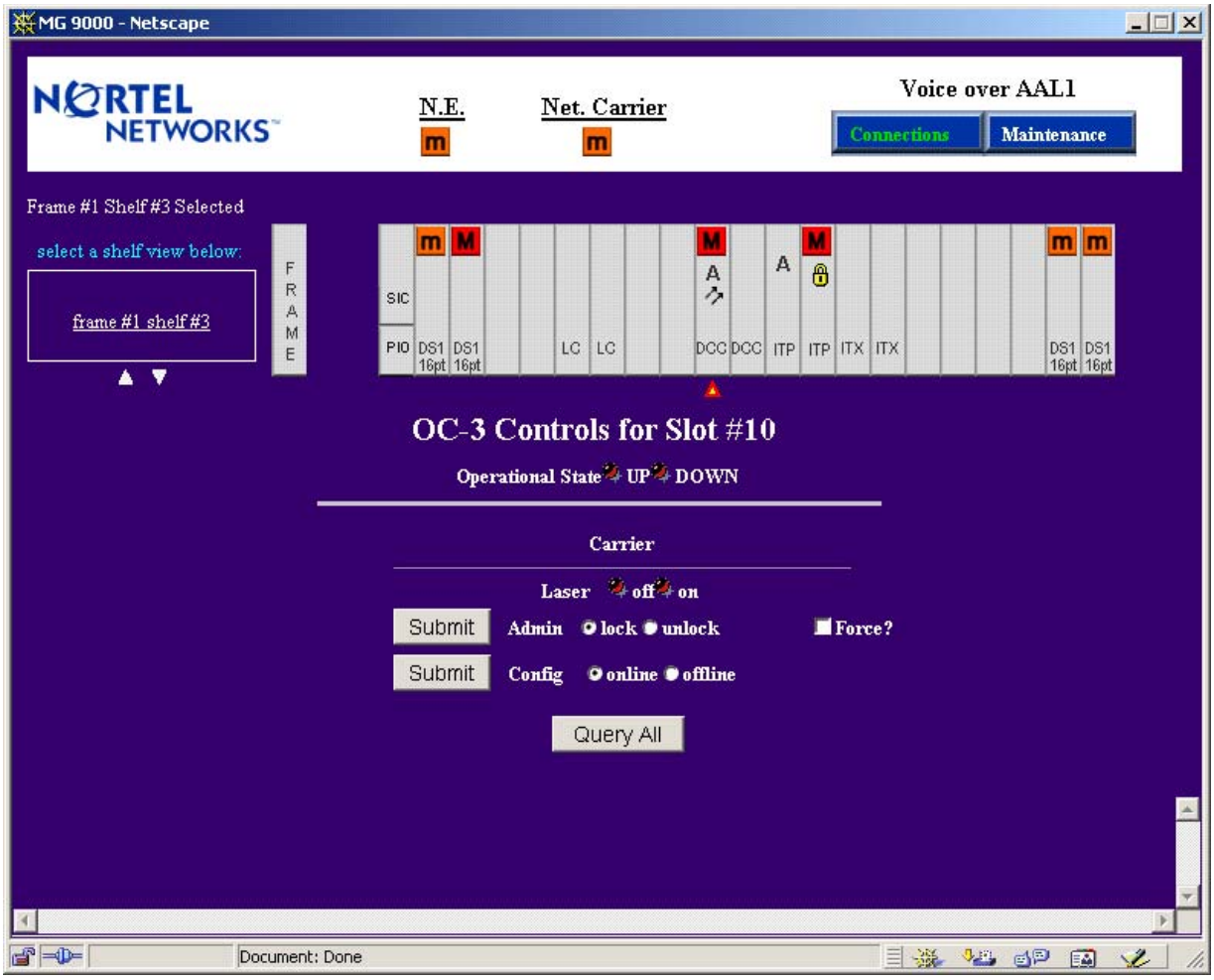


Figure 4 Carrier Controls Screen for SDH and OC3c mode

92.3.2.2 Carrier provisioned in “OC3” mode

In this case an alternative “Carrier Controls” page is displayed to the user as shown in Figure 5.

This page has individual options for locking/unlocking the “OC3 Section/ Line” and the three STS1 paths.

Carrier lock symbol is removed from the DCC card when “OC3 Section/Line” and one of the STS1 paths is unlocked. Under all other conditions, the carrier lock symbol is retained on the DCC card.

Specific error messages are displayed on the active card. The messages guide the user to take appropriate steps while performing any admin/config operations.

Say if the user tries to unlock more than one STS1 paths, then the message “Invalid operation. Only one STS1 Path can be unlocked at any given time” is shown to user.

When the user performs any operations on Controls page, on an inactive card, a general success/failure message is displayed.

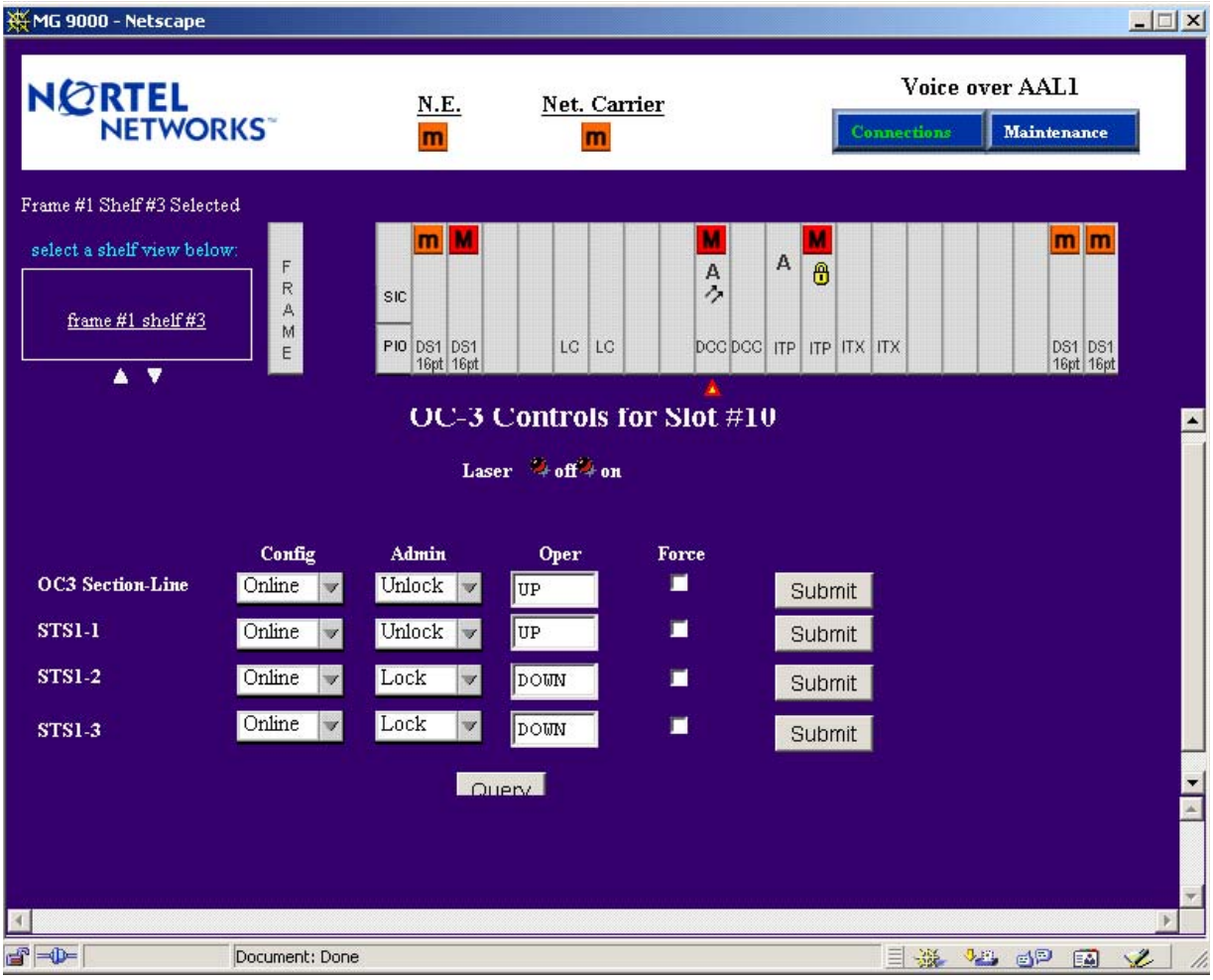


Figure 5 Carrier Controls Screen for OC3 mode

92.3.3 Carrier Status Page

This page is used by the user for viewing the status of the carrier. It is invoked by selecting the DCC card and clicking on the “Carrier à Status” option listed in the Menu.

92.3.3.1 Carrier provisioned in “SDH” and “OC3 Concatenated” mode

In this case, the old “Carrier Status” page is displayed to the user as shown in Figure 6. There is no change in the behavior of this page.

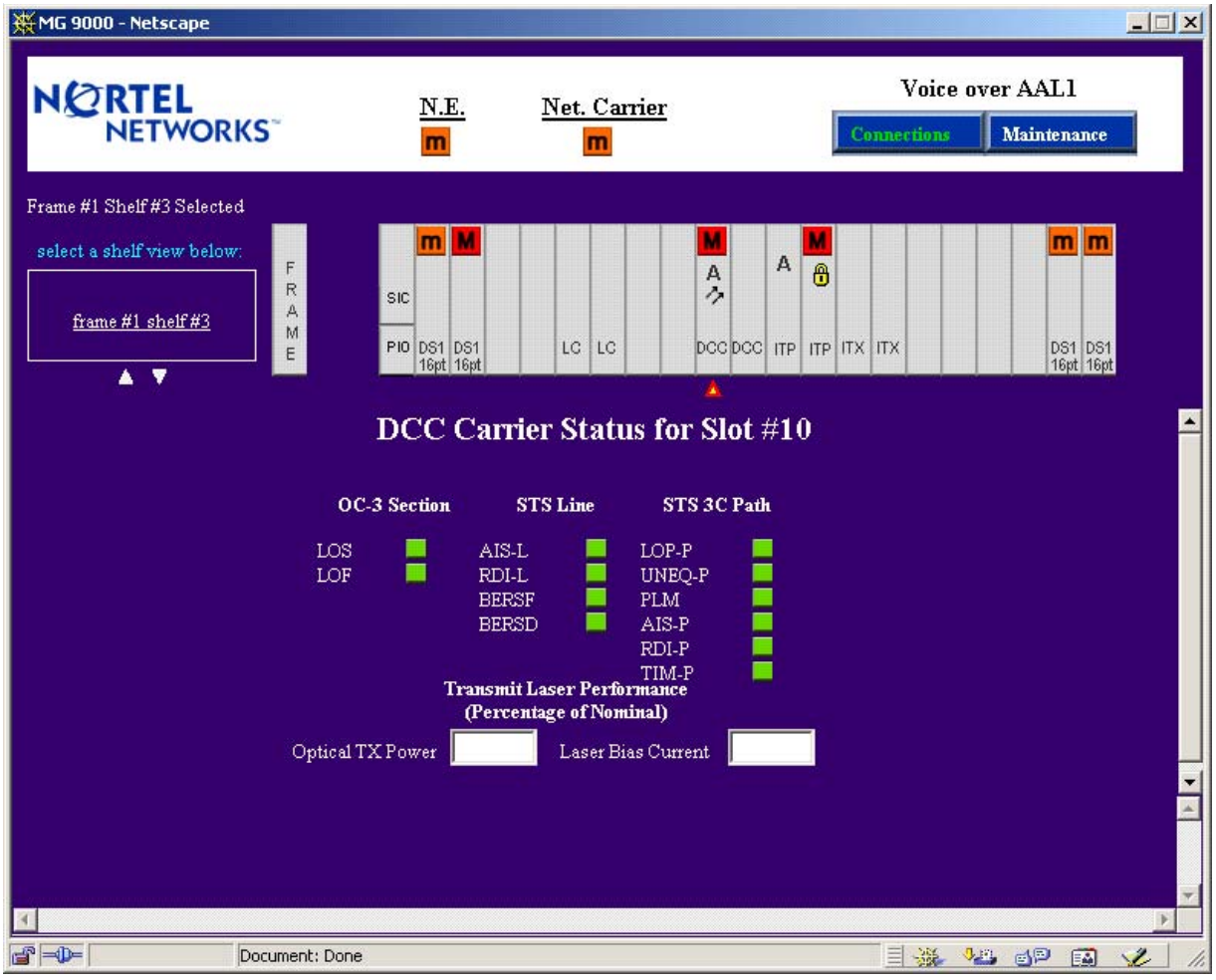


Figure 6 Carrier Status Screen for SDH and OC3c mode

92.3.3.2 Carrier provisioned in “OC3” mode with DS3 Payload

In this case an alternative “Carrier Status” page is displayed to the user as shown in Figure 7. This page will show “OC3 Section”, “STS Line”, 3 STS1 Path and DS3 Path alarms.

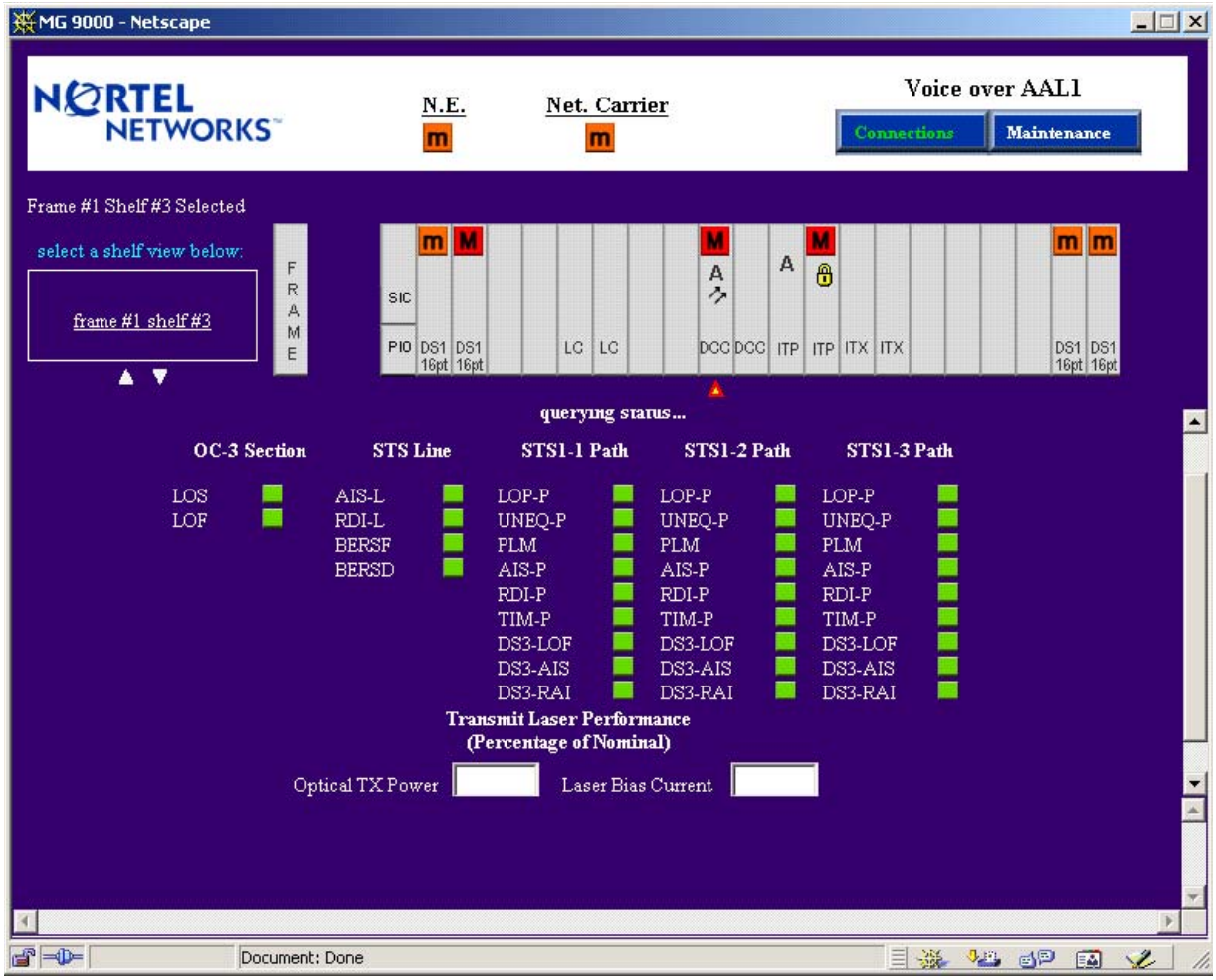


Figure 7 Carrier Status Screen for OC3 mode with DS3 Payload

92.3.3.3 Carrier provisioned in "OC3" mode without DS3 Payload

In this case an alternative "Carrier Status" page is displayed to the user as shown in Figure 8. This page will show "OC3 Section", "STS Line", 3 STS1 Path alarms.

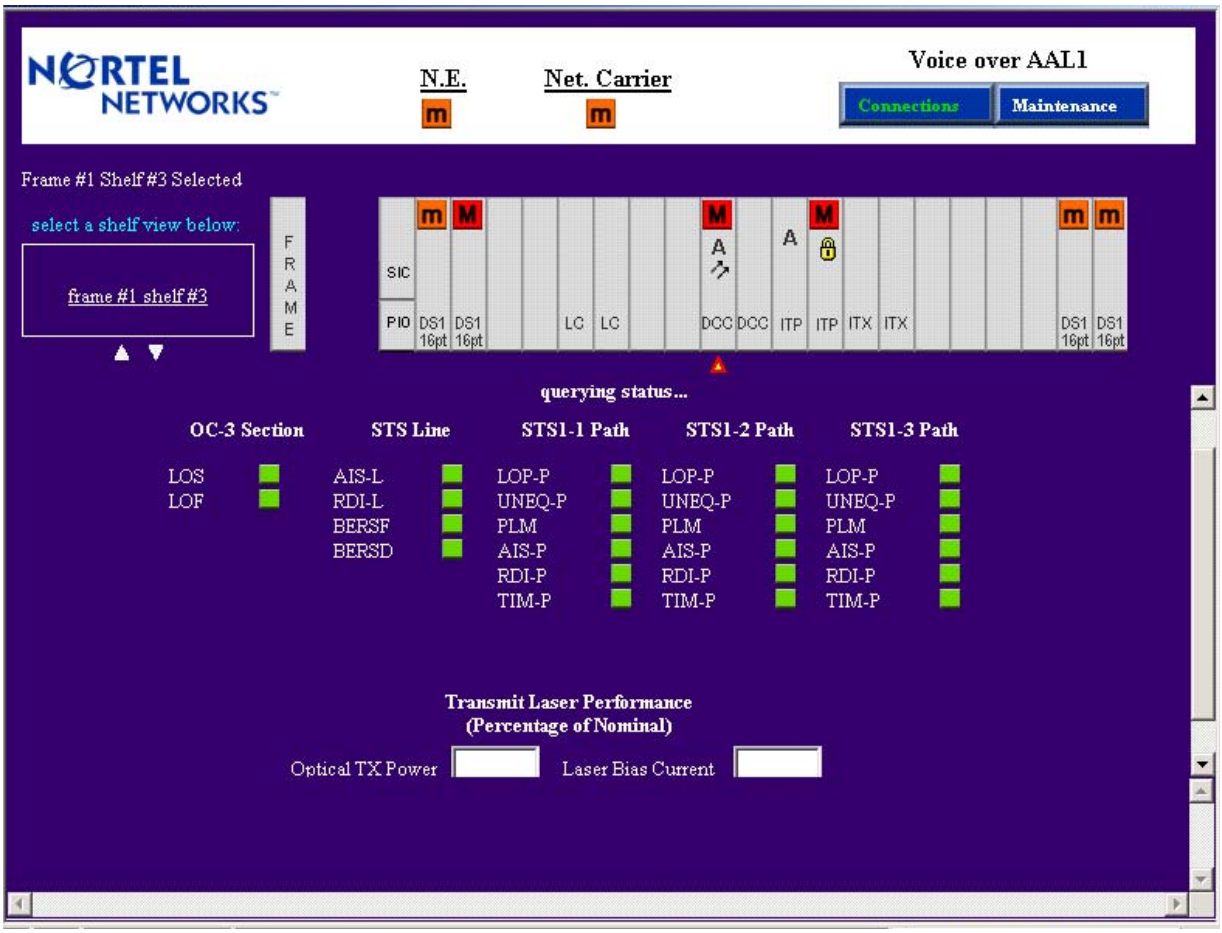


Figure 8 Carrier Status Screen for OC3 mode without DS3 Payload

92.3.4 General

When the LCI user tries to invoke “Carrier Controls” and “Carrier Status” pages prior to provisioning the carrier, a message “Operation cannot be performed as the Carrier is not yet provisioned” is shown.

92.4 Hardware Requirements or Dependencies

There will be no additional hardware requirements introduced as a result of this feature.

92.5 Software Requirements or Dependencies

There will be no additional software requirements introduced as a result of this feature.

92.6 Limitations and restrictions

Upon feature completion, there will not be any visible functional limitations and restrictions on the LCI that may affect the end user.

92.7 Interactions

No change.

92.8 Applicable customer facing sections

Fault Management:

Logs	____N/A__
Alarms	____X____

Configuration:

Data Schema	____X_____
User Interface	____X_____
Element Management	____N/A____
Security	____N/A____
Service Order	____N/A____
Office Parameters	____N/A____

Accounting (includes AMA billing)	____N/A____
Performance (includes operational measurements)	____N/A____

92.9 Glossary

Term	Description
LCI	Local Craft Interface
DCC	Data Controller Card

93: Functional Description (FN): A00003613

93.1 Feature name and Feature ID

SSPFS: CBM CONFIGURATION PARAMETERS A00003613

93.2 Description

This will add three configuration parameters to the existing SSPFS configuration, which will be configured via the existing “cli” tool:

CM Internet Protocol (IP) Address: The address by which the CM may be reached. This address should be reachable by the SSPFS through VLAN’s, which are defined in the network topology.

Login Greeting: A string that will be displayed to remote telnet users before they attempt to login.

System Location: A string defining the physical location of the SSPFS Server

New menu options for each of these parameters will be added to the existing SSPFS “cli” tool.

93.3 Applicable customer facing sections

This section is mandatory to ensure that OSS vendors and other downstream users receive accurate and complete information.

Indicate with an “X” the customer facing section(s) of the DDOC that apply to this functionality. Indicate with “N/A” the customer facing sections(s) of the DDOC that do not apply to this functionality. Once you mark any of the items below with an “X,” you must complete the corresponding chapter of the template.

Fault Management:

- Not Applicable___N/A_____
- Logs ___N/A_____
- Alarms ___N/A_____

Configuration:

- Not Applicable___N/A__
- Data Schema/MIBs___N/A__
- User Interface ____X__

- GUI___N/A__
- Element Management ___N/A__
- Security____X___
- Service Order ___N/A__
- SOC___N/A__
- Office Parameters ___N/A__
- Upgrades impact___N/A__

Accounting ___N/A__

- Not Applicable___N/A__
- Billing changes___N/A__

Performance ___N/A__

- Not Applicable___N/A__
- Operational Measurements___N/A__
- Performance Measurements___N/A__

Realtime ___N/A__

- Not Applicable___N/A__

Engineering Information___N/A__

- Not Applicable___N/A__

93.4 Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced.

93.5 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

93.6 Limitations and restrictions

No limitations or restrictions that is visible to any user are planned as part of this feature.

93.7 Interactions

No interactions between this feature and existing features.

93.8 Glossary

Term	Description

93.9 Configuration

93.9.1 Hardware and Software Requirements

SSPFS platform software and supported hardware are required for this feature.

93.9.2 13.2 Initial Configuration

These new parameters are optional to SSPFS, and will be configured after the initial install or upgrade of SSPFS.

93.10 Office / Subnet parameters (OP/SP) (CM & SESM)

Not Applicable to this feature.

93.11 Upgrade Impact

No upgrade impacts.

93.12 Data schema (DS) (CM, MIBS, RDB)

Not Applicable to this feature.

93.13 Service Orders (SO) (CM & SESM)

Not Applicable to this feature.

93.14 Software optionality control (SOC)

Not Applicable to this feature.

93.15 Element Management

93.15.1 New/modified GUIs

Not Applicable to this feature.

93.15.2 GUI information

Not Applicable to this feature.

93.15.3 CLUI Interface

The existing SSPFS “cli” menu tool will be updated to configure the three new parameters. Details of this are described in the User interface changes section.

93.16 User interface changes

93.16.1 Directory: Configuration/ OAMP Application Configuration

93.16.1.1 Directory description

This existing menu level contains commands to configure switch specific settings that are used by OAMP Applications.

93.16.1.2 Accessing directory: OAMP Application Configuration

93.16.1.3 Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

93.16.2 Command: cm_conf (Configure CM IP Address)

93.16.2.1 Command type: Listed MENU

93.16.2.2 Command target: Other, SSPFS system

93.16.2.3 Command availability: RES

93.16.2.4 Command description

This command will allow the user to configure enter or change the CM IP address. The CM IP address parameter will also be displayed in the CLI Menu level “View”, “software configuration” and the capt_gather tool.

93.16.2.5 Command syntax

This command only takes one parameter, which is an IP address. The IP address must be of the format “0-255.0-255.0-255.0-255”. .

Table 1_ <CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure CM IP Address	IP address of the CM

93.16.2.6 Qualifications and warnings

User must be root to change this value.

93.16.2.7 Responses

93.16.2.7.1 Enter the CM IP Address (default: <address>)

This prompts the user for the new CM IP Address. If an address is already configured, it will be displayed in the prompt as the default value. If the user just presses enter, the default value will be taken for this parameter.

93.16.2.7.2 User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

93.16.2.7.3 ERROR: IP Address <address> is not valid

The IP address enter was not of a valid format, the user will be prompted to re-enter the IP address.

93.16.2.7.4 Must be root to use this tool

A non-root user is attempting to change the IP address. The command will exit. The user should become root and re-enter the command.

93.16.2.8 Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "cm_conf"

CM IP:        10.14.71.3

Enter the CM IP Address (default: 10.14.71.3):
10.14.71.5

CM IP:        10.14.71.5

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "cm_conf" completed successfully
```

93.16.3 Command: cm_unconf (Unconfigure CM IP Address)

93.16.3.1 Command type: Listed MENU

93.16.3.2 Command target: Other, SSPFS system

93.16.3.3 Command availability: RES

93.16.3.4 Command description

This command will allow the user to unconfigure the CM IP address. This is used it the CM IP address is no longer needed, or can be automatically determined via application software (such as systems with OC-3 core connectivity).

93.16.3.5 Command syntax

This command only takes no parameters.

Table 1_ <CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Unconfigure CM IP Address	none

93.16.3.6 Qualifications and warnings

User must be root to change this value.

93.16.3.7 User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

93.16.3.7.1 Must be root to use this tool

A non-root user is attempting to unconfigure the IP address. The command will exit. The user should become root and re-enter the command.

93.16.3.8 Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "cm_unconf"

CM IP:         10.14.71.3

CM IP address will be unconfigured
```

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "cm_unconf" completed successfully
```

93.16.4 Directory: Configuration / Login Session

93.16.4.1 Directory description

This existing menu level contains commands to configure login parameters

93.16.4.2 Accessing directory: Login Session

93.16.4.2.1 Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

93.16.5 Command: telnet_greeting (Telnet Login Greeting)

93.16.5.1 Command type: Listed MENU

93.16.5.2 Command target: Other, SSPFS system

93.16.5.3 Command availability: RES

93.16.5.4 Command description

This command will allow the user to configure enter or change the message shown to users before they attempt to login to this server. This text message may contain multiple lines and has no size limit. This may contain information about this system and or warnings to un-authorized users. On fresh installs or upgrades from older loads, the default message will be “Authorized use only, activities logged”.

93.16.5.5 Command syntax

This command only takes one parameter, which is a text field.

Table 1_ <CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure telnet login greeting	Message to be displayed to users before they attempt to login

93.16.5.6 Qualifications and warnings

User must be root to change this value.

93.16.5.7 Responses

93.16.5.7.1 Enter the Telnet Login Greeting Message. Enter a blank line to end the message.

This prompts the user for the Telnet Login Greeting. If a greeting is already configured, it will be displayed above this prompt. If the user just enters a blank line, the Login Greeting Message will be cleared.

93.16.5.7.2 User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

93.16.5.7.3 Must be root to use this tool

A non-root user is attempting to change the Telnet Login Greeting address. The command will exit. The user should become root and re-enter the command.

Provide a brief explanation of the response. Define all the variable fields in the response. Indicate if the response is visible on NT40, SUPERNODE, BRISC, All, or Other. If Other specify.

93.16.5.8 Example

Example shown is changing the greeting from the default (user input in bold):

```
=== Executing "telnet_greeting"

Telnet Login Greeting Message:  Authorized use only,
activities logged

Enter the Telnet Login Greeting Message.
Enter a blank line to end the message:
Private Database, Authorized users only

Telnet Login Greeting Message:   Private Database,
Authorized users only

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "telnet_greeting" completed successfully
```

93.16.6 Directory: Configuration / Location Configuration

93.16.6.1 Directory description

This new menu level contains commands to configure system parameters. The current time zone command “chg_tz (Change Timezone)” will be moved to this level. The new command “sys_loc (System Location)” will also be at this level.

93.16.6.2 Accessing directory: Location Configuration

93.16.6.2.1 Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

93.16.7 Command: sys_loc (System Location)

93.16.7.1 Command type: Listed MENU

93.16.7.2 Command target: Other, SSPFS system

93.16.7.3 Command availability: RES

93.16.7.4 Command description

This command will allow the user to configure enter or change a text string describing the system location. On fresh installs or upgrades from older loads, this string will be empty by default. The System Location parameter will also be displayed in the CLI Menu level “View”, “software configuration” and the capt_gather tool.

93.16.7.5 Command syntax

This command only takes one parameter, which is a text field.

Table 1_ <CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure System Location	A line of text decribing the systems physical location

93.16.7.6 Qualifications and warnings

User must be root to change this value.

93.16.7.7 Responses

93.16.7.7.1 Enter the System Location (default: <location>)

This prompts the user for the System Location. If this is already configured, the current value will be displayed and set as the default choice.

93.16.7.7.2 User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

93.16.7.7.3 Must be root to use this tool

A non-root user is attempting to change the system location. The command will exit. The user should become root and re-enter the command.

93.16.7.8 Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "sys_loc"

System Location:        NCRTP Lab 4

Enter the CM IP Address (default: NCRTP Lab 4): NCRTP
Lab 5

System Location:        NCRTP Lab 5

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "sys_loc" completed successfully
```

93.17 Security

Only the Login Greeting has any security implications. The greeting should not reveal any system information and if often using to inform persons that only authorized or employee use is allowed. As other Nortel products have this same mechanism, we anticipate customers will have a Login Greeting message established.

93.18 Configuration Walkthrough

These parameters may be configured at any time. On SSPFS system which will use the CBM applications, these parameters must be set. These parameters are not required on other SSPFS systems. However their use should be encouraged.

94: Functional Description (FN): A00003615

94.1 Feature name and Feature ID

SSPFS: A00003615 - SSPFS packaging/patch enhancements

94.2 Description

This feature is divided into five completely individual parts:

Part one - Patching Enhancements - Deals with patching SSPFS electronically. It includes the building of incremental patching.

Part two - Platform Upgrade Downtime Reduction - Reduce platform upgrade down time to be less than a target of 1 hour.

Part three- Debugging Tools - Enhanced debugging tools, this includes the inclusion of Sun Explorer and an enhanced platgather.

Part four - Provide a cli tool to mount an iso image on the SSPFS unit.
Part five - SSPFS 3rdparty software upgrades.

94.3 Applicable customer facing sections

Fault Management	
Not applicable	_____
Logs	___Y___
Alarms	___Y___
Configuration	
Not applicable	_____
Data Schema/MIBs	_____
User Interface	__Y____
GUI	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____

SOC _____

Upgrades impact ___Y___

Accounting (includes AMA billing) _____

Not Applicable _____

Billing changes _____

Performance _____

Not Applicable _____

Operational Measurements _____

Performance Measurements _____

Realtime _____

Not applicable _____

Engineering Information _____

Not applicable _____

94.4 Hardware Requirements or Dependencies

To test the reduced SSPFS upgrade downtime, you must have fieldgrade hardware on the t1400 or N240 with the proper disk sizes.

94.5 Software Requirements or Dependencies

N/A

94.6 Limitations and restrictions

N/A

94.7 Interactions

N/A

94.8 Glossary

Term	Description

95: Functional Description (FN): A00003617

This feature serves the following purposes:

1. Use alarmD as the reporting (writing to customer logs and lighting alarm lights) and storage mechanism for all platform related alarms.

2. In addition to existing fault monitors, provide new monitors that will monitor the following system components.

- CPU load average

- Memory usage

- Swap space

In addition to this, the existing file system monitor will be enhanced to monitor a lot more than just file system usage.

95.1 Feature name and Feature ID

Feature Name: AlarmD Integration

Feature ID: A00003617

95.2 Description

This feature serves the following purposes:

1. Use alarmD as the reporting (writing to customer logs and lighting alarm lights) and storage mechanism for all platform related alarms.

2. In addition to existing fault monitors, provide new monitors that will monitor the following system components.

- CPU load average

- Memory usage

- Swap space

In addition to this, the existing file system monitor will be enhanced to monitor a lot more than just file system usage.

3. It will provide interfaces to turn on, turn off and query alarm lights on Netra 1400 and N240 platforms. A command line interface to do the same will also be provided.

4. A command to query all the faults on a system (an aggregate view of the system) will be included. This command can be invoked from command line or through the cli interface.

95.3 Applicable customer facing sections

Fault Management	
Not applicable	___X__
Logs	___2.8 __
Alarms	___2.8__
Configuration	
Not applicable	___X__
Data Schema/MIBs	___X___
User Interface	__2.9___
GUI	___X__
Element Management	___X___
Security	___X___
Service Order	___X___
Office Parameters	___X___
SOC	___X___
Upgrades impact	___X___
Accounting (includes AMA billing)	___X___
Not Applicable	___X___
Billing changes	___X___
Performance	___X___
Not Applicable	___X___
Operational Measurements	___X___
Performance Measurements	___X___
Realtime	___X___
Not applicable	___X___

Engineering Information	___X___
Not applicable	___X___

95.4 Hardware Requirements or Dependencies

Certain components of this feature will be supported only on field grade hardware.

When an alarm is raised or cleared, the corresponding alarm light will be turned on and off only on T1400s and N240s.

Logs will be generated on other platforms. However, the turning on, turning off and querying the state of a light will be supported only on T1400s and N240s.

95.5 Software Requirements or Dependencies

No requirements identified at this time.

95.6 Limitations and restrictions

95.7 Interactions

A00001953 - Common Platform Capabilities - introduced a set of fault monitors. The reporting mechanism used by these monitors was through two separate calls. The first call was to write a customer log. The second was to turn on/ off an alarm light. The state of a fault was not maintained.

As part of this feature, alarmD will be used to write logs and light a light as part of a single call. It will also store the state of a fault associated with a particular monitor. These faults will be aggregated to provide a blanket view of the system at an instant in time. Existing monitors (the ones provided as part of A00001953) will be modified to make use of the capability that alarmD provides.

95.8 New Logs written as part of this feature

CPU Related Logs

Log related to a Major Alarm

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: CPU Load Average threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: CPU

Description: CPU load average is 6.3

Recovery Action: Check System for run away processes.

Log related to Minor Alarm

3X20 * SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: CPU Load Average threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: CPU

Description: CPU load average is 4.3

Recovery Action: Check System for runaway processes.

Log associated with a clear

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: CPU

Description: No CPU problems reported at this time

Swap Space

Logs Related to Major Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Swap Space usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: SwapSpace

Description: Less than 20% of swap space available

Recovery Action: Contact Support.

Logs Related To Critical Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Swap Space usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: SwapSpace

Description: Less than 10% of swap space available

Recovery Action: Contact Support.

Logs Related To Clears

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: Swap Space

Description: Over 20% of swap space available.

Memory Usage

Logs Related to Minor Alarms

3X20 * SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Memory usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: Memory

Description: Scan Rate Exceeded 20

Recovery Action: Contact Support

Logs Related to Major Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Memory usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: Memory

Description: Scan Rate Exceeded 50

Recovery Action: Contact Support

Logs Related To Clears

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: Memory

Description: Reported Scan Rate is less than 20. No memory problems reported at this time.

File System Monitor

Logs Related To Major Alarms

3X20 ** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: FileSystem Not mounted

ProbableCause: SHM: check probable cause

ComponentId: FSMon

Description: Filesystem <mountpoint> not mounted

Recovery Action: Contact Support.

3X20 ** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File System usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 20% of <Filesystem> available

Recovery Action: Remove files from <Filesystem>

Critical Alarms

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 10% of <File System> available

Recovery Action: Remove files immediately from <Filesystem>

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system write failed

ProbableCause: fileError

ComponentId: FSMon

Description: O_SYNC write to <File System> Failed

Recovery Action: Contact support

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system read failed

ProbableCause: fileError

ComponentId: FSMon

Description: O_DIRECT read from <File System> failed

Recovery Action: Contact Support.

Minor Alarm

3X20 * SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File System usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 25% of <Filesystem> available

Recovery Action: Remove files from <Filesystem>

Alarm Clears

3X20 SPFS350 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Software

Component Id: FSMon

Description: No File System related problems reported at this time.

95.9 Cli interface to query platform state.

A cli interface to query the “state” of the system will be made available.

The interface will allow the user to query a comprehensive state of the system (this includes information about all monitors registered with AlarmD) or just the pieces that have faults tagged against them will both be available.

Both these commands can be invoked either from cli or directly from command line.

The output of these commands has not been defined fully yet. In time, this document will be updated to reflect the output of these commands.

The anticipated output looks like this:

The cli interface to these commands will be as shown below:

Step 1: Type in cli

```
> cli
```

This brings up the following menu

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select - 2
```

Step 2: Select choice 2 (Configuration) from the menu. This will bring up the following options.

```
Platform Monitor Status

1 - all Monitor

2 - faults
```

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp_poller (SNMP Poller Configuration)

X - exit

select - 17

Step 3: Select 17 (Succession element configuration). That will bring up the following menu

Succession Element Configuration

1 - RESMON Application Configuration

2 - NPM Application Configuration

3 - PSE Application Configuration

4 - OMPUSH Application Configuration

X - exit

select - 1

Step 4: Select 1 (Resmon Aplication configuration).

RESMON Application Configuration

1 - queryFaults (Query all faults on the box)

2 - enableLocalLogs (Enable Local Logging Of Faults)

3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 1

Step 5: Select 1 (Query Faults).

If there are no alarms on the box the output will look like this

=== Executing "queryFaults"

Alarm database does not conatin Faulted Nodes

=== "queryFaults" completed successfully

If alarms are raised, the output will look like this (sample output)

```
** SPFS310 NOTICE: bge2: link down
        Network Interface down
        Tue Mar 30 17:31:58 2004

 ** SPFS310 NOTICE: bge0: link down
        Network Interface down
        Tue Mar 30 17:32:02 2004
```

95.10 Cli interface to turn off local logging

Run through steps 1-4 from 2.9.

In the RESMON Application Configuration menu ,select 3 (disableLocalLogs).

RESMON Application Configuration

1 - queryFaults (Query all faults on the box)

2 - enableLocalLogs (Enable Local Logging Of Faults)

3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 3

This will print out the following message:

=== Executing "disableLocalLogs"

=== "disableLocalLogs" completed successfully

95.11 Cli option to turn ON local logging

Run through steps 1-4 from 2.9.

In the RESMON Application Configuration menu ,select 3 (disableLocalLogs).

RESMON Application Configuration

1 - queryFaults (Query all faults on the box)

2 - enableLocalLogs (Enable Local Logging Of Faults)

3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 2

This will print out the following message:

=== Executing "enableLocalLogs"

=== "enableLocalLogs" completed successfully

95.12 Glossary

Term	Description
FSMon	File System Monitor
AlarmD	The fault reporting utility that will be provided as part of the SSPFS
CPU	Central Processing Unit
CPU Load	The number of processes on the “ready” queue (that is, processes that are not blocked waiting for IO, but are in a “run” state).
15 minute Load average	The average CPU load over 15 minutes
NIC	Network interface card.

96: Functional description (FN): A00003618

96.1 Feature name and Feature ID

Succession Solaris Platform Foundation Service (SSPFS): High Availability Enhancements A00003618

96.1.1 Description

This feature will enhance the existing SSPFS High Availability framework in the following ways:

Application Groups may have unique IP Address: This allows for IEMS and SESM co-residency and provides a framework for future application co-residency.

Expanded HA API: complete set of C++ and command line tools for applications which needs to interface with the HA framework, such as CBM and NPM.

Cluster Software upgrade: A newer version of the cluster software from Continuous Computing Corporation is introduced. This provides enhanced "split-brain" resolution and memory mapped file handling required by SBA.

Enhanced Ethernet interface fail over: This will introduce Continuous Computing Corporation's UpLink product to provide faster Ethernet interface fail over on both simplex and HA cluster SSPFS system. On simplex systems, this removes the use of Solaris IP multipathing. Solaris IP multipathing required two test IP Addresses, which will no longer be needed, reducing the number of IP Addresses required by SSPFS.

Non-replicated application file systems: This gives applications a new option to have their file systems not replicated by the HA software, required by the CBM applications.

Cluster state change notification to applications: applications may register to be called when a cluster state change occurs (such as a swact).

User option to disable cluster fail over: a new option is added to the existing "cli" tool which allows users to disable cluster fail over (or swact) as needed.

96.1.2 Applicable customer facing sections

Fault Management:

²Not Applicable___N/A_____

²Logs ___N/A_____

²Alarms ___N/A_____

Configuration:

²Not Applicable___N/A__

²Data Schema/MIBs___N/A__

²User Interface ____X__

²GUI ___N/A__

²Element Management ___N/A__

²Security ___ N/A__

²Service Order ___N/A__

²SOC ___N/A__

²Office Parameters ___N/A__

²Upgrades impact___X__

Accounting ___N/A__

²Not Applicable___N/A__

²Billing changes___N/A__

Performance ___N/A__

²Not Applicable___N/A__

²Operational Measurements___N/A__

²Performance Measurements___N/A__

When cluster failover is enabled or disabled, the following log entries will be written to

Feb 22 23:24:49 bimmer maint: Evicting cluster nodes. Cluster failover disabled.

Feb 22 23:26:03 bimmer maint: Joining cluster nodes. Cluster failover enabled.

96.1.3 Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced. All existing field grade SSPFS hardware will work with the Ethernet interface fail over enhancement.

96.1.4 Software Requirements or Dependencies

No new customer viable software or firmware dependencies are introduced in this feature. All software introductions are contained in the SSPFS load.

96.1.5 Limitations and restrictions

Currently, the secondary cluster node is created through cloning process, which takes an extended period of time to complete. Efforts are being made to reduce the time required by this procedure.

96.1.6 Interactions

Interactions between this feature and several existing features. Several of the enhancements are specifically for the CBM and NPM applications.

96.2 Configuration

96.2.1 Hardware and Software Requirements

All preparatory configuration changes were in place since SN06.2 for upLink inclusion. SSPFS platform software and supported hardware are required for this feature.

96.2.2 Initial Configuration

This feature will introduce changes to the SSPFS installation tool to support application specific IP address configuration. These changes will be mirrored in the post-install “cli” tool IP configuration tool discussed below. The menus and behavior for settings IP addresses will be the same at install as in the post-install “cli” tool.

96.2.3 Office / Subnet parameters (OP/SP) (CM & SESM)

Not Applicable to this feature.

96.2.4 Upgrade Impact

The details of an HA cluster upgrade from SN06.2 to SN07 are addressed in a separate activity, corrective caf in SN07, A00004860. However, this feature will alter the Ethernet interface fail over on upgrade (which will 'free up' test addresses in simplex systems) as well as introduce a new version of the cluster software.

96.2.5 Data schema (DS) (CM, MIBS, RDB)

Not Applicable to this feature.

96.2.6 Service Orders (SO) (CM & SESM)

Not Applicable to this feature.

96.2.7 Software optionality control (SOC)

Not Applicable to this feature.

96.2.8 Element Management

96.2.8.1 New/modified GUIs

Not Applicable to this feature.

96.2.8.2 GUI information

Not Applicable to this feature.

96.2.8.3 CLUI Interface

The existing SSPFS “cli” menu tool will be updated. Details of this are described in the User interface changes section.

96.2.9 User interface changes

96.2.9.1 Directory: Configuration/ IP Configuration

96.2.9.1.1 Directory description This existing menu level contains commands to configure the systems IP network settings

96.2.9.1.2 Accessing directory: IP Configuration 1

Access to directory or MAP level and return to CI
As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

96.2.9.2 Command: conf_test (Configure IP Multipathing Test Addresses)

96.2.9.2.1 Command type: Listed MENU

96.2.9.2.2 Command target: Other, SSPFS system 1

96.2.9.2.3 Command availability: RES 1

96.2.9.2.4 Command description

This command will be removed. The functionality provided by this command will be replaced by UpLink. UpLink configuration will be completely automated.

96.2.9.2.5 Command syntax N/A

96.2.9.2.6 Qualifications and warnings N/A.

96.2.9.2.7 Responses

96.2.9.3 Command: config_ip (Configure System IP Addresses)

96.2.9.3.1 Command type: Listed MENU

96.2.9.3.2 Command target: Other, SSPFS system

96.2.9.3.3 Command availability: RES

96.2.9.3.4 Command description

This command will allow the user to configure the public IP addresses on both simplex and HA cluster systems.

96.2.9.3.5 Command syntax

This command is interactive.

96.2.9.3.6 Qualifications and warnings

User must be root to configure the system IP address(es).

96.2.9.3.7 User confirmation After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

96.2.9.3.8 Application association with additional IP address

If the user chooses to configure an additional IP address, then that address must be associated with a particular application. The user will be prompted for the “name” of that application. This application name should match the servman application group name for this application.

In SN07, the only valid combined system, that will require multiple virtual IP addresses, is a system that will support both IEMS and CS2M. So, in SN07, the only reasonable option will be ‘iems’.

96.2.9.3.9 Must be root to use this tool

A non-root user is attempting to configure the IP address. The command will exit. The user should become root and re-enter the command.

96.2.9.3.10 Cluster restart order message

After a successful IP change on an HA cluster system, the cluster units must be restarted in a particular order. This message is given to the user:

```
The network changes have been made, however the cluster requires a restart
of both units.  The units must be restarted in the below order.

1) Login as root on the console of the standby unit and shut it down with
   the command: "shutdown -i 0 -y".
2) After the standby unit has shutdown, restart the acitve unit with
   the command: "shutdown -i 6 -y".
3) After the restart is complete, the new network settings are in effect.
4) Boot the standby unit with the command "boot".
```

96.2.9.3.11 Example

Example of changing the IP Addresses on a cluster (user input in bold). Notice that the current values are indicated in brackets.

****** There will be no error checking on the application string that is entered…the string must be entered accurately. The only check will be to ensure that an alpha-numeric literal is entered. *****

```
=== Executing "config_ip"

Enter the hostname for this cluster [znc0s0jy] znc0s0jx
Enter  primary  cluster ip address for znc0s0jx [47.142.108.199] 47.142.108.11
Configure additional cluster ip address ? [yes] yes
Enter additional cluster ip address for znc0s0jx [47.142.108.201] 47.142.108.12
Enter application for cluster ip address 47.142.108.12 [iems] iems
Configure additional cluster ip address ? [no]
Enter ip address for unit zero   [47.142.108.220] 47.142.108.7
Enter ip address for unit one    [47.142.108.221] 47.142.108.8

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "config_ip" completed successfully
```

96.2.9.4 Directory: Configuration / Cluster configuration

96.2.9.4.1 Directory description

This existing menu level contains configuration commands and directories.

96.2.9.4.2 Accessing directory: Configuration / cluster configuration

Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

96.2.9.5 Command: disable_failover (Disable cluster node Fail over)

96.2.9.5.1 Command type: Listed MENU

96.2.9.5.2 Command target: Other, SSPFS system

96.2.9.5.3 Command availability: RES

96.2.9.5.4 Command description

This command MUST be run from the ACTIVE node in the cluster. This command will allow the user to disable a cluster fail over. (activity will remain on current node of the cluster, data will still be replicated).

96.2.9.5.5 Command syntax

This command takes one parameter, but is interactive. If a user enters this command a series of other questions will be asked to allow user to disable or re-enable failover.

96.2.9.5.6 Qualifications and warnings User must be root to change this value.

96.2.9.5.7 Responses

```
Cluster Fail over is manually disabled.
```

This informs the user that HA fail over has been manually disabled. A Customer log entry will be generated to indicate this state ‘transition’.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

```
Must be root to use this tool
```

This message appears when a non-root user is attempting to disable fail over. The command will exit. The user should become root and re-enter the command.

Example

Example shown (user input in bold):

96.2.9.6 Command: req_failover (manual request to failover)

96.2.9.6.1 Command type: Listed MENU

96.2.9.6.2 Command target: Other, SSPFS system

96.2.9.6.3 Command availability: RES

96.2.9.6.4 Command description

This command MUST be run from the ACTIVE node in the cluster. This command will allow the user to perform/initiate a cluster fail over. (all applications on the active node will stop, and the Active node will give up activity).

96.2.9.6.5 Command syntax

This command takes no parameters. If a user enters this command a series of other questions will be asked to confirm the operation.

96.2.9.6.6 Qualifications and warnings

User must be root to change this value.

96.2.9.6.7 Responses

```
Cluster Failover initiated
```

This informs the user that HA fail over has been manually disabled. A Customer log entry will be generated to indicate this state ‘transition’.

```
User confirmation
```

After a user enters valid parameters for this command, they will be prompted:

*** Warning: This command will initiate a cluster switch of activity ***

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

```
Must be root to use this tool
```

This message appears when a non-root user is attempting to disable fail over. The command will exit. The user should become root and re-enter the command.

96.2.9.6.8 Example

Example shown (user input in bold):

96.2.10 Security

N/A

96.2.11 Configuration Walkthrough

N/A.

97: Functional Description (FN): A00003630

97.1 Feature name

TGCP for the Cable Market

97.2 Description

The TGCP for the Cable Market feature implements the Trunking Gateway Control Protocol (TGCP) for ISDN User Part (ISUP) and Per Trunk Signaling (PTS) trunk groups on the Succession Call Server 2000 (CS2K). Specifically, this activity provides:

- incoming and outgoing interconnection from a North American End Office (EO) to the Public Switch Telephone Network (PSTN) using ISUP trunk groups.
- incoming and outgoing interconnection from a North American EO to the PSTN for Operator Services.
- incoming interconnection from a North American EO to the PSTN for Emergency Services.

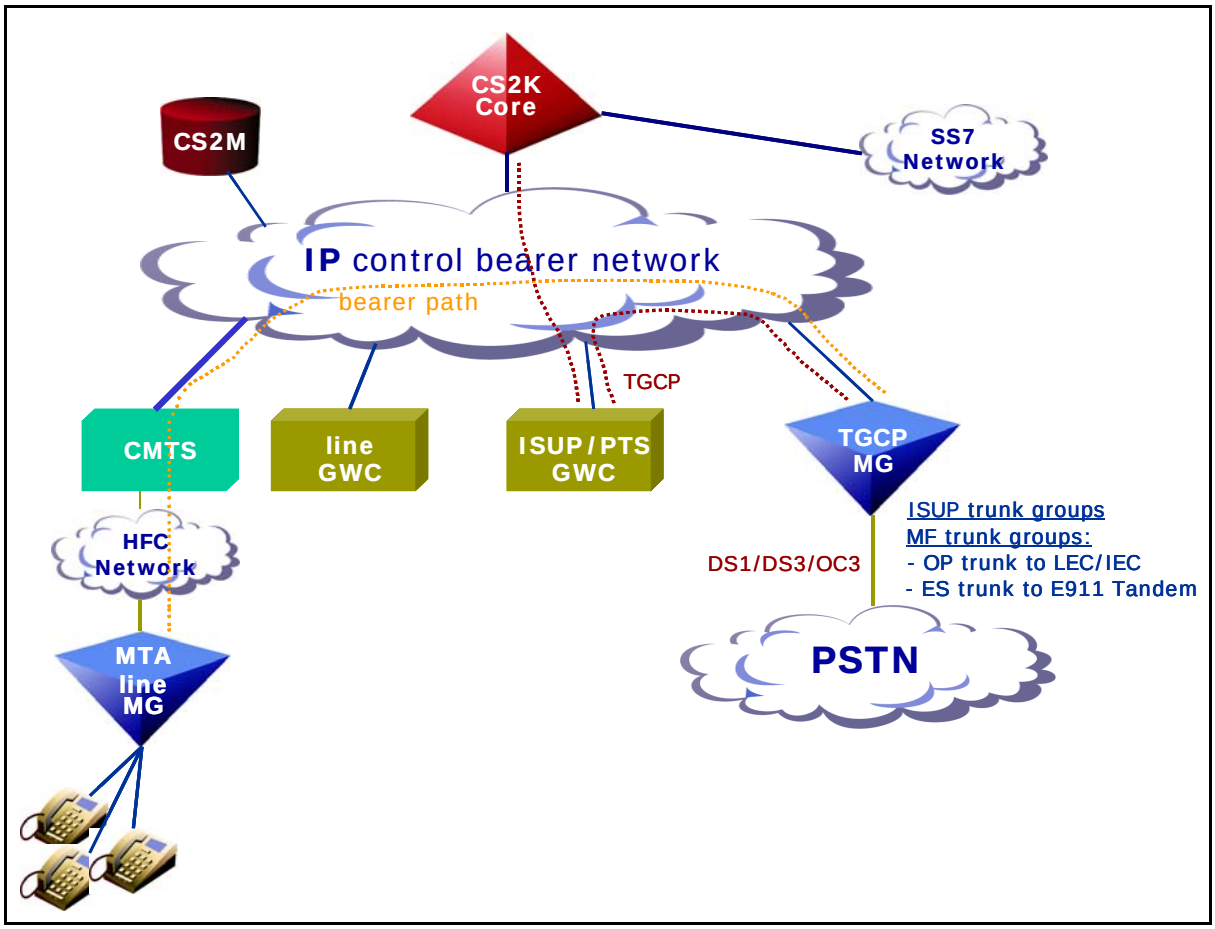
ISUP Inter-Toll (IT) and Access To Carrier (ATC) trunks are supported for interconnection to the PSTN. Multi-Frequency (MF) Operator (OP) trunks are supported for interconnection to a Local Exchange Carrier (LEC) operator system. MF Emergency Service (ES) and OP trunks are supported for interconnection to an Emergency 911 (E911) Tandem switch.

The ISUP and MF trunk interconnection capability provided by this activity is supported for the North American Integrated Access - Cable (IAC) solution.

Figure 1 illustrates the CS2K network components relevant to this activity. PSTN interconnection is provided using ISUP and MF trunks configured on a Gateway Controller (GWC) peripheral type. TGCP is supported between the GWC and the Media Gateway (MG). A third party gateway vendor is providing the Media Gateway functionality. Development on the Media Gateway is beyond the scope of this activity. The goal of this activity is to achieve TGCP third party gateway compliancy on the CS2K.

This activity describes the necessary changes on the Core, GWC, and Call Server 2000 Manager (CS2M) to support ISUP IT, ISUP ATC, MF OP, and MF ES trunk signaling and associated services on a TGCP MG. External signaling transparency is provided for the ISUP and MF trunks configured on a GWC. Additionally, limited service transparency is provided as described in this document. The Core, GWC, and CS2M changes are provided as part of the SN07 software release.

Figure 1 IP Cable Network Configuration



Operator and 911 call *originations* are supported for agents configured on the following MG types:

- Multimedia Terminal Adapter (MTA) line MGs (line agents)

Refer to the solutions specifications for Integrated Access Cable for the complete list of line MGs supported in the SN07 release.

Operator and 911 call originations are **not** supported with MGs other than those listed above. However, there are service interactions that may result in the conferencing or transfer of an OP or ES trunk into a call with an agent other

than those listed above. This activity supports interoperability with the following agent types when a service interaction[1] results in a connection with either an OP or ES trunk:

- Dynamic Packet Trunk (DPT)
- ISUP trunk
- PRI trunk
- line

Interworking between TGCP MGs and the Universal Audio Server (UAS) is supported for providing media services such as voice announcements.

97.3 Functional Description

97.3.1 Operator Services Interconnection

Interconnection from the CS2K EO to a LEC operator switch is provided using MF OP trunk types.

Traditional Bell and Modified Operator Services Signaling (MOSS) are supported. Both signaling types provide two stage signaling:

	stage 1	**stage 2**
Traditional Bell	KP+called number+ST/STP/ST2P/ST3P	KP+I[a]+7 digit ANI+ST
Modified OSS	KP+called number+ST/STP/ST2P/ST3P	KP+II+7 digit ANI+ST/ STP[b]

a. A single information (I) digit is provided with Traditional Bell, two information (II) digits with MOSS.
b. ST is signaled for LEC call completions. STP is signaled for IEC call completions and is provided for completeness.

To configure an OP trunk for Traditional Bell signaling, field EA in table TRKGRP must be provisioned as ‘N’. To configure an OP trunk for MOSS signaling, fields EA and EAOSS must be provisioned as ‘Y’ and ‘N’ in table TRKGRP respectively.

The capabilities listed below are supported by this activity. For these capabilities, transparency is provided with the legacy switching system:

- LEC interconnection
- Traditional Bell signaling

[1]Examples of service interactions include, but are not limited to, three-way calling and call transfer. Call forwarding is excluded. Call forwarding to an OP or ES trunk is not supported.

- MOSS
- Busy Line Verification (BLV)
- Operator Barge-In (BI)
- Operator Ringback
- Operator Recall
- Outgoing OP trunk
- Incoming OP trunk support for BLV and BI
- Hold types of Term Hold and No Hold
- MF signaling
- Reversal ANI request type
- Flexible ANI (FANI) digits - applies to MOSS only
- Intercept calls

The key ***exclusions*** for this activity are listed below. For a complete list of restrictions and limitations, refer to section "97.6 Limitations and restrictions" on page 987.

- Coin control signals
- DP and DTMF[1] address signaling
- Exchange Access Operator Services Signaling (EAOSS)
- 2-way OP trunks

Table control restrictions are added by this activity to enforce the SN07 restrictions for MF OP trunks. Refer to the Configuration customer facing section of this document for more information on these restrictions.

97.3.2 Emergency Services Interconnection

Interconnection from the CS2K EO to an E911 tandem switch is provided using MF ES or MF OP trunk types. In SN07, only an *outgoing* MF ES trunk type or an *outgoing* MF OP trunk type is supported. For call completions from the E911 tandem switch back to the CS2K EO, Signaling System Number 7 (SS7) trunks must be configured.

Two stage Traditional Bell signaling is supported on the OP trunk type as described in section 97.3.1 on page 975. Two stage Traditional Bell signaling is supported on the ES trunk type, providing the called number (i.e. 911) and Automatic Number Identification (ANI) digits to the E911 tandem switch as follows:

[1]Restriction applies to DTMF signaling of the called and ANI address digits. DTMF signaling related to pressing keys on the originating line's keypad is supported.

	stage 1	stage 2
Traditional Bell	KP+911+ST	KP+I+7 digit ANI+ST

The capabilities listed below are supported by this activity for both the OP and ES trunk types (unless noted otherwise). For these capabilities, transparency is provided with the legacy switching system:

- E911 tandem interconnection
- Ringback
- Outgoing ES and outgoing OP trunk [only]
- Hold type of Term Hold
- MF signaling
- Reversal ANI request type

In addition to the list above, ES trunk types provide specific capabilities that are controlled through provisioning in table TRKGRP. The following TRKGRP capabilities are also supported by this activity for the ES trunk type:

- Audible Ringing:

  Field AUDRING specifies whether audible ringing should be applied to the originator. The values Y and N are supported by this activity.

- Automatic Number Identification (ANI) Type:

  Field ANI specifies what type of outpulsing to provide on the ES trunk. Only a value of “ANISPILL” is supported by this activity. “ANISPILL” specifies the called digits (i.e. 911) should be outpulsed followed by the ANI digits.

- Switch Hook Status:

  Field SWST specifies the action taken when the switch detects the originating subscriber has gone onhook. Only a value of “DC” is supported by this activity. “DC” provides an onhook signal towards the E911 tandem when the originating subscriber goes onhook.

- Calling Line Identification:

  Field CLI specifies whether CLI logs should be generated by the switch. The values Y and N are supported by this activity.

- Abandon Hold Time:

  Field ABNHLDTM ensures ANI outpulsing completes in the event the calling party goes onhook prior to the completion of outpulsing. A timer value, in seconds, is specified. All timer values are supported by this activity.

- Special Billing Directory Number:

  Field SPBDN controls whether to signal the calling number or special billing number as the ANI digits for line originations. The values Y and N are supported by this activity for this field.

The key ***exclusions*** for this activity are listed below. For a complete list of restrictions and limitations, refer to section "97.6 Limitations and restrictions" on page 987.

- B911 interconnection
- DP and DTMF[1] address signaling
- Incoming and 2-way ES trunks and OP trunks

Table control restrictions are added by this activity to enforce the SN07 restrictions for MF ES trunks. Refer to the Configuration customer facing section of this document for more information on these restrictions.

97.3.3 ISUP interconnection to PSTN

Interconnection from the CS2K EO to the PSTN is provided using ISUP IT or ISUP ATC trunk types.

The key ***exclusions*** for this activity are listed below. For a complete list of restrictions and limitations, refer to section "97.6 Limitations and restrictions" on page 987.

- Digit collection on ISUP trunks

97.3.4 Provisioning

The provisioning in Succession CS2K is distributed among several interfaces:

- the CS2M is used to provision GWC nodes, register MGs with GWCs, and bulk provision endpoints (i.e., by carrier);
- the CS2K core can be used to provision GWC node data and trunk related data; and
- OSSGate can also be used to provision trunk related data, register MGs with GWCs, and bulk provision endpoints by carrier.

97.3.4.1 GWC Node Provisioning

The CS2M is used to provision trunking GWC nodes with TGCP ISUP and MF trunks. The provisioning of the GWC includes:

- updating table SERVRINV on the CS2K core;

[1]Restriction applies to DTMF signaling of the called and ANI address digits. DTMF signaling related to pressing keys on the originating line's keypad is supported.

- configuring TGCP MGs on the GWC; and
- provisioning carriers/endpoints on the GWC.

97.3.4.1.1 New GWC Exec Lineup

Upon adding a GWC node, table SERVRINV is updated with the GWC node data including node number, tone data, and exec line-up data. A new exec line-up, GWCABEX, is created for the GWC. The new exec line-up is provisionable in table SERVRINV and applies to a term type of ABTRK. This exec line-up must be provisioned in table SERVRINV for GWCs that support MF OP and/or ES trunks.

Refer to the Configuration customer facing section of this document for further information on the new exec line-up.

The CS2M interface for configuring GWC nodes allows the selection of the GWCABEX exec line-up for TRUNKNA (N.A. trunking) GWCs. Refer to the Configuration customer facing section of this document for further information on the CS2M.

97.3.4.1.2 Configuring TGCP MGs

TGCP MGs are registered with a GWC via the CS2M. For this activity, the CS2M interface for associating an MG with a GWC is expanded to include the TGCP protocol type and a new gateway profile name.

Refer to the Configuration customer facing section of this document for further information on the CS2M.

97.3.4.1.3 GWC Endpoint Provisioning

The CS2M provides the capability to provision endpoints of a GWC on a carrier basis (i.e., 24 or 31 endpoints). The endpoints on a GWC must be provisioned prior to adding the tuple entries in table TRKMEM. The CS2M provides a list of terminal identifiers which must be entered in the tuple for table TRKMEM.

For GWCs supporting TGCP MGs, CS2M permits provisioning carriers of 24 endpoints at a time. The carrier naming convention follows the TGCP convention outlined below.

TGCP Endpoint Naming Convention
The TGCP endpoint naming convention follows the standards proposed in the PKT-SP-TGCP-I05-030728 TGCP Specification.The format supports a DS-0 channel endpoint type on a trunking gateway:

- **ds/<unit-type1>-<unit #>/<unit-type2>-<unit #>/.../<channel #>** where

— **<unit-type>** is defined to be one of “s”, “su”, “oc3”, “ds3”, “e3”, “ds2”, “e2”, “ds1”, and “e1”;

— **<unit #>** is a decimal value referring to the particular instance of <unit-type>;

— **<channel #>** is a decimal value indicating the channel number at the lowest level in the hierarchy (e.g., DS-0); and

— **ds** is fixed, identifying the endpoint naming scheme.

For SN07, the CS2M and GWC support TGCP MGs with DS1 interfaces, OC3 interfaces containing channelized DS3 and DS1 levels, and DS3 interfaces with channelized DS1 levels as defined in Table 1, “TGCP MG interfaces and Endpoint Naming” below.

Table 1 TGCP MG interfaces and Endpoint Naming

TGCP MG Interface	Endpoint Naming Convention
DS1 interface	ds/ds1-#/#
OC3 interface with DS3 and DS1 levels	ds/oc3-#/ds3-#/ds1-#/#
DS3 interface with DS1 level within a logical processor (or slot)	ds/s-#/ds3-#/ds1-#/#
DS3 interface without DS1 framing	ds/s-#/ds3-#/#

Refer to the Configuration customer facing section of this document for further information on the CS2M.

97.3.4.2 Trunk Group Provisioning

GWC ISUP and MF trunk related data is provisioned on the CS2K core using the same data tables as for legacy TDM trunks, namely tables CLLI, TRKGRP, TRKSGRP, TRKOPTS, and TRKMEM (ISUP trunks also require tables ISUPDEST and C7TRKMEM to be provisioned). Additionally, a new option is added in table TRKOPTS which must be assigned to OP and ES trunks groups provisioned on a GWC.

When provisioning an MF trunk group on a GWC, there are no restrictions regarding the distribution of the trunk members. An MF trunk group may be configured with trunk members spanning one or more GWCs or spanning one or more MGs. The trunk group can consist of any number of channels on a DS1 (e.g. 1, 5 or 24 channels).

MF trunk groups consisting of trunk members distributed across different peripheral types, such as a GWC and DTC, are ***not*** supported.

There are no restrictions regarding provisioning ISUP trunk groups on a GWC. Hybrid ISUP trunk groups are supported.

ISUP and MF trunk groups on the same GWC are supported. ISUP and MF trunk groups on the same MG are supported (the MG vendor is responsible for supporting ISUP and MF trunk groups on the same MG).

97.3.4.2.1 Table TRKOPTS

A new trunk group option, GWCPTSTK, is added in table TRKOPTS. This option identifies PTS packet trunks that provide connectivity between the packet network and the PSTN. Option GWCPTSTK must be provisioned against the MF OP or ES trunk group CLLI ***after*** provisioning table TRKGRP and ***prior*** to adding trunk members in table TRKMEM.

The GWCPTSTK option is used to restrict trunk group, subgroup, and member capabilities incompatible with GWC PTS trunks. This option cannot be added to a trunk group with the trunk group and subgroup restrictions listed in “97.6 Limitations and restrictions” on page 987.

This option can not be added to a trunk group that has pre-existing entries in table TRKMEM[1]. Additionally, this option can not be removed until all entries in table TRKMEM have been deleted.

The GWCPTSTK option contains a single sub-option, PRELOADANI. This sub-option identifies PTS packet trunk groups which support a call model that allows the ANI digits to be sent from the Core to the GWC without receiving an ANI request from the far-end. The MG is responsible for handling the ANI request and responding with the ANI digits stream.

Refer to the Configuration customer facing section of this document for further information on the new trunk group option.

97.3.4.2.2 Table TRKGRP

The tuple entry in table TRKGRP for ISUP IT, ISUP ATC, MF OP, and MF ES trunks remains unchanged. However, restrictions are added to table TRKGRP to prevent the activation of capabilities not supported on GWC MF trunks in the SN07 release. Refer to section “97.6 Limitations and restrictions” on page 987 and the Configuration customer facing section of this document for further information.

97.3.4.2.3 Table TRKSGRP

With an IP network configuration, the responsibility of providing low-level MF signaling requirements is delegated to the MG (e.g., A/B bit transition). As

[1]This can occur only if an attempt is made to add option GWCPTSTK to a trunk group with members on a peripheral type other than a GWC, such as a DTC.

a result, data currently provisioned in table TRKSGRP is not applicable to OP and ES trunks configured on a GWC. Specifically, the IDGTIME and TRKGRDTM fields in table TRKSGRP are not used by the CS2K. The MG is expected to comply with GR-505 and GR-506 regarding MF timings. Refer to the MG provisioning guidelines for further information related to administering this data.

Restrictions are added to table TRKSGRP to prevent the activation of capabilities not supported on GWC MF trunks in the SN07 release. Refer to section "97.6 Limitations and restrictions" on page 987 and the Configuration customer facing section of this document for further information.

97.3.4.2.4 Table TRKMEM

The tuple entry in table TRKMEM for a GWC peripheral type requires a node number and terminal number be entered[1]. The terminal numbers are obtained when the endpoints are provisioned on the GWC using the CS2M. Endpoint provisioning must be completed prior to provisioning table TRKMEM. Refer to section "97.3.4.1.3 GWC Endpoint Provisioning" for further information.

The option GWCPTSTK must be provisioned in table TRKOPTS prior to adding MF OP or ES trunk members in table TRKMEM. Table control for table TRKMEM enforces this restriction. Additionally, if option GWCPTSTK exists on a trunk group, table control disallows the addition of trunk members on peripheral types other than a GWC, such as a DTC.

Refer to the Configuration customer facing section of this document for further information on the table TRKMEM restrictions.

97.3.4.3 OSSGate

OSSGate provides a machine interface for provisioning components within Succession. The main functionality of OSSGate is to act as a gateway to the Node, Carrier, Trunk, and Line provisioning applications and the Trunk Maintenance application.

OSSGate supports provisioning of tables TRKSGRP and TRKMEM for ISUP and MF trunks on GWCs. OSSGate is subject to the provisioning restrictions described in sections "97.3.4.2.3 Table TRKSGRP" on page 981 and "97.3.4.2.4 Table TRKMEM" on page 982.

For carrier provisioning, OSSGate supports the naming convention of TGCP described in section "97.3.4.1.3 GWC Endpoint Provisioning" on page 979.

Refer to the Configuration customer facing section of this document for further information on OSSGate.

[1]Changes to table TRKMEM to support a GWC PMTYPE were provided in a previous Succession release.

97.3.5 Echo Cancellation

Echo cancellation must be applied from the TDM side of the network. This is because any delay that enters the packet network can become too long for the echo cancellers on the MGs to handle.

In the SN07 release for OP and ES trunk groups, echo cancellation is always performed by the MG. With TGCP, the MG always performs echo cancellation by default.

Table control restrictions are added to table TRKSGRP to reflect that external echo cancellation is always applied by the MG. Table control enforces field ESUPR be provisioned as "N" and field ECSTAT be provisioned as either "EXTERNAL" or "INTERNAL". ECSTAT set to "INTERNAL" indicates that the echo cancellation is performed in the MG; ECSTAT set to "EXTERNAL" indicates that the echo cancellation is performed on the TDM trunk. See NTP NN10068-461 "Upgrading the GWC" for further details.

For GWC ISUP trunks in SN07, echo cancellation is performed by the MG based on trunk data (i.e., ECSTAT field in table TRKSGRP) unless the echo cancellation info in the ISUP messages (e.g., IAM, ACM, CPG) indicate that it has already been performed between the CS2K and the source of the echo.

97.3.6 TGCP Package Requirements

The TGCP packages used to support ISUP, MF OP, and MF ES trunks in the SN07 release include:

- ISUP Trunk (IT) Package
- MF FGD Operator Services (MO) Package
- MF Terminating Protocol (MT) Package

97.3.7 Trunk Maintenance

In the IP network architecture, the MG owns the physical hardware. The DS1 carrier is no longer owned or maintained by the CS2K. As a result, the maintenance behavior of ISUP and MF trunks configured on a GWC is changed.

97.3.7.1 CS2K Trunk States

The trunk state of carrier failure (CFL) has a new definition for trunks configured on a GWC. The CFL trunk state indicates the circuit on the MG is out-of-service. The CS2K places a trunk into the CFL state when a TGCP RestartInProgress (RSIP) message with a RestartMethod of "forced" is received from the MG. Recovery from the CFL state back to an IDLE state only occurs if the MG notifies the CS2K the circuit is back in service. The MG

notifies the CS2K a circuit is back in service by sending an RSIP with a RestartMethod of “restart”.

In the packet cable architecture, the Media Gateway Controller (MGC) does not have knowledge of the reason the MG has taken one or more circuits out of service. There could be a card failure, carrier failure or a maintenance action being performed on the circuit by the MG. The reason for the removal of a circuit from service is beyond the scope of the CS2K.

The CS2K supports receiving an RSIP on an individual endpoint, carrier, or gateway basis. If a carrier failure occurs on the MG, the MG may send twenty-four individual RSIP messages or one RSIP message on the carrier to the CS2K.

97.3.7.2 Trunk Test Position (TTP)

Limited maintenance is supported at the TTP level of the MAP for TGCP MF trunks provisioned on a GWC. Restrictions also apply to the MANUAL, MONITOR and DATA levels of the MAP (accessed through the “Level_” command on the TTP). Refer to Table 2 for a summary of the commands supported and not supported in the SN07 release.

Table 2 TTP Level Command Summary

Level	Supported Commands	Unsupported Commands
TTP	Quit, BSY[a] (with optional states INB, MB), RTS, BSY ALL, FRIs, Post_, Hold, NEXT, Level_, *TST*, *Ckt_*	BSY[b] (with optional state SB), **SEIZE**, **CktInfo**, CktLoc, TrnslVf_, StkSdr_, Pads
MONITOR[c]	Quit, Post_, BSY, RTS, Hold, NEXT, FRIs, *TST*, *MonTalk*,	MONPOST, MONLINK, **CktMon**, **CPos_**, **RLS**
MANUAL	Quit, Post_, BSY, RTS, Hold, NEXT, *LOSS*, *TGEN*, *TST*, *Noise*, *TDET*, *Hset*	**OP_**, Jack_, **SGNL**, CallTrf, **RLS**
DATA	Quit, Post_, BSY, RTS, Hold, NEXT, FRIs, *BERT_*	**Seize**, **BTerm_**, **RLS**

a. BSY at all levels is supported only with optional states INB and MB.
b. BSY with optional state SB is blocked at all levels.
c. MONITOR level is inaccessible is if GWC MF trunk is posted and no InterWorking (IW) bridges are available.

Several of the unsupported commands in Table 2 are prevented by existing maintenance restrictions added in a prior release. This activity implements only those restrictions required above the existing maintenance restrictions (shown in **bold** text in the table), e.g., the outpulse command (**OP_**) is not supported at the MANUAL level of the MAP.

Several supported commands (shown in *italics* text in the table) are dependent on the availability of certain components in the IAC solution. Test line tests of trunk connections (*TST* command at the TTP, MONITOR and MANUAL levels) require appropriate test line facilities on the Audio Controller[1]. The other TTP commands require Interworking (IW) bridges to provide the necessary functionality. These hardware dependencies also apply for manual test line trunk tests performed from the Automated Test Trunk (ATT) level of the MAP.

Maintenance support at the TTP MAP level for TGCP ISUP trunks is subject to the same set of supported/unsupported commands listed in Table 2, with the exception of the MF restricted commands (shown in **bold** text) which are supported for ISUP. In addition, any existing restrictions at the C7TTP MAP level for GWC ISUP trunks also apply to TGCP ISUP trunks.

Refer to the Configuration customer facing section of this document for further information on the restrictions added by this activity.

97.3.7.3 Trunk Maintenance Manager (TMM)

Trunk maintenance for ISUP and MF trunks is supported through TMM. TMM is an existing trunk maintenance application which uses an interface provided by CS2M. The following TMM maintenance commands are supported:

- POST by gateway name, trunk group/CLLI, or carrier;
- BSY, BSY INB, RTS, FRLS, and Query Endpoint State (QES) on posted set.

The Post by Carrier supports the carrier naming convention of TGCP described in section “97.3.4.1.3 GWC Endpoint Provisioning” on page 979.

97.3.7.4 Trunk Audits

The trunk audits for PTS trunks on legacy peripherals are changed as necessary to align with the new behavior for PTS trunks configured on a GWC. Automatic recovery actions are no longer performed on PTS trunks in CFL state. Placement into and out of the CFL state is strictly controlled by notification from the MG (as discussed in section “97.3.7.1 CS2K Trunk States” on page 983). Enhancements are provided to audits both on the core and GWC.

Trunk audits of GWC ISUP trunks was added in a prior Succession release.

[1]The availability of test line facilities on the Audio Controller are indicated by the office parameter EXTERNAL_GATEWAY_TEST_LINES in table OFCVAR on the core.

97.3.8 Initialization

When the GWC is initially brought into service it awaits notification from the MG that it is inservice and ready to process calls. The trunks transitions from a PMB state to a CFL state[1] at this time. Upon receipt of an RSIP (with a RestartMethod of "restart") on the gateway from the MG indicating the MG is inservice, the CS2K begins the process of bringing all CFL trunks into an inservice state. This process includes setting the trunk state to IDL and sending an acknowledgement of the RSIP to the MG. The MG begins scanning for seizures (e.g., remote make busy, call setups) from the far-end (note that seizure-state changing events are persistent in TGCP).

Note that following a restart if the MG has a number of endpoints (e.g., channels) out of service, the GWC/CS2K is unaware of this.

The GWC is also capable of handling RSIPs on a trunk/endpoint basis. However, to minimize the number of messages generated, it is recommended the MG send an RSIP on the gateway when coming inservice.

97.3.9 Swacts and Restarts

This activity provides support for CS2K core restarts, CS2K core swacts, GWC node restarts, and GWC swacts.

For core reload and cold restarts or GWC cold swact and node restarts, all MF calls on the GWC(s) are taken down. The CS2K initiates the necessary cleanup of resources on the MG using TGCP signaling. The same behavior applies to warm restarts on the core and warm swacts on the GWC with one exception, stable MF calls on the GWC(s) remain active. ISUP and MF calls in the answered state are considered stable on the CS2K core.

This activity also supports norestart swact, restartswact and abortswact on the CS2K core.

97.3.10 IP Network loss between the GWC and MG

The GWC monitors its connection to the MG by sending a heartbeat message (in the form of an AuditEndpoint (AUEP) message wildcarded on the gateway) every 10 seconds in the absence of any other messaging between the GWC and MG. A heartbeat loss is detected if after 40 seconds no acknowledgement to the heartbeat message is received by the GWC from the MG.

Upon detecting heartbeat loss, the GWC transitions the trunks on the MG to a CFL state and begins sending heartbeat messages every 2 minutes. During this period, if the GWC receives any message from the MG, the GWC/CS2K

[1]Note trunks in the MB or INB state are unaffected. Trunks remain in these states until manually brought into service via the TTP or TMM.

begins the process of trunk recovery by: deleting all connections on the MG; and re-starting the regular heartbeat message with the MG.

97.3.11 QoS Reporting

QoS reporting on the GWC is supported to measure voice quality. The TGCP end-of-connection statistics are reported by the MG to the GWC. The GWC collects and transfers the end-of-connection statistics to a QoS Collector Application (QCA) server, where they are correlated with the billing records.

97.3.12 Accounting

Transparency is provided with the Automatic Message Accounting (AMA) records generated for the legacy billing system. No changes are required by this activity.

97.3.13 Fault Management

Transparency is provided with the trunk related Operational Measurements (OM), Logs and Alarms supported for the legacy OA&M system. No changes are required by this activity.

97.4 Hardware Requirements or Dependencies

This activity has the following hardware dependencies:

- The MG functionality is provided by a third party gateway vendor supporting TGCP as described in the PKT-SP-TGCP-I05-030728 TGCP specification.
- Test Line tests of TGCP MG trunk connections to the PSTN require an Audio Controller (AC), an UAS, and a SAGE 945RTS testhead unit to perform tests.

97.5 Software Requirements or Dependencies

This activity enhances the CS2K core, GWC, and CS2M to support a TGCP MG hosting ISUP IT, ISUP ATC, MF OP, and MF ES trunks as described in the previous sections. The SN07 software load is required on the CS2K core. The GC070 software load is required in the GWC. The PNM07 software load is required on the CS2M.

97.6 Limitations and restrictions

The TGCP PKT-SP-TGCP-I05-030728 TGCP specification limits support of MF trunk interconnection to a LEC Access Tandem. Interconnection to an Inter-Exchange Carrier (IEC) operator system is not supported.

The CS2K supports manual busying (ManBusy[1]) of ISUP and MF trunks configured on a GWC. The MO package of the TGCP PKT-SP-TGCP-I05-030728 TGCP specification does not support sending a busy signal from the GWC to the MG. When a ManBusy is performed on MF trunks hosted on a TGCP MG, the trunks will go CFL.

IAC (hybrid) configurations involving TDM elements are not supported in SN07.

IAC configurations involving APG components are not supported in SN07. Without APGs, limited support of DPTs is provided: services on DPTs requiring digit collection or applying tones are not supported.

The following limitations and restrictions apply to *both* MF OP and MF ES trunks:

- Hybrid trunk groups are not supported. A trunk group containing members on a GWC can not include members on any other legacy peripheral type (e.g. DTC).
- MF trunks are not supported on a GWC with lines, DPTs, or ACs.
- Test trunk calls are not supported.
- The outpulse (OP_) command at the MANUAL level of MAPCI is not supported.
- Field OPULSTYP in table TRKSGRP is restricted to ‘MF’.
- Only wink start trunks are supported. Field OSTARTSG in table TRKSGRP is restricted to ‘WK’.
- Echo cancellation is always provided by the MG. Field ESUPR is restricted to ‘N’. Field ECSTAT in table TRKSGRP is restricted to ‘EXTERNAL’ or ‘INTERNAL’.
- Coin control signals are not supported. A coin control signal, if sent from the far-end, will be ignored. Field CCONT in table TRKSGRP is restricted to ‘NO’. Although coin control is not applicable to ES trunks, field CCONT is still restricted to ‘NO’.
- Only Ringback signal of ‘MW’ is supported in the CS2K. Field RNGBCK in table TRKSGRP is restricted to ‘NO’ or ‘MW’.

  The MG is responsible for handling the ringback signal sent from the far-end. The CS2K will process all ringback requests as a ‘MW’ ringback request.
- This activity supports operator and 911 *originations* **only** for **line** MGs approved for deployment with the Integrated Access Cable solutions.

[1]i.e., BSY MB from the TTP MAP level

Operator and 911 originations on PRI, ISUP, and DPT trunks are not supported.

Service interactions may result in the conferencing or transfer of an OP or ES trunk into a call. This activity supports interoperability with the following agent types when a service interaction[1] results in a connection with either an OP or ES trunk:

— DPT

— ISUP trunk

— PRI trunk

— line

- Interworking with legacy peripherals is not supported.
- Call forwarding to OP and ES trunks is not supported.

The following limitations and restrictions apply to *MF OP trunks only*:

- Exchange Access Operator Services Signaling (EAOSS) is not supported. Field EAOSS in table TRKGRP is restricted to 'N'.
- Hold type of joint hold is not supported. Field HOLDTYPE in table TRKGRP is restricted to 'TERMHOLD' or "NOHOLD".
- Only ANI request types of reversal is supported. Field ANI_REQUEST in table TRKGRP is restricted to 'REV'.

The following limitations and restrictions apply to *MF ES trunks only*:

- B911 interconnection is not supported. An ES trunk group is supported for E911 Tandem interconnection *only*.
- Incoming and two-way trunks are not supported. Field DIR in tables TRKGRP and TRKSGRP is restricted to 'OG'.
- Field ANI in table TRKGRP is restricted to 'ANISPILL'. The value 'ANISPILL' signals the dialed digits (i.e., 911) followed by the ANI digits. The values 'NOANI' and 'OUTPULSE' are not supported.
- The switch hook status field, SWST, in table TRKGRP is restricted to 'DC'. The value 'DC' signals an onhook towards the E911 tandem when the originating subscriber goes onhook. The values 'AC' and 'ADC' are not supported.

  Note the switch hook status tone field, SWSTTN, in table TRKGRP is only applicable when field SWST is set to 'AC' or 'ADC'. Therefore, field SWSTTN is ignored.
- The forced disconnect timing field, FDISCTIM, in table TRKGRP is restricted to '0'. Forced disconnect timing is not supported.

[1]Examples of service interactions include, but are not limited to, three-way calling and call transfer. Call forwarding is excluded. Call forwarding to an OP or ES trunk is not supported.

- The disconnect tone type field, DISCTON, in table TRKGRP is specific to B911. This field is not supported. The value provisioned for this field is ignored.
- The integrity tone time field, INTTT, in table TRKGRP is specific to B911. This field is not supported. The value provisioned for this field is ignored.
- Field BILLDN in table TRKGRP is not supported. This field is PRI specific and 911 originations on PRI trunks are not supported. The value provisioned for this field is ignored.

The following limitations and restrictions apply to *both* ISUP IT and ATC trunks:

- feature interactions involving digit collection are not supported including, but not limited to:
  - — CFRA
  - — DISA
  - — AIN

97.7 Interactions

This activity supports interactions between ISUP IT, ISUP ATC, MF OP, and MF ES trunks and the following line based services:

- Three way calling
- Call Transfer
- Call Forwarding (all variations except CFRA)[1]
- Call Waiting

Transparency with the legacy DMS service set is provided for these services. The same service interactions and restrictions that exist with legacy MF OP and ES trunks also apply to MF OP and ES trunks configured on a GWC.

This activity supports interoperability with the following agent types when a service interaction, such as three way calling or call transfer, results in a connection with either an OP or ES trunk:

- DPT
- ISUP trunk
- PRI trunk
- line

[1]Call forwarding for operator and 911 is not supported in the legacy switching system. Attempts to call forward to operator or 911 is blocked by the switch software. CS2K is consistent with legacy and blocks attempts to call forward.

97.8 Applicable customer facing sections

Fault Management

- Logs __N/A_
- Alarms __N/A_

Configuration

- Data Schema ___X__
- User Interface ___X__
- Element Management __N/A_
- Security __N/A_
- Service Order __N/A_
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

97.9 Glossary

Term	Description
AIN	Advanced Intelligent Network
AMA	Automatic Message Accounting
ANI	Automatic Number Identification
APG	Anchor Packet Gateway
ATT	Automated Test Trunk
AUEP	AuditEndpoint
B911	Basic 911
BI	Barge-In
BLV	Busy Line Verification
CAS	Channel Associated Signaling
CFL	Carrier Failure
CFRA	Call Forward Remote Access
CLI	Calling Line Identification

Term	Description
CMTS	Cable Modem Termination System
CS2K	Call Server 2000
CS2M	Call Server 2000 Manager
DISA	Direct Inward Service Access
DMS	Digital Multiplex System
DN	Directory Number
DP	Dial Pulse
DPT	Dynamic Packet Trunk
DTC	Digital Trunk Controller
E911	Emergency 911
EAOSS	Exchange Access Operator Services Signaling
EO	End Office
ES	Emergency Service
FGC	Feature Group C
GWC	Gateway Controller
HFC	Hybrid Fiber Coax
I	Information (I) digit
IAC	Integrated Access - Cable
IEC	Inter-Exchange Carrier
IETF	Internet Engineering Task Force
II	Information (II) digits
IP	Internet Protocol
ISUP	ISDN User Part
LEC	Local Exchange Carrier
MAP	Maintenance and Administration Position
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MOSS	Modified Operator Services Signaling

Term	Description
MTA	Multimedia Terminal Adapter
OM	Operational Measurement
OP	Operator
PPVM	Peripheral Processor Virtual Machine
PRI	Primary Rate Interface
PTS	Per Trunk Signaling
PSTN	Public Switched Telephone Network
QCA	QoS Collector Application
QoS	Quality of Service
RSIP	ReStartInProgress
SS7	Signaling System Number 7
TDM	Time Division Multiplex
TGCP	Trunking Gateway Control Protocol
TMM	Trunk Maintenance Manager
TTP	Trunk Test Position
UAS	Universal Audio Server

98: Functional Description (FN): A00003649

98.1 Feature name

SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core

98.2 Description

Many of Nortel's customers plan to migrate their existing ATM networks to IP networks in the near future. These customers perceive that IP networks might be cheaper to deploy than ATM networks, or that IP will become the end-user convergence protocol for developing new revenue-generating services.

By adding IP interfaces to the existing MG4K product, our customers will be able to migrate from an ATM network to an IP network simply by upgrading existing equipment. Thus the birth of MG4K-IP product.

The protocol chosen for communication between the MG4K-IP and the XA-Core via the IP network cloud is SCTP.

SCTP has been designed to overcome the limitations of TCP as well as supporting the extra requirements of PSTN signalling over IP networks. (Please refer to SCTP RFC for more details of TCP limitations as well as SCTP requirements.)

In short, SCTP offers:

- Acknowledged error-free non-duplicated transfer of user data
- Application-level segmentation to conform to discovered MTU size
- Sequenced delivery of user datagrams within multiple streams, with an option of order-of-arrival delivery for individual datagrams
- Optional multiplexing of user datagrams into SCTP datagrams, subject to MTU size restrictions
- Enhanced reliability through support of multi-homing at either or both ends of the association.

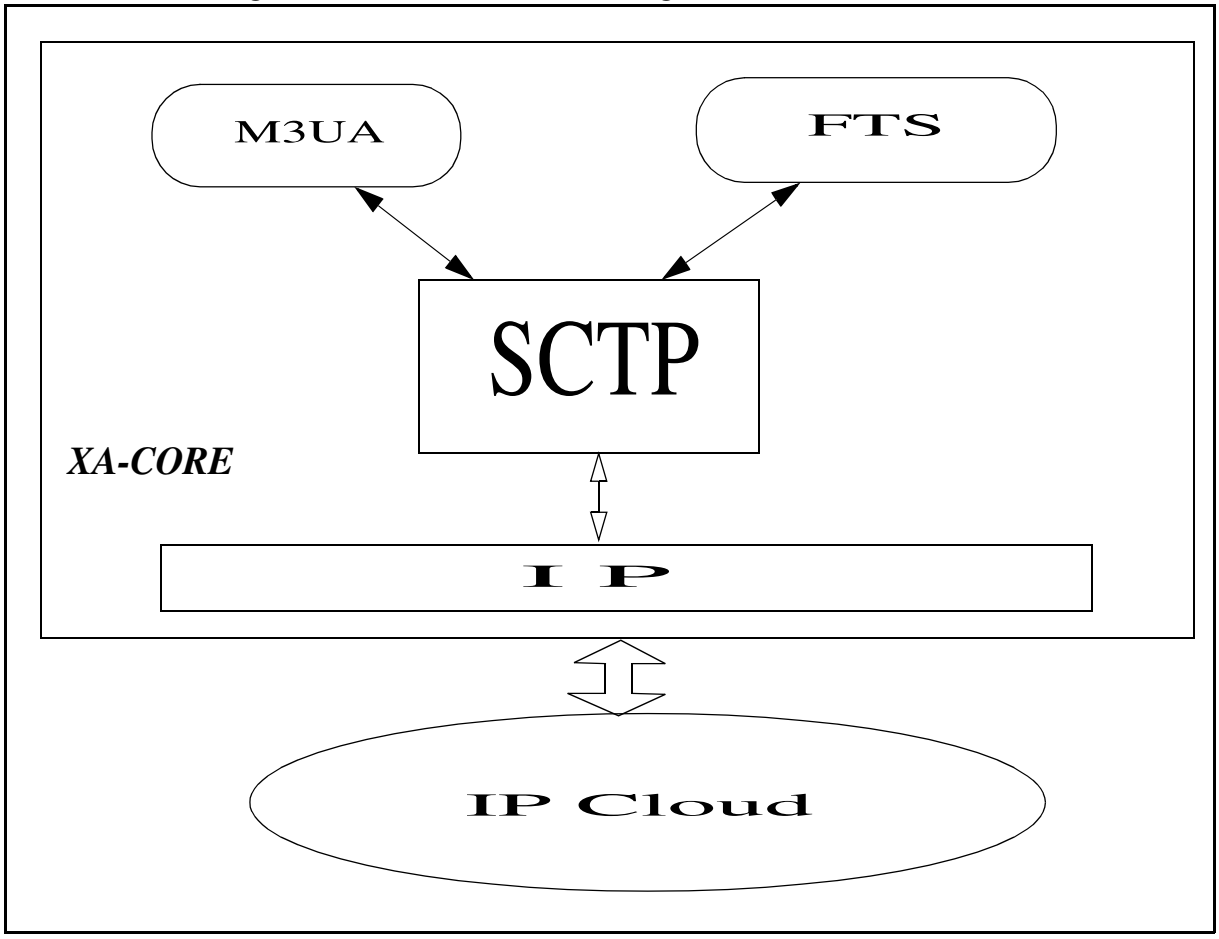
This feature aims at enhancing the existing SCTP framework on the XA-Core, implemented under feature A59023997, so as to

- achieve the desired messaging rate of 4500 msg/sec from the current 400 msg/sec. This will translate to supporting 30 MG4k-IPs

- improve the message transmission reliability as well as sustainability

The Figure 1 on page 995 shows the functional behaviour for SCTP

Figure 1 Functional Behavior Diagram



98.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies introduced by this feature

98.4 Software Requirements or Dependencies

Table 1 Project Requirements

#	**Requirement number and source document/version/page** **Requirement text**	**Critical** (R/S/D) **Compliant** (Y/N/C/P/Cnn)	**Comments**
1		R	
	Increase SCTP messaging rate from 400 msg/sec to 4500 msg/sec	Y	
2		R	
	Operate within the EN task timing restrictions with regards to latency and blocking	Y	This requirement came from the group responsible for EN task under which SCTP will run at message reception. This is an internal requirement
3		R	
	Add a new method in the Upper layer API - sctp_fast_send	Y	This requirement came from the IP-CCM group. This is also an internal requirement
4			

Compliant value definitions:

- Y – Element will be compliant upon feature completion.
- N – Element will not be compliant upon feature completion.
- C – Existing code currently compliant and will not be affected.
- P – Element will be partially compliant at feature completion.
- Cnn – Element conflicts with element number “nn”. The element that will be compliant will have value of “Y” for compliancy.

98.5 Limitations and restrictions

None

98.6 Interactions

SCTP is the transport layer protocol used by M3UA and CALEA. There will be no changes to the APIs for these applications

98.7 Applicable customer facing sections

Fault Management

- Logs _ N/A _
- Alarms _ N/A _

Configuration

- Data Schema _ N/A _
- User Interface _ N/A _
- Element Management _ N/A _
- Security _ N/A _
- Service Order _ N/A _
- Office Parameters _ N/A _

Accounting (includes AMA billing) _ N/A _

Performance (includes operational measurements) _ N/A _

98.8 Glossary

Term	Description
API	Application Protocol Interface
ATM	Asynchronous Transfer Mode
FTS	Frame Transport System
IP	Internet Protocol
PSTN	Public Switched Telephone Network
SCTP	Stream Control Transmission Protocol
TCP	Transmission Protocol

99: Functional Description (FN): A00003650

99.1 Feature name

A00003650: MG4K-IP Logs Core Component

99.2 Description

This feature provides logs for the MG4K-IP product in SN07. The log series MG4I is introduced by this activity. The following logs are supported:

- MG4I 501 - Stream Control Transmission Protocol (SCTP) IP Control Connection Maintenance (CCMT) Core connection state change
- MG4I 502 - SCTP IPCCM Peer connection state change
- MG4I 300 - Media Integrity Failure

The MG4I 501 and 502 logs are used by the IPCCM subsystem to generate logs to track the state transitions of SCTP connections from the MG4K-IP node to the core and peer nodes. The MG4I 300 is generated for problems reported by the corresponding subsystem in the CEM/GEM on the MG4K-IP node. However, the changes required in the CEM/GEM for these logs is to be implemented in SN08.

99.2.1 SCTP IP CCMT connection state change

The MG4I 501 log is generated for state change of the SCTP connection between the call server and the MG4K-IP node.

```
RTPH *** MG4I501 MAY02 22:04:48 800 INFO SCTP Core Conn State Change
      State Change From: ESTABLISHED To: CLOSED
      Reason : FAR END DISCONNECTED
      From Node : CORE (47.108.11.3:5050; Associd: 10)
         To Node : SMG4 6 (47.142.211.1:5050)
      Location: SPM 6 Type: SMG4 Fabric: IP
```

The MG4I 502 log is generated for state change of the SCTP connection between an MG4K-IP node and its peer node.

```
RTPH MG4I502 MAY02 22:04:48 800 INFO SCTP Peer Conn State Change
   State Change From: ESTABLISHED To: CLOSED
   Reason : FAR END DISCONNECTED
   From Node : SMG4 6 (47.108.11.3:5050; Associd: 10)
      To Node : SMG4 5 (47.142.211.1:5050)
   Location: SPM 6 Type: SMG4 Fabric: IP
```

99.2.2 Media Integrity Failure

The MG4I 300 log is generated for any integrity failure detected in the media path for a call.

```
RTPH MG4I300 SEP04 03:41:44 2801 TBL  Media Integrity Failure
      Call Type: G711
      Src IP: 47.108.11.3:5050 Dest IP:47.142.211.1:5050
      Description: RTCP Media Integrity Timer Expired
      Location: SPM 1    Type: SMG4    Fabric: IP
```

99.3 Hardware Requirements or Dependencies

This feature is specific to the MG4K-IP product line with associated hardware.

99.4 Software Requirements or Dependencies

No new software dependencies are introduced by this activity.

The MG4I 300 log is generated for problems reported by the corresponding subsystem in the CEM/GEM on the MG4K-IP node. However, the changes required in the CEM/GEM for these logs is to be implemented in SN08.

99.5 Limitations and restrictions

None.

99.6 Interactions

These logs are accessible through the LOGUTIL CI interface in SOS. The craftsperson can access the MG4K-IP specific logs as follows:
>logutil
>open MG4I
>back all

99.7 Applicable customer facing sections

Fault Management	
Logs	__X__
Alarms	_N/A_
Configuration	
Data Schema	_N/A_
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

99.8 Glossary

Term	Description
SCTP	Stream Control Transfer Protocol
CCMT	Control Connection Maintenance
IP	Internet Protocol
GEM	Gigabit Ethernet Module
CEM	Common Equipment Module
IPCCM	Internet Protocol Control Connection Maintenance
CI	Command Interface

100: Functional Description (FN): A00003651

100.1 Feature name

MG4K-IP XA-Core Support for IPCCM (IP Control Connection Management) & OAM (Operations Administration & Maintenance)

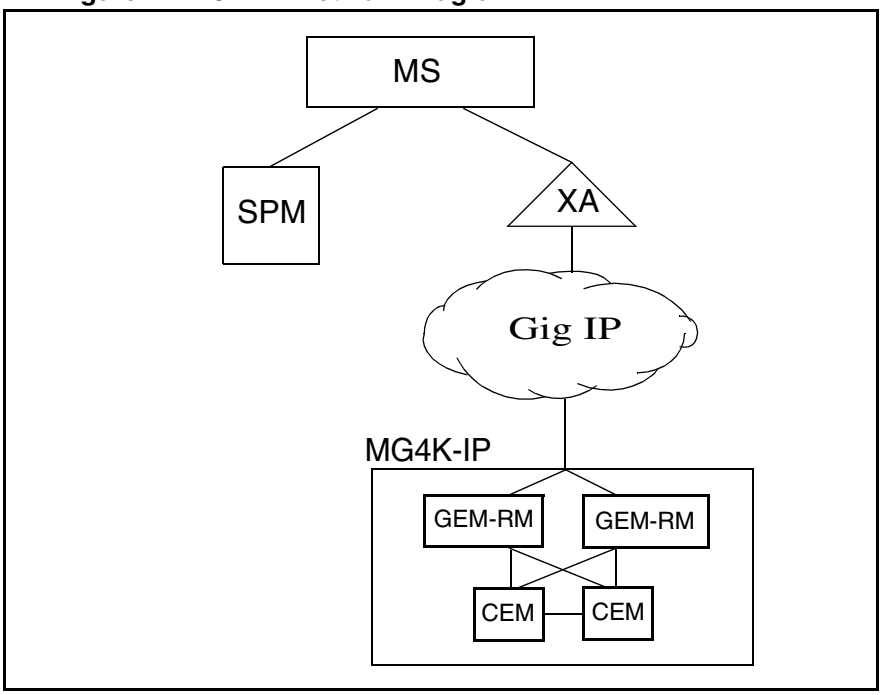
100.2 Description

This activity is a part of the set of SN07 activities associated with the MG4K-IP Program. This program provides the capability of IP connected MG4K gateways as part of the general Succession Voice-Over-Packet portfolio.

Within this document, the term MG4KIP refers to a node of type SPM, of class SMG4, or IW, which is connected to the XA-Core via a Gigabit Ethernet Network.

This activity's focus is on the MG4KIP "Data Link Management" and "Data Link OAM" aspects.

Figure 1 MG4KIP Network Diagram



100.3 Hardware requirements

No new hardware dependencies are introduced by this feature per se. This feature utilizes existing GEM-RM hardware (Product Equipment Code = NTLZ20BA) and other existing hardware associated with the MG4K platform.

100.4 Limitations and restrictions

In Succession Release SN08, a maximum of 30 IP-based MG4K nodes are supported in a given office.

100.5 Interactions

This feature provides the mechanism and interfaces for MAPCI-based management of the Xa-Core-To-MG4KIP (aka “core”) connections, and MG4IP-To-MG4KIP (aka “peer”) connections.

The maintenance paradigm is based directly on what exists today for ATM-based MG4K nodes, in order for the OAM interface for the nodes to be consistent, regardless of the network fabric type.

100.6 Logs (LG)

Not Applicable.

100.7 Data schema (DS)

Not Applicable.

100.8 Office parameters (OP)

Not Applicable.

100.9 Service orders (SO)

Not Applicable.

100.10 Alarms (AL)

Not Applicable.

100.11 Command interface (CI)

100.11.1 New/modified commands

Table 1 New or modified commands

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/MAP level name	MENU/NON-MENU /HIDDEN
IPCONN	New		SPMDIR/SPM	Menu
CORECONN	New		IPCONN/ IPCONN	Menu
BSY	New		CORECONN/ CORECONN	Menu
RTS	New		CORECONN/ CORECONN	Menu
PEERCONN	New		IPCONN/ IPCONN	Menu

This feature introduces 3 new map levels and 4 new subcommands. The 'IPCONN' map level is visible when posting any SPM at the 'PM' level. (This map level is consistent with the existing 'ATMCONN' map level which is also visible when posting any SPM from the PM level).

For any SPM which has GEM-RMs provisioned, selecting the IPCONN map level will provide access to the 'Coreconn' and 'Peerconn' MAP levels, for display and management of the core and peer connections respectively. This functionality is consistent with what exists today when selecting the ATMCONN map for SPMs which have ATM-RMs provisioned.

For more details, please refer to the CI section of this document.

100.12 Operational measurements (OM)

Not Applicable.

100.13 AMA/Billing information (AM)

Not Applicable.

100.14 Software optionality control (SOC)

Not Applicable.

100.15 Glossary

Term	Description

CEM	Common Equipment Module - the controlling module of the Spectrum platform
CIBINCOM	Command Interpreter Binary Command
FTS	Frame Transport System
GEM	Gigabit Ethernet Module
GTM	Generic Transport Mechanism - A messaging system between the core and an SPM RM built on top of MTS
INM	Integrated Node Maintenance
IP	Internet protocol
IPCCM	IP Control Connection Management
MAP, MAPCI	Maintenance and Administration Position (Command Interpreter) - a common user interface to the XA-Core
MG4K	Media Gateway 4000 - a Spectrum-based access gateway
MTS	Message Transport System
RM	Resource Module - a hardware component of SPM
SCTP	Stream Control Transport Protocol
SOTS	SPM OM Transport System - Provides an interface for OM transfer between the Core and the SPM

100.16 References

101: Functional Description (FN): A00003662

This ducument presents an overview of the software functionality to be deliverred in this feature. It also helps determine if customer documentation is required.

101.1 Feature name

Trimodal Call Server Bridge Maintenance.

101.2 Description

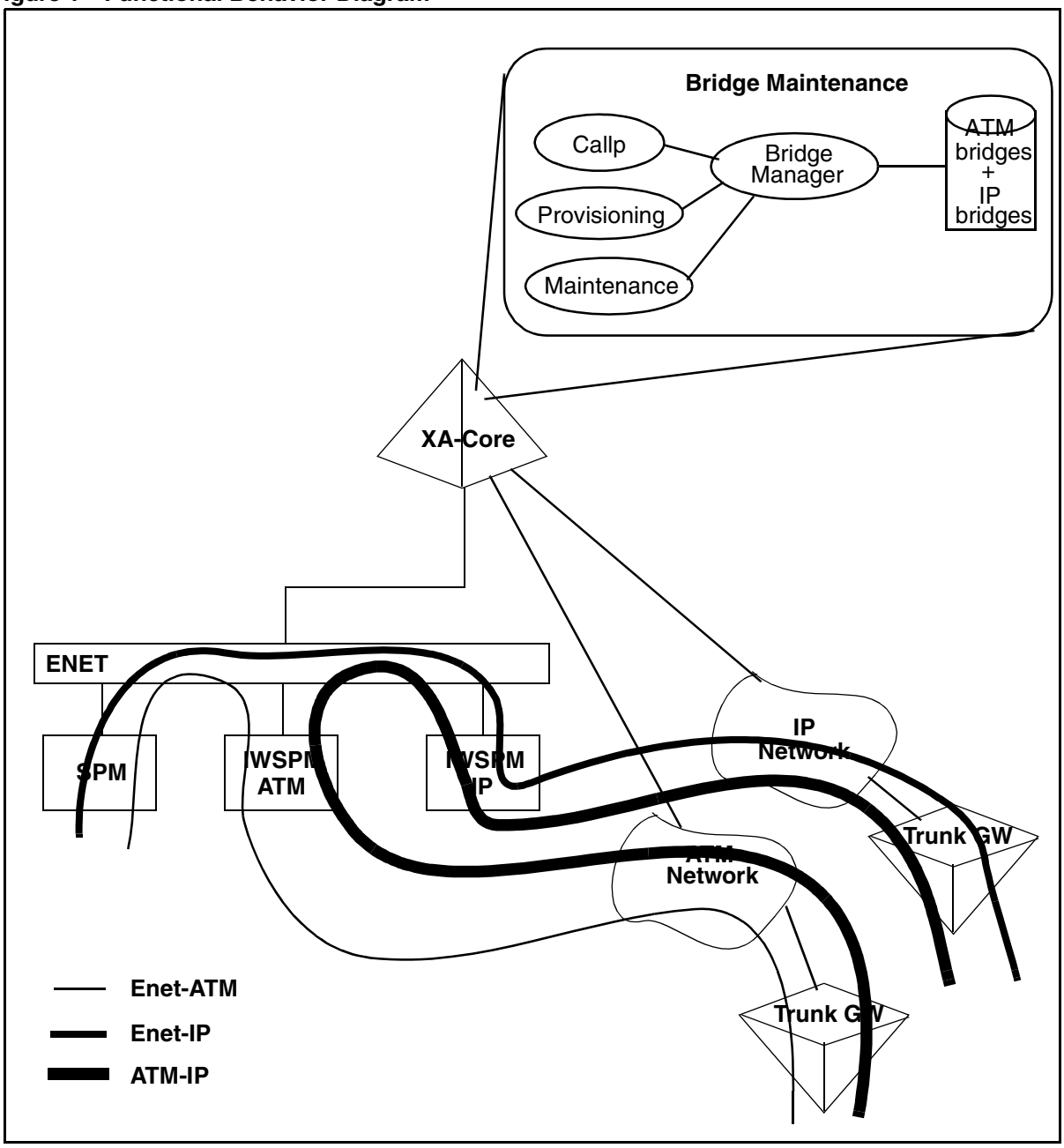
Currently, in SN06, the XA-Core can support only one packet bearer fabric, ATM or IP.

The Bridge Maintenance should be able to support multi bearer fabric Call Server configurations. In SN07, Tri-modal Call Server configurations will support ATM and IP as external bearer fabrics at the same time. Bridge Maintenance should be able to manage the bridges so that ENET-ATM, ENET-IP and ATM-IP connections can be realized.

To realize ATM to IP bridging, two bridges will be inserted in the call. One bridge provides the ENET-ATM connection and the other one provides the ENET-IP connection. These two bridges will then be connected at the ENET providing the ATM to IP end to end path. See Figure 1.

This feature does not cover the OM and logs impacts. The OMs and l;ogs work for the Bridge Manager area will be covered in feature A0003947 (Tri-modal Logs and OMs).

Figure 1 Functional Behavior Diagram



101.3 Hardware Requirements or Dependencies

N/A

101.4 Software Requirements or Dependencies

N/A

101.5 Limitations and restrictions

N/A

101.6 Interactions

N/A

101.7 Applicable customer facing sections

Fault Management

- Logs ___X__
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) ___X__

101.8 Glossary

Term	Description
IWSPM	InterWorking Spectrum Peripheral Module

102: Functional Description (FN): A00003667

102.1 Feature name

A00003667 - SESM NB Alarm Interface Changes required for OSS

Succession Element and Subelement Manager Northbound Alarm Interface Changes required for OSS

102.2 Description

This SN07 feature (A00003667 - SESM NB Alarm Interface Changes required for OSS) modifies some of the existing functionality in the SESM alarm system. Primarily, it refines and updates the CORBA interface to include data that enhances the usability of the alarm notifications. This includes a resynchronization mechanism, improved performance, and a change to the data passed to include additional alarm information.

The majority of these changes do not impact the customer as they are transparent to the user. The customer areas impacted include:

- SESM Alarm GUI - removal of acknowledge and de-acknowledge interface. This change is discussed in the configuration section.
- SESM Syslog Alarm Feed - this feed will be disabled by default as the primary northbound feed will be CORBA notifications to the IEMS. The resulting Nortel Standard or SCC2 logs should be identical to those generated in previous releases. This change is discussed in the configuration section.
- Change to alarm log generated when SESM cannot communicate with a managed device. Previously, the log was owned by the device, now it will be a SESM alarm and will be a major instead of a critical. This change is discussed in the fault management section.
- Creation of a log to identify when SESM is encountering difficulties generating CORBA notifications for alarm events. This change is discussed in the fault management section.
- Creation of a log upon startup and shutdown of SESM.

102.3 Hardware Requirements or Dependencies

N/A - No new hardware is required.

102.4 Software Requirements or Dependencies

The change to the interface requires that all clients of the SESM alarm system are upgraded to be able to continue to use the alarm notifications. Without

being upgraded, existing clients of the alarm system notifications will not function.

102.5 Limitations and restrictions

With this feature, the SESM alarm GUI no longer allows alarm acknowledgements. This ability is present in the IEMS alarm GUI and all alarm acknowledgements should be done there.

102.6 Interactions

N/A

102.7 Applicable customer facing sections

Fault Management

- Logs ___X__
- Alarms ___X__

Configuration

- Data Schema _____
- User Interface _____
- Element Management ___X__
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

102.8 Glossary

Term	Description

103: Functional Description (FN): A00003669

103.1 Feature name

Media Gateway 4000 - Internet Protocol (MG4K-IP) Prep Feature

103.2 Description

MG4KIP Product to support following table control changes

- FABRIC field is included in table MNNODE
- It enforces restriction on RM datafill based on the FABRIC type in MNNODE.
- RM datafill restriction in table MNCKTPAK.
- Signalling Address datafill in MNMGPIP for MG4K (and IW) tuples
- VLAN TCIs datafilled in MNMGPIP for Bearer and Signalling paths on GEM RMs
- DIFFSERV codepoints for signalling and voice data added to table MNIPPARM
- Media Integrity Indicator added to table MNIPPARM

Note that the signalling address design description is described under feature A00003659.

103.3 Hardware Requirements or Dependencies

No new hardware requirements for this feature.

103.4 Software Requirements or Dependencies

This feature requires SN07 loads in the call server, MG420 loads in the MG4K CEMs and GEM20 in the GEM RMs.

103.5 Limitations and restrictions

- New SGFABRIC field is only for the MG4K SPMs. It is not part of the IW or DMSCP SPMs node datafill.
- SGFABRIC field change is restricted - certain conditions must be met before the tuple is allowed to change.
- Signalling IP address changes are restricted on MG4K - GEM must be out of service because this would cause node isolation.

- Signalling IP address cannot be enabled unless a valid signalling IP address has already been datafilled. Once enabled, the signalling IP address cannot be changed without disabling it first.
- VLAN TCI-VID for bearer is restricted to 255 on NTLZ20AA, BA, and CA cards due to Broadcom Calisto DSP specification.
- Media Integrity Indicator requires RTCP to be enabled prior to enabling MI.

103.6 Interactions

This feature interacts with functionality provided by A00003659, which did not include an FN or a CN section. All table changes are documented in this feature instead.

103.7 Applicable customer facing sections

Fault Management

Logs n/a____

Alarms n/a____

Configuration

Data Schema X_____

User Interface n/a____

Element Management n/a____

Security n/a____

Service Order n/a____

Office Parameters n/a____

Accounting (includes AMA billing) n/a____

Performance (includes operational measurements) n/a____

103.8 Glossary

Term	Description
VLAN TCI	Virtual Lan Tag Component Indicator
DIFFSERV	Differentiated Services, using codepoints to potentially assign priority to packets for different applications. See IETF document RFC3260

104: Functional Description (FN): A00003672

104.1 Feature name

NTLZ20CA Core Definition

104.2 Description

This feature provides the software support for the new NTLZ20CA 1000bLX (1300 nm, single mode) w/ LC connector peccode for the IP MG4K/IW GEM card.

104.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies being introduced by this feature. This is simply adding a new peccode to the existing list of supported peccodes for MG4K and IW SPMs.

Note: The actual new card hardware is NOT required for this peccode to be implemented as a supported peccode for MG4K.

104.4 Software Requirements or Dependencies

There are no software requirements or dependencies being introduced by this feature. This is simply adding a new peccode to the existing list of supported peccodes for MG4K and IW SPMs.

104.5 Limitations and restrictions

There are no limitation introduced by this feature. This is simply adding a new peccode to the existing list of supported peccodes for MG4K and IW SPMs.

104.6 Interactions

There are no interactions with other features introduced by this feature. This is simply adding a new peccode to the existing list of supported peccodes for MG4K and IW SPMs.

104.7 Applicable customer facing sections

Fault Management

Logs	_N/A_____
Alarms	_N/A_____

Configuration

Data Schema	_X____

User Interface _N/A__

Element Management _N/A__

Security _N/A__

Service Order _N/A__

Office Parameters _N/A__

Accounting (includes AMA billing) _N/A__

Performance (includes operational measurements) _N/A__

104.8 Glossary

Term	Description
IP	Internet Protocol
GEM	Gigabit Ethernet Module

105: Functional Description (FN): A00003687

105.1 Feature name

TOPS Wireless Intelligent Network Integration

105.2 Description

This feature enhances Table TOPSTLDN, introduced in SN06, to make it easier to deploy and maintain TOPS feature A00000816: "TOPS Wireless ADACC with Release." The enhancement is to allow the temporary local directory number (TLDN) to be chosen based on the identity of the originating mobile switching center (MSC). MSC is a generic term for a wireless (cellular) end office.

This feature also allows TOPS to send short text messages to a wireless phone using Short Message Service (SMS). TOPS can send short text messages using either Interim Standard 41 (IS-41) or Global System for Mobile Communications (GSM) specifications. IS-41 and GSM provide different definitions of a Mobile Application Part (MAP) layer which sits on the Transaction Capabilities Application Part (TCAP) layer of Signalling System #7 (SS7).

This feature also adds some preparatory work for supporting ADACC with Release in a GSM environment. This function cannot be used at this time.

Finally, this feature removes operational measurement (OM) group IS41TOPS and replaces it with three new OM groups. The new groups can be used for GSM as well as IS-41 and for SMS as well as wireless ADACC.

105.3 Background

105.3.1 TOPS support of wireless intelligent network (WIN) capabilities

In SN06, TOPS feature A00000816: "TOPS Wireless ADACC with Release" added the capability to release cellular directory assistance (DA) calls back to the originating MSC for call completion. This release is accomplished using IS-41 messages to transmit the requested directory number (DN) from TOPS to the MSC. The MSC then releases the trunk to TOPS and connects forward to the requested DN. Prior to this SN06 feature, such calls were "hairpinned," meaning the trunks to and from TOPS stayed in the voice path between the calling and called parties for the duration of the call.

The IS-41 TCAP messages used for the TOPS DA call completion call flow are part of the Wireless Intelligent Network (WIN) modifications to IS-41. These modifications are described in standard IS-771.

A successful IS-41/IS-771 ADACC with Release call flow is depicted in figure 1 on page 1017.

105.3.2 TOPS support of short message service (SMS)

TOPS positions can already send short text messages using an e-mail interface over the Internet. Such an SMS message might contain the address of the requested listing on a DA call. The TOPS switch is not aware of these messages.

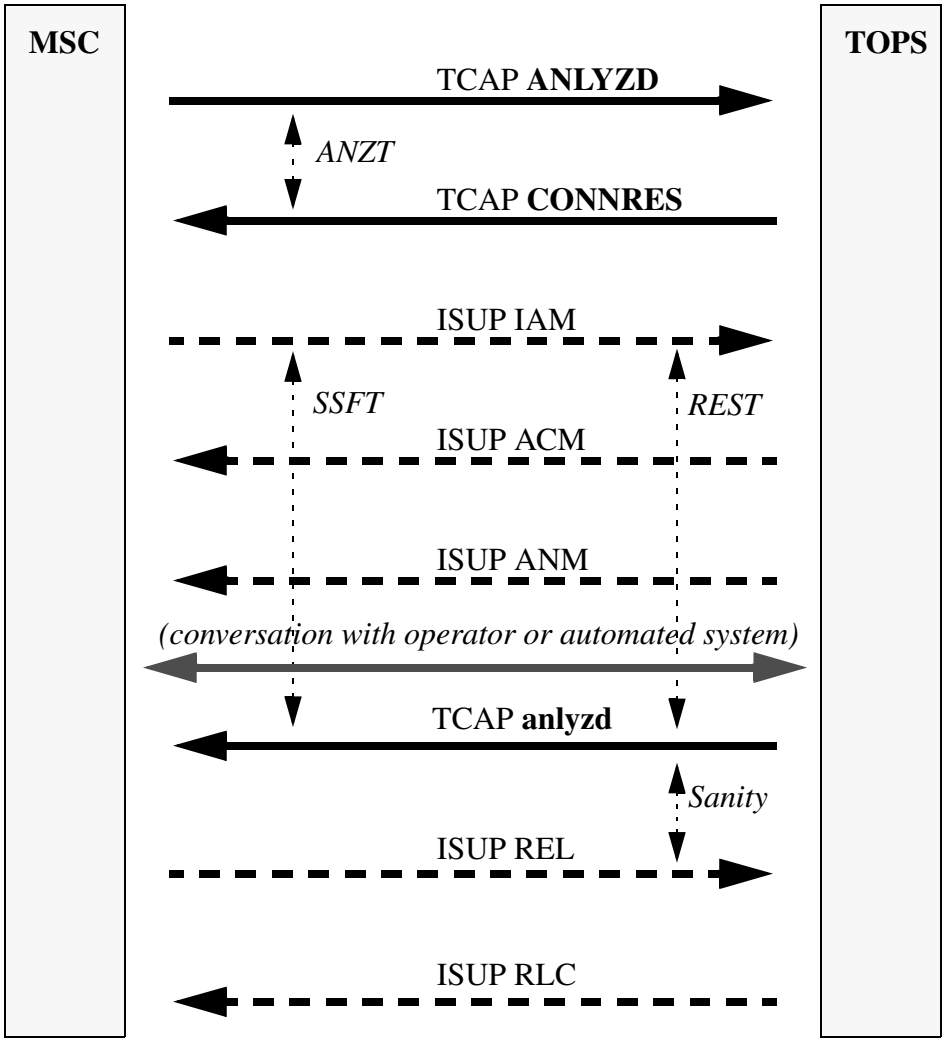
TOPS switches have supported SS7 TCAP applications for a long time, and SS7 TCAP is a common way to transport SMS in today's wireless networks. This feature allows TOPS to send SMS using either IS-41 or GSM, which are based on SS7 TCAP. By using TCAP to send TOPS SMS, the customer can avoid IP security and connectivity issues. The customer can also track the performance of TOPS SMS via operational measurements (OMs) and logs.

105.4 Specifications

This feature is based on the following IS-41 and GSM specifications:

- ANSI-41D (Wireless Intersystem Operations, formerly IS-41)
- 3GPP TS 29.002 V4.C.0: Mobile Application Part (MAP) specification, phase 4

Figure 1 Successful TOPS IS-41 ADACC with release, introduced in SN06



In the above diagram,

- A horizontal solid arrow and a message type in **bold** represents a TCAP message as defined in the IS-41 WIN specifications.
- A horizontal dashed arrow represents an ISUP message.
- A vertical dashed arrow on the MSC side represents an IS-41-defined timer. A vertical dashed arrow on the TOPS side represents an internal TOPS timer.
- The horizontal double-ended arrow represents two-way speech path between the wireless caller and TOPS.

105.5 Feature overview

This feature contains the following components. The work is divided into two areas, with some changes affecting both.

105.5.1 Wireless ADACC with Release

- Modified DMS table TOPSTLDN (TOPS Temporary Local Directory Number) which allows the customer to datafill TLDNs to be used in TOPS IS-41 call flows. Previously, any TLDN could be sent to any wireless end office. This feature allows TLDNs to be chosen on a per MSC basis. This helps the telco when they are activating WIN TOPS call flows in new MSCs (and desire a smaller or different TLDN range) but do not wish to affect existing MSCs.
- New table MSCIDMAP (MSC Identifier Mapping) which provides a mapping from MSC identifiers (MSCIDs) to entries in Table TOPSTLDN. This mapping allows the telephone company to control which TLDNs are sent to which MSCs.
- Addition of a new RLT type, RLT_GSM, to Table ISUPTRK. This table already allows datafill of three different RLT types: RLT_REL, RLT_FAR, and RLT_IS41. **Value RLT_GSM is for future use and cannot be datafilled at this time.**
- Removal of tuple NUM_OF_IS41TOPS_EXT_BLKS in Table OFCENG. This parameter controlled the number of extension blocks allocated for TOPS IS-41 calls. This parameter had to be set manually. It is replaced by to NUM_OF_WIN_TOPS_EXT_BLKS in Table OFCAUT. Table OFCAUT automatically allocates extension blocks for IS-41 and GSM calls. Also, the name of the EXT block is changed from IS41TOPS_EXT_BLK to WIN_TOPS_EXT_BLK. This name shows up when using OMSHOW to view the registers in OM group EXT.
- Addition of tuple RLT_FOR_GSM in Table TOPSFTR. This tuple will be used to control GSM ADACC with Release. **Tuple RLT_FOR_GSM is for future use and cannot be set to 'Y' at this time.** GSM ADACC with Release is under the control of existing Software Optionality Control (SOC) option OSEA0104, and tuple RLT_FOR_GSM acts as an on/off switch once the SOC option is enabled. This SOC option also controls IS-41 ADACC with Release.

105.5.2 Short message service (SMS)

- TOPS support of the following TCAP SMS messages, as described in the specifications listed in section 105.4. These messages allow TOPS to send short text messages to wireless phone callers and receive acknowledgment from the message center (MC).
  - — IS-41 SMSDeliveryPointToPoint INVOKE (from TOPS to MC)

— IS-41 SMSDeliveryPointToPoint RETURN RESULT (from MC to TOPS)

— GSM ForwardShortMessage (from TOPS to MC)

— GSM ForwardShortMessage Ack (from MC to TOPS)

- New field, WIRELESS, in Table TOPSTOPT. This field allows the customer to mark a trunk group as connecting to a wireless network. If so, the customer can datafill whether the network uses IS-41 or GSM for TCAP messaging. This field is used when TOPS sends a short message on a non-WIN call. On a WIN call the network type is already known.
- New TOPS parameter in Table TOPSPARM, SMS_LOG_MC_FAILURE. This parameter controls whether a TOPS131 log is generated when the message center returns a negative acknowledgment following a TOPS SMS attempt. A negative acknowledgment always pegs OMs in new groups SMSTOPS and TC7WRLSS, but the TOPS131 log can provide additional information.
- New TOPS parameter in Table TOPSPARM, SMS_TIMEOUT. This parameter controls the duration of the timer which is set when TOPS sends an SMS. If TOPS does not receive a response from the message center when the timer expires, the message is considered timed out, and resources are freed. See “105.7 TOPS short message service (SMS)” on page 1025 for more information.
- A new SS7 global title translation name, MDNMCGT. This translation name is used to route IS-41 and GSM short messages to the correct message center (MC).
- New DMS table TOPSMCDB for lab testing of TOPS SMS.
- Two additional DMS SS7 subsystems, TIS41SIM and TGSMSIM, to be used for TOPS lab testing.

105.5.3 Changes affecting both areas

- Creation of three new operational measurement (OM) groups to record events for IS-41 SMS, GSM SMS, IS-41 WIN, and GSM WIN[1]. The new groups will record application level events as well as transport level events. The new OM groups are SMSTOPS, WINTOPS, and TC7WRLSS. These three groups replace group IS41TOPS, which is removed.
- Update to TOPS131 log added in SN06. This feature allows the log to be used for GSM as well as IS-41, and for short message service as well as ADACC service.

[1]GSM WIN is known as Customised Applications for Mobile network Enhanced Logic (CAMEL). TOPS uses the term Wireless Intelligent Network (WIN) to describe both IS-41 WIN and GSM CAMEL calls flows. These call flows attach a TOPS operator or service node to provide a transient service, and then the MSC releases TOPS and the wireless call proceeds.

- A new DMS Signaling System #7 (SS7) subsystem, GSMTOPS. This subsystem resides on the TOPS node and will initially be used to send and receive GSM SMS messages. The subsystem number is datafilled in Table C7LOCSSN.

This feature does not introduce any TOPS Automatic Message Accounting (AMA) changes.

105.6 TLDN selection by mobile switching center identifier (MSCID)

105.6.1 Changes to Table TOPSTLDN

Prior to this feature, Table TOPSTLDN defined one large pool of TLDNs to be used on WIN calls. Several tuples might be present in Table TOPSTLDN, but these tuples were combined together to make a single pool. When an IS-41 AnalyzedInformation (ANLYZD) message arrived from an MSC, TOPS would pick any idle TLDN from the overall pool and send it to the MSC in the ConnectResource (CONNRES) message. These messages are shown in Figure 1 on page 1017.

This strategy works for a few MSCs but is not sufficient when deploying the feature across many MSCs. If hundreds of MSCs from across a region are using TOPS IS-41, they must all share the same TLDN pool. This means that when the customer is initially provisioning their network for TOPS IS-41, they must ensure that every TOPS TLDN is available and usable in every MSC as well as in every intermediate tandem switch on the way to the TOPS switch.

A better approach is to allow differentiation of TLDN chosen based on the identity of the originating MSC. To do this requires a change in Table TOPSTLDN as well a new table, MSCIDMAP, which is described in the next section.

This feature changes Table TOPSTLDN such that each group of TLDNs is identified by a pool ID. A maximum of 2,000 pools can be datafilled, and a maximum of 2,000 TLDNs can be datafilled. The pool ID is used in Table MSCIDMAP. The following figures show the change to Table TOPSTLDN.

Note that each tuple defines a range of TLDNs. In Figure 2, the following ranges of TLDNs are defined:

- 2012201234 to 2012201234: 1 TLDN
- 2013364400 to 2013364899: 500 TLDNs
- 2018591400 to 2018591489: 90 TLDNs

Figure 2 Table TOPSTLDN in SN06, prior to this feature

```
TABLE: TOPSTLDN
                   KEY
---------------------
2012201234 2012201234
  20133644   20133648
 201859140  201859148
```

This feature identifies each range of TLDNs with a pool ID, and expands the TLDNs to 10 digits for better readability. So the datafill in Figure 2 would appear as follows in SN07. This datafill still represents 591 TLDNs.

Figure 3 Table TOPSTLDN in SN07

```
TABLE: TOPSTLDN
POOLID   FROMDIGS     TODIGS
---------------------------
0      2012201234 2012201234
1      2013364400 2013364899
2      2018591400 2018591489
```

TLDN ranges in Table TOPSTLDN are allowed to overlap. This helps the customer when they are verifying the function on a new MSC while other MSCs are processing live traffic. The following figure shows overlapping TLDN ranges.

Figure 4 Table TOPSTLDN in SN07

```
TABLE: TOPSTLDN
POOLID   FROMDIGS     TODIGS
---------------------------
0      2012201200 2012201259
1      2012201250 2012201269
2      2012201200 2012201200
```

105.6.1.1 TLDN methodology

The telco's goal should be to have one large TLDN pool, or several smaller TLDN pools, serving all MSCs. This allows the TLDNs to be selected quickly. So the goal should be to minimize the number of tuples in Table MSCIDMAP (see next section).

The main reason for these tables is to assist in deployment of TOPS wireless intelligent network services. Established MSCs might be using hundreds of TOPS TLDNs, while a new MSC might need TLDNs from the same pool, but

only a small subset while the feature is being set up. Once the feature is verified on the new MSC, the MSC's datafill can be changed so it uses the main pool.

The telco providing operator services will reserve the TOPS TLDNs for these call types. Even in a nationwide network it should be possible to find enough TLDNs, since the TLDNs chosen probably begin with the NPA-NXX of the TOPS switch. If the TOPS switch supports several NXXs, this makes finding available DNs easier.

2,000 is the maximum number of TLDNs which can be datafilled on a TOPS switch. Due to the short holding time of under one second, a couple hundred TLDNs should be enough to handle heavy WIN TOPS traffic. If problems begin to occur, TLDNs can remain held for up to 30 seconds before the TLDN selection code re-uses them.

105.6.1.2 Dump and restore for Table TOPSTLDN

When upgrading from SN06 to a later release, each TOPSTLDN tuple from the SN06 side is restored with sequential pool IDs starting at 0, and each TLDN is expanded to 10 digits. So the Figure 2 and Figure 3 represent a dump and restore from SN06 to a later release.

105.6.2 New table MSCIDMAP

This feature introduces Table MSCIDMAP which allows the selection of TLDNs on a per-MSC basis.

The MSC Identifier (MSCID) is defined in IS-41D, chapter 5, section 6.5.2.82. It consists of a market identifier (16 bits) and a switch number (8 bits). It is a mandatory field in the IS-41 ANLYZD message which initiates a TOPS IS-41 ADACC with Release call.

When TOPS receives an ANLYZD, it selects an idle TLDN from Table TOPSTLDN and sends it back to the MSC in the TCAP CONNRES message. This feature allows TOPS to select a TLDN based on the MSCID in the ANLYZD. This is done using new Table MSCIDMAP. Table MSCIDMAP maps the MSCID from the ANLYZD to a list of TLDN pool IDs from Table TOPSTLDN. TOPS then selects an idle TLDN from one of these pools.

The following figure shows sample datafill in Table MSCIDMAP. Up to 255 TLDN pool IDs can be datafilled against a given MSCID.

Figure 5 Table MSCIDMAP

```
TABLE: MSCIDMAP
MSCID          POOLIDS
----------------------
12  100  (0) (1) (2) $
65    2      (0) (1) $
65    3          (0) $
66   27          (1) $
66   29      (1) (2) $
700   2          (2) $
```

105.6.2.1 Switch number wildcarding

Because a TOPS switch might be serving hundreds if not thousands of MSCs, Table MSCIDMAP is designed with some wildcarding capabilities. It is not necessary to datafill every switch number within a market ID. If a tuple is datafilled with just the market ID, and no switch number, the tuple will match all MSCIDs with the same market ID.

It is also possible to datafill several market ID and switch number combinations for the same market ID, and then add a market ID wildcard tuple for all other switch numbers using the same market ID.

The following figure shows examples of switch number wildcarding. All MSCIDs beginning with market ID 65 will match the first tuple, except MSCID (65, 3) which matches the second tuple.

Figure 6 Table MSCIDMAP with switch number wildcarding

```
TABLE: MSCIDMAP
MSCID          POOLIDS
----------------------
65  $    (0) (1) (2) $
65  3          (0) $
66 27          (1) $
66 29      (1) (2) $
67  $      (0) (2) $
```

105.6.2.2 Market ID wildcarding

Tuple {$, $} matches any MSCID not otherwise matched in Table MSCIDMAP. If present, it is the default tuple. If the MSCID in the TCAP ANLYZD message does not match any other tuple in Table MSCID (including any tuples with wildcarded switch numbers), tuple {$, $} is used.

Figure 7 Table MSCIDMAP with default tuple

```
TABLE: MSCIDMAP
MSCID          POOLIDS
----------------------
 $  $    (0) (1) (2) $
65  3            (0) $
66  $            (1) $
66 29        (1) (2) $
67  $        (0) (2) $
```

105.6.2.3 Failure to match MSCID

If the MSCID for a given call does not match any tuple in Table MSCIDMAP (either explicitly or via wildcarding), a RETURN ERROR is sent to the MSC so the wireless 411 call is disconnected. A TOPS131 log is generated indicating no TLDNs are available.

A failure to match implies that the market ID wildcard tuple is not present, since this tuple matches any MSCID.

105.6.2.4 Dump and restore

When performing a switch upgrade from an SN06 TOPS switch to a later release, the following steps are performed automatically:

1. Table TOPSTLDN is restored as described in section 105.6.1.
2. If TOPSTLDN contains any datafill on the restore side, a {$, $} tuple is created in Table MSCIDMAP containing all pools from Table TOPSTLDN.

This will create one large pool serving all MSCs, which is equivalent to the SN06 function of Table TOPSTLDN.

105.7 TOPS short message service (SMS)

105.7.1 Message flow

This feature allows TOPS to send short text messages into the SS7 network. TOPS sends these messages when requested by the operator position or automated service node.The message flow is summarized below. Later subsections show message diagrams, OMs pegged, etc.

- A TOPS call arrives from a wireless (cell) phone. TOPS knows the calling party is using a wireless phone if at least one of the following conditions hold:
  - — The call originated with a WIN message transaction (ANLYZD/ CONNRES)
  - — New TOPSTOPT field `WIRELESS` indicates the calling trunk group is from a wireless network (non-WIN)

  When presenting the call to the Open Position Protocol (OPP) compliant position or Open Automated Protocol (OAP) compliant service node, TOPS indicates that the calling party is using a wireless phone.
- The operator position sends a short text message and a destination directory number (DN) to TOPS switch using OPP, or the service node sends a short text message and a destination DN using OAP.
- TOPS checks whether the destination DN is the same as the calling number. This feature allows TOPS to send an SMS to the calling party only. TOPS denies the SMS attempt with an appropriate OPP or OAP message if the destination DN is not equal to the calling number.
- TOPS decides whether to send SMS using IS-41 or GSM. This decision is made as follows:
  - — If the TOPS call originated using IS-41 WIN, TOPS already knows the originating wireless network type, and TOPS uses IS-41.
  - — If the TOPS call did not originate using IS-41 WIN, TOPS looks at the calling trunk group datafill in Table TOPSTOPT. New field `WIRELESS` in Table TOPSTOPT indicates whether the calling trunk is IS-41 or GSM. TOPS chooses to use IS-41 or GSM based on the contents of this field.
  - — If the TOPS call did not originate using IS-41 WIN, and calling trunk group is not marked as wireless in Table TOPSTOPT, TOPS sends a failure indication to the operator position or service node using OPP or OAP, respectively. The call is not a wireless phone call, and TOPS did not indicate to the position or service node that the call is from a wireless phone. The position or service node should not request an SMS when the calling phone is not a wireless phone.

- Once TOPS has decided which standard to use, TOPS composes an outgoing TCAP INVOKE containing the short message.
- To route the TCAP INVOKE, TOPS looks in the global title translation tables C7GTTYPE and C7GTT. This feature adds a new SS7 translation name, MDNMCGT, for routing short messages to the message center (MC). TOPS uses the destination number to index the global title translation tables. This will route the SMS to the calling party's home message center.
- TOPS sends the TCAP INVOKE. If the message is sent successfully, TOPS returns a success indication to the position or service node using OPP or OAP, respectively. If the message is not sent successfully, TOPS indicates the failure to the position or service node.
- TOPS starts an internal timer equal to the new `SMS_TIMEOUT` parameter in Table TOPSPARM. If this timer expires, a log and OM are generated to notify the telephone company.
- When the acknowledgment from the message center arrives, TOPS pegs an OM and/or generates a log based on the response (success or failure). TOPS does not send a notification to the position if the SMS succeeded or failed.

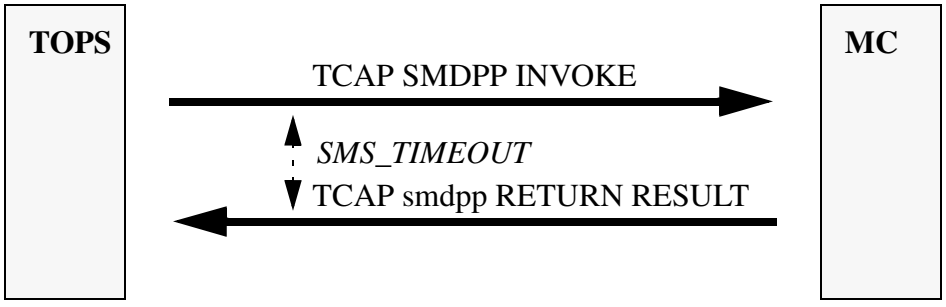
The following sections show diagrams of SMS messaging for IS-41 and GSM.

105.7.2 Successful IS-41 SMS transaction

In this scenario, TOPS sends the SMS to the message center, which responds with a positive acknowledgement. According to IS-41, the absence of a Cause Code parameter indicates success.

TOPS pegs OMs SMSSENT and SMSSUCC in group SMSTOPS (key `IS41`). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key `SMS_IS41`).

Figure 8 Successful TOPS IS-41 SMS to message center



105.7.3 Unsuccessful IS-41 SMS transaction

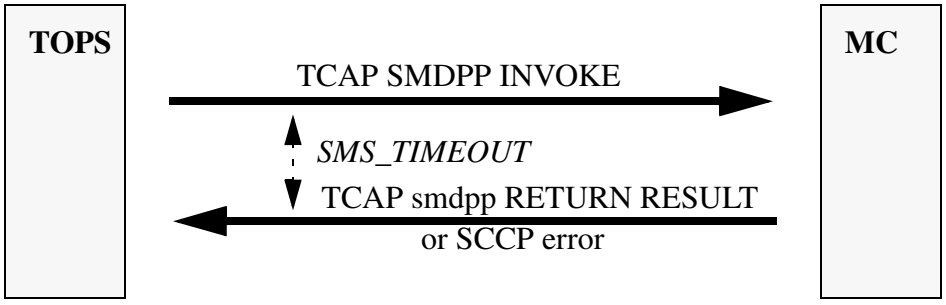
In this scenario, TOPS sends the SMS to the message center, but failures occur in the network, or the message center cannot process the SMS. TOPS receives a negative acknowledgment from an intervening node or from the message center, depending on where the error occurred. The message center's response contains a Cause Code field indicating why the message could not be delivered.

Possible reasons for failure include network problems, terminal (cell phone) problems, radio interface problems, and other miscellaneous problems (e.g. message format).

TOPS pegs OMs SMSSENT and SMSFAIL in group SMSTOPS (key `IS41`). TOPS also pegs one of the failure reason OMs (SMSNETWK, SMSTERM, SMSRADIO, and SMSMISC). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key `SMS_IS41`).

TOPS generates a TOPS131 log indicating the reason for failure, as directed by new Table TOPSPARM parameter `SMS_LOG_MC_FAILURE`.

Figure 9 Unsuccessful TOPS IS-41 SMS to message center (smdpp contains cause code)



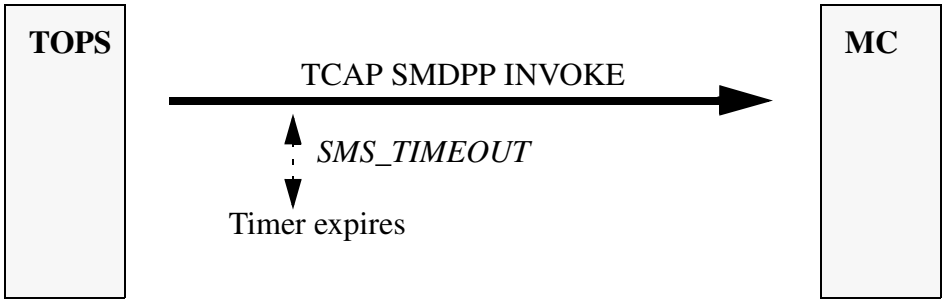
105.7.4 SMS time-out (IS-41)

In this scenario, TOPS sends the SMS to the message center but receives no reply within the time-out period (as defined by parameter `SMS_TIMEOUT` in Table TOPSPARM).

TOPS pegs OMs SMSSENT and SMSTIME in group SMSTOPS (key `IS41`). TOPS also pegs OM INVOKES in group TC7WRLSS (key `SMS_IS41`).

TOPS generates a TOP131 indicating an SMS time-out occurred.

Figure 10 SMS time-out (IS-41)

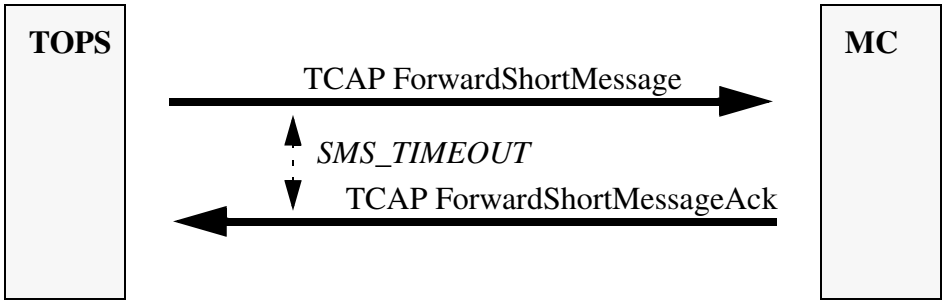


105.7.5 Successful GSM SMS transaction

In this scenario, TOPS sends the SMS to the message center, which responds with a positive acknowledgement.

TOPS pegs OMs SMSSENT and SMSSUCC in group SMSTOPS (key `GSM`). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key `SMS_GSM`).

Figure 11 Successful TOPS GMS SMS to message center



105.7.6 Unsuccessful GSM SMS transaction

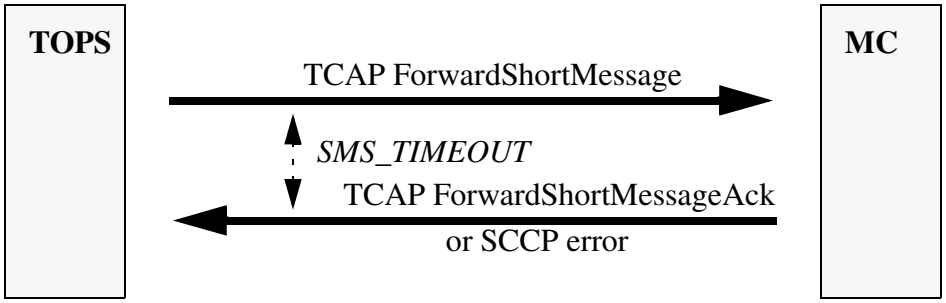
In this scenario, TOPS sends the SMS to the message center, but failures occur in the network, or the message center cannot process the SMS. TOPS receives a negative acknowledgment from an intervening node or from the message center, depending on where the error occurred. The message center's response contains the error cause and any diagnostic information.

Possible reasons for failure include network problems, terminal (cell phone) problems, radio interface problems, and other miscellaneous problems (e.g. message format).

TOPS pegs OMs SMSSENT and SMSFAIL in group SMSTOPS (key GSM). TOPS also pegs one of the failure reason OMs (SMSNETWK, SMSTERM, SMSRADIO, and SMSMISC). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key SMS_GSM).

TOPS generates a TOPS131 log indicating the reason for failure, as directed by new Table TOPSPARM parameter SMS_LOG_MC_FAILURE.

Figure 12 Unsuccessful TOPS GSM SMS to message center (ack contains cause code)



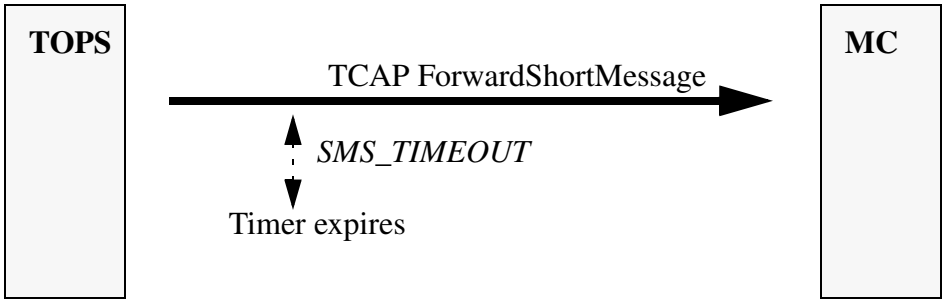
105.7.7 SMS time-out (GSM)

In this scenario, TOPS sends the SMS to the message center but receives no reply within the time-period (as defined by parameter SMS_TIMEOUT in Table TOPSPARM).

TOPS pegs OMs SMSSENT and SMSTIME in group SMSTOPS (key GSM). TOPS also pegs OM INVOKES in group TC7WRLSS (key SMS_GSM).

TOPS generates a TOP131 indicating an SMS time-out occurred.

Figure 13 SMS time-out (GSM)



105.7.8 TOPS SMS engineering considerations

Short messages sent by TOPS can be up to 200 characters in length. When headers and ancillary fields are added in, the overall message length can reach 250 bytes. Each time a position or automated node sends a SMS which is then forwarded to the SS7 network, the SMS is actually sent twice: once using OPP or OAP over IP from the position or service node to the switch, and once over the SS7 links into the network.

If a switch is supporting 300 active operators handling 20-second directory assistance calls, and an SMS containing the listing is sent on each call, this represents 54,000 calls per hour at 250 bytes per call. The total is 13.5 megabytes per hour which is equivalent to 3.75 kilobytes per second.

Both the IP links to the positions and service nodes as well as the SS7 links to the network must be able to handle this increased messaging. Call durations, numbers of operators, and SMS-to-call ratio should be taken into account when deploying this feature.

105.7.9 Operator and automated node interaction

Operators and automated service nodes receive an immediate indication that the SMS was successfully sent or could not be sent. They do not receive the later acknowledgment from the message center. The reason is that the SMS might be sent at the end of the call, and TOPS call throughput would be diminished if the operator or automated service node had to wait for the acknowledgment from the message center before leaving the call.

TOPS still tracks the message center results of the SMS (using OMs and logs) but the operator or service node is not aware of the outcome.

Another effect is that the response from the message center might arrive after the AMA record for the call is generated. So this feature does not record in AMA whether the SMS was successfully received by the message center.

105.8 IS41TOPS OM group modification

In SN06, the original TOPS IS-41 feature added OM group IS41TOPS. This group recorded application-level and transport-level events for the IS-41 ADACC with release call flow.

This SN07 feature is adding support of GSM and SMS. The number of registers to record application-level and transport-level events for combinations of the two applications (RLT and SMS) and the two protocol standard (IS-41 and GSM) requires more than 32 registers, which is the maximum number of registers in an OM group.

So this feature creates the following three groups. All three groups use a key field with values IS-41 and GSM, so all three groups are used for both wireless network standards.

- SMSTOPS: This group records application-level events for the TOPS short message service.
- WINTOPS: This group records application-level events for wireless ADACC with release. This group uses WIN in the name since wireless intelligent network capabilities are used to provide ADACC with release for both IS-41 and GSM.
- TC7WRLSS: This group records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).

All events formerly pegged in IS41TOPS are now pegged in the new groups. The following table shows the new representations of the IS41TOPS OMs.

IS41TOPS register (SN06)	New group (SN07), key IS41 or WIN_IS41	New register (SN07)
ANINFINV	WINTOPS	WINBEGIN
ANINFIN2	WINTOPS	WINBEGI2
CONNRES	WINTOPS	REQCONN
CONNRES2	WINTOPS	REQCONN2
ANINFRR	WINTOPS	CONNECT
ANINFRR2	WINTOPS	CONNECT2
ANINFRD	WINTOPS	DISCONN
ANINFRD2	WINTOPS	DISCONN2
RESTIMR	WINTOPS	RESTIMR
RESTIMR2	WINTOPS	RESTIMR2
TLDNTIME	WINTOPS	TLDNTIME
SANTIMR	WINTOPS	SANTIMR
CFRABAN	WINTOPS	ABANDON
CFRDISC	WINTOPS	ERRDISC
CFRFAIL	WINTOPS	ERRCONN
CFRSSFT	WINTOPS	ERRSSFT
RETERRS	TC7WRLSS	RETERRS
RETERRR	TC7WRLSS	RETERRR
REJECTS	TC7WRLSS	REJECTS
REJECTR	TC7WRLSS	REJECTR

IS41TOPS register (SN06)	New group (SN07), key IS41 or WIN_IS41	New register (SN07)
NOTLDNS	WINTOPS	NOTLDNS
NODATA	WINTOPS	NODATA
RXLAFAIL	WINTOPS	RXLAFAIL
MBFULL	TC7WRLSS	MBFULL
RTFNOXLA	TC7WRLSS	RTFNOXLA
RTFNOXLS	TC7WRLSS	RTFNOXLS
RTFSUBCG	TC7WRLSS	RTFSUBCG
RTFSUBFL	TC7WRLSS	RTFSUBFL
RTFUNEQ	TC7WRLSS	RTFUNEQ
RTFNETFL	TC7WRLSS	RTFNETFL
RTFNETCG	TC7WRLSS	RTFNETCG
RTFMISCE	TC7WRLSS	RTFMISCE

For more information on the groups created by this feature, refer to the Performance chapter of this document.

105.9 Customer visible changes

As mentioned in “105.5 Feature overview” on page 1018, this feature has several customer-visible changes.

105.9.1 Wireless ADACC with Release

- Table TOPSTLDN (changed) and Table MSCIDMAP (new): Together, these tables map MSC identifiers to TLDN pool(s) used when selecting a TLDN at the beginning of an IS-41 WIN call. See “105.6 TLDN selection by mobile switching center identifier (MSCID)” on page 1020, as well as the Configuration chapter of this document.
- Changed tables OFCENG, OFCAUT, and ISUPTRK: The TOPS IS-41 extension block parameter is removed from Table OFCENG and added to Table OFCAUT. In Table ISUPTRK, a value is created for future use. See the Configuration chapter of this document.
- Table TOPSFTR: This feature adds a new tuple, `RLT_FOR_GSM`, which controls GSM ADACC with Release. GSM ADACC with Release is under the control of existing SOC option OSEA0104.

105.9.2 Short message service (SMS)

- Changed table TOPSTOPT: A new field, WIRELESS, is added for defining the wireless network type on a non-WIN wireless call.
- Changed table TOPSPARM: Two new TOPS parameters, SMS_LOG_MC_FAILURE and SMS_TIMEOUT, are added. See the Configuration chapter of this document.
- SS7 datafill and maintenance: Action is required on the TOPS switch to define and activate the new SS7 subsystem, GSMTOPS, in order to send and receive GSM SMS TCAP messages. Please refer to “105.16 Appendix A: Datafill changes for SMS” on page 1038.
- SS7 global title translation name: A new translation name, MDNMCGT, is added to allow TOPS to route IS-41 and GSM short messages to message centers. This translation name is datafilled in existing table C7GTTYPE. Please refer to “105.16 Appendix A: Datafill changes for SMS” on page 1038.
- Existing OM groups: This feature creates a new SS7 subsystem, and many existing OM groups have registers which are pegged when this new subsystem is in use. See “105.17 Appendix B: Operational measurements (OMs)” on page 1040 for more information.
- Test tool: This feature adds a TOPS SMS test tool consisting of new Table TOPSMCDB and new SS7 subsystems TIS41SIM and TGSMSIM. See “105.18 Appendix C: TOPS message center (TOPSMC) test tool” on page 1042 for more information.

105.9.3 Changes affecting both areas

- Changed operational measurement (OM) group IS41TOPS: OM group IS41TOPS is replaced by three new OM groups: SMSTOPS, WINTOPS, and TC7WRLSS. See “105.8 IS41TOPS OM group modification” on page 1030, as well as the Performance chapter of this document.
- Changed log TOPS131: This log appears when problems occur during the course of a wireless TOPS RLT call. Additional text reasons are added for SMS failures. See the Fault Management chapter of this document.
- Existing logs: This feature generates existing TCAP logs (such as the TCAP100) when errors occur in TCAP message formats, or unexpected TCAP messages are received. See Nortel Networks Log Report Reference Manual (297-8021-840) for more information about TCAP logs.

105.10 Hardware Requirements or Dependencies

Not applicable.

105.11 Software Requirements or Dependencies

Not applicable.

105.12 Limitations and restrictions

105.12.1 General restrictions

- TOPS Wireless ADACC with Release is supported in North American TOPS offices only.

105.12.2 TOPS Wireless Intelligent Network restrictions

- Only one form of RLT (ISUP, IS-41, or GSM) can be employed a given trunk group. A trunk group cannot support both IS-41 and GSM RLT.
- A maximum of 4,096 market identifiers can be datafilled in Table MSCIDMAP (see “105.6.2 New table MSCIDMAP” on page 1022).
- A maximum of 32,767 MSCIDs can be datafilled in Table MSCIDMAP. An MSCID is a combination of a market ID and a switch number.
- TOPS does not support GSM CAMEL calls at this time. The `RLT_GSM` value in field RLT of Table ISUPTRK is for future use.
- Pool IDs cannot be added to Table TOPSTLDN unless they already exist in Table MSCIDMAP.
- TLDN pools in Table TOPSTLDN cannot be changed or deleted if they are in use in Table MSCIDMAP. This helps prevent the customer from altering a TLDN’s internal store while the TLDN is in use.
- It is not possible to add a wildcard market ID and non-wildcard switch number tuple to Table MSCIDMAP.

105.12.3 TOPS SMS restrictions

- The SMS can be sent to the calling party only.
- In North America, the length of the SMS destination number must be 10 digits.
- The position or service node cannot send a second SMS while the first is in progress.
- SMS is supported on IP positions only, due to the maximum length of the SMS (200 bytes). Service nodes already use an IP datapath.
- SMS is not supported in the Time Division Multiplex (TDM) operator centralization (OC) environment[1], again due to length. If the OC environment uses a TDM data path, the SMS cannot be transmitted from the host switch to the remote switch, so the SMS attempt is denied. To support sending the SMS from the host to the remote, OC-IP must be employed.

[1]TDM OC uses the TOPS Message Switch (TMS) for the OC data path.

- SMS is supported in the Operator Services System Automated Intelligent Network (OSSAIN) centralization environment, known as OSAC. OSAC already uses an IP data path so SMS messages can be transmitted.
- Since TOPS might not have the International Mobile Subscriber Identity (IMSI) or Mobile Identification Number (MIN), there is no provision for routing SMS based on these numbers.
- Since TOPS only sends SMS to the calling party, there is no provision for prepending the country code prior to global title translation. The routing is based on the national number only.
- TOPS does not support SMS notification, a supplementary service which informs the message originator that the SMS was delivered to the destination phone. TOPS indicates in outgoing SMS TCAP messages that SMS notification is not required. If TOPS receives an SMS notification message, it is ignored.
- The AMA record does not indicate if the SMS was successfully acknowledged by the message center. For more information, see "105.7.9 Operator and automated node interaction" on page 1030.

105.13 Interactions

105.13.1 Interactions with cell phone users

Interactions involving wireless (cell) phone features and IS-41 or GSM processing on the MSC are outside the scope of this feature. This feature is limited to TOPS behavior given the following inputs:

- IS-41 and GSM messaging
- ISUP messaging
- Behavior of operator or automated service node

105.13.2 Interactions with intelligent TOPS peripherals

This feature allows Open Position Protocol (OPP) compliant operator positions to send short messages into the SS7 network via the TOPS switch. This feature also allows Open Automated Protocol (OAP) compliant automated service nodes to send short messages via the TOPS switch. To support these capabilities, OPP and OAP are updated. Please refer to the latest releases of OPP and OAP for information on the transport of SMS from the operator position or service node to the TOPS switch.

105.13.3 Wireless number portability

Wireless number portability allows a wireless customer to keep their dialable Mobile Directory Number (MDN) while moving to another service provider. Their nondialable IS-41 mobile identification number (MIN) or GSM international mobile subscriber identity (IMSI) changes, but their MDN remains the same.

The MDN is sent to TOPS as the calling party number when originating a call from a cell phone which has been ported. When a land line calls a ported cell phone, the original ("donor") MSC uses WNP capabilities to determine where the call should be routed.

This has the following effects on the call flows and functions of this feature.

105.13.3.1 Wireless intelligent network

TOPS WIN call setup is based on the initial WIN message and the originating trunk group. Whether the calling party has ported or not, the originating MSC sends an IS-41 ANLYZD or GSM InitialDP to start the call, and TOPS knows which protocol to use when handling the call.

The call arrives on an ISUP trunk group in Table ISUPTRK. IS-41 RLT or GSM RLT is datafilled against the trunk group, so the calling party number is not a consideration.

In a different case, a wireless caller uses TOPS WIN to connect to another wireless phone which has been ported. The TOPS WIN call flow is not changed. TOPS forwards the MDN of the called wireless phone to the MSC using the **analyzd** or Connect message. The MSC must then determine if the MDN has been ported. In other words, the WNP work is done after TOPS leaves the call, and TOPS does not need to indicate if a number is ported.

105.13.3.2 Short message service

At this time, TOPS can only send an SMS to the calling party. The MDN is sent as the calling party number. So TOPS sends the SMS to the MDN, which routes the SMS to the message center associated with the "donor" switch. The donor switch's MC then does the work to determine that the MDN has been ported. The donor switch's MC then forwards the SMS to the proper MC. So again, TOPS is not affected by WNP.

105.14 Applicable customer facing sections

Fault Management

Logs	___X__
Alarms	__N/A_

Configuration

Data Schema	___X__
User Interface	__N/A_
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_

Office Parameters ___X__

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) ___X__

105.15 Glossary

Acronym	Expansion
ACM	ISUP Address Complete message
ADACC	Automated DA Call Completion
AMA	Automatic Message Accounting
ANLYZD	IS-41 AnalyzedInformation message
ANM	ISUP Answer message
CONNRES	IS-41 ConnectResource message
DA	Directory Assistance
GSM	Global system for mobile communications
IAM	ISUP Initial Address message
IMSI	International Mobile Subscriber Identity
IP	Intelligent Peripheral
IP	Internet Protocol
IS-41	Interim Standard 41
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
MC	Message Center
MDN	Mobile Directory Number
MIN	Mobile Identification Number
MSC	Mobile Switching Center
OAP	Open Automated Protocol
OC	Operator Centralization
OPP	Open Position Protocol
OSAC	OSSAIN Centralization

Acronym	Expansion
OSSAIN	Operator Services System Advanced Intelligent Network
RLT	Release Link Trunking
RTP	Release To Pivot
SCCP	Signaling Connection Control Part
SCP	Service Control Point
SMS	Short Message Service
SS7	Signaling System #7
TCAP	Transaction Capabilities Application Part
TDM	Time Division Multiplex
TLDN	Temporary Local Directory Number
TMS	TOPS Message Switch
TOPS	Traffic Operator Position System
WNP	Wireless Number Portability

105.16 Appendix A: Datafill changes for SMS

Enabling TOPS SMS requires datafill and other action in the following categories:

- **SS7**: Enable the IS41TOPS and GSMTOPS subsystems.
- **Global title translation:** Update Table C7GTTYPE and C7GTT to route SMS TCAP messages to the proper message centers.
- **Trunk group**: Mark incoming wireless calls as IS-41 or GSM on a trunk group basis in Table TOPSTOPT.

These actions are described in this appendix.

105.16.1 A.1: SS7 datafill and maintenance

The following items are required to enable TOPS IS-41 and GSM TCAP messaging.

- Table C7LOCSSN: Add tuples for the IS41TOPS and GSMTOPS subsystems. Define two different subsystem numbers which will be used by MSCs to send TCAP messages to TOPS.

- MAP operation: From the SCCPLOC level of the MAP (MAPCI;MTC; CCS;CCS7;SCCPLOC), post and return to service the IS41TOPS and GSMTOPS subsystems.
- Table C7RTESET: TOPS SMS will not work unless there are CCS7 route set(s) defined to the message centers of calling parties. Depending on the configuration of the SS7 network, it might be possible to reuse the ISUP trunk route sets for TOPS SMS.

105.16.2 A.2: Global title translation

This feature adds an SS7 translation name, MDNMCGT, which is used for routing outgoing TOPS SMS messages to the appropriate message center. MDNMCGT is datafilled in Table C7GTTYPE and is already present in Nortel Networks MTX switches.

The following figures show datafill for Table C7GTTYPE and Table C7GTT. This datafill routes all TOPS SMS (whether IS-41 or GSM) messages to a service transfer point (STP) which already has significant SMS translation datafill. This TOPS datafill offloads the SMS global title translation to the customer's existing STP named STPA. The datafill assigns a global title number of 17 which is commonly used for mobile directory number (MDN) to message center (MC) routing.

Figure 14 Table C7GTTYPE

```
TABLE: C7GTTYPE
GTTNAME GTTYPE GTTID
----------------------------
TOPSSMS ANSI7 17 (MDNMCGT) $
```

Figure 15 Table C7GTT

```
TABLE: C7GTT
GTTKEY GTTRSLT
----------------------------------------
TOPSSMS 0 9 PCONLY (TOPSTOSTPA_RS 0) $ GT
```

105.16.3 A.3: Trunk group datafill

On a WIN call, the wireless network type is already known, since IS-41 messages were exchanged to begin the call. On a non-WIN wireless call (e.g. 0-, or 411 when WIN is not supported) the call arrives with standard trunk signalling and no indication that the calling party is using a cellular phone.

This feature allows customers to mark trunk groups as carrying wireless (cellular) traffic, and to further indicate whether the wireless network connected by the trunk group is IS-41 or GSM. TOPS uses this datafill when composing a short message. The trunk group datafill determines whether TOPS composes the SMS using IS-41 or GSM.

This requires the customer to segregate incoming trunk groups into IS-41 wireless, GSM wireless, and non-wireless categories. This is necessary since there is no ISUP signal which indicates that the calling party is using a cellular phone. Also, with wireless number portability (WNP), the NPA-NXX of the calling party number can no longer be used to determine the network type based on the originating MSC. A WNP user may have ported their mobile directory number from an IS-41 switch to a GSM switch or vice versa.

The following diagram shows three trunk groups in Table TOPSTOPT. One is from a wireline end office, one is from an IS-41 end office, and one is from a GSM end office.

Figure 16 Table TOPSTOPT

```
TABLE: TOPSTOPT
GRPKEY ORGAREA DISPCLG ADASERV ADASANS ANITOCLI OLNSQRY DCIBIDX LNPCLGAM
XLASCHEM SPIDPRC TRKSPID BILLSCRN ANIFSPL MAXCONNS DISPSPID WIRELESS
-------------------------------------------------------------------------
LANDLINE_EO   N Y NONE NA Y N NONE 0 N N N N N N 0 N N
WIRELESS_IS41 N Y NONE NA Y N NONE 0 N N N N N N 0 N Y IS41
WIRELESS_GSM  N Y NONE NA Y N NONE 0 N N N N N N 0 N Y GSM
```

105.17 Appendix B: Operational measurements (OMs)

This feature creates three new OM groups: SMSTOPS, WINTOPS, and TC7WRLSS. The registers in these groups count specific events occurring during TOPS IS-41 and GSM call processing. Please refer to “105.8 IS41TOPS OM group modification” on page 1030 and the Performance chapter of this document for more information on these new OM groups.

The following appendix describes this feature’s effects on existing OM groups.

105.17.1 B1: SS7 operational measurements

Several existing OM groups are defined for pegging events relating to SS7 and TCAP messaging. These groups usually start with “C7” or “TCAP.” More information about these groups can be found in NTP 297-8021-814: “Operational Measurements Reference Manual.”

Two existing TCAP OM groups, TCAPUSAG and TCAPERRS, are useful when tracking this feature, since these OM groups have SS7 subsystem as their

key. To track TOPS IS-41 events, use subsystem name IS41TOPS as the key. To track TOPS GSM events, use subsystem name GSMTOPS as the key.

OM group TCAPUSAG contains several registers which are pegged during the course of a wireless TOPS call in addition to the pegs in the new groups introduced by this feature. The following table maps the OM registers in group TCAPUSAG to messages sent and received during a wireless TOPS call.

Table 1 TCAPUSAG mapping to TOPS IS-41 and GSM ADACC event

Register	Description and applicability to TOPS IS-41 ADACC
TCMSGOUT, TCMSGOU2	Total TCAP messages originating on this node Pegged for all IS-41 and GSM TCAP messages sent by TOPS
TCMSGIN, TCMSGIN2	Total TCAP messages terminating at this node Pegged for all IS-41 and GSM TCAP messages received by TOPS
TCUNIDIR, TCUNIDI2	Total TCAP msgs sent/rcvd w/ package type UNIDIRECTIONAL Not pegged on wireless TOPS calls
TCQWPERM, TCQWPER2	Total TCAP msgs sent/rcvd w/ package type QUERY W/ PERM Pegged when TOPS receives ANLYZD. Also pegged when TOPS sends an SMS.
TCQNPERM, TCQNPER2	Total TCAP msgs sent/rcvd w/ package type QUERY W/O PERM Not pegged on wireless TOPS calls
TCCWPERM, TCCWPER2	Total TCAP msgs sent/rcvd w/ package type CONV W/ PERM Pegged when TOPS receives CONNFAILRPT
TCCNPERM, TCCNPER2	Total TCAP msgs sent/rcvd w/ package type CONV W/O PERM Pegged when TOPS sends CONNRES and RESETTIMER
TCRESPNS, TCRESPN2	Total TCAP msgs sent/rcvd w/ package type RESPONSE Pegged when TOPS sends anlyzd. Also pegged when TOPS receives response from message center.
TCINVKL, TCINVKL2	Total components sent/rcvd of type INVOKE LAST Pegged when TOPS received ANLYZD and CONNFAILRPT; also when TOPS sends CONNRES and RESETTIMER; also when TOPS sends an SMS.
TCINVKNL, TCINVKN2	Total components sent/rcvd of type INVOKE NOT LAST Not pegged on wireless TOPS calls
TCRSLTL, TCRSLTL2	Total components sent/rcvd of type RETURN RESULT LAST Pegged when TOPS sends anlyzd
TCRSLTNL, TCRSLTN2	Total components sent/rcvd of type RETURN RESULT NOT LAST Not pegged on wireless TOPS calls

Table 1 TCAPUSAG mapping to TOPS IS-41 and GSM ADACC event

Register	Description and applicability to TOPS IS-41 ADACC
TCRTERR, TCRTERR2	Total components sent/rcvd of type RETURN ERROR Pegged when TOPS sends AnalyzedInformation RETURN ERROR
TCREJECT, TCREJEC2	Total components sent/rcvd of type REJECT Pegged when TOPS sends AnalyzedInformation REJECT, or receives SMS REJECT
TCABORT, TCABORT2	Total TCAP msgs sent/rcvd w/ package type ABORT Not pegged on wireless TOPS calls

105.18 Appendix C: TOPS message center (TOPSMC) test tool

This feature introduces a test tool for verifying TOPS short message service. The test tool consists of two service control point (SCP) processes, one for IS-41 and one for GSM, which simulate message centers (MCs). These SCP processes run on the TOPS switch.

The simulated message centers are reached using the SS7 network. When an operator or automated node creates an SMS, TOPS formats the SMS into a TCAP message. TOPS uses either IS-41 or GSM, depending on the wireless network type of the calling party. TOPS then uses global title translation to send the TCAP message into the SS7 network.

The message arrives at one of the SCP simulators, which uses the destination number to index new Table TOPSMCDB (TOPS Message Center Database) to determine the disposition of the message. Possible results are:

- Successful acknowledgment sent back to TOPS switch
- Negative acknowledgment with cause code sent back to TOPS switch
- TCAP REJECT with reject reason sent back to TOPS switch
- Time-out (no response)

When TOPS receives the response (or the `SMS_TIMEOUT` timer expires), TOPS pegs OMs in new groups SMSTOPS and TC7WRLSS. In failure situations TOPS generates a TCAP log or a TOPS131 log.

Recall that the protocol chosen (IS-41 or GSM) is based on WIN messaging. If the call is not a WIN call, the protocol chosen is based on incoming trunk group datafill in Table TOPSTOPT. If the protocol is IS-41, but the global title translation datafill routes the SMS to the GSM simulator, the GSM simulator will generate a TCAP log and reject the SMS before accessing Table TOPSMCDB. The same is true for sending a GSM SMS to the IS-41 MC simulator.

The components are as follows, and the remainder of this appendix describes them in more detail.

- Table TOPSMCDB: This table allows datafill of destination numbers and SMS dispositions for these numbers.
- SS7: New subsystems TIS41SIM and TGSMSIM
- Global title translation: C7GTTYPE and C7GTT datafill is required to route SMS messages to the simulators.

105.18.1 C.1: Table TOPSMCDB

Table TOPSMCDB allows datafill of up to 64 SMS destination numbers. The disposition of the short message attempt is datafilled against each number. Table TOPSMCDB can serve short messages based on IS-41 and GSM.

The available dispositions are as follows:

- SUCCESS: A successful SMS acknowledgment is sent back to TOPS.
- ERROR: A negative acknowledgment with a cause code is sent back to TOPS. The cause codes are different for IS-41 and GSM, so datafilling ERROR requires the datafill of an IS-41 cause code and a GSM cause code.
- REJECT: Setting a disposition of REJECT causes a TCAP REJECT message to be sent back to TOPS. Since IS-41 and GSM share TCAP REJECT reasons, separate fields are not necessary. The reject reason consists of two fields, a problem type and a problem code.

If an SMS arrives at a simulator and the destination number is not found in Table TOPSMCDB, the SMS is ignored. Eventually the TOPS SMS timer will expire and the SMSTOPS OM TIMEOUT will be pegged. The TOPS SMS timer is set by parameter SMS_TIMEOUT in Table TOPSPARM.

A final TOPSMCDB field, DELAYSEC, indicates how long the simulators should wait before sending the SMS response. This is used to simulate real-world exchanges with message centers. It is datafilled for all dispositions.

> ***Note:*** The simulator is not multi-threaded. SMS messages arriving during the DELAYSEC delay are not processed until the delay time has expired. If several SMS messages arrive at once, they are processed sequentially. So the response time for the later short messages can easily exceed normal SMS time-out values.

The following figure shows three destination numbers in Table TOPSMCDB.

Figure 17 Table TOPSMCDB

```
TABLE: TOPSMCDB
DESTDIGS RESPAREA DELAYSEC
-------------------------------------------------
6199421465 ERROR SMSNOTSUPPORT FACILITYNOTSUPPORT 2
9194321234 REJECT GENPROB BADCOMPSTRUCT 2
9199910000 SUCCESS 2
```

105.18.2 C.2: SS7 datafill and maintenance

The following items are required to enable the TOPS IS-41 and GSM message center simulators.

- Table C7LOCSSN: Add tuples for the TIS41SIM and TGSMSIM subsystems.
- MAP operation: From the SCCPLOC level of the MAP (MAPCI;MTC; CCS;CCS7;SCCPLOC), post and return to service the TIS41SIM and TGSMSIM subsystems.
- Table C7RTESET: Datafill of Table C7RTESET is optional, since it is possible to define an internal SS7 link to the simulators, as described in the next section.

  It is also possible to set up looparound SS7 links, or to set up a looparound which goes through an STP. When setting up looparound links, datafill in C7RTESET and other SS7 tables (e.g. C7LKSET) is required. Using looparound links, or links to a second test switch where the TOPS MC simulators are running, is a more realistic way to test the SMS function.

105.18.3 C.3: Global title translation

The following figure shows datafill which will route all SMS attempts to the TOPS MC IS-41 simulator using internal SS7 links. The tuple in Table C7GTT can be split into several tuples in order to send some SMS attempts to the IS-41 MC simulator while other SMS attempts go to the GSM MC simulator.

Figure 18 Table C7GTTYPE

```
TABLE: C7GTTYPE
GTTNAME GTTYPE GTTID
----------------------------
TOPSSMS ANSI7 17 (MDNMCGT) $
```

Figure 19 Table C7GTT

```
TABLE: C7GTT
GTTKEY GTTRSLT
------------------------------
TOPSSMS 0 9 SSNONLY TIS41SIM $
```

106: Functional Description (FN): A00003693

106.1 Feature name

MG9K ESA for SMSI subtending ABI

Adding SMS to the supported peripheral types for Emergency Stand Alone (ESA) service for lines off the Access Bridge Interface (ABI) cards of an MG9K Media Gateway 9000 (MG9K).

106.2 Description

Another SN07 feature A00002380 provides the ability for the Succession Call Server 2000 (CS2000) to support Emergency Stand Alone calling on the following DMS-100 Legacy Extended Peripheral Modules (XPM) subtending a Media Gateway 9000 (MG9K):

- LGC, LGCI
- LTC, LTCI
- SMA2

This feature A00003693 adds SMS to the list of supported XPM types.

106.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies for this feature.

106.4 Software Requirements or Dependencies

This ESA activity on the MG9000 is dependent upon the following activity for successful completion.

A00003567: MG 9000 Element Mgr Support for ABI ESA

The primary function of this component is to pull ESA data from the Core, organize this information in the EM in a meaningful way for the MG9K, and put it into the ESA subsystem on the ABI in a usable format.

A00002380: MG9K ABI ESA

This feature is the base feature which provides ESA service for lines off the ABI cards on an MG9K.

A00003489: Subtending SMS from ABI

This feature is adding support for SMS to the ABI. It is another SN07 feature.

The following activities support ITP ESA. ABI ESA and ITP ESA have a common design and the ITP documents should be considered as preliminary reading. The ABI ESA documentation supersedes the ITP ESA documentation.

A00002020: ESA Translation Download [ITP - CM]

A00002019: ESA EM Enhancements [ITP - MG9000 EM]

A00001982: ESA Enhancements [ITP - MG9000]

The following activities are related to this activity.

A00003486: Gateway Location Information [CM]

106.5 Limitations and restrictions

106.5.1 Entering ESA

- Only calls that are in an active state (i.e. talking state) will survive warm entry into ESA mode.
- Calls that are intraswitched on RLCMs, OPMs, or OPACs can survive warm entry (not just network switched calls).
- Calls that won't survive entry into ESA mode may be released over a period of time (not immediately).
- Since P-phones are not supported on an RCS, they are not impacted by this feature.

106.5.2 During ESA

- Coin loop-start lines will be supported in ESA; however, ESA will supervise coin return upon call completion. The MG9K only supports CDF (Coin Dial First) and Coinless Coin phones.
- ESA between physical MG9000 master shelves (separate MGs) is not allowed.
- All members of a MADN group will be allowed to originate calls.
- Dialing a MADN member will result in a termination to the first idle MADN member and only this member. Not all MADN members will receive ringing.
- ESA is unavailable when DCC packs are out of service.

- ESA call processing is only supported between VMGs (ABIs or ITPs) currently in ESA on the same MG9000. Partial ESA (one VMG in ESA and another VMG not in ESA but on the same MG9000--commonly called *one up, one down*) is not supported.
- Emergency service (i.e. 911) translations are supported, but not emergency service features.
- No maintenance actions (whether from LCI, EMs, card-pulls, etc.) are recommended while in an ESA operational mode.
- Hunting is linear to those DNs physically residing on a VMG. Hunting on a hunt group that is divided across several VMGs does not guarantee true linear hunting for the entire group.
- Dialing directly to a DNH hunt member will cause a termination to that member. If the member is not available, hunting will be done only on the group members local to that VMG.
- If the "H" selector is used in table ESAPXLA then a call dialed with those digits will hunt through all hunt group members on the VMG. The Sequence Number, which normally causes hunting to start from a specific member, is not supported.
- The ESAPXLA table in the Core should be provisioned with the emergency service numbers (i.e. 911) needed while in ESA. Each VMG (as represented by an ABI XPM or LGRP) must be provided with its own emergency service line as well as table ESAPXLA translations terminating to the DN of that line.
- Basic call processing during ESA is supported for analog lines on RLCMs, OPMs, and OPACs. Intraswitching is not supported.

106.5.3 Exiting ESA

- Warm exit from ESA is not supported. Any call attempts or stable calls that coincide with exit from ESA will be torn down by the controlling MGC.
- Service codes are only supported on a limited basis for ESA. Emergency service 911 calls (or any other call using a service code) will not be preserved over ESA exit.

106.6 Interactions

While ABI ESA will be supported for the Legacy XPMs noted in section 106.2, it will not supersede Legacy ESA for Remote Switching Center (RSC) XPMs. RSCs that subtend an ABI XPM will enter existing Legacy ESA when an isolation occurs. They will not be controlled by ABI ESA. All existing RSC ESA functionality will remain intact.

106.7 Applicable customer facing sections

Fault Management

- Logs _ x ___
- Alarms _NA___

Configuration

- Data Schema _ x ___
- User Interface _ x ___
- Element Management _NA__
- Security _NA__
- Service Order _NA__
- Office Parameters _ x ___

Accounting (includes AMA billing) _NA__

Performance (includes operational measurements) _NA__

106.8 Glossary

Term	Description
ABI	Access Bridging Interface
AUL	Automatic Lines
CM	Computing Module
DCC	Data Controller Card
DLH	Distributed Line Hunt
DN	Directory Number
DNH	Directory Number Hunt
EM	Element Manager
ESA	Emergency Stand Alone
GW	Gateway
GWC	Gateway Controller
IBN	Integrated Business Network
ITP	Integrated Telephony Processor

Term	Description
LCI	Local Craft Interface
LGC	Line Group Controller
LGRP	Logical Group
LTC	Line/Trunk Controller
MADN	Multiple Appearance Directory Number
MG	Media Gateway
MG9K	Media Gateway 9000
MGC	Media Gateway Controller
MLH	Multi-line Hunt
OPAC	Outside Plant Access Cabinet
OPM	Outside Plant Module
PDN	Primary Directory Number
POTS	Plain Old Telephone Service
RLCM	Remote Line Concentrating Module
RLS	Release Key
RSC	Remote Switching Center
SCA	Single Call Arrangement
SMA2	Subscriber-Carrier Module Access 2
SMS	Subscriber Carrier Module SLC-96
VMG	Virtual Media Gateway
XPM	Extended Peripheral Module

107: Functional Description (FN): A00003698

107.1 Feature name

A00003698 - Razor Gateway Requirements For Trunking.

107.2 Description

This feature provides an extension to the existing CALLTRAK/TRMTRACE functionality found on the Core. Currently there isn't a way to initiate a Trmtrace to capture incoming SIP based calls. This shortcoming is addressed by functionality delivered to the Core, GWC, and the Session Server network elements.

This feature is primarily targetted to Customer Support groups like GNPS. While the tool will be available in the field, due to the impact of running a Calltrak session on the capacity of the field office, it should not be done on a regular basis or at high traffic levels.

107.2.1 Background information

Previous releases of the Calltrak/Trmtrace functionality provided the interfaces required to turn on and off the GateWay Controller Trmtrace functionality. Prior to SIP based calls, the Core was able to start the Trmtrace on the GWC for a new call and so capture the trace from the beginning of the call. For SIP calls, this was no longer sufficient. The Core found out about SIP calls too late in the Call sequence to start the trmtrace. Also, the SIP GWC that would be used for a SIP call was not always pre-defined. These shortcomings are addressed by the functionality delivered by this feature.

The Session Server and the Core will now be able to track and initiate the Trmtrace on a SIP call for both incoming and outgoing SIP trunks. The user will only need to know the trunk group CLLI for that SIP trunk (or Access Link) in order to capture the GWC Trmtrace from the beginning. The Session Server will also capture (locally) the SIP messages and GCP messages used in the life of the traced call.

107.2.2 Overview and Core information

The following is an overview of a typical tracing session.

1. Using the Calltrak interface, the user will select the SIP trunk (using the DPT select option). (No Changes to functionality)
2. The user will then start the calltrak trace. This has the following behaviour:
   a. The selected DPT trunk (in this case a SIP trunk) is noted and a 'setup' message is sent to a sip GWC.

b. The SIP GWC sends the setup message to each NGSS.

c. Each NGSS starts its trace on the selected trunk group/Link.

3. First call starts (either in the Core or NGSS).

a. The origination point sends a 'start_trmtrace' message to the selected SIP GWC.

b. The selected GWC initialized the trmtrace module to capture the trmtrace information on the supplied TID.

c. The selected GWC will also initialize a buffer to capture the messages (GCP messages specifically).

4. Other calls may or may not start/stop during this time.

5. First call Stops (either in the Core or the NGSS, based on which started it and knows it is being traced).

a. The release is sent followed by the 'stop_trmtrace' message for that TID.

b. The GWC stops the trmtrace for that TID (but doesn't touch other in-progress tracing).

6. More of the other calls...

7. The user stops the calltrak trace.

a. The setdown message is sent to the arbitrary SIP GWC.

b. GWC forwards the message to each NGSS

c. Each NGSS stops in-progress call trmtraces and responds to the GWC with a list of stopped trmtrace descriptions (ie, like in the core output: GWC 9, TID 17...) for each TID that was traced on.

d. This GWC then collects all responses and sends one or more unsolicted message to the core with this information.

e. Core outputs the list of stopped trmtrace messages to the user (using existing interface).

8. User is able to retrieve the captured information from the appropriate network elements in the GWC list and the NGSS.

There are no new Core interfaces. The current CallTrak and TRMTRACE interfaces are utilized along with the SELECT DPT option. Once a SIP trunk group is SELECTed, the TRMTRACE ON and START commands will work together to initiate the functionality.

Every effort is made to keep the user interfaces the same where they existed previously. For example the CallTrak interface to select a SIP based trunk is unchanged (the SELECT DPT option is utilized) and no other option needs to be set.

107.2.3 GWC information

The GateWay Controller interface to display the captured trmtrace information will be the same (trmtrc, printout, dumpall). There will not be another interface to display the captured GCP messages (as these are captured on the NGSS). There is a command to display the TID to CallID mapping for calls that are traced from the NGSS. The following is an example:

From the GWC Telnet session (or PMDEBUG session, although that is very slow and is not recommended):

GWCUP>NGss

Config,Debug,Traces.

NGss> Traces

CLearlistcalli,GCPDebugtrace,GCPDPtdebugtra,GCPDPTMsgtrace,

GCPIsupdebugtr,GCPISUPMsgtrac,GCPISUPProctra,GCPMsgtrace,

GCPUDPDebugtra,GCPUdpmsgtrace,MTCDebugtrace,MTCMsgtrace,

MTCProctrace,**TRmtrccallidti**.

GCPDebug>TRmtrccallidti

Sorry, No Call Data available

(or if there is something, it will have a list of callID to TID's)

Traces> CLearlistcalli

!! List is Empty

(or list is cleared)

There are limitations to the output from the commands. Only the last 20 calls will be output in the callID to Tid mapping list for this GWC. The data is stored in a circular buffer and will over-write the oldest data first when more than 20 calls have been trmtraced from the NGSS.

107.2.4 NGSS information

The Session Server will only have a file that needs to be looked at to collect the information that is captured. The file is located in the application traces directory:

/opt/apps/logs

And the filename is:

NGSS_trmtrace.trace

The file will never be deleted automatically by the tool (unless it is very old and the partition has reached it's upper limit - see limitations section), so the craft will always have to ensure to remove the file after collecting the information. The file can be looked at using on board tools like 'cat', 'vi', and 'more'. Also the file could be copied off board for downstream use.

The file will contain SIP messages, GCP messages, and basic call flow information like timestamp, direction of call, and callID. This information will be presented in ASCI format (indented to provide readability).

107.3 Hardware Requirements or Dependencies

Customer offices without the Session Server will not have the functionality delivered by this feature.

107.4 Software Requirements or Dependencies

The Session Server feature, A00003280 (SP2K Debug and Tracing) must be available. Also, certain other features developed for the Session Server will be required (Call Processing support, etc) as well.

107.5 Limitations and restrictions

The feature will only apply to offices with the Session Server, SIP application. The VRDN support will not be implemented with this feature.

There will be a limitation on the file size in use on the NGSS per session. The upper limit of data per session will be 10 Mb. The size of the NGSS_trmtrace.txt file will continue to grow over multiple sessions as the information will not be removed unless the craftperson takes a manual action. The upper limit of the /opt/apps/logs directory will be enforced within the trace server application (see Actiivty A00003280), but the only files that will be removed autonomously are the the ones that have their name start with "siptrace".

The GWC will only contain a listing of the latest 20 calls that started TrmTrc from the NGSS. The mapping of NGSS CallID to TID will be limited to this.

107.6 Interactions

N/A

107.7 Applicable customer facing sections

Fault Management

- Logs _____N
- Alarms _____N

Configuration

- Data Schema _____N
- User Interface _____N
- Element Management _____N
- Security _____N
- Service Order _____N
- Office Parameters _____N

Accounting (includes AMA billing) _____N

Performance (includes operational measurements) _____N

107.8 Glossary

Term	Description
NGSS	Another acronym for the Session Server
GWC	GateWay Controller
SIP	In-band signalling protocol, RFC 2962
VRDN	GWC that provides the SIP session server functioanlity, to be replaced by the NGSS.

108: Functional Description (FN): A00003704

108.1 Feature name

OSSAIN Enhancements for SN07

108.2 Description

The feature enhances the OSSAIN product with the following:

- Short Messaging Service
- Wireless Release Link Trunking for Directory Assistance Call Completion
- Alternate Hosting for Passive Operators
- Alter Speech Path for no ANI Calls
- Passive Operator Message Capacity Enhancement
- DA SN Request for DAS Only Service
- Alter Speech Path during Passive Function Provider Connections
- OSAC Session Pool State Inform Message Usage
- Authorization Codes and Module Code 305
- AMA Service ID Usage
- Resource Increases
- OSSAIN Open Automated Protocol (OAP) Version 9.0 and SOC

Short Messaging Service (SMS) is fully designed under feature A00003687; however this feature provides the needed OSSAIN changes to support SMS for SNs. This includes informing the SN of a wireless caller, and processing an SMS message received from the SN.

Wireless Release Link Trunking (RLT) for Directory Assistance Call Completion is designed under feature A00000816 and A00003687; however, this feature will add the wireless RLT functionality for OSSAIN SN DACC calls.

Alternate Hosting for Passive Operators is supported by this feature. It allows an alternate host to be selected for passive operator requests which cannot be serviced by the primary host.

Alter Speech Path for no-ANI Calls is supported by this feature. Incoming IT trunks which do not forward ANI but use DA SN functionality require the ability to split/join the calling party as needed.

Passive Operator Message Capacity Enhancement reduces the amount of OPP messaging sent to position when a SN releases itself from the call.

DA SN Request for DAS-only service allows a SN to request DAS services without attaching an operator.

Alter Speech Path during Passive Function Provider Connections allows a SN to forward an optional datablock to the switch to indicate the switch should alter the speech path when connecting a passive operator.

OSAC Session Pool State Inform Message Usage allows the SN to be informed of OSN state changes for SN originated session pools. It disables the unnecessary message from being used for other origination types such as subscriber originated.

Authorization Codes allow a SN to send an authorization code to TOPS to be included in AMA for calling cards, commercial credit cards, and authcodes. This feature also updates AMA and TDR to support generating an alphanumeric authcode for commercial credit cards.

AMA Service ID ensures the service id sent from the SN will be used in AMA records instead of one defined in datafill in either table AMASRVID or TQMSSERV.

Resource Increases ensures OAP can support increases to the number of operators, positions, services, and call queues.

OAP Protocol Version 9.0 adds support for the above new functions. With the addition of version 9.0, the number of back releases will be increased to also support version 5.0. Version 9.0 is included in SOC option, OSAN0102; however, it has a new TOPSFTR entry, OSSAIN_RELEASE_20, to activate the functionality.

108.2.1 Short Messaging Service (SMS)

SMS functionality, as provided by feature A00003687, can be used to send text messages to a wireless caller. It allows an operator or a SN to forward SMS text messages to TOPS; TOPS will forward the message on to a Message Center (MC); and the MC forwards it to the subscriber. In order for a SN to send a SMS message to TOPS, OAP enhancements are needed and provided by this feature.

To send SMS messages, a SN will need to know if the caller is wireless. TOPS will use phone class type of ‘mobile’ for all wireless callers supported.

For wireless (mobile) calls, a SN can utilize a new OAP operation to send SMS messages to the caller. The new operation, **SMS Request Operation**, includes

one new datablock. The new datablock, **SMS Datablock**, contains the following fields:

- existing field, **Directory Number Digit Count**, to record number of digits in the destination number
- existing field, **Directory Number**, to record the destination number
- new field, **SMS Text Block Length**, to indicate length of text message
- new field, **SMS Text Block**, to include the text message up to 200 bytes

The switch will respond with either one of the following responses:

- **SMS Success Response**
- **SMS Error Response**

The responses indicate the switch has processed the message and attempted to forward it to the Message Center. Responses from the Message Center are not forwarded to the SN.

New OM registers are added to existing OM group, OAPCP10, to record the usage of this new operation and it's responses.

Note: OAP will not restrict the allowed character set for SMS messages.

108.2.2 Wireless RLT for Directory Assistance Call Completion (DACC)

Features A00000816 and A00003687 provide wireless services which include DACC and RLT for the TOPS environment. This feature supports RLT for wireless DACC calls in the OSSAIN environment.

The SN will be informed if RLT is eligible for the wireless call. If so, and the SN requests RLT in the float request for DACC, then OSSAIN will perform wireless RLT and release the call.

108.2.3 Alternate Hosting for Passive Operators

Alternate hosting, as provided by feature NC0152, is supported in OSSAIN for passive operators with this feature's release. If a passive operator is requested from a host which either is not available or the call deflects/overflows, table OCHOSTQ is consulted to determine if an alternate host is datafilled.

If an alternate host is defined in table OCHOSTQ for the passive operator's call queue, then it will be used based on the options datafilled. The options include datalink failure, deflection, and queue overflow. If one of these options occurs and is datafilled, then the call will route to the alternate host datafilled. Only one alternate host can be datafilled for all options per call queue.

Thus, if a passive operator request was received by TOPS and the call was sent to a host which deflected the call (for example), then TOPS would check table

OCHOSTQ, per the call queue, and determine if an alternate host is available for deflect purposes. If found, TOPS would request an operator from the alternate host giving the passive operator request a second chance.

OSSAIN supports both standalone and OC environments for alternate hosting as defined by existing table OCHOSTQ and OCPARMS parameter, SWITCH_NAME.

The SN is only informed once for either a success or failure. It will not be informed when the first attempt fails and an alternate host is selected. Thus, if the SN runs a timer and chooses to utilize alternate hosting, the timer should be increased to account for alternate host requests.

108.2.4 Alter Speech Path for no ANI calls

A SN is able to alter the speech path for a calling party with no directory number. This is necessary for IT trunks which do not send ANI but do use Service Nodes for DA Automation.

108.2.5 Passive Operator Message Capacity Enhancement

This feature enhances the AN1926: OSSAIN Simultaneous Interactions design by reducing the number of OPP messages sent to position when the SN releases itself. The original design sent all call details when the position was connected and again when the SN was released. The new design will eliminate resending full call details when the SN is released for certain scenarios.

If only the following operations or no operations are sent from the SN between connecting the passive operator and releasing the SN, then full call details will not be sent.

- Speech Path Request
- Pass Thru Request
- Gen AMA Request
- Append AMA Request

These operations either alter the operator's display when the operation is processed or has no effect on displays.

Other operations which do not affect the operator displays on SN release may be added in a future release; however, this initial structure introduced will ensure the reduction in OPP messaging for basic DAA calls.

108.2.6 DA SN Route to DAS-only Service

A DA SN may need to route a call to the DAS environment without attaching an operator. It may do this to utilize DAS automated functions such as announcements and call completion.

This feature changes the TOPSAUTO option of table OAFUNDEF to include a DAS option. Since the DAS option will require a CT4Q and refinement option, instead of OPRONFL, the TOPSAUTO option is now broken into refinement areas for each automated system.

When the DAS automated function is used, the call will be routed to the DAS without an operator being attached. If ADASPLUS is available for the call, the DAS Call Begin message will contain the ADASPLUS eligible indicator. There are no changes to the ADAS+ functionality nor is this feature dependent on ADAS+.

If an error occurs, such as timing out after sending the call begin, then call is then sent to an operator.

Table 1 Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DAS_NO_OPER	TOPSAUTO DAS DAS_ONLY N
2	DAS_OPER	TOPSOPER DAS_OPER N
3	AABS	TOPSAUTO AABS AABS_CT4Q
4	DA_SN	SN DASERV N N N N Y CQ17 N

```
TYPE IS FUNCTYPE_VAR_AREA              MULTIPLE WITH
        FUNCTYPE                       {SN,TOPSOPER,TOPSAUTO} REFINEMENTS:
        {SN}                           MULTIPLE WITH
            ... unchanged

        {TOPSAUTO}                        MULTIPLE WITH
            AUTOSYS_AREA              MULTIPLE WITH
              AUTOSYS                 {AABS,MCCS,ACTS,BRANDING,DAS} REFINEMENTS:
              {AABS}                  MULTIPLE WITH
                OPRONFL               TQMS_SR_CALL_TYPE_FOR_QUEUEING
              {MCCS}                  MULTIPLE WITH
                OPRONFL               TQMS_SR_CALL_TYPE_FOR_QUEUEING
              ...
              {DAS}                   MULTIPLE WITH
                DASCT4Q               TQMS_SR_CALL_TYPE_FOR_QUEUEING
                QMS_AREA              MULTIPLE WITH
                  QREFINMT               {N,Y} REFINEMENTS:
                  {Y}                    MULTIPLE WITH
                       CQORDER           {PREOPR,POSTAUTO,RECALL,ASST}
                  {N}                    QMS_REFINE_N_REFINEMENT

        {TOPSOPER}                        MULTIPLE WITH
            ... unchanged
```

108.2.7 Alter Speech Path during Passive Function Provider Connections

There is a DAA (Directory Assistance Automation via DA SN) scenario in which an operator and the subscriber are incorrectly hearing portions of music on hold and call arrival tones. The following further describes the scenario and the enhancement to alleviate this problem.

For a DA SN, a passive operator request can result in the caller being placed into queue for a brief period of time. When an operator becomes available, he/she is connected to the call and the SN is notified. The SN may respond by sending speech path change requests to alter the speech path for the calling party so they do not hear the call arrival tones and the operator does not hear the music on hold announcement.

Since there is a small amount of processing time, pre-SN07 functionality does allow the subscriber to hear call arrival tones and the operator to hear part of the music on hold announcement (all varying based upon processing time).

Following is a possible DAA passive operator call scenario and OAP messaging:

1. Subscriber dials a DA call. TOPS connects a service node voice link to the call and routes the call to a DAA node.
2. TOPS sends the Session Begin message to the DAA node.
3. The DAA node (active node) collects the city and listing information from the subscriber.
4. DAA node sends TOPS a Passive Function Provider Request.
5. TOPS responds by sending a Call Queue Information DB indicating the call has been queued.
6. At this point the DAA node begins playing an announcement to the subscriber indicating their queued condition.
7. Once a position becomes available, TOPS informs the DAA node by sending a Passive Operator Being Connected Message.
8. Shortly after the above message, TOPS sends the Passive Operator Connected Message.
9. The DAA node sends TOPS a Speech Path Request message instructing TOPS to make the subscriber voice path 0-way.

Before TOPS can execute the Node's instruction the call arrival tones have already been played and the operator may hear music on hold.

10. The DAA node plays the city and listing information to the operator.

OSSAIN is enhanced in SN07 to allow the Speech Path DB to be optionally included in the Passive Function Provider Request operation. If included it will be stored and processed when the passive operator is connected. It includes a new range of options to indicate the party and status to apply when the operator is connected. OAP 9.0 is required to support this new option.

108.2.8 OSAC Session Pool State Inform Message Usage

For Operator Services Nodes (OSN) in an OSAC remote, this feature restricts the usage of the Session Pool State Inform message to SN originated session pools only. It removes the unnecessary message from being sent for other session pool originators, such as subscriber, in an OSN.

- When an OSN session pool, datafilled as SN origtype in table OASESNPL of the OSAC remote, changes state (busy or return to service), the SN will be informed so it does not attempt to originate a session to the remote.
- When other OSN session pool originators (subscriber, OSACORIG, OSACTERM) change state in the remote, the SN does not need to be notified. This feature disables the ability to send the message for these session pools.

108.2.9 Authorization Codes

There are a number of scenarios in which a SN may need to send TOPS an authorization code to be placed into the AMA record. This feature enhances OAP version 9.0 to support a new datablock and fields to provide authorization codes from the SN to TOPS.

To support both alphanumeric and numeric codes, the new OAP field allows up to 20 ASCII characters. The SN will need to ensure any BCD formatted authcode is converted prior to populating OAP. TOPS will read the field as ASCII and convert to other formats as needed.

The SN will also need to populate OAP with the type of authorization code being sent. Included in AMA records, and available in OAP, are the following:

- Calling cards - Module Code 611 with generic context id 80002 supports up to 15 digits to record authorization code received from the bank.
- Commercial Credit cards - New Module Code 305 supports up to 15 EBCDIC characters to record the alphanumeric authorization code received from the clearing house.
- Authcode - Module Code 102 supports 14 digits to record the authorization code entered by the subscriber and validated by the bank.

108.2.9.1 AMA Module Code 305 and TDR

New module code 305 is supported to generate an alphanumeric authorization code as provided by commercial credit card clearing houses. It will be used in place of module code 611, which generates a numeric authorization code used by calling cards.

Both AMA and TDR billing systems have been updated to include the new information. AMA supports new module code 305; while TDR supports a new field, commercial credit card authcode, in the appropriate templates.

The downstream billing processors will need to be prepared to accept the commercial credit card authorization code information when working with commercial credit cards.

Note: AMA module code 305 uses OFCENG/OFCAUT CRS_SUBRU_POOL2_SIZE and thus it must be re-provisioned appropriately.

108.2.10 AMA Service ID Usage

TOPS allows a user-defined service id to be placed into AMA. TOPS can obtain the service id from datafill or from an OAP message. This feature ensures a service id sent from a SN via OAP is used instead of datafill defined in tables AMASRVID or TQMSSERV.

108.2.11 Resource Increases

This feature ensures OAP can support resource increases for the following:

- Operator IDs up to 65,535
- Position IDs up to 9999
- Call Queue IDs up to 8190

Note: Although this feature ensures OAP can send and receive these higher ranges, it does not alter either TOPS base or AMA functionality. To utilize these new ranges, ensure TOPS base and AMA modifications have been completed.

108.2.12 OAP Protocol Version 9.0

OAP protocol version 9.0 includes all new OAP information provided by this feature and discussed in this document. The enhancements include:

108.2.12.1 New / changed Fields

- New field, SMS Text Block
- New field, SMS Text Block Length
- Existing field, Speech Path Status is expanded to include options to indicate to alter speech path when the operator is connected
- New field, Authorization Number Type (Format)
- New field, Authorization Code Length
- New field, Authorization Code

108.2.12.2 New / Changed Datablocks

- New datablock, SMS DB
- New datablock, Authorization Number DB

108.2.12.3 New / Changed Operations

- New operation, SMS Request
- New operation, SMS Success Response
- New operation, SMS Error Response
- Existing operation, Passive Function Provide Request has a new optional datablock, Speech Path DB.
- Existing operation, Class Charge Request, has a new optional datablock, Authorization Code DB.

  Note: OAP 5.0 will be supported along with OAP 9.0. This feature changes support for 3 versions back to 4 versions back.

Please reference *OSSAIN OAP Specification Document - NIS Q235-1 (version 2.0)* for details of the changes.

108.2.13 SOC and Table TOPSFTR

OAP 9.0 and functionality described in this document are controlled by existing SOC option OSAN0102; however, table TOPSFTR is changed to included a new entry for OSSAIN_RELEASE_20. TOPSFTR can be used to turn this feature's functionality on/off as needed.

108.3 Hardware Requirements or Dependencies

None

108.4 Software Requirements or Dependencies

- OSSAIN Enhancements, SOC option OSAN0102
- OSSAIN base functionality, SOC option OSAN0101
- TOPS base functionality, SOC option OSB00101

108.5 TOPS SMS engineering considerations

Short messages sent by TOPS can be up to 200 characters in length. When headers and ancillary fields are added in, the overall message length can reach 250 bytes. Each time a position or automated node sends a SMS which is then forwarded to the SS7 network, the SMS is actually sent twice: once using OPP or OAP over IP from the position or service node to the switch, and once over the SS7 links into the network.

If a switch is supporting 300 active operators handling 20-second directory assistance calls, and an SMS containing the listing is sent on each call, this represents 54,000 calls per hour at 250 bytes per call. The total is 13.5 megabytes per hour which is equivalent to 3.75 kilobytes per second.

Both the IP links to the positions and service nodes as well as the SS7 links to the network must be able to handle this increased messaging. Call durations, numbers of operators, and SMS-to-call ratio should be taken into account when deploying SMS functionality.

108.6 Limitations and restrictions

- SMS may affect EIU provisioning. Please refer to the above engineering considerations and the OSSAIN User's Guide for more information.
- Although this feature ensures OAP can handle resource increases as noted, it does not modify TOPS base nor AMA functionality necessary to utilize the new ranges.
- New TOPSAUTO function, DAS can be used for transferring; however, like all TOPSAUTO functions, it is not available for triggering/recalls nor passive operator requests.

108.7 Interactions

The new DAS function in table OAFUNDEF does not interact with existing ADAS+ functionality. ADAS+ can be setup for the DAS function, but is not required to obtain DAS-only service.

108.8 Glossary

Term	Description
ANI	Automated Number Identifier
CT4Q	Call Type For Queuing
DAA	Directory Assistance Automation
DACC	Directory Assistance Call Completion
DB	DataBlock
EIU	Ethernet Interface Unit
OAP	OSSAIN Open Automated Protocol
OSAC	OSSAIN Centralization
OSN	OSAC Service Node

Term	Description
OSSAIN	Operator Services Systems Advanced Intelligent Network
RLT	Release Link Trunking
SMS	Short Messaging Service
SN	Service Node

109: Functional Description (FN): A00003711

109.1 Feature name

CS2000 SUPPPORT FOR GateWay Inter Machine Trunk (GWIMT) ON Passport Voice Gateway

109.2 Description

This activity provides a limited set of gateway services on the long distance application of Succession Communication Server 2000 with a partial compliance of ITU-T Recommendation Q.767 Blue Book version signaling protocol and ITU-T Recommendation Q.764 White Book version) (ISUP92) signaling protocol (international use only). This functionality is supported on the IMT GLOBAL trunk agency which are provisioned as gateway trunk agents[1]. This feature supports interworking the gateway trunk agency with a set of supported national long distance signalling agencies.

109.3 Functional overview

109.3.1 Background

The IMT Global trunk agency on the Succession CS2000 is enhanced to support a limited set of gateway services and a partial compliance of ITU-T Recommendation Q.767 Blue Book version (Q.767) and an international use of ITU-T Recommendation Q.764 White Book version (ISUP92).

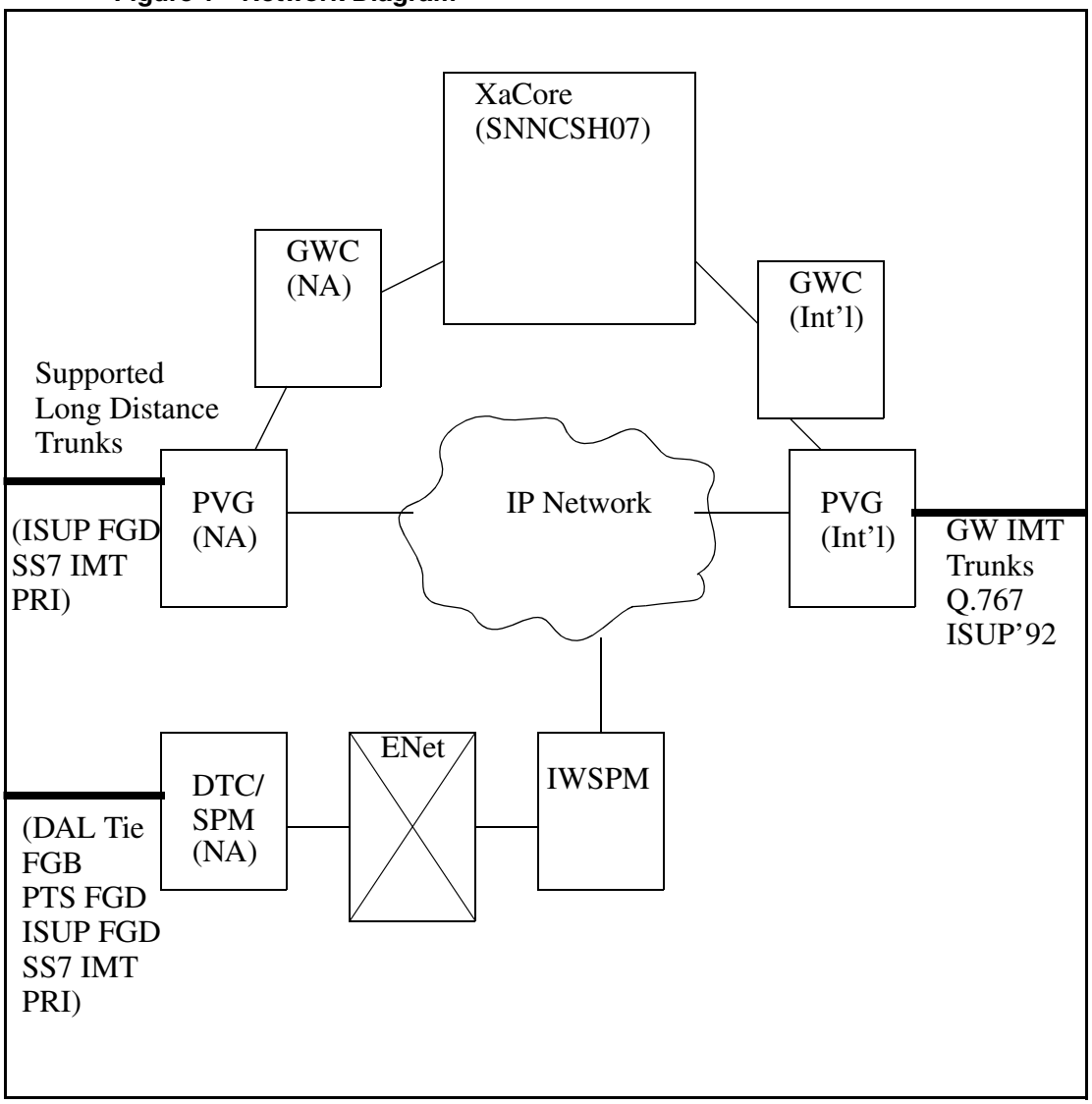
This feature allows Inter-eXchange Carriers (IXC) in World Zone-1 countries to provide limited gateway services on the Succession Communication Server 2000 operating as a UCS DMS-250 with either Q.767 or ISUP92 protocols.

109.3.2 Network Overview

This feature allows the IXCs to connect Succession CS2000 directly to foreign exchanges in the international network with either Q.767 or ISUP92 protocol signalling. This feature supports interworking gateway trunk agency with a set of existing UCS national trunk agencies. The following diagram shows the network connectivity for gateway trunk on Succession CS2000.

[1]IMT trunk agent in Table TRKGRP provisioned with NETSPEC field value of GLOBAL and new table TRKGRP option GWYTRK

Figure 1 Network Diagram



109.3.3 Supported Gateway services

The limited set of gateway functionality is supported by this feature on the Succession CS2000 and is only applicable in the World Zone-1 (WZ-1) market. The new functionality introduced by this feature includes:

- Introduction of new option GWYTRK in table TRKGRP to provision the IMT GLOBAL trunks agents as gateway trunks.
- Support for Q.767 and ISUP92 (international use) signalling protocol on the IMT GLOBAL trunk agency with GWYTRK option.
- Message Compatibility and Parameter compatibility procedures on gateway trunks with ISUP92 protocol.

- Interworking between ISUP92/Q.767 gateway trunks and supported national long distance trunk agencies:
  - IMT Inter
  - IMT Intra
  - FGD SS7
  - FGD PTS[1]
  - UCS PRI
  - FGB[1]
  - DAL TIE[1] [2]
- Support of direct termination and transit 15-digit IDDD calls.
- Support direct termination and transit Code 11 and Code 12 calls (operator assisted calls).
- Support of tie-route connection between Succession CS2000 Communication Servers within WZ-1 using ISUP92/Q.767 gateway trunks.
- Mapping of new cause values defined in ITU-T Recommendation Q.850 received on ISUP92 to normal_unspecified on non-ISUP92 trunks.
- Introduction of new protocol Q.767 in table CSEMAP and TMTMAP for ISUP92/Q.767 gateway trunk agents.
- Calling Party Category (CPC) screening, routing, and override.
- Data calls
- Test calls
- Supporting Q.767 and ISUP92 gateway trunks as terminating agents for Carrier AIN (AIN) calls on supported national long distance trunk agents.
- Support of table C7UPTMR for Q.767 and ISUP92 gateway trunks
- New SOC option GIMT0003 to control gateway services.

109.4 Feature description

109.4.1 Enhancements to IMT Global trunk agency

The existing IMT Global trunk agency is enhanced to provide gateway services. Gateway trunks are provisioned in table TRKGRP as IMT Global trunks~~,~~ with GWYTRK option selected.

[1]PTS trunks supported only in hybrid configuration

[2]Supported DAL TIE pulse type of MF and DT and start signal of WINK.

The GWYTRK option prompts for two fields SERVCC and C11C12PT. The field SERVCC identifies the serving country code of the foreign exchange in which the gateway trunk is connected. The field C11C12PT provides a pretranslator name for Code 11 and Code 12 calls received on the gateway trunk agency. Please refer to section 1.4.3 Gateway Services for applications of these fields.

On the gateway trunks, two versions of SS7 protocol for international use are supported:

- ISUP92

ISUP92 refers to partial compliance to ITU-T Recommendation Q.764 White Book version that is provided by this feature. The ISUP92 protocol is provisioned in table TRKSGRP with protocol CCITT version ISUP92 and variant V1.

- Q.767

Q.767 refers to ITU-T Recommendation Q.767 BlueBook version that is provided by this feature. The Q.767 protocol is provisioned in table TRKSGRP with protocol CCITT version BLUE and variant V1.

109.4.2 Message Protocols

The following sections describe the support for limited set of Q.767 and ISUP92 protocols that this feature provides.

109.4.2.1 Support for ISUP92 protocol

This feature provides the following support for ISUP92 protocol agencies:

1. Allows IMT Global trunks to be provisioned as ISUP92 trunks in table TRKSGRP with protocol CCITT, version ISUP92 and variant V1 (hereafter referred to as ISUP92 gateway trunk).
2. This features introduces a new option GWYTRK for IMT Global agents in table TRKGRP. This option enables gateway functionality on the ISUP92 trunks and provisions the trunk for international use of the ISUP92 protocol.
3. Message Compatibility Parameter (MCP) processing as per the ISUP92 recommendations in Q.764, Section 2.9.5.2 - 2.9.5.4
4. Parameter Compatibility Parameter (PCP) processing as per the ISUP92 recommendations in Q.764, Section 2.9.5.2 - 2.9.5.4
5. Mapping of new cause values received on ISUP92 trunks to Normal unspecified (31) if the other trunk in the call is one of the other supported trunk agencies.

For more information see “APPENDIX A: Messages and Parameters Supported on ISUP92” on page 1123.

109.4.2.1.1 Handling of Unexpected messages received on ISUP92 An unexpected or out of sequence message is a message which is supported, and is valid, but has been received when it is not expected in the call.

If such messages are received, the following applies:

- If a Release (REL) message is received for a circuit which is idle, it is acknowledged with a Release Complete message.
- If a Release Complete message is received relating to an idle circuit, it is ignored.
- If any other message is received relating to an idle circuit, a reset message is sent.

In general, unexpected messages received relating to call processing busy circuit, are ignored with the following qualifications:

- Release message and any circuit supervision messages are accepted and processed at any time during the call.
- After sending an IAM, and prior to receiving an ACM or CON, only REL and CPG messages are accepted. Receipt of any other message causes a release sequence to be initiated.
- After a Release message is received, any other call-related messages are discarded.
- If a Release Complete message is received relating to a busy circuit for which a Release message has not been sent, the circuit is released and a Release message sent.
- Blocking messages may be received at any time.

109.4.2.1.2 MCP/PCP processing

109.4.2.1.2.1 Compatibility procedures

The compatibility procedures[1] described below have been designed to ensure predictable network behavior, when the switch receives unrecognized signaling information. Refer to ISUP92 Q.761-Q.764 for a more detailed explanation of the compatibility procedures.

The ISUP92 recommendation Q.764, Section 2.9.5.3, recommends that if a message arrives that is unrecognized, or contains unrecognized parameters, the switch follows a compatibility procedure. Two new optional parameters

[1]In this document MCP means Message Compatibility information Parameter and PCP means Parameter Compatibility information Parameter.

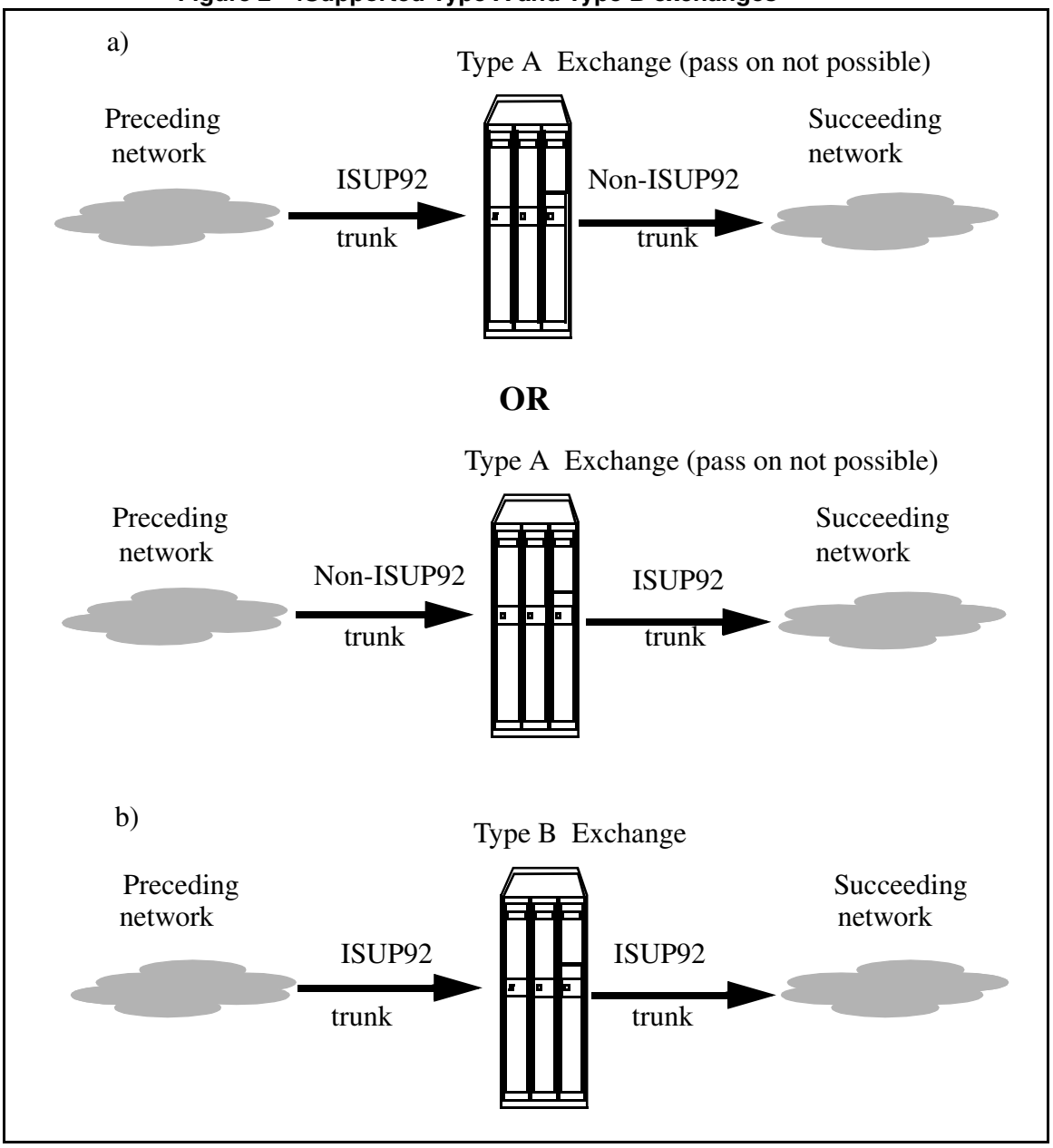
provide the functionality of the compatibility procedure: the message and parameter compatibility parameters.

109.4.2.1.2.2 Operation of the CS2000 as a Type A and Type B exchange

The Succession CS2000 interprets compatibility procedures found in
compatibility parameters according to the type of exchange. The Succession CS2000 behaves as a Type B exchange when both trunks (the originating and terminating trunks) in the call are ISUP92 gateway trunks; otherwise, Succession CS2000 behaves as a Type A exchange (pass on not possible). Succession CS2000 does not support behaving as a Type A exchange (pass on possible).

Examples of Type A and Type B exchanges supported by Succession CS2000 are given in Figure 2

Figure 2 .Supported Type A and Type B exchanges



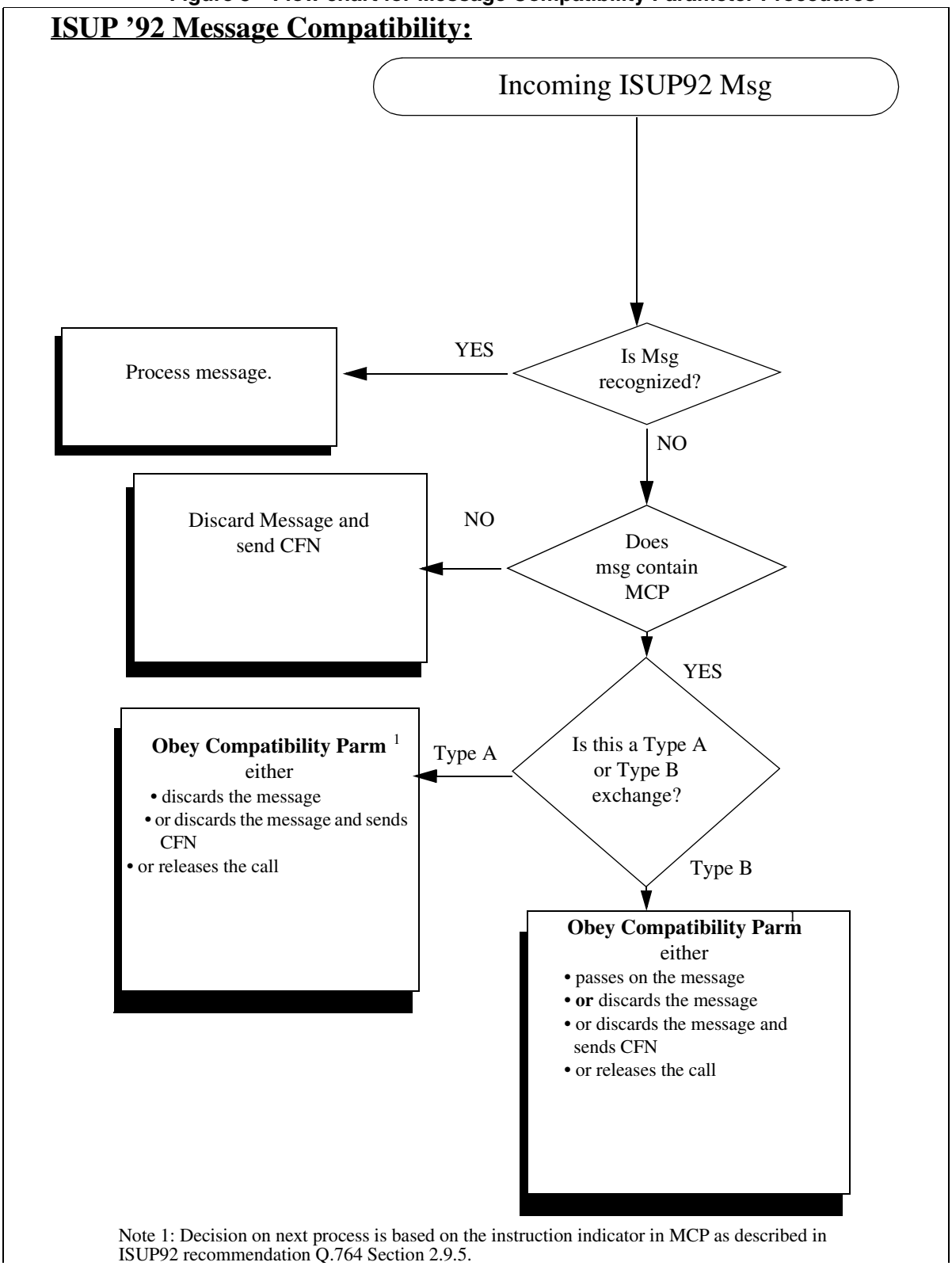
109.4.2.1.2.1 Message Compatibility Parameter Procedure

The MCP information pertains to the procedure to be followed, if the switch does not recognize an incoming message. Compatibility procedures can be applied at either a Type A or Type B exchange.

This feature provides the functionality to scan any unrecognized message received from an ISUP92 trunk for the optional MCP. If the message contains the parameter, the Succession CS2000 obeys the parameter. If there is no MCP in an unrecognized message, the switch discards the message and returns a confusion message. All CFN messages generated as a result of MCP processing contain appropriate cause and diagnostic information.

When the Succession CS2000 acts as a Type A exchange, it may receive an ISUP92-compliant Network Resource Message (NRM). The NRM is not one of the minimum set of mandatory messages that the Succession CS2000 must recognize, as stated in the ISUP92 recommendation Q.761, Table 3. Upon receipt of this message at the Succession CS2000, the switch scans the NRM for
the optional MCP. If the switch finds the parameter, it applies the message compatibility parameter procedure for Type B exchange. Figure 3 shows a flowchart of the procedure followed upon receipt of an ISUP92 message at the Succession CS2000.

Figure 3 Flow chart for Message Compatibility Parameter Procedures



Note 1: Decision on next process is based on the instruction indicator in MCP as described in ISUP92 recommendation Q.764 Section 2.9.5.

Note:
As a Type B exchange, the Succession CS2000 may transit an unrecognized message. As a Type A exchange, the Succession CS2000 does not transit an unrecognized message.

Table 1 and Table 2 explain how the switch interprets the instruction indication's bit patterns to execute the subsequent process. This is based on ISUP92 recommendation Q.764, Section 2.9.5.

Table 1 Message Compatibility for a Type A exchange (pass on not possible)

Bits								Meaning
H	***G***	***F***	**E**	**D**	**C**	**B**	**A**	
X	X	X	X	X	X	1	X	Release Call
X	X	X	0	0	X	0	X	Release Call
X	X	X	1	0	0	0	X	Discard Message
X	X	X	1	0	1	0	X	Discard Message and send CFN[a]
X	X	X	X	1	0	0	X	Discard Message
X	X	X	X	1	1	0	X	Discard Message and send CFN[a]

a. CFN messages contain an appropriate cause value and diagnostic information.

Table 2 Message Compatibility for a Type B exchange

Bits								Meaning
H	***G***	***F***	**E**	**D**	**C**	**B**	**A**	
X	X	X	X	X	X	1	1	Release Call
X	X	X	X	0	X	0	1	Pass on Message
X	X	X	X	1	0	0	1	Discard Message
X	X	X	X	1	1	0	1	Discard Message and send CFN[a]
X	X	X	X	X	X	X	0	Pass on Message

a. CFN messages contain an appropriate cause value and diagnostic information.

where bit A is Transit at Intermediate Exchange Indicator,
0 = Transit interpretation
1 = End node interpretation

Note:

Only type B exchanges examine this indicator. If it is set to "Transit Interpretation", the other indicators are ignored. If it is set to "End Node Interpretation", the following actions are performed.

bit B is Release Call Indicator,
0 = Do not release
1 = Release call
bit C is Send Notification Indicator,
0 = Do not send
1 = Send notification
bit D is Discard Message Indicator,
0 = Do not discard message
1 = Discard message
bit E is Pass On Not Possible Indicator,
0 = release call
1 = discard information
bits F-G are spare bits,
bit H is Extension Indicator, and
X means a don’t care value.

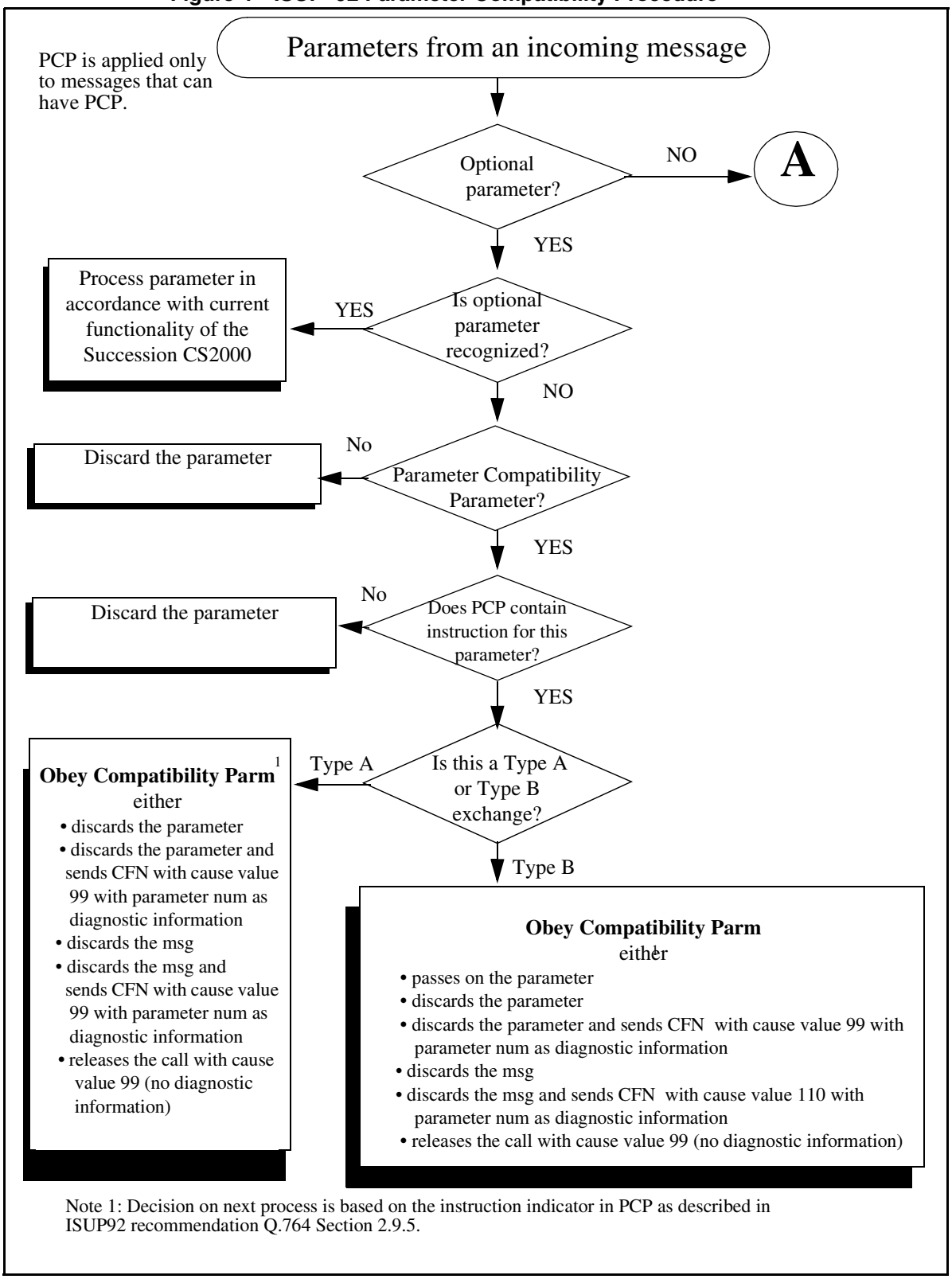
109.4.2.1.2.0.1 Parameter Compatibility Parameter Procedure

The PCP contains information pertaining to the procedure the Succession CS2000 follows if it recognizes an incoming message, but it does not recognize one of the parameters contained in that message. The switch can only treat optional parameters as unrecognized parameters, since it always recognizes mandatory parameters.

This feature allows the Succession CS2000 to scan messages for the optional PCP when it receives the messages from an ISUP92 trunk. If the switch finds a PCP within the message, it obeys the instruction of the parameter. Please refer to Figure 4 and Figure 5 for the procedure the switch follows when it receives unrecognized information in messages that can have PCP.

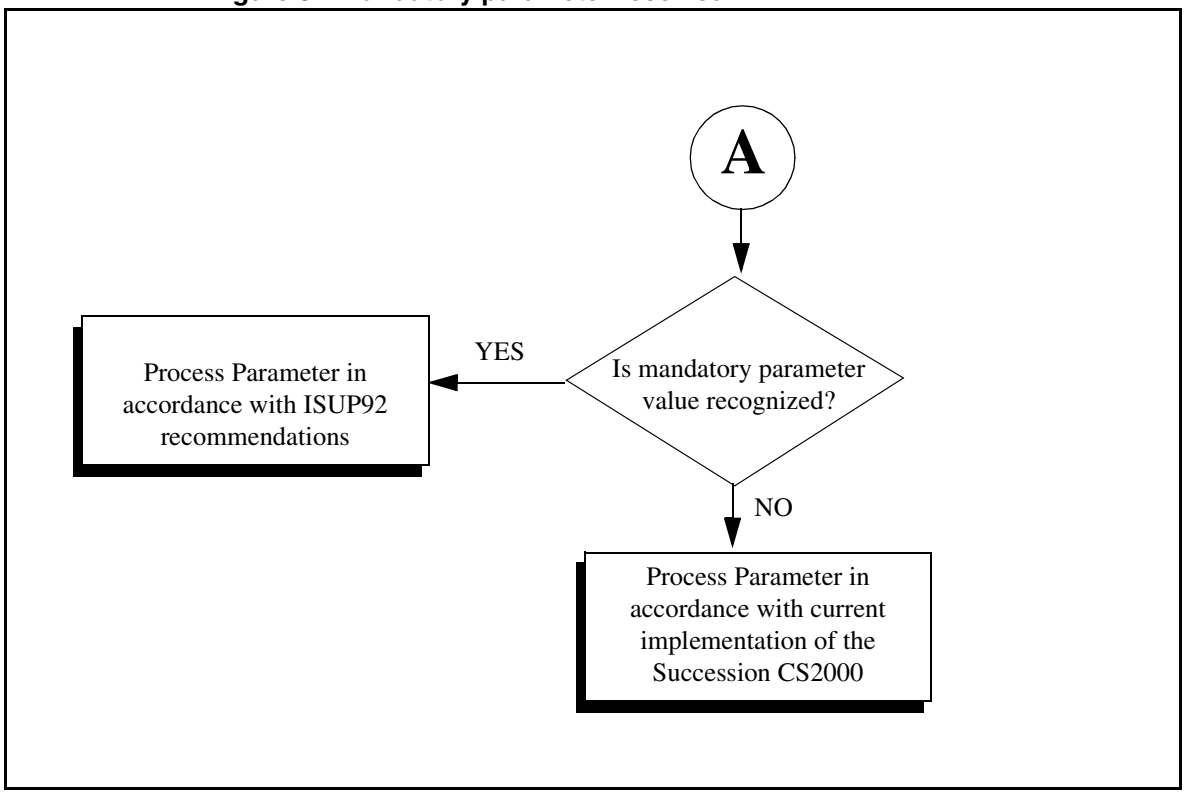
All CFN messages generated as a result of PCP processing contain appropriate cause and diagnostic information.The Diagnostic Information includes all the parameters that caused

Figure 4 ISUP '92 Parameter Compatibility Procedure



Note 1: Decision on next process is based on the instruction indicator in PCP as described in ISUP92 recommendation Q.764 Section 2.9.5.

Figure 5 Mandatory parameter received



If the Succession CS2000 receives a mandatory parameter with an unrecognized value, it functions as specified in the Q.764 recommendations. If the switch receives a recognized optional parameter with an unrecognized value, it functions as specified in the Q.764 recommendations.

If the Succession CS2000 receives a message containing an unrecognized optional parameter without related parameter compatibility information, the switch discards the parameter and allows the call to proceed.

Table 3 and Table 4 explain how the Succession CS2000 interprets the PCP instruction based on ISUP92 recommendation Q.764, Section 2.9.5. See Figure 4 and Figure 5 for detail.This feature uses the following approach for PCP implementation.

- For IAM message if the instruction indicates **discard message** OR **discard message and send notification**, it is treated as equivalent to **release call**.
- For IAM message If more than one instruction is received for a parameter, the most severe instruction that was received is applied. This is achieved by performing the logical OR operation of all instructions per parameter.

- If an instruction contains multiple indicators, the precedence followed depends on the type of exchange.

  For type A exchange, the precedence (higher to lower) is

  — release call

  — discard parameter and send notification

  — discard parameter

  — pass on

  For type B exchanges, the indicator precedence followed for:

- BIT A is set to 0 i.e. Transit_node Interpretation is

  — pass on (If BIT A is set to 0 i.e. Transit_node Interpretation) PCP along with the parameters included in the PCP parameter are tandemed, unless another PCP instruction contravenes this indication, in which case the end_node interpretation precedence would be followed.

- BIT A is set to 1 i.e. End_node Interpretation is

  — release call

  — discard parameter and send notification

  — discard parameter

  — pass on

- If more than one PCP is received, the PCP that was received first is used.
- In the REL message, only discard / pass on parameter instructions are applicable.
- The PCP parameter itself is tandemed only if the type of exchange is type B.

The following tables explain how the switch interprets the PCP instruction based on ISUP92 recommendation Q.764, Section 2.9.5.

Table 3 Parameter Compatibility for a Type A exchange (pass on not possible)

Bits								Meaning
H	*G*	*F*	E	D	C	B	*A*	
X	X	X	X	X	X	1	X	Release the call
X	X	X	X	1	0	0	X	Discard the message[a]
X	X	X	X	1	1	0	X	Discard the message and send CFN [b]
X	X	X	1	0	X	0	X	Discard the parameter[c]

Bits								Meaning
H	*G*	*F*	E	D	C	B	*A*	
X	0	0	0	0	X	0	X	Release the call
X	0	1	0	0	0	0	X	Discard the message[a]
X	0	1	0	0	1	0	X	Discard the message and send CFN [b]
X	1	0	0	0	X	0	X	Discard the parameter[c]
X	1	1	0	0	X	0	X	Release the call

a. If the message is the IAM message, the switch releases the call.
b. CFN messages contain an appropriate cause value and diagnostic information.If the message is the IAM message, the switch releases the call and returns no CFN.
c. If bit C is set, the switch returns a CFN message. CFN messages contain an appropriate cause value and diagnostic information.

Table 4 Parameter Compatibility for a Type B exchange

Bits								Meaning
H	*G*	*F*	E	D	C	B	*A*	
X	X	X	X	X	X	1	1	Release the call
X	X	X	X	1	0	0	1	Discard the message[a]
X	X	X	X	1	1	0	1	Discard the message and send CFN[b]
X	X	X	1	0	X	0	1	Discard the parameter[c]
X	X	X	X	X	X	X	0	Pass on the parameter
X	X	X	0	0	X	0	1	Pass on the parameter

a. If the message is an IAM, the switch releases the call.
b. CFN messages contain an appropriate cause value and diagnostic information. If the message is an IAM, the switch releases the call and returns no CFN.
c. If bit C is set, the switch returns a CFN message. CFN messages contain an appropriate cause value and diagnostic information.

bit A means that is transited at Intermediate Exchange Indicator

0 = Transit interpretation
1 = End node interpretation

Note:

Only type B exchanges examine this indicator. If the exchange sets it to Transit Interpretation, the other indicators are ignored. If the exchange is set to End Node Interpretation, the switch performs the following actions:

bit B is Release Call Indicator

0 = Do not release
1 = Release call

bit C is Send Notification Indicator
0 = Do not send
1 = Send notification

bit D is Discard Message Indicator
0 = Do not discard message
1 = Discard message

bit E is Discard Parameter Indicator
0 = Do not discard parameter (pass on)
1 = Discard parameter

bits F-G are pass on not possible indicator:
00 = Release the call
01 = Discard the message
10 = Discard the parameter
11 = Release the call

bit H is Extension Indicator

Note:

If pass on is set (bit D =0 or bit E = 0) but not possible, then bits C, F and G are examined

109.4.2.2 Support for Q.767

This feature provides the following support for Q.767 protocol agencies:

1. Allows IMT Global trunks to be provisioned as Q.767 gateway trunks in table TRKSGRP with protocol CCITT, variant v1 and version BLUE (hereafter referred to as Q.767 trunk).
2. This features introduces a new option GWYTRK for IMT Global agents in table TRKGRP. This option enables limited gateway functionality on the Q.767 trunks and provisions the trunk for international use of Q.767 protocol on Succession CS2000.

For more information see “Appendix B: Messages and Parameters Supported on Q.767” on page 1138.

109.4.2.2.1 Handling of Unrecognized & Unexpected messages For Q.767

All messages that are not included in table 32 (***Appendix B: Messages and Parameters Supported on Q.767***) are considered as unrecognized messages and are treated as per ITU - T Blue Book Q.767 section 4.1.1. Unrecognized messages are discarded without disrupting normal call handling. No logs are produced for unrecognized messages.

An unexpected or out of sequence message is a message which is supported, and is valid, but has been received when it is not expected in the call.

If such messages are received in the Q.767 to Q.767 case, the following applies:

- If a Release (REL) message is received for a circuit which is idle it is acknowledged with a Release Complete message.
- If any other message is received relating to an idle circuit a reset message is sent.
- If a Release Complete message is received relating to an idle circuit it is ignored.

In general, unexpected messages received relating to call processing busy circuit are ignored with the following qualifications:

- Release message and any circuit supervision messages are accepted and processed at any time during the call.
- After sending an IAM, and prior to receiving an ACM or CON, only REL and CPG messages are accepted. Receipt of any other message causes a release sequence to be initiated.
- After a Release message is received, any other call-related messages are discarded.
- If a Release Complete message is received relating to a busy circuit for which a Release message has not been sent, the circuit is released and a Release message sent.
- Blocking messages may be received at any time.

109.4.2.3 Q.767/ISUP92 Cause value handling

This feature enhances the keys into table TMTMAP and table CSEMAP to include a new protocol Q.767 for calls originating/terminating on Q.767 and ISUP92 trunk agents.

For calls that release at terminator first with a cause value other than *Normal call clearing* (cause value of 16), Succession CS2000 accesses table CSEMAP with the originating trunk agent protocol and the cause value. The cause value is mapped to an extended treatment value when the fields RTEADV and RECOL are set to ‘N’ in table CSEMAP.

This extended treatment value along with the trunk agent protocol is then used to access table TMTMAP to determine the action to be taken for the call. For calls in which Succession CS2000 have applied a treatment, the applied treatment along with the protocol of the trunk agent is used to access table TMTMAP to derive the action to be taken for the call.

For calls with an action of local treatment (table TMTMAP field TMTPROC value of either LOCAL, ISLOCAL, or INTLOCAL), existing Succession CS2000 functionality is applied.

For calls with an action of non-local treatment (table TMTMAP field TMTPROC value of NOLOCAL) and originated on Q.767 or ISUP92 trunk agents, the carrier is responsible to properly provision the Q.767 protocol in table TMTMAP to reflect the proper location field value of INTL_NET (*International network*) to reflect the generation of the location took place in the international network.

The following excerpt is from ITU-T Recommendation Q.850 which identifies the proper handling of the location field in the CAUSE parameter for international exchanges:

i) If the event causing the generation of the location field takes place in an international exchange (i.e. incoming or outgoing or international transit exchange) the location is set to *International network.*

For calls originating on UCS trunk agent and has terminated to Q.767 or ISUP92 trunk agent, the CS2000 modifies the LOCATION field derived from table TMTMAP with the LOCATION field value of INTL_NET (*International network)* to reflect the generation of the location took place in the international network.

For calls originating on UCS trunk agent and has **not** successfully routed to a Q.767 or ISUP92 trunk agent or has terminated to a UCS trunk agent, the existing table TMTMAP functionality is utilized and the location field is not modified.

For type A exchanges (ISUP92 trunk agents interworking with non-ISUP92 trunk agents), the CS2000 maps the following ISUP92 cause values to *normal, unspecified* (Cause value 31) prior to accessing table CSEMAP and also CS2000 maps the following ISUP92 cause values from table TMTMAP to *normal, unspecified* (Cause value 31) prior to sending the CAUSE value for non-local treatments:

- Preemption (T1.619) (8 or CSE_8)
- Pre-emption Circuit reserved for re-use (9 or CSE_9)
- Subscriber absent (20 or CSE_20)
- User information discarded (43 or CSE_43)

- No Preempt Circuit Available(46 or CSE_46)
- Incompatible Agents(53 or CSE_53)
- Inconsistency in designated info (62 or CSE_62)
- Non-existent CUG (90 or CSE_90)
- Message with unrecognized parameter discarded (110 or CSE_110)

For type B exchanges (ISUP92 trunk agent interworking with ISUP92 trunk agent), the CS2000 does not perform the ISUP92 cause value mappings to *normal unspecified* (Cause value 31) as performed on type A exchanges.

109.4.2.3.1 Mapping of ISUP92 cause values for non-ISUP92 trunks The following table summarizes the mapping of ISUP92 cause values for non-ISUP92 trunks.

Table 5 Mapping of ISUP92 cause values for non-ISUP92 trunks

Release Incoming Trunk	CSEMAP Cause	Release Outgoing Trunk	Outgoing Cause
ISUP92	ISUP92 Cause	ISUP92	CSEMAP Cause Value
ISUP92	Non-ISUP92 Cause	ISUP92	CSEMAP Cause Value
ISUP92	ISUP92 Cause	Q767	Normal Unspecified
ISUP92	Non-ISUP92 Cause	Q767	CSEMAP Cause Value
ISUP92	ISUP92 Cause	UCS Agent	Normal Unspecified
ISUP92	Non-ISUP92 Cause	UCS Agent	CSEMAP Cause Value
Q767	ISUP92 Cause	ISUP92	Normal Unspecified
Q767	Non-ISUP92 Cause	ISUP92	CSEMAP Cause Value
Q767	ISUP92 Cause	Q767	Normal Unspecified
Q767	Non-ISUP92 Cause	Q767	CSEMAP Cause Value
Q767	ISUP92 Cause	UCS Agent	Normal Unspecified
Q767	Non-ISUP92 Cause	UCS Agent	CSEMAP Cause Value
UCS Agent	ISUP92 Cause[a]	Q767	Normal Unspecified
UCS Agent	ISUP92 Cause[a]	ISUP92	Normal Unspecified
UCS Agent	Non-ISUP92 Cause	Q767	CSEMAP Cause
UCS Agent	Non-ISUP92 Cause	ISUP92	CSEMAP Cause

a. CSEMAP does not differentiate between CCITT coding standard or National coding standard.

109.4.2.4 Q.767 and ISUP92 Protocol Timers

This feature allows flexibility to set timers per trunk sub-group basis for the Q.767/ISUP92 trunks. Table TRKSGRP field TMRNAME value provides the index into Table C7UPTMR. Table C7UPTMR allows to set timers based on a per trunk sub-group basis. If the TMRNAME field is not provisioned, then the default values are used.

For more information see “Appendix C: Q.767/ISUP92 Timers” on page 1146.

109.4.2.4.1 Q.118 Timer This feature does not support suspend (SUS) and resume (RES) functionality on the ISUP92/Q.767 trunk agency. The gateway functionality is required to tandem any received SUS or RES messages (when the appropriate indicators indicate the message is network initiated) and not process these messages when the originating agency is Gateway trunk. For other originating agencies the existing suspend-resume functionality is performed. For this reason, Q.118 timer in section 4.3.2 in ITU Q.118 recommendation is not supported. Timer value associated with T6 is ignored and the timer is not set which corresponds to a infinite timer value.

109.4.3 Gateway services

109.4.3.1 Supported calltypes

The Q.767/ISUP92 gateway trunks support the following calltypes:
- direct termination and transit IDDD calls
- direct termination and transit international operator assisted calls
- direct termination and transit Code 11/Code 12 calls

All calltypes are handled as automatic service calls. This feature also supports tie-route connections between two Succession CS2000 Communication Servers using the ISUP92/Q.767 trunk agency.

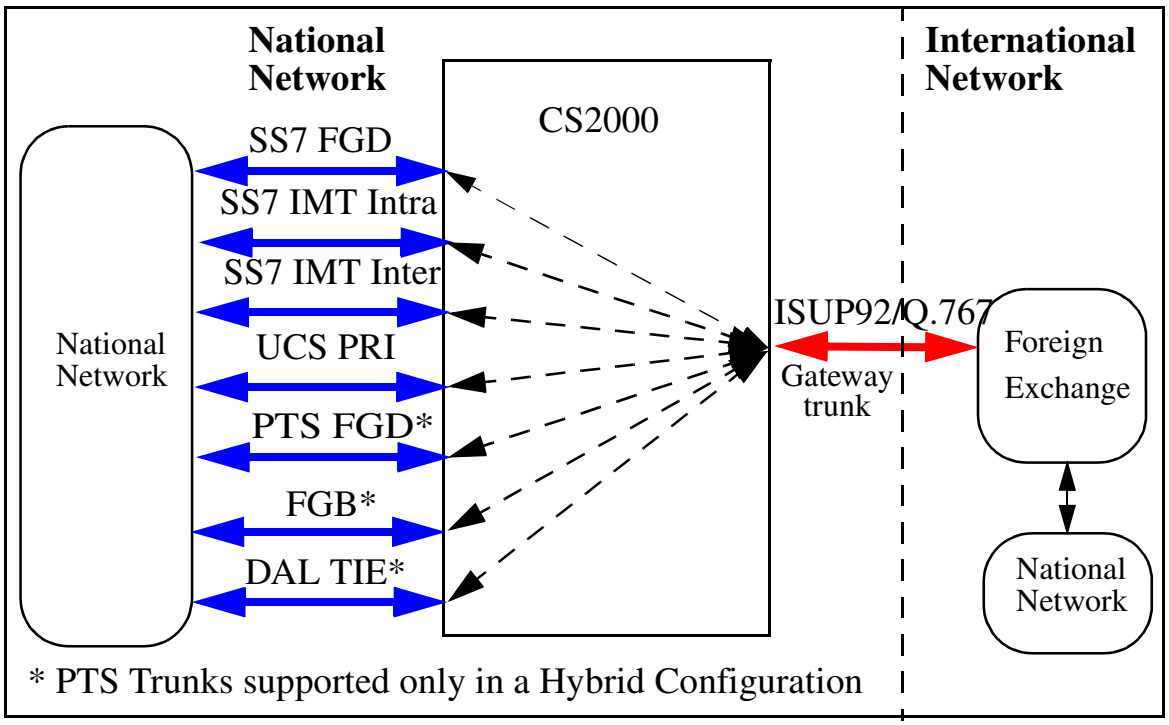
This feature supports 15-digit IDDD requirements for both the called party number and the calling party number. The ISUP92/Q.767 trunk agency supports receiving and outpulsing two Nature of Address (NOA) values for both calling party number and called party number based on below mentioned supported calltypes:
- National significant number (0000011)
  - direct termination IDDD calls
  - direct termination operator assisted calls
  - direct termination Code 11/Code 12 calls
- International significant number (0000100)
  - transit IDDD calls
  - transit operator assisted calls
  - transit Code 11/Code 12 calls

The Q.767/ISUP92 gateway trunks are used to inter-connect to foreign exchanges. The table TRKGRP GWYTRK option field SERVCC identifies the serving country code of the foreign exchange. The foreign exchange provides the international interface for the national network of the serving country code.

The Succession CS2000 provides the international interface for the national network associated with the table OFCVAR parameter OFC_SERVING_CC. Table OFCVAR parameter OFC_SERVING_CC is provisioned with the country code that is associated with the country that resides the Succession CS2000. This feature is only supported in WZ-1 countries; therefore, the only supported country code for the office parameter OFC_SERVING_CC is 1. The supported UCS trunk agents are associated with the country code of the office parameter OFC_SERVING_CC.

The following figure illustrates the supported trunk agencies interworking and the international interface between the national network being served by Succession CS2000 and the international network.

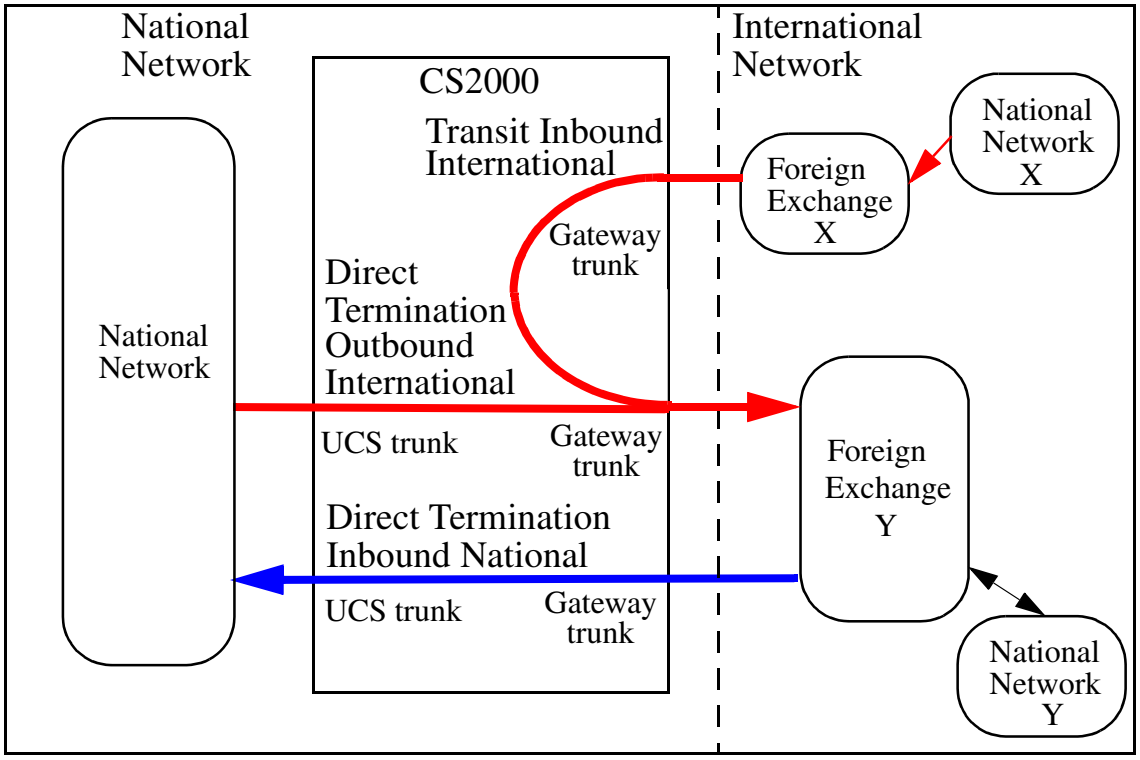
Figure 6 Supported trunk agent interworkings



109.4.3.1.1 Direct Termination calls Direct termination outbound international calls pertains to IDDD calls which are routed to a foreign exchange which serves the country code prefixed to the called number. The foreign exchange would serve the national network of the country code. For direct termination outbound international (IDDD) calls, the call would be routed to a ISUP92/Q.767 trunk which is connected to the foreign exchange that serves the country code prefixed on the called number.

Direct termination inbound national calls pertain to national calls routed from a foreign exchange which are destined for the country (serving country code) in which the Succession CS2000 resides. For direct termination inbound national calls, the call would be routed (via translations) to the supported UCS agents. The supported UCS agents are associated with the national network of the serving country code. Figure 7 illustrates supported direct termination calltypes.

Figure 7 Direct Termination calltypes



Direct Termination Outbound International:

For direct termination outbound international calls, the call origination occurs on one of the supported UCS trunk agents or a ISUP92/Q.767 trunk agency (in the case of a transit inbound international call from a foreign exchange) and terminates to a ISUP92/Q.767 trunk agency where the call is typed as an international (IDDD) call. The terminating ISUP92/Q.767 trunk agency is connected to the foreign exchange serving the country code prefixed on the called number. For the call to be classified as a direct termination outbound international call, the serving country code (table TRKGRP GWYTRK option field SERVCC) that is associated with the terminating ISUP92/Q.767 trunk agency would be EQUAL to the country code prefixed on the called number.

For originations on the supported UCS agents, this feature supports existing international (IDDD) translations (IP and IN translations) and existing Carrier AIN functionality to allow the call to be routed to the terminating ISUP92/ Q.767 trunk agency. For originations on ISUP92/Q.767 trunk agency, this feature supports existing international (IDDD) translations (IP and IN translations) to allow the call to be routed to the terminating ISUP92/Q.767 trunk agency.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples”for more details on DMS250 processing of direct termination outbound international calls.

Direct Termination Inbound National:

For direct termination inbound national calls, the connected foreign exchange routes the call as a national call to the Succession CS2000 via ISUP92/Q.767 trunk agency. For the call to be classified as a direct termination inbound national call, the Succession CS2000 would call type the call as a national call (via table STDPRTCT CT selector with CALLFEAT of OFFNET or table STDPRTCT S/T selectors).

The ISUP’92/Q.767 trunk agency would utilize table TYP2PRTM to derive the pretranslator name (to access table STDPRTCT) based on the received called party number NOA. This feature supports the following pretranslation selectors from table STDPRTCT:

- CT selector (calltype of OFFNET)
- S selector
- T selector

The other pretranslation selectors are not supported.

This feature supports existing national translation system (HNPACONT). This feature supports the following translation routing selectors from table HNPACONT:

- S route selector
- N route selector
- T route selector (supported UCS routing tables)
- SX route selector
- TRMT route selector

The other translation routing selectors are not supported.

The outgoing call information is updated based on the information/translations derived/performed by the Succession CS2000.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for more details on DMS250 processing of direct termination inbound national calls.

109.4.3.1.2 Transit calls

Transit calls pertains to international calls which are routed to a foreign exchange (gateway) which does not serve the country based on the country code prefixed on the called number. This foreign exchange would then route the call as either a direct termination inbound national call or a transit outbound international call to another foreign exchange that is serving the country code prefixed on the called number.

Transit inbound national call pertains to national calls (gateway serving the country code prefixed on the called number) which were transit through a foreign exchange that did not serve the country code of the subscriber (calling party number) and terminates to the serving country code of the Succession CS2000. Transit inbound national calls are handled in the same manner as direct termination inbound national call.

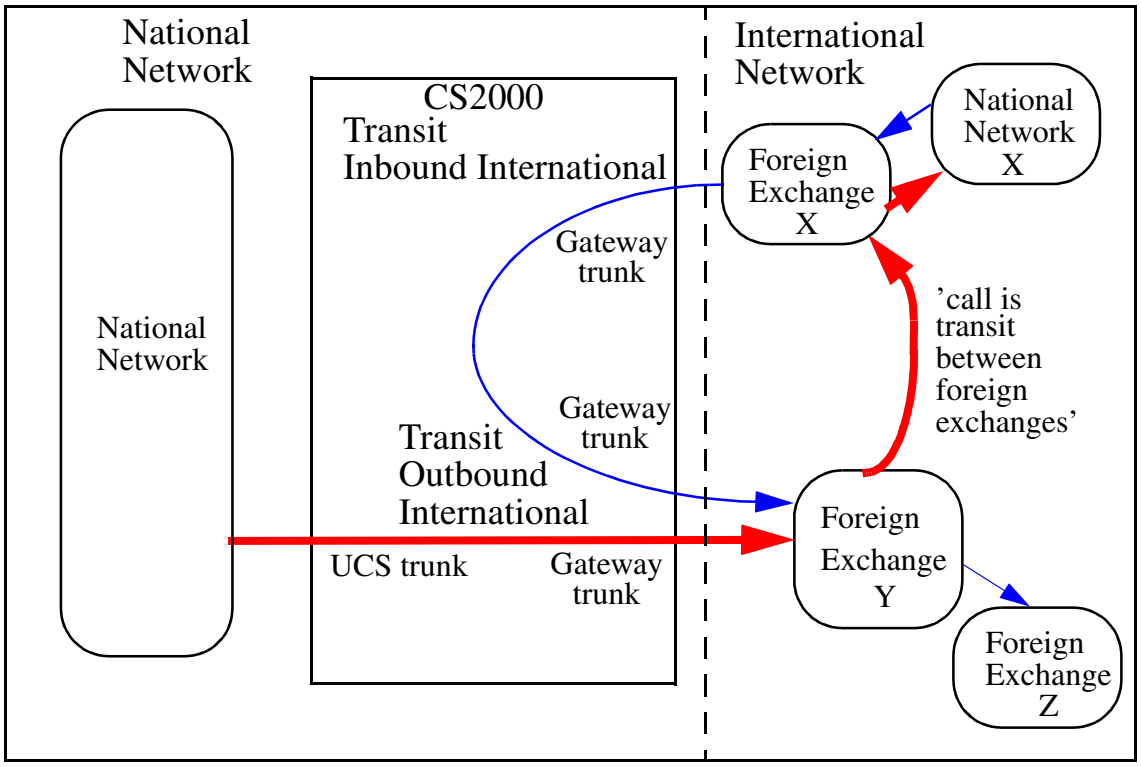
For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for more details on CS2000 processing of transit calls.

Transit Outbound International

For transit outbound international calls, the call origination occurs on either the supported UCS agents or ISUP92/Q.767 trunk agency and the call is typed as an international (IDDD) call. Transit outbound international (IDDD) calls could have originated from the national network serving the Succession CS2000 (originated on supported UCS agents) or from a foreign exchange using the Succession CS2000 as a transit foreign exchange (gateway) where the incoming call is a transit inbound international call and the outgoing call is a transit outbound international call.

Figure 8 illustrates transit outbound international calls coming from either the national network (origination on supported UCS trunk agent) or international network (origination on ISUP92/Q.767 trunk agent).

Figure 8 Transit outbound international call type



For ISUP92/Q.767 trunk agency originations existing international translations (IP and IN translations) is supported and for supported UCS agents originations existing international translations (IP and IN translations or Carrier AIN) are supported.

The ISUP92/Q.767 trunk agency would utilize table TYP2PRTM to derive the pretranslator name (to access table STDPRTCT) based on the received called party number NOA.

International translations would have routed the call to a ISUP92/Q.767 trunk agency. For the call to be classified as a transit outbound international call, the terminating trunk agent is an ISUP92/Q.767 trunk agent and the serving country code (table TRKGRP option GWYTRK field SERVCC) for ISUP92/Q.767 trunk agent is NOT EQUAL to the country code prefixed on the called number.

109.4.3.1.3 Operator calls

This feature supports following types of operator assisted calls:

- Inbound national OA calls (Direct)
- Outbound international OA calls (Direct & Transit)
- Inbound national Code 11 and Code 12 calls (Direct)
- Outbound international Code 11 and Code 12 calls (Direct & Transit)

109.4.3.1.3.1 Inbound National OA calls (Direct)

Calls originating on Q.767/ISUP92 gateway trunk agents, are identified as inbound national operator assisted (OA) call via pretranslations (in table STDPRTCT, subtable STDPRT, S selector with TYPCALL field value of OA or T selector with TYPCALL field value of OA). The S and T selector by default call type the call as a national call (OFFNET). Succession CS2000 treats inbound national OA call (S and T selectors with TYPCALL value of OA in table STDPRTCT) as direct termination inbound national calls except the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR) in the outgoing call information (ISUP or PRI trunk terminations).

Inbound national OA calls can also use the CT selector with CALLFEAT value of OFFNET to pretranslate the call. The CT selector with CALLFEAT value of OFFNET has the option of using the new option CPCSCRN to perform CPC screening, routing, or override the incoming CPC but the call is treated as a direct termination inbound national call.

The carrier is responsible to append any WZ-1 prefix digits.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for detail on CS2000 processing of inbound national OA calls.

109.4.3.1.3.2 Outbound international OA calls (Direct & Transit)

Direct termination outbound international OA and Transit outbound international OA calls originate on supported UCS agents or Q.767/ISUP92 gateway trunk and terminate on Q.767/ISUP92 gateway trunk. These calls are identified as international operator assisted call via NT selector with TYPCALL field value of OA in table STDPRTCT, subtable STDPRT.

The NT selector call types the call as an international call. Succession CS2000 treats outbound international OA call (NT selector in table STDPRTCT) as either a direct termination outbound international call or a transit outbound international call based on the comparison between the country code prefixed on the called number and the serving country code (table TRKGRP option GWYTRK field SERVCC) of the terminating Q.767/ISUP92 gateway trunk agent. For either case, the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR or the NT selector option CPCSCRN functionality). The NT selector option CPCSCRN in table STDPRTCT provides the optionallity to perform CPC screening, CPC routing, and CPC override for calls originating on Q.767/ISUP92 gateway trunk agents.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for details on CS2000 processing of outbound international OA calls.

109.4.3.1.3.3 Code 11/Code 12 calls:

An operator can place international calls to other operators by including Code 11 (Hexadecimal B) or Code 12 (Hexadecimal C) in called number. Code 11 (`B’) is used internationally to signify Directory Assistance and Code 12 (`C’) is used to indicate General Operator Assistance.

109.4.3.1.3.3.1 Outbound International Code 11/12 calls (Direct & Transit)

These calls originate either on Gateway trunk or UCS Agents and terminate on Gateway trunk.

In WZ-1, code 11digit (B) and code 12 digit (C) are commonly translated to “121” and “131” respectively. For outbound international Code 11 and Code 12 calls, the national operator includes 121 or 131 in place of the Code 11 or Code 12 digit in the called number. The international exchange would then convert the 121 and 131 to Code 11 digit (B) and Code 12 digit (C), respectively.

The called number contents from a national operator position could have the following format (Recommendation Q.107):

<01> + <country code> + <extra digit> + <121 or 131> + <digits>
- ‘01’: WZ-1 prefix digits for international operator assisted calls
- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

For calls originating on Q.767/ISUP92 gateway trunk agents, the CS2000 scans the called number for the Code 11 and Code 12 digits. If the Code 11 or Code 12 digits exist in the called number, the Succession CS2000 replaces these digits in the called number with 121 or 131, respectively along with prefixing the called number with 0 or 01 based on the NOA of the called number. Succession CS2000 uses the pretranslator name from table TRKGRP option GWYTRK option field C11C12PT to access table TYP2PRTM along with the NOA of the called number.

The IAM called number contents from a foreign operator position via foreign exchange could have the following format (Recommendation Q.107):

<country code> + <extra digit> + <code 11 or code 12> + <digits> + #F
- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

The Succession CS2000 would treat the call as either a direct termination outbound international OA call or transit outbound international OA call based on the comparison between the country code prefixed on the called number and the serving country code (table TRKGRP option GWYTRK field SERVCC) of the terminating Q.767/ISUP92 gateway trunk agent. For either case, the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR or by NT selector option CPCSCRN in table STDPRTCT).

The carrier is responsible to remove any WZ-1 prefix digits and perform digit manipulation (via translations) to convert the 121 and 131 digits to Code 11 digit and Code 12 digit, respectively.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for details on DMS250 processing of outbound international code 11/12 calls.

109.4.3.1.3.3.2 Inbound National Code 11/12 calls (Direct)

These calls originate on Gateway trunk and terminate on UCS agent.

For calls originating on Q.767/ISUP92 gateway trunk agents, the CS2000 scans the called number for the Code 11 and Code 12 digits. If the Code 11 or Code 12 digits exist in the called number, the Succession CS2000 replaces these digits in the called number with 121 or 131, respectively.Also, Succession CS2000 prefixes digit(s) 0/01 based on the incoming NOA. Succession CS2000 uses the pretranslator name from table TRKGRP option GWYTRK option field C11C12PT to access table TYP2PRTM along with the NOA of the called number.

The IAM called number contents from a foreign operator position via foreign exchange could have the following format (Recommendation Q.107):

<extra digit> + <code 11 or code 12> + <digits> + #F

- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

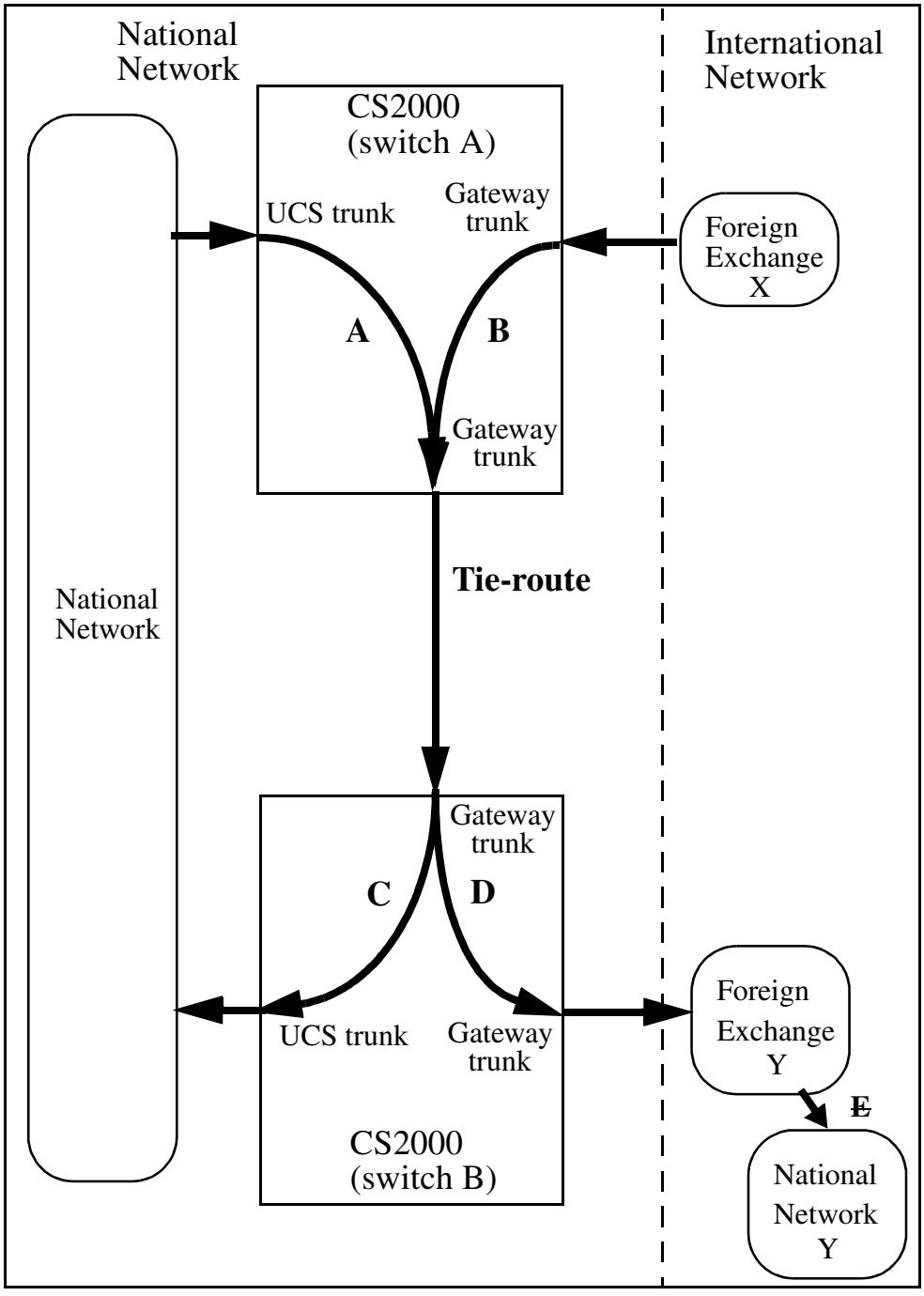
The Succession CS2000 would treat direct termination inbound national code 11 or code 12 call as a direct termination inbound national OA call based on pretranslations.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1149.“109.17 Appendix E: Callflow diagram” and “109.18 Appendix F: Datafill examples” for details on DMS250 processing of inbound national code 11/12 calls.

109.4.3.2 Tie-route support

Tie-route connections are used when the carrier has more than one switch with the gateway functionality. These switches would be directly connected to each other via gateway trunk agency. The tie-route connection may be used by the carrier to route calls between the switches based on which switch has the available connection to the destination foreign exchange or the destination national network. Figure 9 illustrates the supported tie-route connection between two CS2000 Communication Servers.

Figure 9 Tie-route connection



The carrier would be expected to use the national backbone to tandem any national traffic within the carrier's network or within the national network. The tie-route connection could be used to route the following gateway calltypes:

- direct termination inbound national calls (connection B to connection C)
- direct termination outbound international calls (connection A to connection D)
- any transit outbound international calls (connection B to connection D)

Please refer to Section "109.19 Appendix G: Tie-route Connection Example" on page 1183. for example on tie-route connection.

109.4.3.3 Calling Party Category(CPC) handling

New table CPCSCRN is implemented to provide the following functionality:

- CPC screening
- CPC routing
- CPC override

Table CPCSCRN is only accessible by ISUP92 and Q.767 gateway trunk agencies. Table CPCSCRN is accessed as a two part key with the NT/CT option CPCSCRN index value (CPCINDEX) and the incoming call CPC value (0 to 255). If the tuple is not present in table CPCSCRN, the call is allowed to continue.

A new Table STDPRTCT option CPCSCRN is added to NT selector for the DD and OA type of call (TYPCALL field) and CT selector with CALLFEAT of OFFNET. CPCSCRN option requests for an index value (0 to 255).

Table 6 Table STDPRTCT CT selector

Selector	CALLFEAT	MINDIGS	MAXDIGS	NOPREDIGS	OPTIONS
CT	OFFNET	0 TO 18	0 TO 18	0 to 7	CPCSCRN

Table 7 Table STDPRTCT NT selector

Selector	TYPCALL	NOPREDIG	TRANSYS	OPTIONS
NT	DD	0 to 7	IP,IN	CPCSCRN
NT	OA	0 to 7	IP,IN	CPCSCRN

TYPCALL can have the following values:
DD: Direct Dial

OA: Operator Assisted
NP: Nil type of call (CPCSCRN option is not available for this value)
NL: No prefix local (CPCSCRN option is not available for this value)

Table 8 CT/NT option CPCSCRN

Options	CPCSCRN Index
CPCSCRN	0 to 255

Table CPCSCRN contains three fields:

- Action:
  - Continue: allows the call to proceed
  - Block: routes the call to treatment
- Override STS:
  - N: STS is not overridden
  - Y: STS is overridden with provisioned STS. Table control prompts for STS when Override STS is set to 'Y'.
- Override CPC:
  - N: CPC is not overridden
  - Y: CPC is overridden with provisioned CPC. Table control prompts for CPC value (0 to 15) when Override CPC is set to 'Y'.

Table 9 Table CPCSCRN

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
CPCINDEX	{0 TO 255}	NEW	N/A
CPC	Alphanumeric character string, which are mapped to range 0-255. The first 16 values are same as given in table 36. Other values are from CPC_16 to CPC_255.	NEW	N/A
ACTION	{ACTION_CONTINUE, ACTION_BLOCK}	NEW	ACTION_ CONTINUE
OVRDSTS	{Y, N}	NEW	N
STS	{000 TO 999}	NEW	N/A
OVRDCPC	{Y, N}	NEW	N

Table 9 Table CPCSCRN

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
CPC	Alphanumeric character string, which are mapped to range 0-15. The values are same as given in table 10.	NEW	N/A

Table 10 Table CPCSCRN CPC values

CPCSCRN CPC value	Integer value of CPC
UNKNOWN	0
OP_FRENCH	1
OP_ENGLISH	2
OP_GERMAN	3
OP_RUSSIAN	4
OP_SPANISH	5
CPC_6	6
CPC_7	7
CPC_8	8
OP_NATIONAL	9
SUBSCRIBER1	10
PRIORITY	11
DATA	12
TEST	13
NON_VOICE	14
PAYPHONE	15

The field *Action* is used to screen the incoming CPC value based on the CPCSCRN index value obtained from the new CT/NT option CPCSCRN in table STDPRTCT and the incoming CPC value. The field ACTION either allows the call to continue or blocks the call by routing the call to Call Not AlloweD (CNAD) treatment.

The field *OVRDSTS* is used to provide a new STS value for the call when the *Override STS* value is set to 'Y'. If the value is set to 'N', table CPCSCRN does not prompt for a new STS value and the last derived STS value is used for the call.

The field *OVRDCPC* is used to override the incoming CPC value with a new CPC value for the call when *Override STS* value is set to 'Y'. If the value is set to 'N', table CPCSCRN does not prompt for a new CPC value and the incoming CPC value is maintained for the call.

The following CPC values were extracted from ITU-T Recommendation Q.767 section 3.11:

00000000 : Unknown
00000001 : operator, language French
00000010 : operator, language English
00000011 : operator, language German
00000100 : operator, language Russian
00000101 : operator, language Spanish
00000100 : available to Administrations
to for selecting a particular
00001000 : language by a mutual agreement
00001001 : reserved (see Recommendation Q.104) (Note)
00001010 : ordinary calling subscriber
00001011 : calling subscriber with priority
00001100 : data call (voice band data)
00001101 : test call
00001110 : spare
00001111 : payphone
00001000 :
to spare
11011111 :
11100000: reserved
to for
11111110: national use
11111111: spare

Example datafill:

```
Table STDPRTCT, subtable STDPRT

0117 0117 NT DD 3 IP (CPCSRCN 1)$
```

Table CPCSCRN is accessed with the CPCINDEX value of 1 along with the call CPC value of 2 (OP_ENGLISH).

```
Table CPCSCRN

1 OP_ENGLISH CONT Y 611 Y OP_SPANISH
```

For a call with the CPC value of 2 (OP_ENGLISH), the call is allowed to continue (ACTION_CONTINUE), the STS for the call is updated to 611, and the CPC for the call is updated with a value of OP_SPANISH (5).

The call CPC is also allowed to be overridden by using the SX selector during translations of the call. The SX selector provides the index to access table RTEATTR. The REPLACE field in Table RTEATTR is enhanced to prompt for a CPC value. Table-10 provides table RTEATTR CPC values.

The CPC value replaces the CPC value for the Calling Party Category parameter in the outgoing IAM on the trunk provisioned against the SX selector. This functionality is only available for Q.767 and ISUP92 gateway trunk agents.

Table 11 Table RTEATTR CPC values

RTEATTR CPC value	Integer value of CPC
UNKNOWN	0
OP_FRENCH	1
OP_ENGLISH	2
OP_GERMAN	3
OP_RUSSIAN	4
OP_SPANISH	5
CPC_6	6
CPC_7	7
CPC_8	8
OP_NATIONAL	9
SUBSCRIBER1	10
PRIORITY	11
DATA	12
TEST	13

Table 11 Table RTEATTR CPC values

RTEATTR CPC value	Integer value of CPC
NON_VOICE	14
PAYPHONE	15

Example datafill:

```
Table HNPACONT, subtable RTEREF

724 (SX GITU1E1AN03 CPC_OVRD) $
```

CPC_OVRD is the index into table RTEATTR.

```
Table RTEATTR

CPC_OVRD $ $ CPC SUBSCRIBER1
```

The outgoing CPC value is set to SUBSCRIBER1

109.4.3.4 Satellite Restrictions

This feature supports the existing Succession CS2000 satellite functionality for the ISUP92/Q.767 trunk agent to enable double satellite hop restriction. Double satellite hop restriction is invoked when the terminating trunk agent TRKSGRP field SAT is provisioned with a value of 'Y'.

Double satellite hop restriction:

For originating calls on the Succession CS2000 which have an indication that the call has been previously involved in a satellite connection (via originating trunk agent table TRKSGRP field SAT with a value of 'Y' and/or the Nature of Connection with an indication of at least one satellite circuit in the connection), the Succession CS2000 restricts the call from terminating on a trunk agent with an indication of a satellite connection (via terminating trunk agent table TRKSGRP field SAT value of 'Y'). Succession CS2000 performs route advance to the next available route in the route list.

109.4.3.4.1 Gateway (ISUP92/Q.767) satellite indication:

The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

  N: No satellite circuit in the connection

Y: Satellite circuit in the connection

The value of ‘Satellite indicator’ in ‘Nature of Connections parameter’ is interpreted as below:

- Nature of Connection (reflected as ’O/G ind.’ below tables):

  00: No satellite circuit in the connection

  01: One satellite circuit in the connection

  10: Two satellite circuit in the connection

  11: spare

109.4.3.4.2 UCP Inter/Intra ISUP IMT satellite indication: The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

  N: No satellite circuit in the connection

  Y: One satellite circuit in the connection

The value of ‘Satellite indicator’ in ‘Nature of Connections parameter’ is interpreted as below:

- Nature of Connection (reflected as ’O/G ind.’ below tables):

  00: No satellite circuit in the connection

  01: One satellite circuit in the connection

  10: Two satellite circuit in the connection

  11: Three or more satellite circuits in the connection

- I3PA (II digits reflects satellite connection):

  II digits (Facility code) of I3PA dialplan is a two digit value reflecting the following information:

  calltype (first digit of facility code)

  - 0x: national calls
  - 2x: COS
  - 56: data call

  second digit of facility code

•queued at previous switch

•satellite at previous switch

109.4.3.4.3 SS7 FGD satellite indication:

The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

  N: No satellite circuit in the connection

  Y: One satellite circuit in the connection

The value of 'Satellite indicator' in 'Nature of Connections parameter' is interpreted as below:

- Nature of Connection (reflected as 'O/G ind.' below tables):

  00: No satellite circuit in the connection

  01: One satellite circuit in the connection

  10: Two satellite circuit in the connection

  11: Three or more satellite circuits in the connection

109.4.3.4.4 UCS PRI, PTS FGD, FGB, DAL TIE satellite indication:

These trunk agencies are only supported on land-base transmission medium and do not provide any type of outgoing indicator that a satellite was involved in the call.

109.4.3.4.5 ISUP 'Satellite indicator' values in the outgoing IAM

The following table gives the value of 'ISUP Satellite indicator' in 'Nature of Connection Parameter' in outgoing IAM.

Note: *Please note that, call is ROUTE ADVANCED until a terminator with SAT set to N (not equipped with satellite), for all other combination of values which are not listed in Table12, Table13 and Table 14.*

Table 12 ISUP 'Satellite indicator' values for Gateway terminating to UCS agent

Originator		Terminator						
Gateway		SS7 IMT			SS7 FGD		Gateway	
I/C ind.	Trks grp	Trks grp	O/G ind.	I3PA Satel. ind.	Trks grp	O/G ind.	Trks grp	O/G ind.
00	N	N	00	N	N	00	N	00
00	Y	N	01	Y	N	01	N	01
00	N	Y	01	Y	Y	01	Y	01
01	N	N	01	Y	N	01	N	01
01	Y	N	01	Y	N	01	N	01
10	N	N	10	Y	N	10	N	10
10	Y	N	10	Y	N	10	N	10
11	N	N	10	Y	N	10	N	10
11	Y	N	10	Y	N	10	N	10

Table 13 ISUP 'Satellite Indicator' values for UCS agent terminating to Gateway

Originator		Terminator	
FGD SS7/ IMT SS7		Gateway	
I/C ind.	Trks grp	Trks grp	O/G ind.
00	N	N	00
00	N	Y	01

Table 13 ISUP 'Satellite Indicator' values for UCS agent terminating to Gateway

Originator		Terminator	
FGD SS7/ IMT SS7		Gateway	
I/C ind.	Trks grp	Trks grp	O/G ind.
00	Y	N	01
01	N	N	01
01	Y	N	01
10	N	N	10
10	Y	N	10
11	N	N	10
11	Y	N	10

Table 14 ISUP 'Satellite Indicator' values for UCS PTS/PRI agent terminating to Gateway

Originator	Terminator	
PTS/ PRI	Gateway	
Trks grp	Trks grp	O/G ind.
N	N	00
N	Y	01
Y	N	01

109.4.3.5 Test calls on Gateway Trunks.

Test lines are used to test trunk connections to other offices, both local and toll. Test Line Tests (TLT) are run under the control of the calling office, and can be initiated either manually from the Trunk Test Position (TTP) level or automatically from the Automatic Trunk Test (ATT) level of Maintenance & Administration Position (MAP). TLT can test both the originating and terminating ends of trunks, and can be used to simulate most conditions that may arise under normal operating conditions.

Test calls are defined as calls originating from test facilities on the near end switch, going over the trunk to be tested and finally terminating on test equipment of far end switch. This feature supports test calls on Q.767/ISUP92 gateway trunk for the following testlines:

— T100 (Balanced Termination testline)

— T101[1] (Communication testline)

— T102 (Milliwatt testline)

Test facilities, supported by this feature include ATT, and the TST and OP commands of the TTP MAP level. ATR originated test calls are not supported by this feature.

Please refer to Section “109.20 Appendix H: Test Call” on page 1187. for more details on test calls.

109.4.3.6 Data Calls on Gateway Trunks.

This feature supports data calls for calls originating and/or terminating on Q.767/ISUP92 gateway trunk agencies. Data calls are supported on the following bearer services:

- 64kbps Unrestricted
- 56kbps

Following matrix shows the interworking supported by this feature for data calls:

[1]T101 testline is supported only in a hybrid configuration.

Table 15 Interworking Matrix For Data calls

	Terminating Agency							
Orig. Agency	Gateway	UCP Intra	UCP Inter	FGD SS7	FGD PTS	UCS PRI	FGB	DAL TIE
Gateway	X	X	X	X	X	X	X	X
UCP Intra	X							
UCP Inter	X							
FGD SS7	X							
FGD PTS	X							
UCS PRI	X							
FGB	X							
DAL TIE	X							

Please refer to Section “109.21 Appendix I: Data Call” on page 1195. for more details on data calls.

109.4.3.7 ECAN support

Echo Canceller support is integrated into the PVG for ISUP92/Q.767.

Following section describes the messaging and office configuration for ECAN.

Please refer to Section “109.22 Appendix J: ECAN” on page 1203.

109.4.3.7.1 Echo Control Messaging

In relation to the ISUP messaging protocol, echo canceller control operates according to the following picture. The echo control information in the first forward-going message and the first backward-going message per call is used for the duration of that call.

Typically the IAM is the first forward-going message, and the ACM is the first backward-going message. However, a CON, CPG or ANM may also be sent as the first backward-going message. The logic to enable / disable the EC in backward-going message is described in more detail later.

Forward Address Parameter for Echo Cancellation (IAM)

Figure 10 IAM Message for Q.767/ISUP92

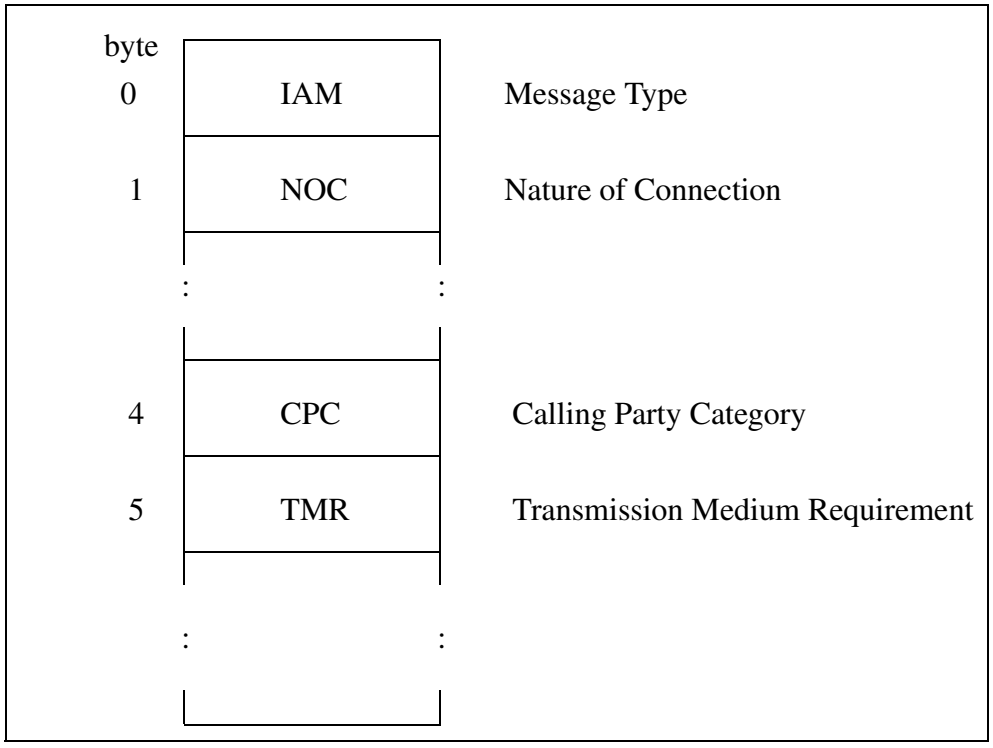
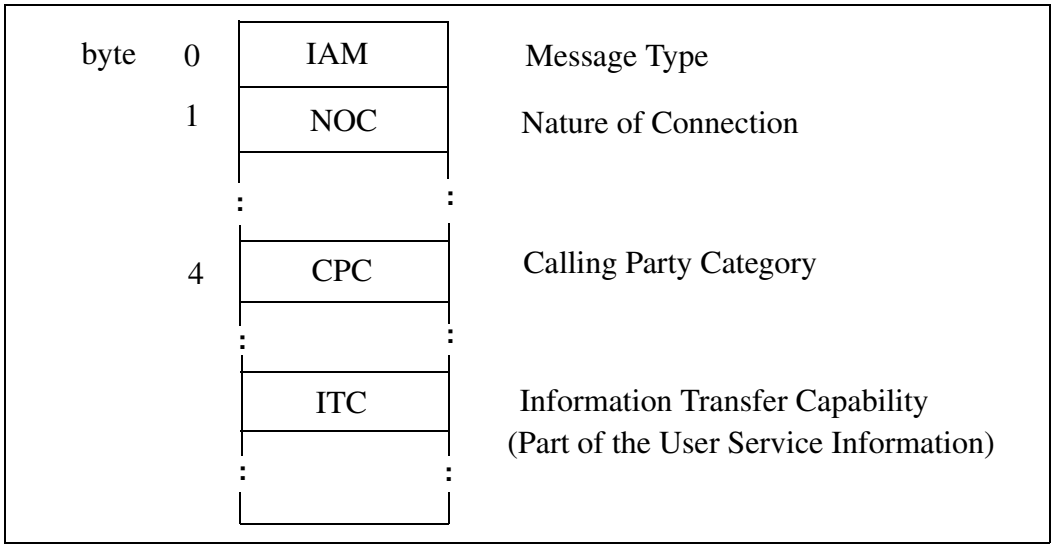


Figure 11 IAM Message for UCS ISUP



Nature of Connection (For both UCS and Q.767/ISUP92)

H	G	F	E	D	C	B	A
			X				

E = Echo Control

0 - outgoing half echo device not included

1- outgoing half echo device included

Transmission Medium Requirement (For Q.767/ISUP92 only)

H	G	F	E	D	C	B	A
						X	X

0000 0000 = speech

0000 0011 = 3.1 kHz audio

0000 0010 = 64 kb/s data call

Information Transfer Capability (For UCS only)

H	G	F	E	D	C	B	A
			X	X	X	X	X

00000 = speech

01000 = Unrestricted digital Information - data call

10000 = 3.1 kHz audio

Data Call:

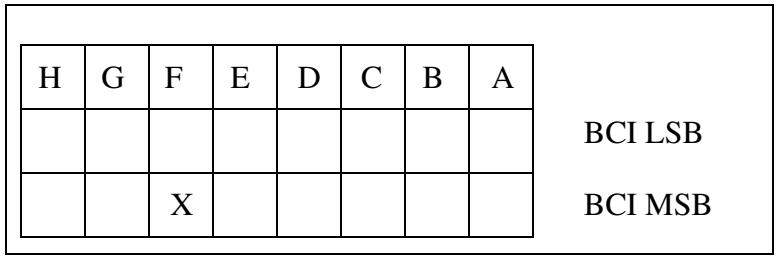
If the TMR or ITC in USI parameter in the incoming IAM indicates that it is a

data call, the echo controllers at the incoming and outgoing exchange remains OFF for the duration of the call, regardless of the echo control bit in any message.

Backward Call Indicator (ACM, CON, CPG, ANM)

The backward call indicator is included in ACM, CON, CPG and ANM messages for both ITU protocol and UCS protocol.

Figure 1 Echo cancel indication bit in Backword call indicator



BCI MSB

0000 0000 = incoming half echo device not included

0010 0000 = incoming half echo device included

Indication of an incoming echo canceller included by a transit switch is given in the BCI of the ACM, CON, CPG or ANM. The BCI of the ACM and the CON is mandatory but is optional in the ANM and CPG.

The EC information in the first backward-going protocol message (e.g. ACM, CON, CPG or ANM) per call is used to notify EC status to the transit switch. EC information in the later messages is ignored. So, two cases may occurred during the call processing. In most cases, EC-bit is a mandatory part of the messages. However, in the case where EC-bit is optional and is not present, the next message is examined. In all cases, by the time the call reaches to the answer stage (after received ANM), at least one message with EC-bit should be sent to both trunks in the incoming and outgoing directions.

109.4.3.7.1.1 Table TRKSGRP

Echo canceller control is provided on a trunk subgroup basis, in table TRKSGRP. No checking is done in table control to ensure that all trunks in this subgroup do in fact have echo cancelling equipment present. Three fields pertain to echo canceller control:

- **ECSTAT** -this should be datafilled '**INTERNAL**' to allow the echo canceller to be used by call processing when required. If left at the default of 'UNEQ', the canceller remains OFF at all times.
- **ABCNTL** - this should be datafilled '**NONE**' to indicate that the echo canceller does not monitor the trunk's AB bits for activation information.

109.4.3.8 A-LAW/U-Law Conversion

The Succession CS2000 should be configured to use u-law PCM encoding in world zone-1. The ISUP92/Q.767 trunk agencies are only supported on E1 spans using A-law PCM encoding. The PVG will perform A-law to u-law conversion as required.

PCM encoding conversion on a per call basis is enabled, if transmission medium requirement parameter indicates speech and 3.1 kHz (PCM encoding conversion requirements is based on Q.764 section 2.1.1.3 b). The user information layer 1 protocol identification field of the user service information (USI) parameter in IAM must reflect the proper PCM encoding: 'Recommendation G.711 u-law' for supported UCS SS7 trunk agents (SS7 FGD, SS7 IMT Intra, and SS7 IMT Inter) and 'Recommendation G.711 A-law' for the ISUP92/Q.767 trunk agent. For UCS PRI trunk agent, user information layer 1 protocol identification field of the Low layer compatibility element in the Q.931 Setup must reflect 'Recommendation G.711, u-law speech'.

For 64K unrestricted data calls, the conversion between A-law and u-law PCM encoding on a per call basis is disabled. The user information layer 1 protocol identification field must reflect the proper PCM encoding value as stated in the previous paragraph.

109.4.3.9 Overlap Sending

Gateway trunks support overlap sending and that the field OVRLAP in table TRKSGRP is required to be set to enter overlap sending. If a 'F' digit is not received on called number when field OVRLAP in table TRKSGRP is set to 'Y', CS2000 will wait based on T35 timer value (if table C7UPTMR is not used, then default value is 5 seconds) for a subsequent address message (SAM) prior to processing the called number. If SAM is not received within the T35 time, CS2000 will proceed processing the called number.

CS2000 does not support overlap receiving and will always outpulse the called number in 'ENBLOC' format.

109.4.4 ISUP92/Q.767 interworking with supported national trunk agencies.

The supported CS2000 trunk agencies interworking with Q.767/ISUP92 trunks:

- SS7 IMT Inter(UCP)
- SS7 IMT Intra(UCP)
- FGD SS7(UCP)
- FGD PTS[1]
- UCS PRI
- FGB[1]
- DAL TIE[1] [2]

The following interworkings are supported by this feature:

Table 16 Interworkings Supported

Originating Agency	Terminating Agency
ISUP92	ISUP92
Q.767	Q.767
ISUP92	Q.767
Q.767	ISUP92
ISUP92/Q.767	IMT Intra
ISUP92/Q.767	IMT Inter
ISUP92/Q.767	DAL TIE
ISUP92/Q.767	FGB
ISUP92/Q.767	FGD PTS
ISUP92/Q.767	FGD SS7
ISUP92/Q.767	PRI
FGD SS7	ISUP92/Q.767
FGD PTS	ISUP92/Q.767

[1]PTS trunks supported only in a hybrid configuration

[2]Supported DAL TIE pulse type of MF and DT and start signal of WK.

Table 16 Interworkings Supported

Originating Agency	Terminating Agency
FGB	ISUP92/Q.767
IMT Intra	ISUP92/Q.767
IMT Inter	ISUP92/Q.767
DAL TIE	ISUP92/Q.767
PRI	ISUP92/Q.767

109.4.4.1 Interworking between UCP ISUP & ISUP92 /Q.767

The supported UCP ISUP[1] messages that are interworked to ISUP92/Q.767 are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Initial Address Message (IAM)
- Release (REL)

The supported ISUP92/Q.767 messages that are interworked to UCP ISUP are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Connect Message (CON)
- Initial Address Message (IAM)
- Release (REL)

For details on interworking between UCP ISUP & ISUP92 /Q.767 Please refer to Section “109.23 Appendix K: UCP ISUP & ISUP92/Q.767 Interworking” on page 1207.

109.4.4.2 Interworking ISUP92/Q.767 with PTS agents

The supported ISUP92/Q.767 messages that are interworked to PTS agencies are:

- Address complete message (ACM)
- Answer message (ANM)
- Initial Address message (IAM)
- Release message (REL)

[1]UCP ISUP protocol on Succession CS2000 is implemented on IMT and SS7 FGD agents.

- Release complete message (RLC)

For details on interworking between PTS agents & ISUP92/Q.767 Please refer to Section “109.24 Appendix L: Interworking of ISUP92/Q.767 with PTS agents” on page 1236..

109.4.4.3 Interworking with PRI agents

109.4.4.3.1 UCS PRI & ISUP92/Q.767 Message Interworking

The supported UCS PRI messages that interwork to ISUP92/Q.767 are:

- Setup Message (SETUP)
- Alerting Message (ALERT)
- Progress Message (PROG)
- Connect Message (CONN)
- Disconnect Message (DISC)
- Release Message (REL)
- Release complete Message (REL COM)

The supported ISUP92/Q.767 messages that interwork to UCS PRI are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Connect Message (CON)
- Initial Address Message (IAM)
- Release Message(REL)
- Release Complete Message (RLC)

For details on interworking between UCS PRI and ISUP92/Q.767 Please refer to Section “109.25 Appendix N: Interworking between ISUP92/Q.767 and UCS PRI” on page 1243.

109.4.4.4 Interworking between ISUP92 and Q.767 protocols

This feature supports interworking between ISUP92 trunks and Q.767 trunks.

All the Messages except the following is interworked between ISUP92 and Q.767. These messages are supported only on ISUP92 trunks. The below messages on Q.767 trunk are considered as unrecognized messages and are treated as per ITU - T Blue Book Q.767 section 4.1.1. Unrecognized messages are discarded without disrupting normal call handling. No logs are produced for unrecognized messages.

- Confusion Message (CFN)
- Facility Request Message (FAR) != 02
- Facility Reject Message (FRJ)
- Facility Accept Message (FAA)
- User to User Information Message (USR)

All the Parameters except the following are supported in Q.767. These parameters are supported only on ISUP92 trunks. On Q.767 trunks they are discarded.

- Redirecting Number
- Redirection Information
- Redirection Number
- Parameter compatibility information
- Message compatibility information
- Call Diversion information

The other interworking issues are:

- Mapping of new cause values: For information on this issue please refer to section 1.4.2.3.
- Handling of MCP and PCP parameters: For more information on this issue, please refer to section 1.4.2.1.2.

109.4.5 Optionality

The functionality provided by this feature is controlled by SOC option GIMT0003.

109.4.6 Data schema (DS)

This feature introduces, the following two new tables:

- CPCSCRN
- CCTABLE

The following tables are modified by this feature:

- TRKGRP
- TRKSGRP
- STDPRTCT
- RTEATTR

- CSEMAP
- TMTMAP

This feature introduces one new office variable - OFC_SERVING_CC in OFCVAR.

Please refer to the “Data Schema Changes (DS)” section of this feature document (A00003711) for more details about this.

109.4.7 AMA/Billing information (AM)

This feature supports UCS13 CDR template. The fields are captured as per the existing support, except the following fields:

INCINTL: This field is set based on the ‘Nature of Address’ in ‘Calling Party Address’ parameter. If the ‘Nature of Address’ in ‘Calling Party Address’ parameter is set to ‘Intl_sig_number’ then the field is set to ‘Y’.

CLGPTYNO: This field captures up to most significant 15 digits calling party address digits received in the ‘Calling Party Address’ parameter of IAM.

CALLEDNO: This field captures most significant 15 digits of called party address used in translations.

DIALEDNO: This field captures most significant 15 digits of called party address after pretranslations.

OUTPULNO: This field captures most significant 15 digits of outpulsed number. If translations insert a ‘B’ or ‘C’ digits in the outpulsed number then these digits will be represented by ‘*’ and ‘#’ in the TBCD digit format respectively.

PREDIG: Three bits defining dialed prefix digits. For Code11 and Code12 calls, this field captures ‘0’.

CNPREDIG: The called number prefix digits. For Code11 and Code 12 calls, this field captures ‘0’.

109.5 Feature impact

109.5.1 Interactions

109.6 Hardware Requirements or Dependencies

GWIMT trunks are supported via dedicated PVG VSPs and international carrier (E1or STM-1) interfaces. PVG VSPs for GWIMT trunks are separate from any VSPs which may be used to provide trunking to the national network in world zone 1. GWIMT PVG VSPs must also be controlled by one or more dedicated Gateway Contollers.

109.7 Software Requirements or Dependencies

GWIMT is supported initially in the Succession North American Combo load SNNCSH07; the corresponding GWC load supporting GWIMT trunks in this release is the international GC070 variant (GI070).

109.8 Limitations and restrictions

- GWIMT trunks are not supported on DTC type peripherals in SNNCSH07. Only PVG based GWIMT trunks are supported.
- Echo Cancelation is provided by the PVG VSP under this activity. Support for external echo cancelors is not provided.
- Carrier AIN calls can terminate to GWIMT trunks, however calls originating on GWIMT trunks do not encounter Carrier AIN (CAIN) triggers.
- CLI screening on ISUP92/Q.767 gateway trunk agency is not supported.
- Gateway trunk agencies (ISUP92/Q.767) supports only ADDR dialplan. This restriction is provided as datafill restriction.
- When option GWYTRK is datafilled in table TRKGRP, the fields CLIREQ and CLISCRN must be set to N. This is also implemented as datafill restriction.
- Local Number Portability (LNP) is not support on ISUP92/Q.767 gateway trunk agency.
- The maximum number of called number digits supported by this feature is 15 (15-digit IDDD) excluding the end-of-digit signal (F).
- The maximum number of calling number digits supported by this feature is 15 (15-digit IDDD) excluding the end-of-digit signal (F).
- The feature implements only a limited set of GSP features, on Succession CS2000 in the role of a UCS DMS-250 switch.
- Support for ISUP92 and Q.767 protocols are subject to partial compliance as stated within this feature.

- This feature support only internal echo cancellers, in which case ESUPR field should be set to N, ECSTAT field should be set to INTERNAL, and ABCNTL field should be set to NONE in table TRKSGRP.
- For transit inbound code 11/code 12 calls a maximum of 14 called party address digits are supported.
- For code 11/code 12 calls, only one code 11 or code 12 signal codes is supported in the called party address digits stream.
- RLT functionality is not supported by this feature. This includes support of RLT option on ISUP92/Q767 agencies and interworking of ISUP92/Q767 agencies with RLT trunk agents.
- CGETS functionality, including IAM priority, is not supported on GWIMT trunks.

109.9 Interactions

109.9.1 CIC routing/CIC delivery

The feature doesn't support CIC routing on ISUP92 and Q.767 trunks. CIC routing on UCS agents are supported as per the existing functionality.

The TNS/CIP parameters received on ISUP92/Q.767 gateway agencies are discarded. In the case when ISUP92/Q.767 gateway trunks are terminating agencies, these parameters are not delivered.

109.9.2 AX0205 'UCS TRKGRP NOA Enhancements'

Feature AX0205 'UCS Trunkgroup NOA Enhancements' enhances Nature of address delivery in called party address parameter of outgoing IAM. This feature affects the INBOUND direct termination calls terminating on Inter/ Intra network ISUP IMTs.

The NOA outpulsed in called party address parameter of outgoing IAM for these calls is the value of OUTNOA datafilled in table TRKGRP. Please refer to feature AX0205 for more details.

109.9.3 Carrier AIN

ISUP92/Q.767 trunk agency as an originator

Carrier AIN functionality is not supported on an incoming call on a ISUP92/ Q.767 trunk agency.

ISUP92/Q.767 trunk agency as a terminator

The ISUP92/Q.767 trunk agency is supported as a terminating agent for incoming calls on the supported CS2000 agencies that are CAIN capable. Any PICs, TDPs, triggers and EDPs supported on the originating CS2000 agencies, are supported by this feature with the following restrictions.

- Any Carrier AIN SS7 parameters that are not supported within the ISUP92/Q.767 trunk agency protocol is not delivered/included in any outgoing messages on the ISUP92/Q.767 trunk agency.

- Direct termination routing to the terminating ISUP92/Q.767 trunk agency is supported via table TERMRTE only.
- The terminating call model is not supported.

109.9.4 User-To-User Parameter Mapping

Reference feature document AD9067 ‘Support for User to User Parameter’ for proper requirements when mapping of the User to User parameter is required.

109.10 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

109.11 References

- A59007112, “Up to 128ms ECAN (Echo Cancelation) on IW-SPM IP”
- A00000284, “ Packet Trunking IP AAL2 test Line Testing Utilizing the UAS and SAGE”

- A59038503, “Test Trunk Support via IW-SPM-IP”
- AR2020 - DMS300 - ISUP92
- AM0115, “UCS PRA on DMS-250”.
- AD1614, “DMS-250 PRA Application Guide”.
- AD9067, “Support For UUI Parameters”.
- AM0184, “Access Transport PRI/SS7 DDOC”
- AD8792, “Route Based Outgoing Parameter Modifications”.
- AD6849, “UCS ANI Delivery Enhancements”.
- ITU-T Recommendation Q.850 (March 1993)
- ITU-T Recommendation Q.767 Blue Book version (February 1991)
- ITU-T Recommendation Q.761-764 White Book version (March 1993)

109.12 Glossary

Term	Description
GWIMT	Gateway Inter Machine Trunk
PVG	Passport Voice Gateway
BSS	Bearer Service Selection
CAS	Channel Associated Signalling
CAIN	Carrier Advanced Intelligent Networks
CCITT	Consultative Committee on International Telephony and Telegraphy
CCS7	Common Channel Signaling No. 7
CDR	Call Detail Record
CGETS	Carrier GETS
CIC	Carrier Identification Code
CLI	Calling Line Identification
CSP	Communications System Platform
CPC	Calling Party Category

Term	Description
DAL	Direct Access Link
DDOC	Design Document
DMS	Digital Multiplexing System
DTC	Digital Trunk Controller
DTCI	Digital Trunk Controller International
DTCO	Digital Trunk Controller Overseas
EC	Echo Canceler
ECC	Echo Canceler Controller
EDP	Electronic Data Processing
EOPS	Enhanced Operator Services
FGB	Feature Group B
FGD	Feature Group D
FSD	Feature Specification Document
GETS	Government Emergency Telecommunications Service
GWC	Gateway Controller
IMT	Inter Machine Trunk
ISUP	ISDN User Part
ITU	International Telecommunications Union
LEC	Local Exchange Carrier
MCP	Message Compatibility Procedure
NORTEL	Northern Telecom
NWM	Network Management
PIC	Point In Call
PCM	Pulse Code Modulation
PCP	Parameter Compatibility Procedure
PSN	Programmable Service Node
PTS	Per-Trunk Signaling
RLT	Release Link Trunk
SOC	Software Optionality Control

Term	Description
SS7	Signaling System No. 7
TDP	Telelocator Data Protocol
TRKGRP	Trunk Group Table
TRKSGRP	Trunk Signaling Group Table
TRM	Transmission Resource Management
UCP	Universal Carrier Protocol
UCS	Universal Carrier Services
UIFN	Universal International Freephone Number
VPN	Virtual Private Network
XPM	eXtended Peripheral Module

109.13 APPENDIX A: Messages and Parameters Supported on ISUP92

Messages and Parameters that are supported on ISUP92 trunks are listed in the following tables in this section.

109.13.1 International ISUP92 message base

The table below represents the list of recognized messages for an international ISUP92 trunk at the Succession CS2000.

Note: S/R means Send/Receive. Dis/CFN means Discard and send CFN (confusion message)

Note: P/T/D means Process (Process the message), Tandem (Tandem message across network) and Discard (Discard and ignore the message) respectively.

Table 17 International ISUP92 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive/ Dis/CFN	Process/ Tandem/Discard
ACM	Address complete	S/R	P
ANM	Answer	S/R	P

Table 17 International ISUP92 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive/ Dis/CFN	Process/ Tandem/Discard
BLO	Blocking	S/R	P
BLA	Blocking Acknowledgment	S/R	P
CPG	Call Progress	S/R	T
CGB	Circuit Group Blocking	R	P
CGBA	Circuit Group Blocking Acknowledgment	S	P
GRS	Circuit Group Reset	S/R	P
GRA	Circuit Group Reset Acknowledgment	S/R	P
CGU	Circuit Group Unblocking	R	P
CGUA	Circuit Group Unblocking Acknowledgment	S	P
CON	Connect	S/R	P
COT	Continuity	S/R	P
CFN	Confusion	S/R	P
CCR	Continuity Check Request	S/R	P
FAA	Facility Accepted	Dis/CFN	Discard
FAR	Facility Request	R[a]	Discard/ Tandem
FRJ	Facility Reject	[b]Dis/CFN	Discard
FOT	Forward Transfer	S/R	T
IAM	Initial Address	S/R	P
INR	Information Request	S[c]	T
REL	Release	S/R	P
RLC	Release Complete	S/R	P
RSC	Reset Circuit	S/R	P
RES	Resume	S/R	T[d]
SAM	Subsequent Address	S/R	P
SUS	Suspend	S/R	T[e]
UBL	Unblocking	S/R	P
UBA	Unblocking Acknowledgment	S/R	P
USR	User-to-user information	Dis/CFN	Discard

a. If FAR != 02 is received, the Succession CS2000 discards the FAR and returns.
If FAR = 02 (user-to-user service), the Succession CS2000 tandems the FAR

b. If FRJ is received, the Succession CS2000 discards the FRJ and returns CFN with cause value 97 with FRJ as the diagnostic information.

c. There is no call processing done for this message, the Succession CS2000 tandems this message. Succession CS2000 always delivers the CLI in enbloc format. If an incomplete CLI is received, the Succession CS2000 does not generate INR msg but instead discards the calling party parameter.
d. RES msg is tandemed only if the Resume indicator is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing Succession CS2000 Suspend/Resume functionality. For all other cases it is discarded.
e. SUS msg is tandemed only if the suspend indicator is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing Succession CS2000 Suspend/Resume functionality. For all other cases it is discarded.

109.13.2 International ISUP92 parameter base

The Succession CS2000 supports the following parameters for the given supported messages in accordance with ISUP92 for the Succession CS2000 exchange.

Notations used are:

F = mandatory fixed length parameter

V = mandatory variable length parameter

O = optional parameter

The proprietary and national parameters are discarded unless specified.

When the Succession CS2000 generates a REL or CFN message, the location field of the cause parameter is set to ‘International Network’. If the REL message is generated using table TMTMAP, the location field of the cause parameter is taken from the ‘location’ field of the table entry. Please refer to section 1.4.2.3 for more details on cause handling.

‘ISUP92 minimum set’ refers to the recommended minimum set of parameters to be supported for each supported message based on ITU-T Recommendation Q.761 White Book version table 4 for international use.

109.13.2.1 Initial Address Message (IAM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the IAM message as shown in Table 18. All parameters not contained in table 18 are subject to the rules of the PCP procedures.

Table 18 Parameters supported in the IAM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Nature Of Connection Indicators	F	Process	ISUP92 minimum set
Forward Call Indicators	F	Process	ISUP92 minimum set
Calling Party's Category	F	Process	ISUP92 minimum set
Transmission Medium Requirement (TMR)	F	Process	ISUP92 minimum set supported values[a].
Called Party Number	V	Process	ISUP92 minimum set
Access Transport	O	Tandem	ISUP92 minimum set
Calling Party Number	O	Process	ISUP92 minimum set
Closed User Group Inter lock Code	O	Tandem	ISUP92 minimum set
Connection Request	O	Discard	
End of Optional Parameters	O	Process	ISUP92 minimum set
Generic Notification	O	Discard	
Generic Number	O	Discard	
Generic Reference	O	Discard	
Location Number	O	Discard	
MLPP Precedence	O	Discard	
Optional Forward Call Indicators	O	Tandem	ISUP92 minimum set
Original Called Number	O	Tandem	ISUP92 minimum set

Table 18 Parameters supported in the IAM Message ISUP92

Parameter Name	Type	Action	Notes
Origination ISC Point Code	O	Discard	
Parameter Compatibility Information	O	See Section 1.4.2.1.2	
Propagation Delay Counter	O	Discard	
Redirecting Number	O	Tandem	ISUP92 minimum set
Redirection Information	O	Tandem	ISUP92 minimum set
Transmission Medium Requirement Prime	O	Discard	
User service information	O	Process	ISUP92 minimum set
User Service Information prime	O	Discard	
User teleservice information	O	Discard	
User-to-user Indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Generic digit	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only
Transit network selection	O	Discard	National use only

a. Supported values are Speech, 64 Kbit/s unrestricted, and 3.1 Khz audio

109.13.2.2 Address complete message (ACM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the IAM message as shown in Table 19. All parameters not contained in table 19 are subject to the rules of the PCP procedure.

Table 19 Parameters supported in the ACM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	F	Process	ISUP92 minimum set
Optional backward call indicators	O	Process	ISUP92 minimum set
Cause indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Generic notification Indicator	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call diversion information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set

Table 19 Parameters supported in the ACM Message ISUP92

Parameter Name	Type	Action	Notes
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

109.13.2.3 Answer message (ANM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the ANM message as shown in Table 20. All parameters not contained in table 20 are subject to the rules of the PCP procedure.

Table 20 Parameters supported in the ANM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	O	Tandem	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Connected number	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
Generic notification indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call history information	O	Tandem	ISUP92 minimum set

Table 20 Parameters supported in the ANM Message ISUP92

Parameter Name	Type	Action	Notes
Generic number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

109.13.2.4 Call progress message (CPG)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CPG message as shown in Table 21. All parameters not contained in table 21 are subject to the rules of the PCP procedure.

Table 21 Parameters supported in the CPG Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Event information	F	Process	ISUP92 minimum set
Backward call indicators	O	Tandem	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
Cause indicators	O	Tandem	ISUP92 minimum set

Table 21 Parameters supported in the CPG Message ISUP92

Parameter Name	Type	Action	Notes
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
Generic notification indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call diversion information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

109.13.2.5 Connect message (CON)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CON message as shown in Table 22. All parameters not contained in table 22 are subject to the rules of the PCP procedure.

Table 22 Parameters supported in the CON Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	F	Process	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Generic notification Indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call history information	O	Tandem	ISUP92 minimum set
Generic number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum se
Connected number	O	Tandem	ISUP92 minimum se

Table 22 Parameters supported in the CON Message ISUP92

Parameter Name	Type	Action	Notes
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

109.13.2.6 Facility Accept (FAA) & Facility Request Messages (FAR)

The Succession CS2000 discards FAA Messages and sends Confusion message on an ISUP92 trunk.If FAR ! = 02, is received, the DMS-250 discards the FAR .If FAR with facility indicator set to User-to-User service (00000010), is received, the DMS-250 tandems the FAR.

109.13.2.7 Continuity Message (COT)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the COT message as shown in Table 23.The proprietary and national use parameters are not supported.

Table 23 Parameters supported in the COT Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Continuity Indicators	F	Tandem	ISUP92 minimum set

109.13.2.8 Circuit Group ReSet (GRS) & circuit Group Reset Acknowledge messages (GRA)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the GRS & GRA messages as shown in Table 24. The proprietary and national use parameters are not supported.

Table 24 Parameters supported in the GRS & GRA Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Range and Status	V	Process	ISUP92 minimum set

109.13.2.9 User-to-User Information Message (USR)

The Succession CS2000 discards USR Messages and sends Confusion message on an ISUP92 trunk.

109.13.2.10 Facility Reject message (FRJ)

The Succession CS2000 discards the FRJ and returns CFN with cause value 97 with FRJ as the diagnostic information.

109.13.2.11 Circuit Group blocking (CGB), block ACK(CGBA), unblocking (CGU), unblock ack (CGUA) messages.

The Succession CS2000 on an ISUP92 trunk supports the mandatory parameters in the CGB, CGBA, CGU, CGUA messages as shown in Table 25. The CGB, CGBA, CGU, or CGUA messages do not have optional parameters.

Table 25 Parameters supported in the CGB,CGBA,CGU,CGUA Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Circuit group supervision msg type indicator	F	Process	ISUP92 minimum set
Range and Status	V	Process	ISUP92 minimum set

109.13.2.12 Blocking (BLO), block ack (BLA), Continuity check request (CCR), unblock (UBL), unblock ack (UBA), Reset circuit (RSC) messages.

The Succession CS2000 on an ISUP92 trunk supports the mandatory parameters in the BLO, BLA, CCR, UBL, UBA, RSC messages as shown in Table 26. The BLO, BLA, CCR, UBL, UBA, RSC messages do not have optional parameters.

Table 26 Parameters supported in the BLO, BLA, CCR, UBL, UBA, RSC Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	

109.13.2.13 Confusion Message (CFN)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CFN message as shown in Table 27.

Table 27 Parameters supported in the CFN Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	V	Process	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set

109.13.2.14 Release Message (REL)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CON message as shown in Table 28. All parameters not contained in table 28 are subject to the rules of the PCP procedure.

Table 28 Parameters supported in the REL Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	F	Process	ISUP92 minimum set
Automatic congestion level	O	Discard	The switch handles this parameter on a link-by-link basis. If received, the parameter is removed from the message and not transited.
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Network specific facility	O	Discard	National use only
Signalling Point Code	O	Discard	National use only
Redirection Number	O	Discard	National use only
Redirection Information	O	Discard	National use only

109.13.2.15 Release Complete Message (RLC)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the RLC message as shown in Table 29. Parameters not contained in table 29 are

treated as unrecognized parameters.

Table 29 Parameters supported in the RLC Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	O	N/A	ISUP92 minimum set
End of Optional Parameters	O	N/A	ISUP92 minimum set

109.13.2.16 Forward Transfer Message (FOT)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the FOT message as shown in Table 30. All parameters not contained in table 30 are treated as unrecognized parameters.

Table 30 Parameters supported in the FOT Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
End of Optional Parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National Use only

109.13.2.17 Suspend (SUS) & Resume (RES) Messages

The Succession CS2000 on an ISUP92 trunk supports the parameters in the SUS & RES messages as shown in Table 31. All parameters not contained in table 31 are treated as unrecognized parameters.

Table 31 Parameters supported in the SUS & RES Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Suspend/Resume indicators	F	Tandem/ Discard[a]	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set
Call reference	O	Discard	National Use only

a. If the Suspend/ Resume indicator (in the SUS/RES message) is set to network initiated and the message is received on the terminator after the ANM, the message is Tandemed. For all other cases it is Discarded.

109.13.2.18 Subsequent Address Message (SAM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the SAM message as shown in Table 32.

Table 32 Parameters supported in the SAM Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Subsequent number	V	Process	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set

109.14 Appendix B: Messages and Parameters Supported on Q.767

Messages and Parameters that are supported on Q.767 trunks are listed in the Tables in this section. Messages and parameters marked for national use, are discarded

109.14.1 International Q.767 Message Base

The Table below represents the list of recognized messages for an international Q.767 trunk at the DMS-250 exchange.

Note: S/R means Send/Receive.

Note: P/T means Process (Process the message), Tandem (Tandem message across network) respectively.

Table 33 International Q.767 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive	Process/ Tandem
ACM	Address complete	S/R	P

Table 33 International Q.767 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive	Process/ Tandem
ANM	Answer	S/R	P
BLO	Blocking	S/R	P
BLA	Blocking Acknowledgment	S/R	P
CPG	Call Progress	S/R	T
CGB	Circuit Group Blocking	R	P
CGBA	Circuit Group Blocking Acknowledgment	S	P
GRS	Circuit Group Reset	S/R	P
GRA	Circuit Group Reset Acknowledgment	S/R	P
CGU	Circuit Group Unblocking	R	P
CGUA	Circuit Group Unblocking Acknowledgment	S	P
CON	Connect	S/R	P
COT	Continuity	S/R	P
CCR	Continuity Check Request	S/R	P
FOT	Forward Transfer	S/R	T
IAM	Initial Address	S/R	P
INR	Information Request	S[a]	P
REL	Release	S/R	P
RLC	Release Complete	S/R	P
RSC	Reset Circuit	S/R	P
RES	Resume	S/R[b]	T
SAM	Subsequent Address	S/R	P
SUS	Suspend	S/R[c]	T
UBL	Unblocking	S/R	P
UBA	Unblocking Acknowledgment	S/R	P

a. There is no call processing done for this message, the DMS-250 tandems this message. DMS-250 always delivers the CLI in enbloc format. If an incomplete CLI is received, the DMS-250 does not generate INR msg but instead discards the calling party parameter.
b. If the Resume indicator (in the RES message) is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing DMS-250 Suspend/Resume functionality, the message is Tandemed. For all other cases it is Discarded.

c. If the Suspend indicator (in the SUS message) is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing DMS-250 Suspend/Resume functionality, the message is Tandemed. For all other cases it is Discarded

109.14.2 International Q.767 Parameter Base

The Succession CS2000 supports the following parameters for the given supported call processing messages in accordance with Q.767 recommendation for the DMS-250 exchange.

F = mandatory fixed length parameter

V = mandatory variable length parameter

O = optional parameter

The proprietary and national use parameters are discarded.

'Q.767 minimum set' refers to the recommended minimum set of parameters to be supported for each supported message based on ITU-T Recommendation Q.767 Blue Book version tables C-5 to C-28.

109.14.2.1 Initial Address Message (IAM)

The Succession CS2000 on an Q.767 trunk supports the parameters in the IAM message as shown in Table 34. All parameters not contained in table 34 are discarded.

Table 34 Parameters supported in the IAM Message at Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Nature Of Connection Indicators	F	Process	Q.767 minimum set
Forward Call Indicators	F	Process	Q.767 minimum set
Calling Party's Category	F	Process	Q.767 minimum set
Transmission Medium Requirement (TMR)	F	Process	Q.767 minimum set
Called Party Number	V	Process	Q.767 minimum set
Access Transport	O	Tandem	Q.767 minimum set

Table 34 Parameters supported in the IAM Message at Q.767

Parameter Name	Type	Action	Notes
Calling Party Number	O	Process	Q.767 minimum set
Closed User Group Inter lock Code	O	Tandem	Q.767 minimum set
End of Optional Parame-ters	O	Process	Q.767 minimum set
Optional Forward Call Indicators	O	Tandem	Q.767 minimum set
User service information	O	Process	Q.767 minimum set
User-to-user information	O	Tandem	Q.767 minimum set
Call reference	O	Discard	National use only
Generic digit	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only
Transit network selection	O	Discard	National use only

109.14.2.2 Address Complete (ACM), Answer Message (ANM), Call Progress (CPG), Connect (CON), Release (REL) Messages.

The parameters supported in these messages are given in Table 35. All the parameters shown in table 35 are tandemed.

Table 35 Parameters supported in ACM, CPG, ANM,CON and REL messages

Message	Parameters tandemed
ACM	Optional Backward Call Indicators, Cause Indicator, User to user indicators[a], User to user information, Access Transport

Table 35 Parameters supported in ACM, CPG, ANM,CON and REL messages

Message	Parameters tandemed
CPG	Optional Backward Call Indicators, Backward Call Indicators, User to user information, Access Transport
ANM	Backward Call Indicators, Connected Number[a], User to user information, Access Transport
CON	Connected Number[a], Backward call indicator, User to user indicators, User to user information, Access Transport
REL	User to user information. Automatic congestion Level[b]

a. It is tandemed only if it is valid as per Q767 recommendations.
b. It is processed as per Q767 recommendations and is not tandemed.

109.14.2.3 Continuity Message (COT)

The Succession CS2000 on an Q.767 trunk supports the parameters in the COT message as shown in Table 36.

Table 36 Parameters supported in the COT Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Continuity Indicators	F	Tandem	Q.767 minimum set

109.14.2.4 circuit Group ReSet (GRS) & circuit Group Reset Acknowledge messages (GRA)

The Succession CS2000 on an Q.767 trunk supports the parameters in the GRS & GRA messages as shown in Table 37.

Table 37 Parameters supported in the GRS & GRA Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Range and Status	V	Process	Q.767 minimum set

109.14.2.5 Circuit Group blocking (CGB), block ack (CGBA), unblocking (CGU), unblock ack (CGUA) messages.

The Succession CS2000 on an Q.767 trunk supports the mandatory parameters in the CGB, CGBA, CGU, CGUA messages as shown in Table 38. The CGB, CGBA, CGU, or CGUA messages do not have optional parameters.

Table 38 Parameters supported in the CGB,CGBA,CGU,CGUA Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Circuit group supervision msg type indicator	F	Process	Q.767 minimum set
Range and Status	V	Process	Q.767 minimum set

109.14.2.6 Blocking (BLO), block ack (BLA), Continuity check request (CCR), unblock (UBL), unblock ack (UBA), Reset circuit (RSC) messages.

The Succession CS2000 on an Q.767 trunk supports the mandatory parameters in the BLO, BLA, CCR, UBL, UBA, RSC messages as shown in Table 39. The BLO, BLA, CCR, UBL, UBA, RSC messages do not have optional parameters.

Table 39 Parameters supported in the BLO, BLA, CCR, UBL, UBA, RSC Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set

109.14.2.7 Release Complete Message (RLC)

The Succession CS2000 on an Q.767 trunk supports the parameters in the RLC message as shown in Table 40. Parameters not contained in table 40 are treated as unrecognized parameters and discarded.

Table 40 Parameters supported in the RLC Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Cause Indicators	O	N/A	Q.767 minimum set
End of Optional Parameters	O	N/A	Q.767 minimum set

109.14.2.8 Forward Transfer Message (FOT)

The Succession CS2000 on an Q.767 trunk supports the parameters in the FOT message as shown in Table 41. All parameters not contained in table 41 are treated as unrecognized parameters.

Table 41 Parameters supported in the FOT Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
End of Optional Parameters	O	Tandem	Q.767 minimum set
Call reference	O	Discard	National Use only

109.14.2.9 Suspend (SUS) & Resume (RES) Messages

The Succession CS2000 on an Q.767 trunk supports the parameters in the SUS & RES messages as shown in Table 42. All parameters not contained in table 42 are treated as unrecognized parameters.

Table 42 Parameters supported in the SUS & RES Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Suspend/Resume indicators	F	Tandem/ discard[a]	Q.767 minimum set

Table 42 Parameters supported in the SUS & RES Message on Q.767

Parameter Name	Type	Action	Notes
End of Optional Parameters	O	Process	Q.767 minimum set
Call reference	O	Discard	National Use only

a. If the Suspend/ Resume indicator (in the SUS/RES message) is set to network initiated and the message is received on the terminator after the ANM, the message is Tandemed. For all other cases it is Discarded.

109.14.2.10 Subsequent Address Message (SAM)

The Succession CS2000 on an Q.767 trunk supports the parameters in the SAM message as shown in Table 43.

Table 43 Parameters supported in the SAM Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Subsequent number	V	Process	Q.767 minimum set
End of Optional Parameters	O	Process	Q.767 minimum set

109.15 Appendix C: Q.767/ISUP92 Timers

Table 44 Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T1 4-15 s	When release message is sent	NQ764T1	1-60 s (15 s)
T2 3 min	When suspend request controlling exchange receives suspend (user) message	NQ764T2	1-240 s (180 s)
T3	Not used on the international interface		
T4	Not used on the international interface		
T5 1 min	When initial release message is sent	NQ764T5	1-180 s (60 s)
T6 Q.118	When controlling exchange receives suspend (network)	NQ764T6	1-240 s (90 s)
T7 20-30 s	When the latest address message is sent	NQ764T7	1-60 s (20 s)
T8 10-15 s	When transit or incoming international exchange receives initial address message requiring continuity check on this circuit, or indicates that continuity check has been performed on a previous circuit	NQ764T8	1-60 s (15 s)
T9 Q.118 2-4 min	When national controlling or outgoing international exchange receives ACM[a]	Q.118	120-240 s (180 s)
T10 4-6 s	When last digit is received in interworking situations	NQ764T10	1-30 s (5 s)
T11 15-20 s	When latest address message is received in interworking situations	NQ764T11	1-60 s (15 s)
T12 4-15 s	When blocking message is sent	NQ764T12	1-60 s (10 s)

Table 44 Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T13 1 min	When initial blocking message is sent	NQ764T13	1-180 s (60 s)
T14 4-15 s	When unblocking message is sent	NQ764T14	1-60 s (10 s)
T15 1 min	When initial unblocking message is sent	NQ764T15	1-180 s (60 s)
T16 4-15 s	When reset circuit message is sent not due to the expiry of Timer T5	NQ764T16	1-60 s (10 s)
T17 1 min	When initial reset circuit message is sent	NQ764T17	1-180 s (60 s)
T18 4-15 s	When group blocking message is sent	NQ764T18	1-60 s (10 s)
T19 1 min	When initial group blocking message is sent	NQ764T18	1-180 s (60 s)
T20 4-15 s	When group unblocking message is sent	NQ764T20	1-60 s (10 s)
T21 1 min	When initial group unblocking message is sent	NQ764T21	1-180 s (60 s)
T22 4-15 s	When circuit group reset message is sent	NQ764T22	1-60 s (10 s)
T23 1 min	When initial circuit group reset message is sent	NQ764T23	1-180 s (60 s)
T24 < 2 s	When check tone is sent	NQ764T24	0.1-2.0 s (1 s)
T25 1-10 s	When initial continuity check failure is detected	NQ764T25	1-30 s (10 s)
T26 1-3 min	When second or subsequent continuity check failure is detected	NQ764T26	1-240 s (120 s)
T27 4 min	When continuity check failure indication is received	NQ764T27	1-300 s (240 s)

Table 44 Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T28	Not used on the international interface		
T29 300-600 ms	Congestion indication received when T29 not running	Not imple-mented	
T30 5-10 s	Congestion indication received when T29 not running	Not imple-mented	
T31	Not used on the international interface		
T32	Not used on the international interface		
T33	Not used on the international interface		
T34	Not used on the international interface		
T35 15-20 s	At receipt of the latest digit and before the minimum or fixed number of digits have been received	NQ764T35	1-60 s (20 s)
T36 10-15 s	When transit or incoming international exchange receives continuity check request message	NQ764T8	1-60 s (15 s)

a. This timer is not used for answer timing. Instead field LCDDUR in table TRKGRP1 is used for answer timing purpose.The value of LCDDUR for terminating trunk provides the answer timing. The range of this field is 0-60, supporting upto 60 minutes. If the value is 0, then no answer timing is done on this switch and call continues.

109.16 Appendix D: Call Information (IAM message) for Gateway Calltypes

This Appendix describes the pertinent information in the ISUP IAM message as it pertains to the supported Gateway Calltypes:

- Direct Termination Outbound International
- Direct Terminational Inbound National
- Transit Outbound International

109.16.1 Direct Termination Outbound International

The CS2000 would calltype the call as a international (IDDD) call and perform the following gateway functions on the outgoing call information (Initial Address message (IAM)):

- Called party number parameter (Refer ITU-T Recommendation Q.107)
  - set Nature of Address (NOA) to value of national significant number (0000011)
  - called number format (15-digit IDDD + F)(<true Country Code>+<NN>+F)
    - strip any international prefix (’011’ for WZ1 format)
    - Strip the country code digits.
    - end-of-digit (#F) is suffixed to the called number
    - called number is delivered using enbloc format
- Calling party number parameter (if received in originating call information)
  - Nature of Address (NOA) would be set to International significant number (0000100)
  - Calling party number would be prefixed with the serving country code of CS2000 (per office basis) Note: maximum of 15-digit is supported.
  - existing CLI (ANI) delivery functionality is used to determine if calling party parameter is delivered.
- Calling party category (CPC) parameter
  - CPC value would be set to (00001010) ’ordinary calling subscriber’ only if the CPC value has not been overridden by the CPCSCRN option and has a value associated with ’not used’ values as defined in recommendation Q.767 section C.3.9. The ’not used’ values are:
    - 00000000: calling party’s category unknown at this time
    - 00001001: reserved (see Recommendation Q.104)
    - 11100000
      to
      11111110: spare for national use
- Forward Call Indicator parameter

- Bit A (National/international call indicator) would have been set to value of 0'call to be treated as a national call'

109.16.2 Direct Terminational Inbound National

For direct termination inbound national calls, the ISUP92/Q.767 gateway trunk agency would expect to receive the following call information (Initial Address message (IAM)) from the preceding foreign exchange:

- Called party number parameter
  - Nature of Address (NOA) would have been set to value of National significant number (0000011)
  - called number format (10-digit NN + F)
    - called number would contain WZ-1 national number (10-digit).
    - If end-of-digit (#F) is suffixed to the called number, CS2000 would strip end-of-digit prior to accessing table STDPRTCT.
    - For incomplete called number (called number not suffixed with end-of-digit ('F' digit)) Succession CS2000 waits for subsequent address message (SAM) until the Succession CS2000 receives either an end-of-digit or time-out occurs waiting for SAM prior to proceeding with translations.
- Calling party number parameter
  - Nature of Address (NOA) would have been set to International significant number
  - Calling party number would have been prefixed with the country code of the subscriber. Maximum of 15 digits are supported (based on 15-digit IDDD format). Most significant digits exceeding 15 digits is removed from the calling party number.
    - If end-of-digit (#F) is suffixed to the calling party number, CS2000 would remove the end-of-digit.
    - If an incomplete calling party number is received (calling party number incomplete indicator (NI) is 'incomplete', CS2000 would discard the calling party number.
- Calling party category (CPC) parameter
  - CPC value would have been set to (00001010) 'ordinary calling subscriber' depending on calltype (DDD, OA)
- Forward Call Indicator parameter
  - If Bit A has not been set to value of'0' (call to be treated as an national call), CS2000 would set Bit A to value of'0'(Recommendation Q.767 section C.3.20).

109.16.3 Transit Outbound International

For transit inbound international calls, the gateway trunk agency would have received the following initial call information (Initial Address message (IAM)) where the preceding foreign exchange would have performed the following function on the initial call information in the IAM:

- Called party number parameter
  - Nature of Address (NOA) would have been set to value of International significant number (0000100)
  - called number format (15-digit IDDD + F)
    - called number would contain WZ-1 national number (10-digit).
    - If end-of-digit (#F) is suffixed to the called number, CS2000 would strip end-of-digit prior to accessing table STDPRTCT.
    - For incomplete called number (called number not suffixed with end-of-digit ('F' digit)) Succession CS2000 waits for subsequent address message (SAM) until the Succession CS2000 receives either an end-of-digit or time-out occurs waiting for SAM prior to proceeding with translations.
- Calling party number parameter
  - Nature of Address (NOA) would have been set to International significant number
  - Calling party number would have been prefixed with the country code of the subscriber. Maximum of 15 digits are supported (based on 15-digit IDDD format).
    - If end-of-digit (#F) is suffixed to the calling party number, CS2000 would remove the end-of-digit.
    - If an incomplete calling party number is received (calling party number incomplete indicator (NI) is 'incomplete', CS2000 would discard the calling party number.
- Forward Call Indicator parameter
  - If Bit A has not been set to value of'1' (call to be treated as an international call), CS2000 would set Bit A to value of'1'(Recommendation Q.767 section C.3.20).

The CS2000 would calltype the call as a international (IDDD) call and perform the following gateway functions on the outgoing call information (Initial Address message (IAM)):

- Called party number parameter (Refer Recommendation Q.107)
  - called number format (15-digit IDDD + F)
  - strip any international prefix based on the national dialing plan
  - Nature of Address (NOA) would have been set to value of International significant number (0000100)
  - called number would have been prefixed with proper country code by the subscriber

- end-of-digit (#F) is suffixed to the called number
- CS2000 delivers the called number in enbloc.

- Calling party number parameter (if delivered based ANI delivery functionality)
  - Nature of Address (NOA) is set to International significant number (0000100)
  - If call originated on Q.767/ISUP92 gateway trunk agent, Succession CS2000 assumes the country code has been prefixed on the calling party number by the preceding foreign exchange. If call originated on UCS agent, the OFC_SERVING_CC office parameter value is prefixed on the calling party number. Note: maximum of 15 digits is supported.
- Calling party category (CPC) parameter
  - CPC value would be set to (00001010)'ordinary calling subscriber' only if the CPC value has not been overridden by the CPCSCRN option and has a value associated with 'not used' values as defined in recommendation Q.767 section C.3.9. The 'not used' values are:
    - 00000000: calling party's category unknown at this time
    - 00001001: reserved (see ITU-T Recommendation Q.104)
    - 11100000
      to
      11111110: spare for national use
- Forward Call Indicator parameter
  - If Bit A has not been set to value of'1' (call to be treated as an international call), CS2000 would set Bit A to value of '1'(Recommendation Q.767 section C.3.20).

109.17 Appendix E: Callflow diagram

The following figures illustrate the call flow for the gateway functionality. The shaded boxes indicate the functionality provided by this feature.

Figure 12 Gateway functionality call flows

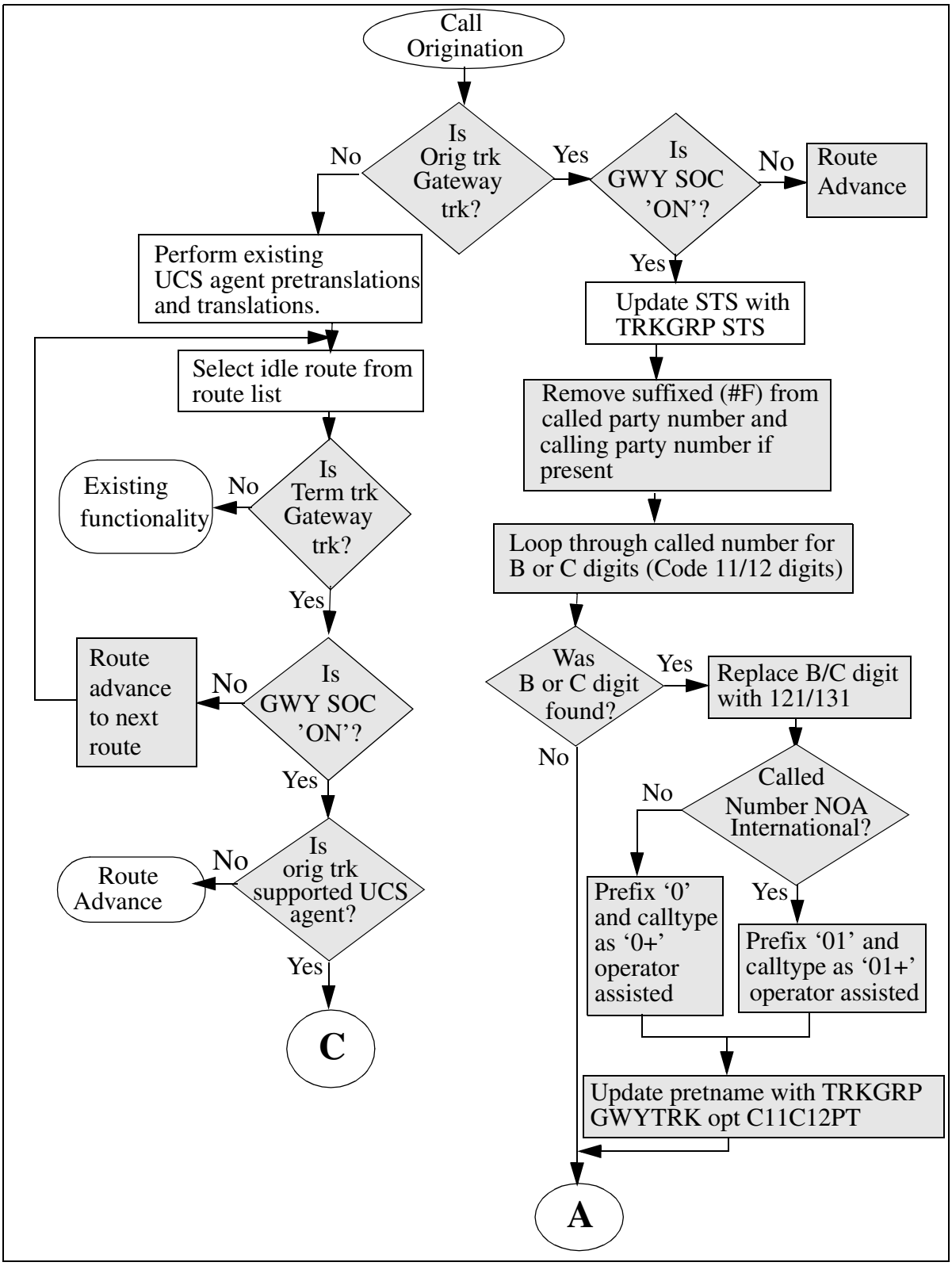


Figure 13 Gateway functionality call flows (continued)

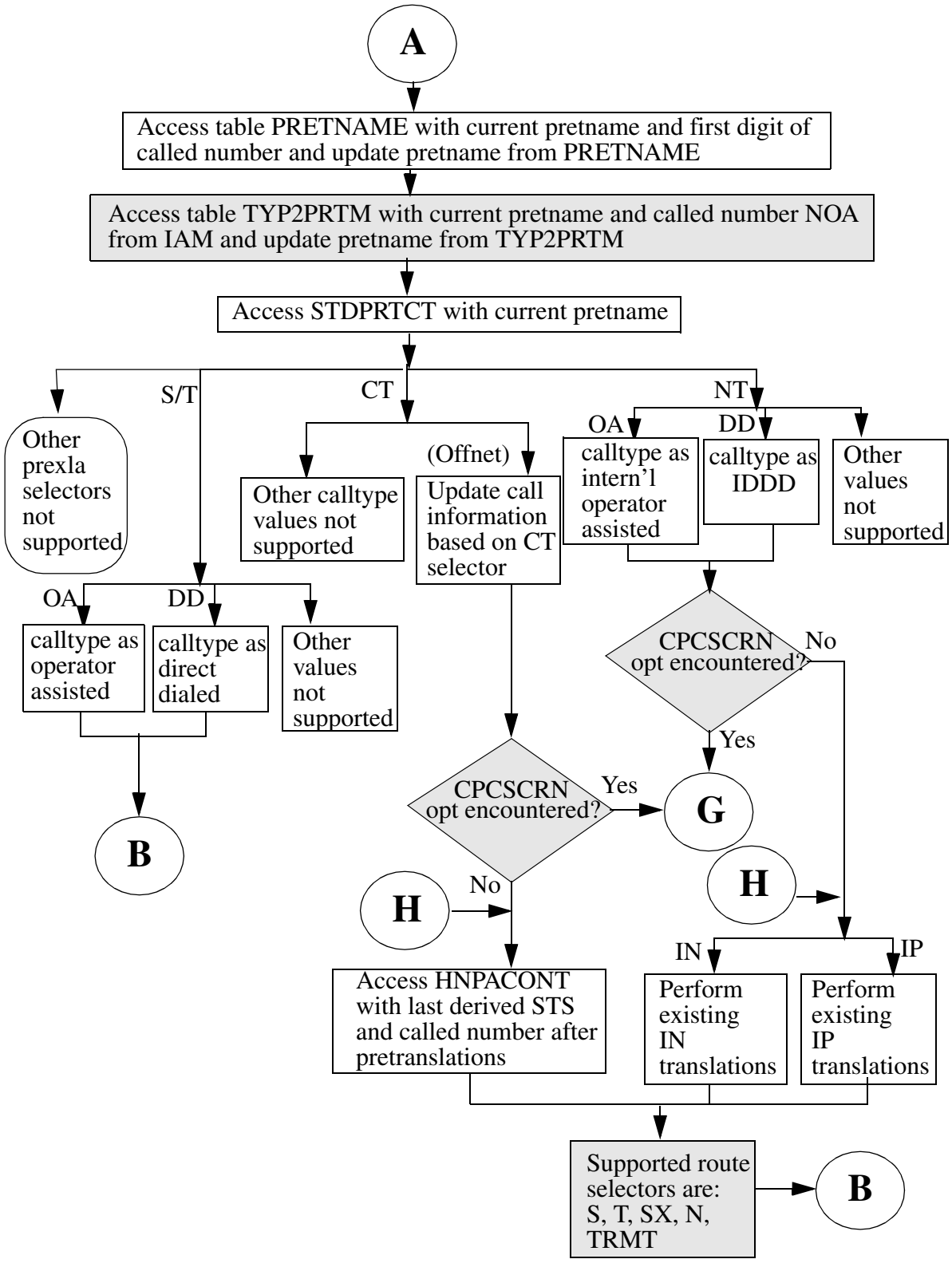

A
Access table PRETNAME with current pretname and first digit of called number and update pretname from PRETNAME
Access table TYP2PRTM with current pretname and called number NOA from IAM and update pretname from TYP2PRTM
Access STDPRTCT with current pretname
S/T
CT
NT
Other prexla selectors not supported
Other calltype values not supported
(Offnet)
Update call information based on CT selector
OA
DD
calltype as intern'l operator assisted
calltype as IDDD
Other values not supported
OA
DD
calltype as operator assisted
calltype as direct dialed
Other values not supported
CPCSCRN opt encountered?
No
Yes
CPCSCRN opt encountered?
Yes
G
B
H
No
H
IN
IP
Access HNPACONT with last derived STS and called number after pretranslations
Perform existing IN translations
Perform existing IP translations
Supported route selectors are: S, T, SX, N, TRMT
B

Figure 14 Gateway functionality call flows (continued)

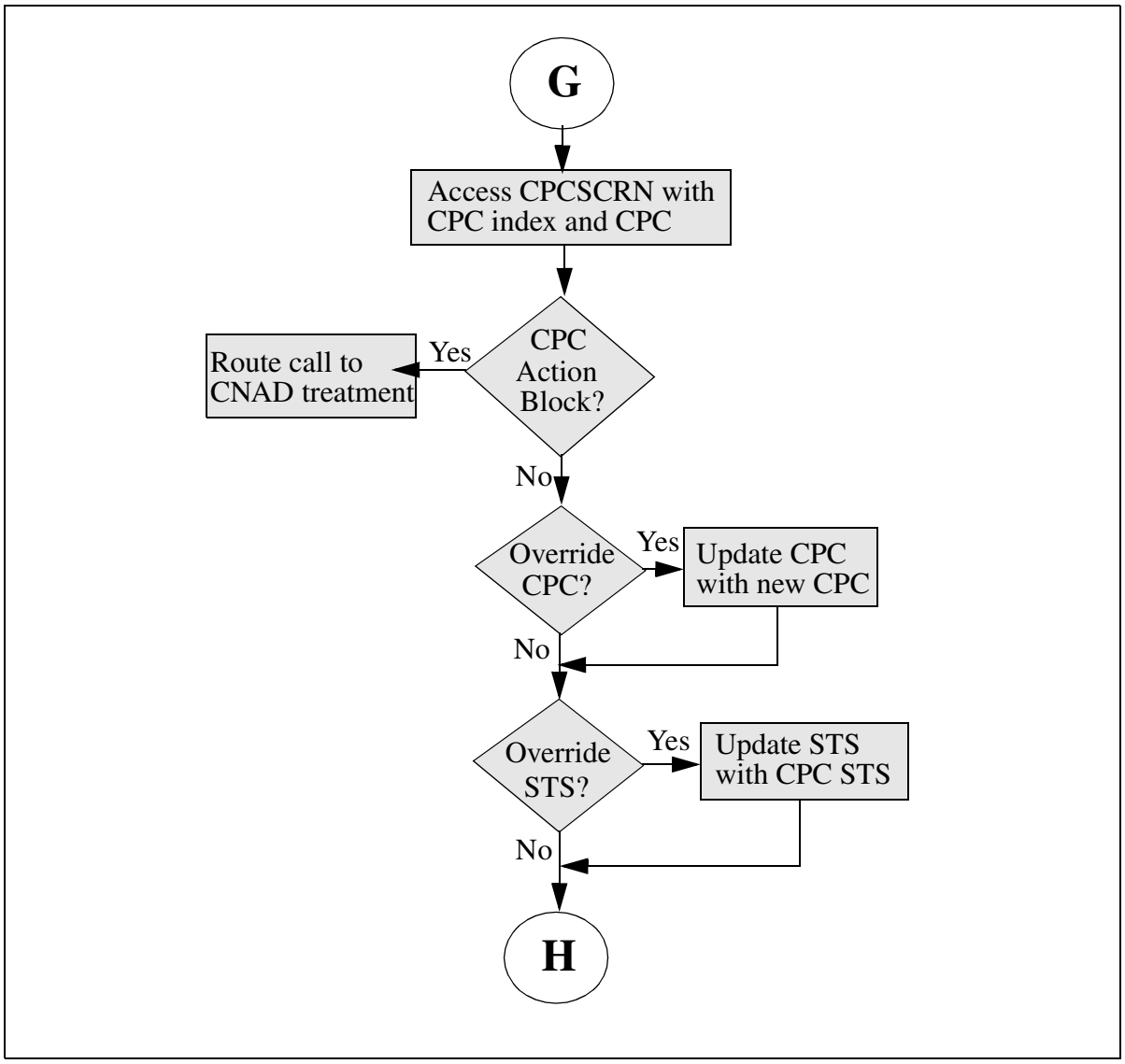


Figure 15 Derive outpulsed number calltype

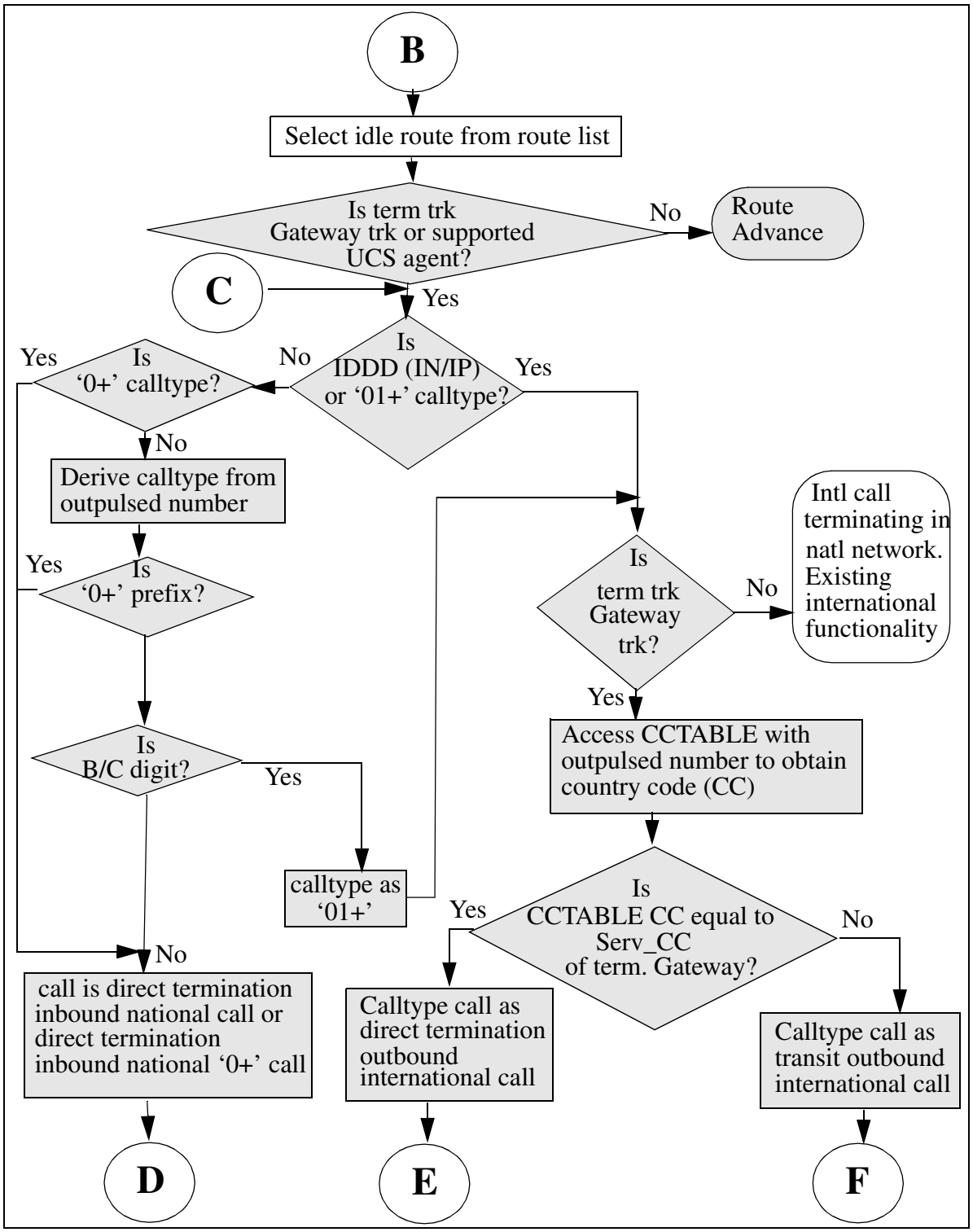


Figure 16 Gateway functionality call flows (Continued)

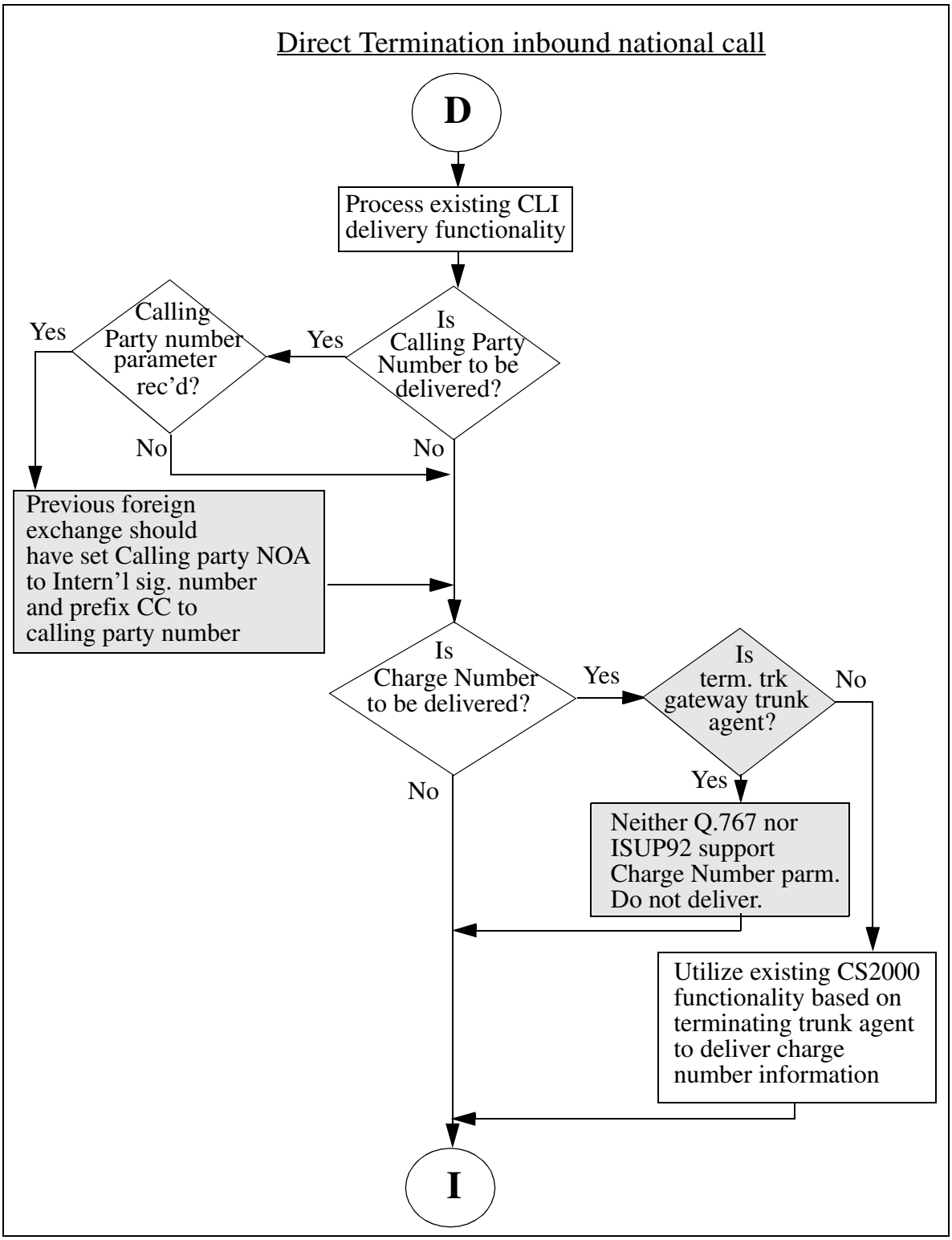


Figure 17 Gateway functionality call flows (Continued)

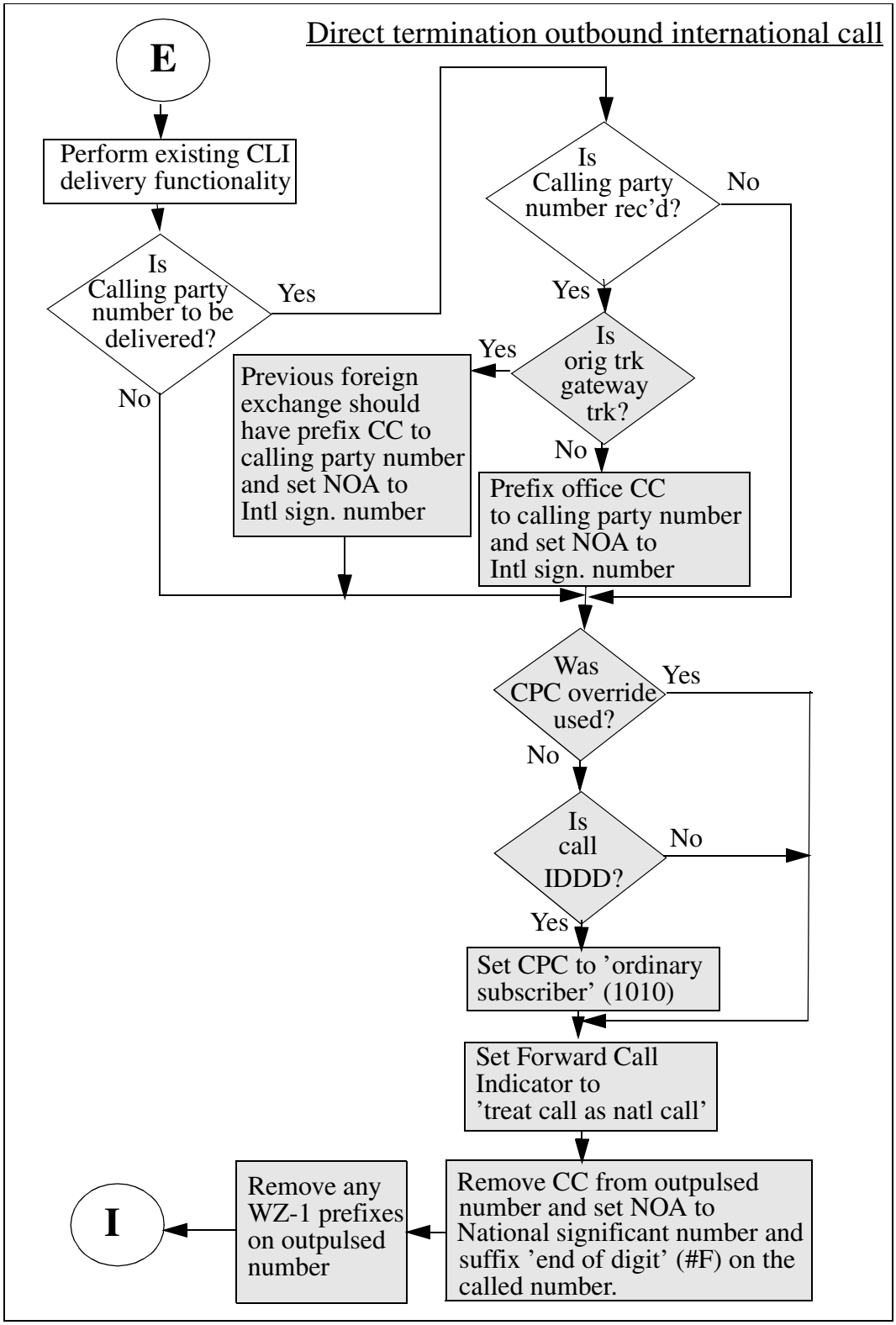

Direct termination outbound international call
E
Perform existing CLI delivery functionality
Is Calling party number to be delivered?
Yes
No
Is Calling party number rec'd?
No
Yes
Is orig trk gateway trk?
Yes
No
Previous foreign exchange should have prefix CC to calling party number and set NOA to Intl sign. number
Prefix office CC to calling party number and set NOA to Intl sign. number
Was CPC override used?
Yes
No
Is call IDDD?
No
Yes
Set CPC to 'ordinary subscriber' (1010)
Set Forward Call Indicator to 'treat call as natl call'
Remove CC from outpulsed number and set NOA to National significant number and suffix 'end of digit' (#F) on the called number.
Remove any WZ-1 prefixes on outpulsed number
I

Figure 18 Gateway functionality call flows (Continued)

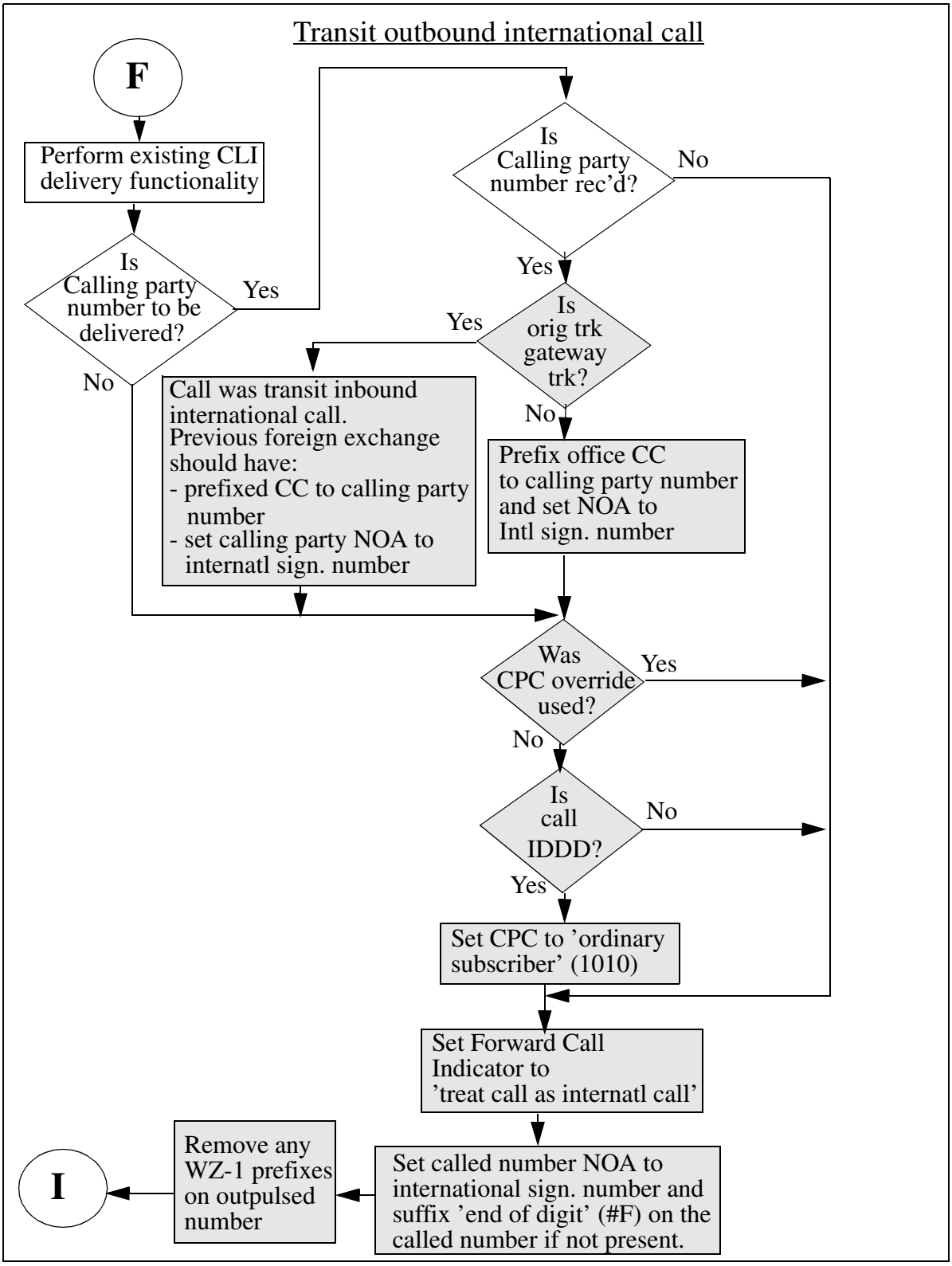
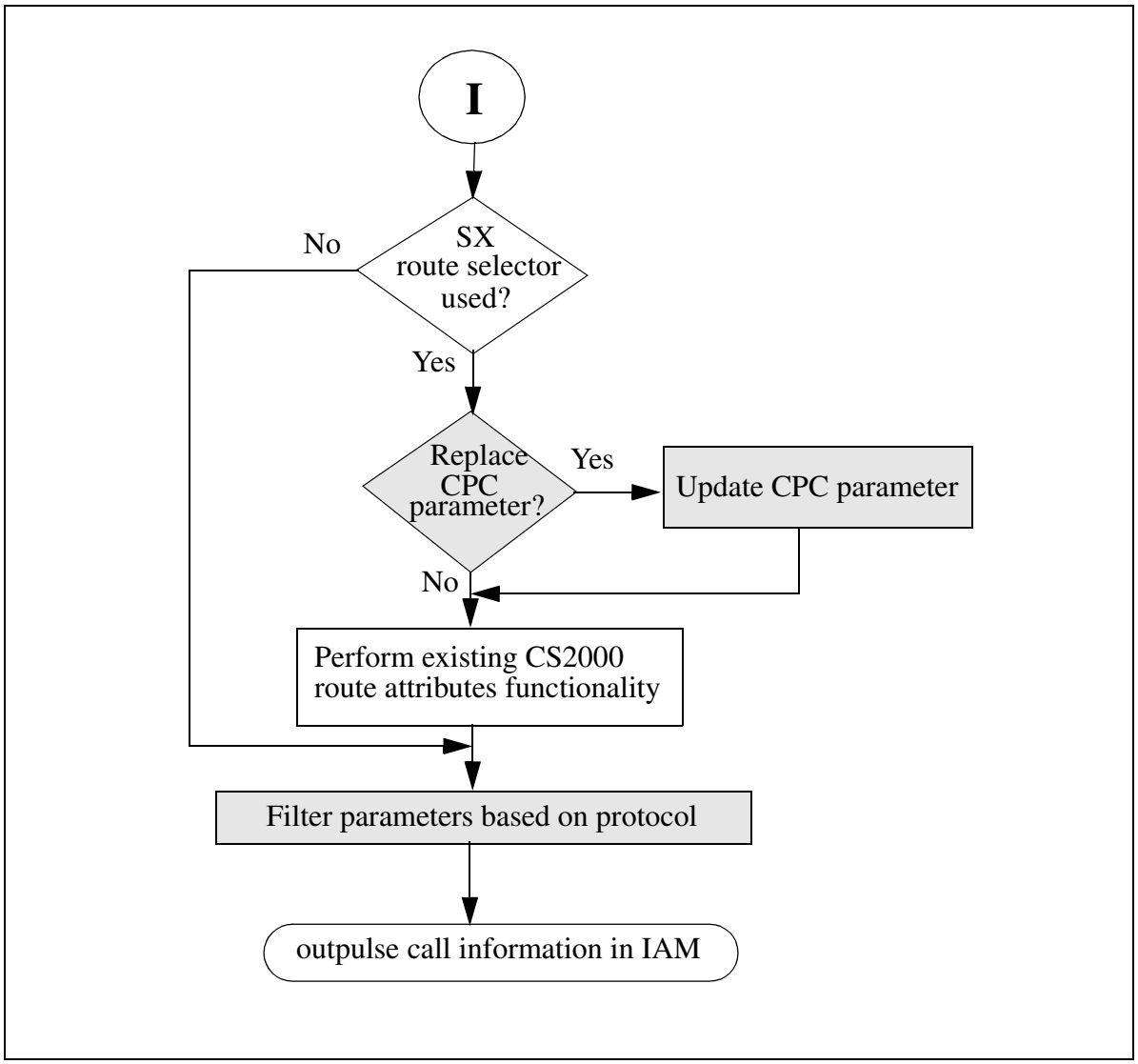

Transit outbound international call
F
Perform existing CLI delivery functionality
Is Calling party number to be delivered?
Yes
No
Is Calling party number rec'd?
No
Yes
Is orig trk gateway trk?
Yes
No
Call was transit inbound international call.
Previous foreign exchange should have:
- prefixed CC to calling party number
- set calling party NOA to internatl sign. number
Prefix office CC to calling party number and set NOA to Intl sign. number
Was CPC override used?
Yes
No
Is call IDDD?
No
Yes
Set CPC to 'ordinary subscriber' (1010)
Set Forward Call Indicator to 'treat call as internatl call'
Set called number NOA to international sign. number and suffix 'end of digit' (#F) on the called number if not present.
Remove any WZ-1 prefixes on outpulsed number
I

Figure 19 Gateway functionality call flows (Continued)



109.18 Appendix F: Datafill examples

This appendix describes example datafill for the different types of calls supported by this feature.

109.18.1 Direct Inbound National Call.

This is an example of a direct inbound national call where a foreign exchange routes a call destined for US to a CS2000 in WZ-1. The CS2000 calltypes the call as a national call and routes the call to a US national trunk agency as a direct inbound national call.

Originating Trunk: Gateway Trunk

IAM msg:

NOA= National (3)

Called Number = 2142221234F

CPC=0

FCI bit A = 0 (National)

TABLE: TRKGRP

GWYTRK1 IMT 40 NPDGP NCIM 0 2W **GWY** MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 772 IMT**) $

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0 DMSNODE Y Y **V1 BLUE** $ NIL CIC

TABLE: TYP2PRTM

GWY NATL GWY

TABLE: PARTOSTS

00 286 786

TABLE: STDPRTCT[1]

GWY (1) (0)

subtable STDPRT

2142221234 21 CT OFFNET 7 10 0 $

TABLE: HNPACONT

786 Y 999 10 (2) (1) (0)

subtable HNPACODE

214 214 HNPA 0

222 222 LRTE 222

subtable RTEREF

222 (S D UCS_Agency) $

Since the terminator is a existing agent (national agent) the call is calltyped as a direct inbound national call.

If terminating UCS_Agency is an SS7 trunk (INTER/INTRA IMT, SS7 FG D) etc, Outgoing IAM is as follows.

IAM msg:

NOA= National (3)

[1] 'F' is removed from the Called Number prior to entering table STDPRTCT.

Outpulsed Number = 2142221234

CPC=0

FCI bit A = 0 (National)

109.18.2 Transit Inbound International Call.

This is an example of a transit inbound international call where a foreign exchange is routing a call destined for Panama (country code of '507') to a CS2000 in WZ-1. The CS2000 routes the call to a foreign exchange in Mexico as a transit outbound international call.

Originating Trunk: Gateway Trunk

IAM msg:

Called number NOA = International (4)

Called Number = 507+7242212345+F

CPC=0

FCI bit A = 1 (International)

TABLE: TRKGRP

GWYTRK1 IMT 40 NPDGP NCIM 0 2W **GWY** MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 772 IMT**) $

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0 DMSNODE Y Y **V1 BLUE** $ NIL CIC

TABLE: TYP2PRTM

GWY INTL GWY

TABLE: PARTOSTS

00 286 786

TABLE: STDPRTCT[1]

GWY (1) (0)

subtable STDPRT

5077242212345 508 NT DD 3 IP (CPCSCRN 1)$

Table 45 TABLE: CPCSCRN

CPCINDEX	CPC	ACTION	OVRDSTS	STS
1	UNKNOWN	ACTION_CONTINUE	Y	611

- Table CPCSCRN was accessed with the CPCINDEX value from table STDPRTCT, CPCSCRN option and the calling party category (CPC) value of ‘0’ (UNKNOWN) from the IAM.

- The corresponding tuple is to take the action of ‘ACTION_CONTINUE’ and override the STS with ‘611’.

TABLE: STS2CCDB

786 UCS786

TABLE: CTCODE

UCS786 7724 7724 RTE (PF 0) (MM 7 15) (DEST 724) $

TABLE: CTRTE

[1] ‘F’ is removed from the Called Number prior to entering table STDPRTCT.

UCS786 724 (SX GWYTRK2 CPC_OVRD[1]) $

TABLE CCTABLE

5070 5079 507

Table 46 TABLE: RTEATTR

KEY	INCLUDE	EXCLUDE	REPLACE	OPTION
CPC_OVRD	$	$	(**CPC SUBSCRIBER1**)	$

TABLE: TRKGRP

GWYTRK2[2] IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0 DMSNODE Y Y **V1 ISUP92** $ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

- Since GWYTRK2 serving country code (SERV-CC) is not equal to the called number country code (‘507’), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code ‘52’) as a transit call to Panama (country code ‘507’).

called number = 507+7242212345+F

[1]CPC_OVRD is an index into table RTEATTR.

[2]It is an ISUP92 gateway trunk

Called number NOA is set to International significant number due to calltype of transit outbound international call.

CPC = 10 Ordinary Subscriber (via table RTEATTR)

109.18.3 Direct Outbound International Call.

This is an example of direct outbound international call where an international call destined for Mexico (country code ‘52’) originated from US national network and is routed to the CS2000. The CS2000 calltypes the call as a international call and routes the call to a gateweay trunk which connects to a foreign exchange in Mexico as a direct outbound international call.

Originating Trunk: Any Supported UCS Agency. (SS7 IMT for this example)

Called Party Number = 011+52+8775221234

If Originating Trunk is an SS7 trunk then IAM contains

Called Party Number NOA= International (4)

Calling Party Number = 2146112211

Calling Party Number NOA= National (3)

CPC = UNKNOWN

TABLE: TRKGRP

IMTTRK1 IMT 40 NPDGP NCIT 0 2W IMT MIDL 16 7 16 16 NILIDX NIL S N NONE 4 ALWAYS ADDR 111 0 INTER N VOICE_DATA NONE 4 160 214 0 $

TABLE: STDPRTCT

IMT (1) (0)

subtable STDPRT

011528775221234 011528775221234 NT DD 3 IN $

TABLE: CCTR

8775221234 T 711 3 15 T OFRT 101 Y

TABLE CCTABLE

52 52 52

TABLE OFRT:

101 (SX GWYTRK1 CPC_OVRD)

Table 47 TABLE: RTEATTR

KEY	INCLUDE	EXCLUDE	REPLACE	OPTION
CPC_OVRD	$	$	(CPC SUBSCRIBER1)	$

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2[1] IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

Note: Since Terminating trunk is a Gateway trunk with the same country code as given by table CCTABLE, this is Direct Termination Outbound call.

Outpulse IAM:

called number = 8775221234+F

Called number NOA = National[2] (3).

[1]It is an ISUP92 gateway trunk

Calling Party Number = 1+2146112211 (Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International[1] (4).

CPC = SUBSCRIBER1 (via Table RTEATTR)

109.18.4 Transit Outbound International Call.

This is an example of a transit outbound international call where a international call destined for Panama (country code '507') originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 011+507+7242212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7 0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00 IMMEDIATE VOICE_DATA 160 $

TABLE: PARTOSTS

00 111 611

TABLE: STDPRTCT

ONT (1) (0)

subtable STDPRT

0115077242212345 0115077242212345 NT DD 3 IP $

[2]NOA is set to national significant number since the call is direct termination outbound call.
[1]NOA is set to international significant number due to the calltype of direct terminating outbound call and the originator is a UCS national agent

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 5077 5077 RTE (PF 0) (MM 7 15) (DEST 722) $

TABLE: CTRTE

UCS611 722 (S D GWYTRK2) $

TABLE CCTABLE

5070 5079 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
DMSNODE Y Y **V1 ISUP92** $ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code (’507’), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of ‘52’) as a transit call to Panama (country code ‘507’).

called number = 507+7242212345+F

Called number NOA = International[1] (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International[2] (4).

CPC = SUBSCRIBER1

109.18.5 Inbound National OA Calls (Direct)

This is an example of a direct inbound national OA call where a foreign exchange routes a call destined for US to a CS2000 in WZ-1. The CS2000 calltypes the call as a national OA call and routes the call to a US national trunk agency as a direct inbound national OA call.

Originating Trunk: Gateway Trunk

IAM msg:

NOA= National (3)

Called Number = 2142221234F

CPC=0

FCI bit A = 0 (National)

TABLE: TRKGRP

GWYTRK1 IMT 40 NPDGP NCIM 0 2W **GWY** MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 772 IMT**) $

[1]NOA is set to international significant number due to calltype of transit outbound international call.
[2]NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0 DMSNODE Y Y **V1 BLUE** $ NIL CIC

TABLE: TYP2PRTM

GWY NATL GWY

TABLE: STDPRTCT[1]

GWY (1) (0)

subtable STDPRT

2142221234 21 T OA 0 OFRT 741 8 11 NONE

TABLE: OFRT

237 (SX IMT741C7DR12 ENG_OP)

TABLE: RTEATTR

ENG_OP $ $ (CPC OP_ENGLISH)

Since the terminator is a existing agent (national agent) the call is calltyped as a direct inbound national OA call.

If terminating UCS_Agency is an SS7 trunk (INTER/INTRA IMT, SS7 FG D) etc, Outgoing IAM is as follows.

IAM msg:

NOA= National (3)

Outpulsed Number = 2142221234

[1] 'F' is removed from the Called Number prior to entering table STDPRTCT.

CPC=2 (op_english)

FCI bit A = 0 (National)

109.18.6 Direct Outbound International OA Call

This is an example of direct outbound international OA call where an international OA call destined for Mexico (country code ‘52’) originated from US national network and is routed to the CS2000. The CS2000 calltypes the call as a international OA call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a direct outbound international OA call.

Originating Trunk: Any Supported UCS Agency. (SS7 IMT for this example)

Called Party Number = 011+52+8775221234

If Originating Trunk is an SS7 trunk then IAM contains

Called Party Number NOA= International (4)

Calling Party Number = 2146112211

Calling Party Number NOA= National (3)

CPC = UNKNOWN

TABLE: TRKGRP

IMTTRK1 IMT 40 NPDGP NCIT 0 2W IMT MIDL 16 7 16 16 NILIDX NIL S N NONE 4 ALWAYS ADDR 111 0 INTER N VOICE_DATA NONE 4 160 214 0 $

TABLE: PARTOSTS

00 111 611

TABLE: STS2CCDB

611 UCS611

TABLE: STDPRTCT

IMT (1) (0)

subtable STDPRT

011528775221234 011528775221234 NT OA 3 IP (CPCSCRN OP_SPANISH) $

TABLE CCTABLE

52 52 52

TABLE CTCODE

UCS611 528 528 RTE (PF 0) (MM 7 15) (DEST 528) $

TABLE CTRTE

UCS611 528 (S D GWYTRK2) $

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2[1] IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

Note: Since Terminating trunk is a Gateway trunk with the same country code as given by table CCTABLE, this is Direct Termination Outbound OA call.

Outpulse IAM:

called number = 8775221234+F

Called number NOA = National[2] (3).

Calling Party Number = 1+2146112211 (Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International[3] (4).

CPC = OP_SPANISH (via Table STDPRTCT CPCSCRN option)

109.18.7 Transit Outbound International OA call

This is an example of a transit outbound international OA call where a international OA call destined for Panama (country code ‘507’) originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international OA call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international OA call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 011+507+7242212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

[1]It is an ISUP92 gateway trunk
[2]NOA is set to national significant number since the call is direct termination outbound call.
[3]NOA is set to international significant number due to the calltype of direct terminating outbound call and the originator is a UCS national agent

ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7 0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00 IMMEDIATE VOICE_DATA 160 $

TABLE: PARTOSTS

00 111 611

TABLE: STDPRTCT

ONT (1) (0)

subtable STDPRT

0115077242212345 0115077242212345 NT OA 3 IP (CPCSCRN OP_SPANISH) $

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 5077 5077 RTE (PF 0) (MM 7 15) (DEST 722) $

TABLE: CTRTE

UCS611 722 (S D GWYTRK2) $

TABLE CCTABLE

5070 5079 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
DMSNODE Y Y **V1 ISUP92** $ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code (’507’), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of ‘52’) as a transit call to Panama (country code ‘507’).

called number = 507+7242212345+F

Called number NOA = International[1] (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International[2] (4).

CPC = OP_SPANISH (via Table STDPRTCT - CPCSCRN option)

[1]NOA is set to international significant number due to calltype of transit outbound international call.
[2]NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

109.18.8 Transit Outbound Code 11/12 International

This is an example of a transit outbound international code 11/12 call where a international code 11/12 call destined for Panama (country code ‘507’) originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international code 11/12 call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international code 11/12 call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 01+507+1212212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7 0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00 IMMEDIATE VOICE_DATA 160 $

TABLE: PARTOSTS

00 111 611

TABLE: STDPRTCT

ONT (1) (0)

subtable STDPRT

015071212212345 015071212212345 NT OA 2 IP (CPCSCRN OP_SPANISH) $

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 507 507 RTE (PF 0) (MM 7 15) (DEST 722) $

TABLE: CTRTE

UCS611 722 (T OFRT 204) $

TABLE: OFRT

204 (N D GWYTRK2 6 507B N) $ $

(Note that this is merely example datafill. There are other methods to appropriately manipulate the number to be outpulsed.)

TABLE CCTABLE

507 507 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) $

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0 DMSNODE Y Y **V1 ISUP92** $ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code (’507’), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of ‘52’) as a transit call to Panama (country code ‘507’).

called number = 507+B2212345+F

Called number NOA = International[1] (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

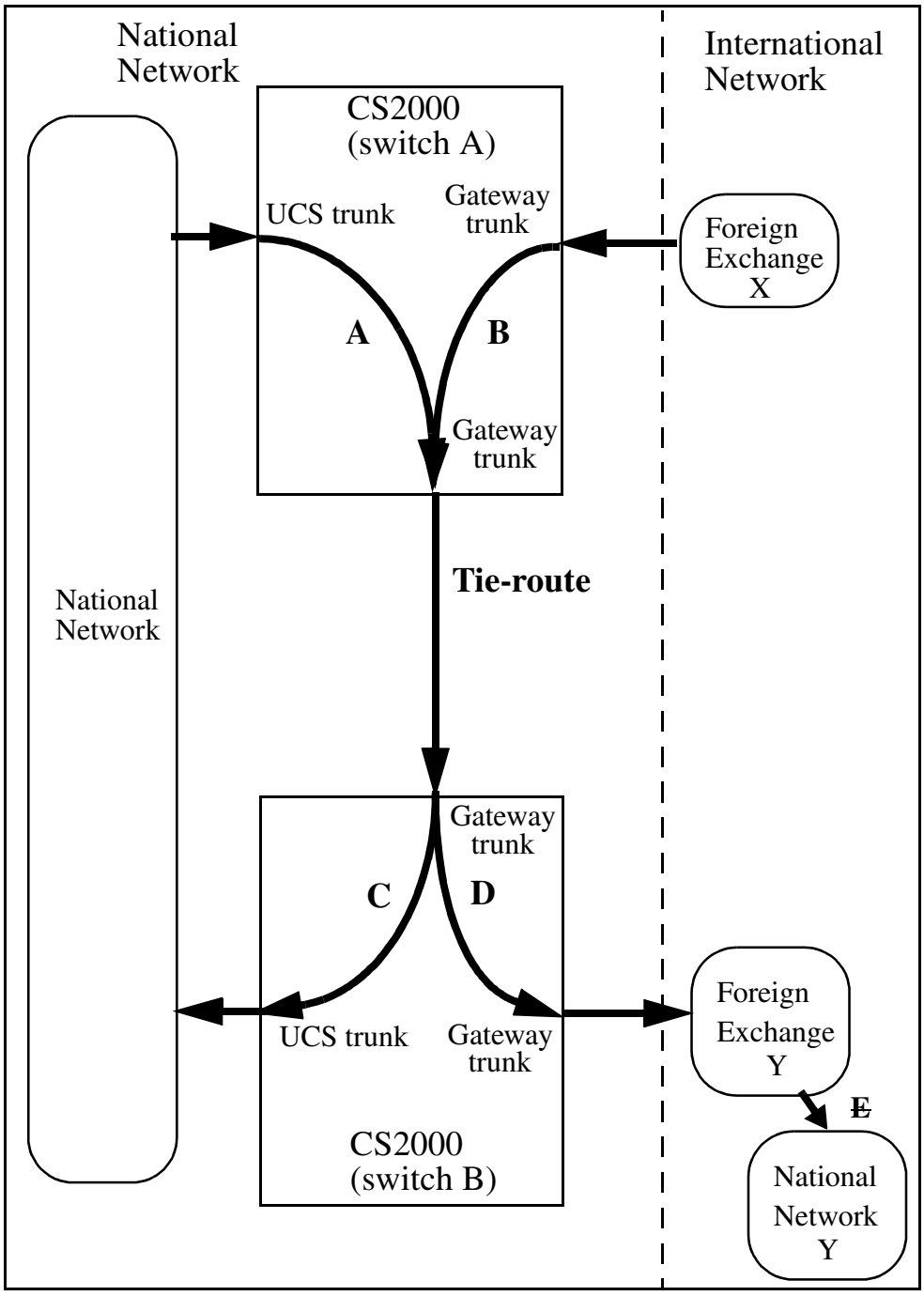
Calling Party Number NOA = International[2] (4).

CPC = OP_SPANISH (via Table STDPRTCT - CPCSCRN option)

[1]NOA is set to international significant number due to calltype of transit outbound international call.
[2]NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

109.19 Appendix G: Tie-route Connection Example

Figure 20 Tie-route connection



Direct termination inbound national calls:

In figure 20, connection B to connection C illustrates direct termination inbound national calls over a tie-route connection. In this case, the call is routed as a national call on switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one on the east coast of the country and one on the west coast of the country. A foreign exchange routes a direct termination inbound national call to the east coast gateway switch but the call destination is on the west coast of the country. The gateway switch on the east coast would route the call as a national call over the gateway trunk agency (tie-route connection). The gateway switch on the west coast would then route the call as a national call to the supported trunk agency which accesses the national network on the west coast.

In figure 20, connection A to connection C illustrates direct termination inbound national calls over a tie-route connection. In this case, the call is routed as a national call on switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country X in WZ-1 and another in country Y in WZ-1 where country Y requires all international traffic to go through a gateway switch. A subscriber in country X dials a 1+national number, the gateway switch translates the call as a national call and routes the call over the tie-route connection (gateway trunk agency).

The gateway switch in country Y would treat the call as a direct termination inbound national call since the call originated on a gateway trunk agency and the calltype is a national call. Based on translations, the call would be routed to a CS2000 trunk agent that accesses the national network in country Y.

Direct termination outbound international calls:

In figure 20, connection A to connection C illustrates direct termination outbound international call over a tie-route connection. In this case, the call is routed as an direct termination outbound international call on switch A and a direct termination inbound national call on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country X in WZ-1 and another in country Y in WZ-1 where country Y requires all international traffic to go through a gateway switch. A subscriber in country X dials a 011+country code (’1’)+national number, the gateway switch translates the call as an international call and routes the call over the tie-route connection (gateway trunk agency). The gateway switch in country Y would treat the call as a direct termination inbound national call since the call originated on a gateway trunk agency and the calltype is a national call. Based on translations, the call would be routed to a CS2000 trunk agent that accesses the national network in country Y.

In figure 20, connection A to connection D illustrates direct termination outbound international call over a tie-route connection. In this case, the call is routed as an direct termination outbound international call on switch A and on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country A in WZ-1 and another in country B in WZ-1 where country B requires all international traffic to go through a gateway switch to access the national network. A subscriber in country B dials a 011+country code for country Y+national number, the gateway switch (switch A) translates the call as an direct termination outbound international call since the country code of the called number is EQUAL to the serving country code of the gateway trunk agency and routes the call over the tie-route connection.

The gateway switch in country B would translate the call as an international call and treat the call as a direct termination outbound international call since the country code of the called number is EQUAL to the serving country code of the gateway trunk agency. The gateway trunk agency would interconnect to the gateway switch in the destination country (country Y).

Transit outbound international calls:

In figure 20, connection B to connection D illustrates transit outbound international call over a tie-route connection. In this case, the call is routed as an transit outbound international call on switch A and on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one on the east coast of the country and one on the west coast of the country. A foreign exchange routes a transit inbound international call to the east coast gateway switch but the call destination is a country that is connected to the gateway switch on the west coast of the country. The gateway switch on the east coast would route the call as an international call over the gateway trunk agency (tie-route connection).

The east coast gateway switch would treat this call as a transit outbound international call since the call is terminating to a gateway trunk agency and the destination country code prefix on called number is NOT EQUAL to the serving country code of the gateway trunk agency (country code of '1' since it resides in WZ-1).

The gateway switch on the west coast would then route the call as an international call to a gateway trunk agency that connects to the transit foreign exchange or could route the call as an international call to a gateway trunk agency that has a direct termination to the destination country (direct termination outbound international call).

In figure 20, connection A to connection D illustrates transit outbound international call over a tie-route connection. In this case, the call is routed as an transit outbound international call on both switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country A in WZ-1 and another in country B in WZ-1 where country B has the connection to a transit foreign exchange. A subscriber in country A dials a 011+country code for country X+national number, the gateway switch (switch A) translates the call as an transit outbound international call since the country code of the called number is NOT EQUAL to the serving country code of the gateway trunk agency (country code of '1' since country B is in WZ-1) and routes the call over the tie-route connection.

The gateway switch in country B would translate the call as an international call and treat the call as a transit outbound international call since the country code of the called number is NOT EQUAL to the serving country code of the gateway trunk agency. The gateway trunk agency would interconnect to a foreign exchange in country Y which has a direct connection to country X.

109.20 Appendix H: Test Call

This feature ensures that testcalls originated from any of the following test facilities:

- TTP - MAP level (Manual tests)
- ATT - MAP level (Automatic tests)

for performing tests on Q767 and ISUP92 Gateway trunks, these are terminated on the specified testlines.

Testlines that are supported by this feature are T100, T101[1], T102.

109.20.1 Origination of Testcall

This feature utilizes TST & OP commands available at MAP level and ATT for supporting origination of test calls on UCS agenda and ISUP92/Q.767.

IAM Message Generation:

The IAM message transmitted from the originating, near end switch to the terminating, far end switch is formatted as a test call IAM. The test call IAM is sent over the ISUP IMT trunks that has to be tested.

The test call IAM contains the following parameters:

- Nature of Connection Indicator
  - — the Satellite Indicator field for test calls depends on TRKSGRP datafill in the same way as for non-test calls
  - — the Continuity Check Indicator field for test calls contains the Continuity Check Not Required code (‘00’) regardless of TRKSGRP datafill
  - — the Echo Suppressor Indicator field contains the Outgoing Half Echo Suppressor Not Included code (‘0’) regardless of TRKSGRP datafill
- Calling Party Category - contains the Test Call code (‘00001101’). This value is sent in the test call IAM regardless of what facility initiates the test, line call or the number of test digits.
- Called Party Address - the Nature of Address and Numbering Plan Indicator fields of the Called Party Address parameter for test calls depend on the address signals to be transmitted. If the Called Party Address parameter contains a called party address having number of address digits greater than three; on the terminating, far end switch, then the Nature of Address field is encoded with the National (Significant) Number code ('0000011') and the Numbering Plan Indicator is encoded with the ISDN/

[1]T101 testline is supported only in a hybrid configuration.

Telephony Numbering Plan code ('001'). If the Called Party Address parameter contains a test line number (i.e. a 3 digit test code) the Nature of Address field is encoded with the Test Line Test code ('1110111') and the Numbering Plan Indicator is encoded with the Unknown numbering plan code ('000'). This allows the terminating, far end switch to apply appropriate dialing plan and translation to the received digits to terminate the call to the desired test line.

- User service information - Layer 1 information field in this parameter is dependent on datafill in CARRMTC table.

109.20.2 Translations & Termination of test call

At the far end switch, pretranslator used for test calls is obtained from the office parameter GLOBAL_TESTCALL_PRTNM, if the Nature of address (NOA) in called party address parameter of incoming IAM for a testcall is Testline Testcode (‘1110111’). If GLOBAL_TESTCALL_PRTNM is NPRT then pretranslator datafilled in PRTNM field of table TRKGRP is used. Ordinarily GLOBAL_TESTCALL_PRTNM is datafilled as ‘C7PT’ as pretranslator for testline numbers.

Dialplan used for a testcall depends upon the Numbering plan indicator field of incoming IAM. If numbering plan indicator is ‘ISDN_TELEPHONY_NUM_PLAN’, dialplan datafilled in TRKGRP is used. If dialplan datafilled in TRKGRP is NIL, dialplan from table OPT250 is taken. If the numbering plan indicator in incoming IAM is ‘UNKNOWN_NUM_PLAN’, dialplan is taken as ADDR.

All optional parameters (including CLI) are ignored while processing incoming Test call IAM. If CLI is received in the incoming IAM, it is not processed but it is delivered to the terminator if terminator is non-testline.

If the NOA in the Called Party Address parameter of incoming IAM indicates testline testcode, then subtable STDPRT of table STDPRTCT should be datafilled as standard route to testlines. If the route is not datafilled in table STDPRTCT then call takes universal translations. Serving Translation Scheme (STS) in such a case is derived in the following manner:

- for calls originating on INTRA IMT, STS is derived from office parameter DEFAULT_STS in table OFCVAR.
- for calls originating on GLOBAL IMT, STS is derived using OPART & TPART fields of table TRKGRP.

The selector, in table STDPRTCT, subtable STDPRT, which are supported for pretranslation of test calls are S, T, D, CT.

Once the Trunk Under Test (TUT) is connected to specified testline at the far end switch, test equipment at the near end switch starts the desired test and after the completion of the test, a log report is generated indicating the results.

109.20.3 TTP MAP level

TST and OP are the two commands at this level which are use for initiating a testcall on a trunk.

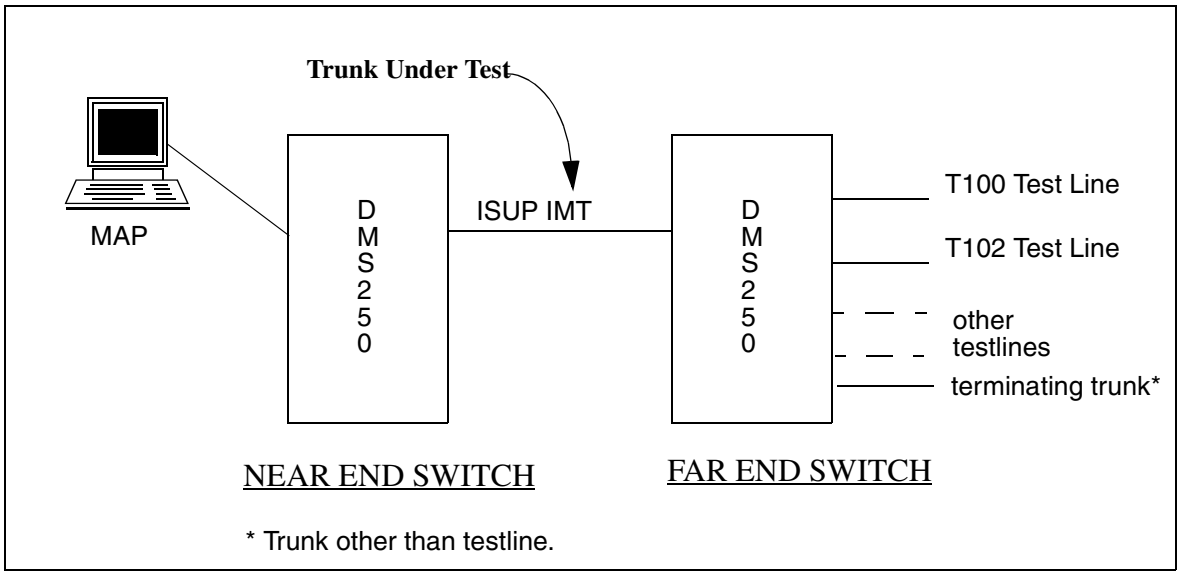
109.20.3.1 TST command

It takes a single parameter identifying the desired test and provides the ability to perform standard tests on a trunk. Following format of the command is supported.

- TST T10X, where X is in the range {0,2}

Example: Following figure depicts the configuration for manually testing the ISUP IMT, supported by this feature, from TTP MAP level:

Figure 21 Trunk testing from the TTP level of the MAP



For command TST T102 (Milliwatt testline) given at the TTP MAP level, the call flow till termination on the testline is as follows:

Origination at the near end switch

Table CLLIMTCE; *pos IMT761C7LP00*

This table gives TSTNOIND, which is used to index into table TSTLCONT and MWIDX, which is used to index into table MWDATA.

Table 48 Table CLLIMTCE;

CLLI	SCLLI	MIN ALM	MAJ ALM	CRIT ALM	SYNC TYPE	TST NO IND	MW IDX	SIG TST	PRFX DIG	DIAG DATA
IMT761LP00	IMT761	5	10	15	NSS	**0**	**0**	N	N	(4)

*Table TSTLCONT; pos **0**; sub TLNOS*; *pos T102*

Table 49 Table TSTLCONT;sub TLNOS

TESTLINE	TLNUMBER	TL_MFC_ OG_SIG
T102	**102**	N

Table MWDATA; pos **0**

Table 50 Table MWDATA

IDXKEY	MWDATA
0	**0 1004**

The table TSTLCONT contains the address digits (102 in this example) to be outpulsed for the corresponding Testline. Outgoing testcall IAM, on the trunk under test, contains these address digits as address information. Since this table cannot be datafilled for more than 12 address digits, TST command can be used to outpulse at the maximum 12 address digits only.

As described in section 1.17.1, since the number of address digits are 3, Nature of Address in the IAM is set to Test line Test Code. This nature of address at the far-end-switch will indicate office parameter GLOBAL_TESTCALL_PRTNM is to be used for pretranslations.

The table MWDATA gives the frequency and the decibel level which near end switch expects from far end switch while performing the milliwatt test.

In this example the decibel level and frequency are 0 and 1004 Hz respectively.

Translation & Termination at the far end switch

Since the Nature of Address is Test Line Test Code, Office Parameter GLOBAL_TESTCALL_PRTNM is looked at to get a pretranslator name for Test Call. If the value is NPRT, then the PRTNM of TRKGRP is used.

Table OFCVAR; *pos GLOBAL_TESTCALL_PRTNM*

Table 51 Table OFCVAR

PARMNAME	PARMVAL
GLOBAL_TESTCALL_PRTNM	**C7PT**

Table STDPRTCT; pos C7PT; sub STDPRT; *pos 102*

Table 52 Table STDPRTCT

FROMDIGS	TODIGS	PRETRTE
102	102	DD 3 **TERM102T** 3 3 NONE

The call terminates on TERM102T Test Line and subsequent tests are performed on the Trunk Group on which the above TST command was initiated.

The above example explains termination of testcall on a testline directly through route specified in table STDPRTCT. A testcall can also be terminated on a testline using universal translation. This is explained in the example of the next section (1.17.3.2).

109.20.3.2 OP command

This command has two formats

- OP ‘xxxxxxx’, where xxxxxxx are valid dialed digits that may be translated at the far end office.
- OP T10X, where T10X identifies a valid trunk testline test.

Example:

For the command OP 2141001234 given at the TTP MAP level, the call flow till termination is as follows:

Origination at the near end switch

As described in section 1.17.1, since the number of address digits are 10, Nature of Address in the IAM is set to National Significant Number. This nature of address at the far-end-switch will indicate that PRTNM of Table TRKGRP is to be used for pretranslations.

Translation & Termination at the far end switch

Table TRKGRP; pos IMT761C7LP00

Table 53 Table TRKGRP

GRPKEY	GRPTYP	TRAFSNO	PADGRP	NCCLS	GRPINFO
IMT761C7LP00	IMT	40	NPDGP	NCIM	UCSUST 0 2W **IMT** MIDL 16 7 16 UCS2UCS NIL CN NONE 4 ALWAYS ADDR **111 0** GLOBAL N N N VOICE_DATA NONE 4 160 (OHQ)(OHQTERM) $

The OPART and TPART obtained from TRKGRP is used to derive STS from Table PARTOSTS.

Table PARTOSTS; pos 00 111

Table 54 Table PARTOSTS

KEY	STS
00 111	611

The PRTNM (IMT in this example) obtained from table TRKGRP along with the incoming NOA (NATL in this example) is used to position into table TYP2PRTM.

Table TYP2PRTM; pos IMT

Table 55 Table TYP2PRTM

KEY	OPRTNM
IMT NATL	**IMT**

Table PRETNAME; pos IMT

Table 56 Table PRETNAME

PRTNM	STDPRTNM	ASTPRTNM	OCTPRTNM
IMT	**IMT**	NPRT	OCTR

Table STDPRTCT; pos IMT; sub STDPRT; pos 214

Table 57 Table STDPRTCT;Sub STDPRT

FROMDIGS	TODIGS	PRETRTE
214	21	CT OFFNET 2 20 0 (**UNIVIDX CT**) $

The STS derived previously is used to index into table STS2CTDB to get the Translator name for the call.

Table STS2CTDB; pos 611

Table 58 Table STS2CTDB

STS	OFFXNAM	ONXNAM
611	**IUCS611**	IUCS611

Table CTCODE; pos; IUCS611 214 214

Table 59 Table CTCODE

XLANAME	FROMD	TOD	XLADATA
IUCS611	214	214	RTE (PF 0) (MM 7 15) (DEST **111**) $

Table CTRTE; pos IUCS611 111

Table 60 Table CTRTE

XLANAME	RTEREF	RTELIST
IUCS611	111	(S **IMT762C7DR03**) $

Hence the call terminates on IMT762C7DR03.

OP T10x command takes the digits to be outpulsed from table TSTLCONT which cannot be datafilled for more than 12 address digits and hence this command cannot be used to outpulse more than 12 address digits.

Please Refer to AD9016 (Open Number Plan for UCS ISUP IMT) for more details on Universal Translations.

Please refer to NTP 297-1001-595 (Trunks Maintenance Guide) for more details on the OP Command.

109.20.4 Parameter Interworking

This section describes the interworking of parameters which are specific to test call.

- For testcalls that originate on ISUP IMT and terminate on ISUP IMT following table shows the interworking of parameters:

Table 61 Parameter Interworking (ISUP to ISUP)

IAM (Incoming)	IAM (Outgoing)
Calling Party Category: ISUP_CPC_TEST_CALL	Calling Party Category: ISUP_CPC_TEST_CALL

- For a test call originating on ISUP92/Q.767 with 3.1KHz audio as TMR, and terminating on any of the supported ISUP IMTs, bearer capapility in the outgoing IAM will be speech.
- When a test call terminates on any of the supported IMTs then following table shows the mapping of Nature Of Address (NOA) and Numbering Plan Indicator of the Called Party Address (CPA) parameter in the outgoing IAM:

Table 62 Outgoing IAM Parameters

Outgoing IAM parameter	CPA length > 3	CPA length < = 3
Called Party Nature of Address	NATIONAL (‘0000011’)	ISUP_TESTLINE(‘1110111’)
Called Party Numbering Plan Indicator	ISDN/Telephony Numbering Plan(‘001’)	Unknown(‘000’)

109.20.5 Billing

Generation of CDRs for testcall can be controlled by office parameter CDR_FOR_TESTLINE in table OFCOPT. If CDR_FOR_TESTLINE is ‘Y’ CDR would be generated for the testcall with COMPCODE field as 7.

After successful completion of call using OP command, ‘RLS R’ command is used at the TTP MAP level to release the trunk. In this case, the COMPCODE field of CDR is populated with ‘5’.

109.21 Appendix I: Data Call

109.21.1 Data call Identification

109.21.1.1 UCP ISUP IMT (INTER/INTRA) Origination

- A call originating on an UCP ISUP IMT (Intra/Inter) is identified as a data call if
  - — information digits in case of I3PA dialplan are ‘56’. In this case the call is a 56k data call.
  - — the Information Transfer Capability(ITC) in User Service Information parameter of incoming IAM, indicates data (UNRESTRICTED DIGITAL[1], RESTRICTED DIGITAL). If ITC is RESTRICTED DIGITAL the call is 64k restricted digital call. If ITC is UNRESTRICTED DIGITAL and User Rate in USI is 56kbps, then the call is 56k digital call else, it is 64k unrestricted digital call.

[1]When Information Transfer Capability in User Service Information parameter of incoming IAM is 3.1kHz or Speech and the dialplan is I3PA, information digits decide whether a call is a datacall.

109.21.1.2 ISUP92/Q767 Origination

- A call originating on an Q.767/ISUP92 is identified as a data call if Transmission Medium Requirement parameter in the incoming IAM indicates data (UNRESTRICTED DIGITAL). The distinction between 56k data and 64k data is done depending upon the User Rate as is done in case of UCP INTRA agency. For these two protocols, TMR is mandatory parameter and USI is optional parameter. If both these parameters are received in IAM then TMR takes precedence in determining if the call is a datacall.

109.21.1.3 PRI Origination

- The Information Transfer Capability(ITC) in Bearer Capability parameter in incoming SETUP message indicates data (UNRESTRICTED DIGITAL, RESTRICTED DIGITAL). If ITC is RESTRICTED DIGITAL, the call is 64k restricted digital call. If ITC is UNRESTRICTED DIGITAL and Access Data Rate in Bearer Capability is 56kbps, then the call is 56k digital call else, it is 64k unrestricted digital call.

109.21.1.4 PTS Origination

For Data calls origination on PTS agents, the BCNAME field in Table TRKGRP for the PTS CLLI should be datafilled with 56KDATA or 64KDATA[1]. Later, that particular PTS agent can be used for making data calls on DMS-250.

109.21.2 Bearer Capability Screening

109.21.2.1 Origination Screening:

The call's BC (CALLBC[2]) is compared with the BCNAME field of the originating trunk (FILEDBC). If screening fails the call is given Service Currently UNavailable treatment (SCUN). BC compatibility check is done using table BCCOMPAT.

[1]Note that while 64KDATA may be datafilled on the PTS (FGD) agent, the rate will be treated as 56K. 64K data rate is not supported on PTS agents.
[2]CALLBC is the bearer capability of the call, and FILEDBC is value of the BCNAME field of table TRKGRP. FILEDBC is used as TERMBC while indexing in table BCCOMPAT.

109.21.2.2 Termination Screening:

The call's BC is compared with bearer capability of the terminating trunk using table BCCOMPAT. If terminating screening fails the call-route advances to the next route choice in the route list. If route exhaustion occurs, call is blocked. The treatment applied at this point is Generalized No Circuit Treatment (GNCT). The screening will pass or fail based on the datafill in table BCCOMPAT. Table 63 shows table BCCOMPAT with example datafills:

Table 63 Table BCCOMPAT to check BC Compatibility

CALLBC[a]	TERMBC[1]
56KDATA	64KDATA
64KDATA	VOICE_DATA
56KDATA	VOICE_DATA
VOICE_DATA	64KDATA
VOICE_DATA	56KDATA

a. CALLBC and TERMBC form the key for table BCCOMPAT.

Table BCCOMPAT defines bearer capability pairs that are compatible with one another. For Example, the fourth tuple in above table means a trunk with BC of VOICE_DATA can allow a call of BC 64KDATA.

Note:

- all the BC s used in this table must be defined in the table BCDEF.

If a data call terminates over a UCP INTRA trunk with I3PA in the dialplan field of TRKGRP then information digits are outpulsed as 56 only when it is a 56k data call.

In the Nature of Connection indicator parameter of the outgoing IAM, satellite indicator field is set to one satellite circuit in the connection.

109.21.3 Interworking

Following matrix shows the interworking supported by this feature:

Table 64 Interworking for Data-calls.

	Terminating Agency							
Orig. Agency	Gateway	UCP Intra	UCP Inter	FGD SS7	FGD PTS	UCS PRI	FGB	DAL TIE
Gateway	X	X	X	X	X	X	X	X
UCP Intra	X							
UCP Inter	X							
FGD SS7	X							
FGD PTS	X							
UCS PRI	X							
FGB	X							
DAL TIE	X							

109.21.4 Parameter Interworking

This section describes the interworking of parameters which are specific to datacall.

109.21.4.1 ISUP92/Q.767 to UCP

The incoming USI and TMR parameters on ISUP92/Q.767 are mapped as follows to the ANSI USI on the outgoing UCP IMT:

Table 65 Mapping of USI on UCP when no USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
64 K Unres.	NONE	Information transfer capability - 64 kbps Unrestricted
		Information transfer rate - 64 kbps
		Coding Standard - National Standard
		Transfer Mode - Circuit mode

Table 66 Mapping of USI on UCP when 2 byte USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI
64kbps Unres.	Information Transfer Capability - Any value supported.	Information transfer capability - 64kbps Unres
	Information transfer rate - 64 kbps - Packet mode calls (00000) - For other values give BCNI[a] treatment.	Information transfer rate - 64 kbps - 64 kbps ***Call fails***
	Coding Standard - All Values	Coding Standard - National Standard
	Transfer Mode - Circuit mode - Packet mode[b]	Transfer Mode - Circuit mode ***Call fails***

a. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment.
b. Packet mode data calls are blocked with FNAL treatment.

Table 67 Mapping of USI on UCP when 4byte USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI
64 kbps unrestricted.	ITC - Any value supported.	ITC - 64 Kbps Unrestricted.
	Information transfer rate[a] - 64 kbps - Packet mode calls (00000) - For other values give BCNI[b] treatment.	Information transfer rate - 64 kbps - 64 kbps ***Call fails***
	Coding Standard - All Values	Coding Standard - National Standard
	Transfer Mode - Circuit mode - Packet mode[c]	Transfer Mode - Circuit mode ***Call fails***
	Layer 1 information - Any supported value	Layer 1 Information[d] - Tandemed
	User Rate - 56 Kbps - All other Values	User Rate - 56 kbps - Not built on the UCP side.

a. Information Transfer Rate with values of 1472 Kbps with Coding Standard as National and Multirate are unrecognized USI values.
b. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment.
c. Packet mode data calls are blocked with FNAL treatment.
d. The layer 1 info. is built on the UCP only if the User Rate is 56 Kbps. The 4 byte incoming USI is sent out as a 4 byte USI only if the User Rate is 56 Kbps. For all other values, the 4 byte USI is sent out as a 2 byte USI.

Note:

3 byte USI is not valid for data calls.

Table 68 Calling party category interworking (ISUP92/Q.767 to UCP)

ITU IAM(Incoming)	UCP (Outgoing)
Calling Party Category: ISUP_CPC_DATA_CALL	Calling Party Category: ISUP_CPC_DATA_CALL

109.21.4.2 ISUP92/Q.767 to ISUP92/Q.767

The supported values of TMR and USI are tandemed in case of an ISUP92/Q.767 - ISUP92/Q.767 call. If no USI is received, then a default 2byte USI is built on the outgoing side if the incoming TMR is 64K Unrestricted.

Table 69 ISUP92/Q.767 to ISUP92/Q.767 call with TMR 64K Unres and no USI

Outgoing ISUP92/Q.767 TMR/USI	
TMR	OPTIONAL USI
- 64 kbps unrestricted	ITC - 64 kbps unrestricted. ITR - 64 Kbps unrestricted Coding Standard - National Standard Transfer Mode - Circuit mode

109.21.4.3 UCP to ISUP92/Q.767

The incoming USI parameter on UCP IMT is mapped as follows to TMR and USI on ISUP92/Q.767:

a. When optional parameters are present in IAM or option ISDNXFER is set in table TRKGRP for originating agency then following table shows the interworking of parameters:

Table 70 Calling party category interworking (UCP to Gateway ISUP)

UCP IAM (Incoming)	ITU IAM (Outgoing)
Calling Party Category: ISUP_CPC_DATA_CALL	Calling Party Category: ISUP_CPC_DATA_CALL

Table 71 Mapping of incoming USI on UCP to TMR & USI on ISUP92/Q.767

UCP ISUP IAM	ITU ISUP IAM	
MANDATORY USI	TMR	OPTIONAL USI
Information transfer capability - 64 kbps unrestricted. - 64 kbps restricted.	 - 64 kbps unrestricted - 64 kbps unrestricted	Information transfer capability - 64 kbps unrestricted. - 64 kbps restricted.
Information transfer rate - 64 kbps - Packet mode calls (00000) - For other values give BCNI[a] treatment.		Information transfer rate - 64 kbps - 64 kbps ***Call fails***
Coding Standard - All Values		Coding Standard - National Standard
Transfer Mode - Circuit mode - Packet mode[b]		Transfer Mode - Circuit mode ***Call fails***
Layer 1 information - Any supported value		Layer 1 information - Value is taken from table CARRMTC

a. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment

b. Packet mode data calls are blocked with FNAL treatment.

b. When there are no optional parameter in IAM and option ISDNXFER is NOT set in table TRKGRP for originating agency then following table shows the interworking of parameters:

Table 72 Mapping of ITU ISUP USI and TMR

Outgoing ITU ISUP IAM	
TMR	OPTIONAL USI

Outgoing ITU ISUP IAM	
- 64 kbps unrestricted	ITC - 64 kbps unrestricted.
	ITR - 64 kbit/s
	Coding Standard - National Standard
	Transfer Mode - Circuit mode
	Layer 1 information - Layer 1 rate adaptation
	User Rate - 56 Kbps

Table 73 Calling party category interworking (UCP to Gateway ISUP)

UCP IAM (Incoming)	ITU IAM (Outgoing)
Calling Party Category: — DATA	Calling Party Category: — SUBSCRIBER1

109.21.5 Billing

DIGDATA field in the CDR indicates if a call is a datacall. It is a boolean and a value ‘Y’ indicates a datacall.

109.22 Appendix J: ECAN

109.22.1 Application of Echo Cancellers on Transit Switch

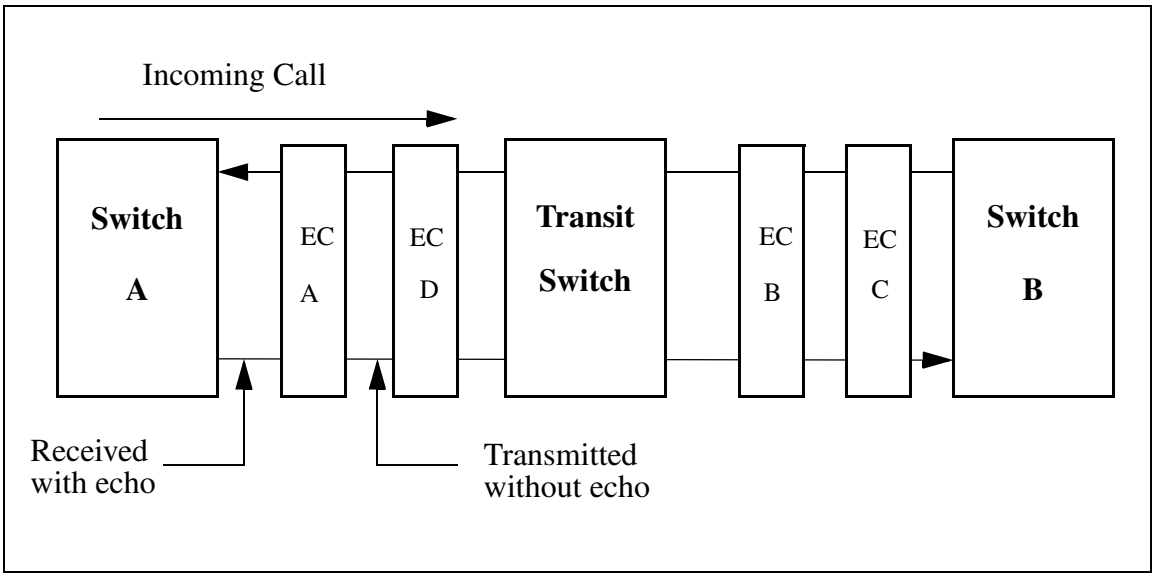
Figure-22 illustrates the use of echo cancellers in a general transit call situation.
Echo canceller A is enabled as the outgoing echo canceller. At the transit switch, a forward message is received indicating that a previous switch has enabled an echo device. Therefore, the transit switch does not enable echo canceller B. At switch B, echo canceller C is enabled as the incoming device. At the transit switch, the first backward acknowledgment indicates

that a succeeding switch has already included an incoming echo device. Thus, it does not enable echo canceller D.

Typically, during call setup in the forward direction, an echo canceller is activated on the outgoing trunk if required. During the backward acknowledgment phase of the call setup, an echo canceller is activated on the incoming trunk if required. This is the conventional setup.

The echo canceller device is physically connected on a per carrier basis, but it can control echo on a per trunk basis (DMS implementation). Since there are two speakers in a call, an echo device is needed in both directions for both parties to benefit. Hence, the term ‘half-echo cancellers’ for one direction. Although, at most, only one incoming and one outgoing echo device should be enabled.

Figure 22 Application of Echo Cancellers on transit switch



109.22.2 Echo Canceller Control Logic

The activation of Echo Canceller is completed at the call setup phase when echo control is required. And it is deactivated at the end of every call.

The diagram below describes how echo control is handled along with a typical ISUP call sequence.

Figure 23 Example of echo control in ISUP messaging

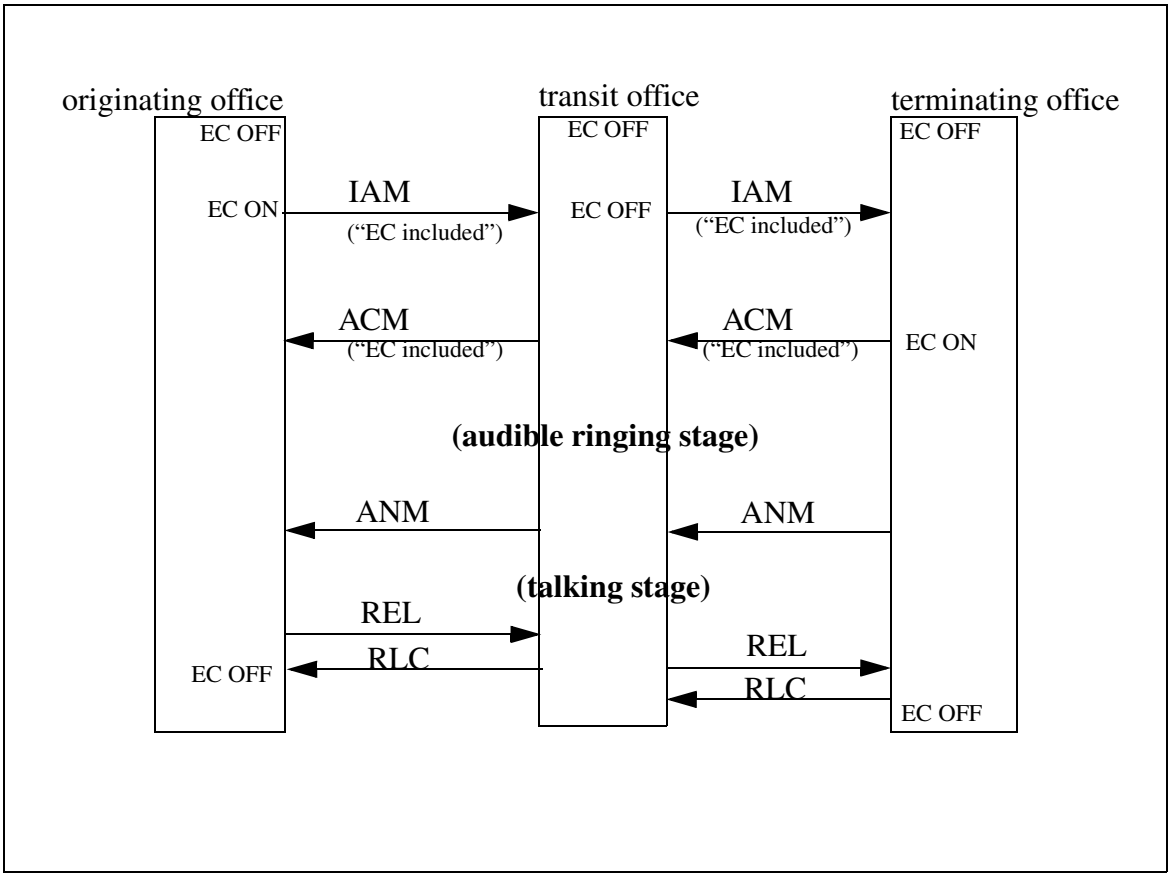
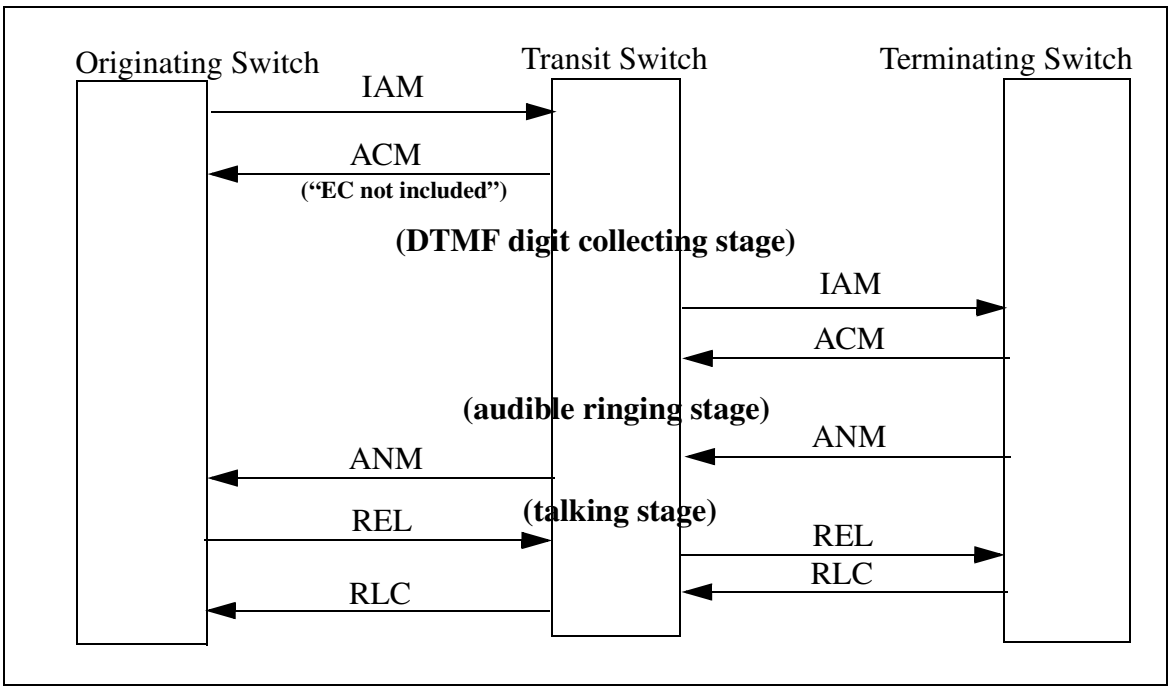


Figure 24 Example of echo control in DTMF digit collection call



For calls which require DTMF digit collection (Figure-24), an ACM message always be send back immediately from the transit switch to the originating switch for requesting the digit collection. Therefore, the EC bit is set to "not included", no matter the transit switch has or has not received the EC indication from the terminating switch.

109.22.3 Outgoing Echo Cancellers

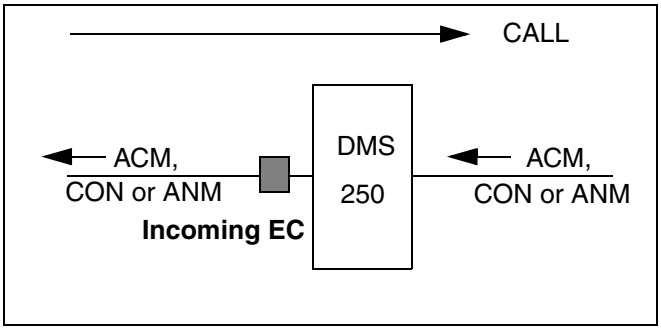
A) Criteria for echo cancellation:

- the incoming seizure (e.g. IAM) indicates no forward echo canceller yet; incoming CPC and TMR fields, if available, indicate voice-only call.
- echo canceller is datafilled in TRKSGRP and is available for use.

B) Signalling upon echo canceller activation:

- outgoing IAM Echo Control bit is set to 'included'.

Figure 25 EC on the trunk in the incoming direction



For the outgoing echo cancellers, the disable/enable commands are send to the EC module after received IAM. However, for the incoming echo cancellers (Figure - 25), the disable/enable commands are not be sent to the EC module until it receives the first backward messages (ACM, CON or ANM).

109.23 Appendix K: UCP ISUP & ISUP92/Q.767 Interworking

The following figures show the message flow diagram for UCP ISUP and ISUP92/Q.767 interworking:

Figure 26 UCP ISUP & ISUP92/Q.767 Interworking (Enbloc)

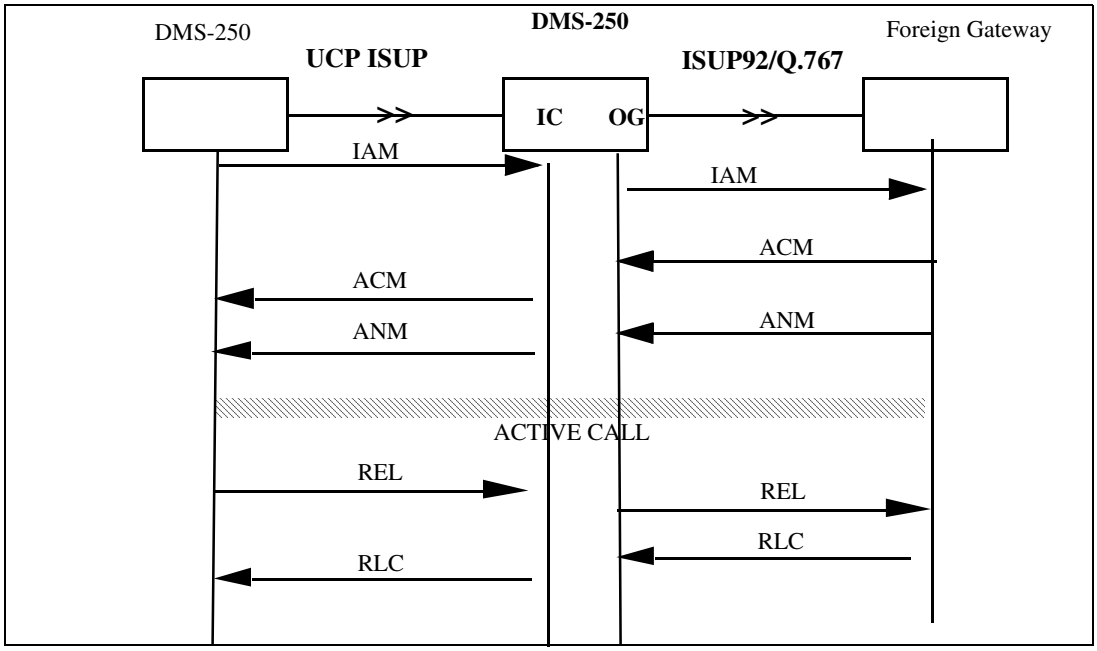
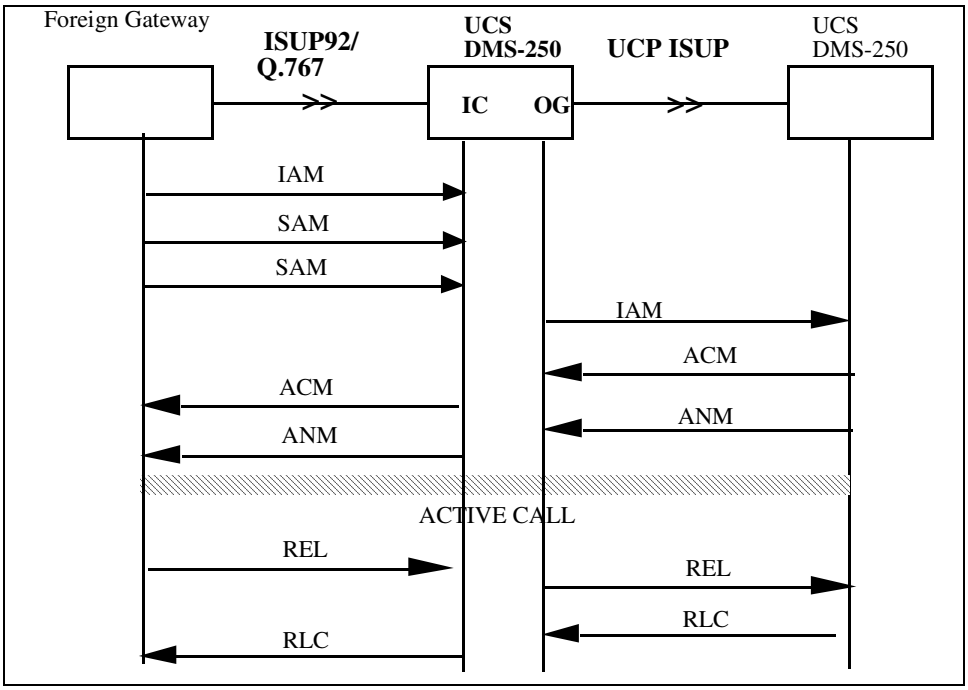


Figure 27 ISUP92/Q.767 & UCP ISUP Interworking (Overlap Sending)



Overlap method of address signaling supports the transport of called party address digits in multiple messages. If the incoming IAM message contains no digits in the Called Party Number, or incomplete digits in the Called Party Number (end-of-digit (F) is not suffixed on the called number), and the field OVLAP in table TRKSGRP is set to 'Y', the DMS-250 enters in overlap mode. Upon receipt of such an IAM message, a timer is started. The DMS-250 waits until all the information is available (via SAMs), or the timer is expired, before translations are performed. It should be noted that the DMS-250 always sends all the Called Party address digits in the Initial Address Message.

Message parameters which need to be interworked, are described in this section. Parameters are keyed as 'F' for fixed mandatory, 'V' for variable length mandatory and 'O' for optional.

Table 74 IAM - UCP ISUP to ISUP92/Q.767

UCP ISUP IAM	ISUP92 IAM
Nature of Connection Indicator (F)	Nature of Connection Indicator (F)
Called Party Number (V)	Called Party Number (V)

Table 74 IAM - UCP ISUP to ISUP92/Q.767

UCP ISUP IAM	ISUP92 IAM
Calling Party Number $(O)_1$	Calling Party Number (O)
Charge Number $(O)_2$	
Transit Network Selection Parameter (O) Carrier Identification Parameter (O)	
Forward Call Indicator (F)	Forward Call Indicator (F)
Calling Party Category (F)	Calling Party Category (F)
User Service Information (V)	Transmission Medium Requirement $(F)_3$ User Service Information (O)

$_1$Note:The Calling Party Number is considered valid and is supported on gateway trunks only if the fields “calling party number incomplete indicator (NI)” is set to “Complete” and the “screening indicator” is “user provided, verified and passed” or “network provided” otherwise it is invalid and is discarded.

$_2$Note: Charge Number is not supported in ISUP92/Q.767 IAM.

$_3$ Note: User Service Information is a mandatory parameter in UCP while it is optional in ISUP92/Q.767. When interworking from UCP to ISUP92/Q.767, the information in the USI parameter is mapped to both the USI optional parameter and to the TMR parameter in the ISUP92/Q.767 IAM.

The formats of the TMR and USI parameters are provided below for reference.

Table 75 Transmission Medium Requirement (in ISUP92/Q.767)

	8	7	6	5	4	3	2	1
Octet 1	Transmission Medium Requirement							

Table 76 User Service Information (in UCP ISUP)

	8	7	6	5	4	3	2	1
Octet 1	Ext	Coding standard		Information transfer capability				
Octet 2	Ext	Transfer mode		Information Transfer rate				
Octet 3	Ext	User layer protocol id						
Octet 4	Ext	Spare		Rate				

Table 77 USI, Information Transfer Rate to TMR Mapping

USI - Information Transfer Rate	TMR - Transmission Medium Requirement
speech	speech
64 Kbit/s unrestricted digital info.	64 Kbit/s unrestricted
64 Kbit/s restricted digital info.	64 Kbit/s unrestricted
3.1 kHz audio	3.1 kHz audio
7 kHz audio	3.1 kHz audio*
15 kHz Audio	3.1 kHz audio*

* Based on Table BCCOMPAT datafill. If this mapping is not datafilled, then the call is treated due to bearer incompatibility.

The following shows the interworking of the ISUP92/Q.767 IAM message to UCP ISUP IAM message:

Table 78 IAM - ISUP92/Q.767 to UCP ISUP

ISUP92/Q.767 IAM	UCP ISUP IAM
Nature of Connection Indicator (F)	Nature of Connection Indicator (F)
Forward Call Indicator (F)	Forward Call Indicator (F)
Calling Party Category (F)	Calling Party Category (F)
Transmission Medium Requirement (F)	User Service Information $(V)_1$

Table 78 IAM - ISUP92/Q.767 to UCP ISUP

ISUP92/Q.767 IAM	UCP ISUP IAM
Called Party Number (V)	Called Party Number (V)
Transit Network Selection (O)	
User Service Information (O)	User Service Information (V)
Calling Party Number $(O)_2$	Calling Party Number (O)

$_1$Note: The User Service Information in the UCP IAM message is encoded based on the USI of the ISUP92/Q.767 IAM if received. If the USI parameter is not received in the ISUP92/Q.767 IAM, then the TMR parameter is used to encode the USI as shown in the Table below.

$_2$Note: The Calling Party Number is considered valid and is supported on gateway trunks only if the fields “calling party number incomplete indicator (NI)” is set to “Complete” and the “screening indicator” is “user provided, verified and passed” or “network provided” otherwise it is invalid and is discarded.

Table 79 ISUP92/Q.767 TMR to UCP ISUP USI Parameter Mapping

ISUP92/Q.767 Transmission Medium Requirement	UCP ISUP User Service Information
	Coding Standard - CCITT standardized coding (default)
Transmission Medium Requirement - Speech - 64 kbit/s unrestricted - 3.1 kHz audio	Information Transfer Capability - Speech - 64 kbit/s Unrestricted digital Info - 3.1 kHz audio
	Transfer mode - Circuit mode (default)
	Information Transfer Rate - 64 kbit/s (default)
	User layer1 protocol Information (default)

109.23.1 Parameters Mapping for messages going from Q.767 to UCP ISUP

109.23.1.1 Initial Address Meesage (IAM)

Table 80 shows the discarding and tandeming of parameter for a Q.767 to UCP IAM.

Table 80 Q.767 -> UCP parameters in the IAM message

Q767 Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process
Calling Party's Category	F	Process
Transmission Medium Requirement (TMR)	F	Mapped
Called Party Number	V	Process
Access Transport	O	Tandem
Calling Party Number	O	Process
Closed User Group Interlock Code	O	Tandem
Optional Forward Call Indicators	O	Tandem
User service information	O	Process
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.1.2 Address Complete Message (ACM)

Table 81 shows the discarding and tandeming of parameters for a Q.767 to UCP ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to ‘Y’.

Table 81 Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Cause indicators	O	Tandem
Optional backward call indicators	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Table 82 shows the discarding and tandeming of parameters in Q.767 to UCP ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to ‘Y’.

Table 82 Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Cause indicators	O	Tandem
Optional backward call indicators	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem

Table 82 Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
End of optional parameters	O	Tandem

109.23.1.3 Answer Message (ANM)

Table 83 shows the tandeming and discarding of parameters inQ.767 to UCP ANM.

Table 83 Q.767 -> UCP parameters in the ANM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Connected number	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.1.4 Call Progress Message (CPG)

Table 84 shows the tandeming and discarding of parameters from a Q.767 to UCP CPG.

Table 84 Q.767 -> UCP parameters in the CPG message

Q767 Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Optional backward call indicators	O	Tandem

Table 84 Q.767 -> UCP parameters in the CPG message

Q767 Parameter	Type	Action
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.1.5 Connect Message (CON)

CON message is not supported in UCP protocol. Table 85 shows the parameters which will be tandemed and discarded while sending an ANM to the UCP trunk.

Table 85 Q.767 -> UCP parameters in the CON message

Q767 Parameter	Type	Action
Message type	F	Mapped
Backward call indicators	F	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
Access transport	O	Tandem
Connected number	O	Discard
End of optional parameters	O	Tandem

109.23.1.6 Continuity Test Message (COT)

Continuity test message is tandemed to the UCP trunk as shown in table 86 .

Table 86 Q.767 -> UCP parameters in Message COT

Q767 Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

109.23.1.7 Forward Transfer Message (FOT)

Forward transfer message is tandemed to the UCP trunk.

Table 87 Q.767 -> UCP parameters in message FOT

Q767 Parameter	Type	Action
Message type	F	Tandem
End of optional parameters	O	Tandem

109.23.1.8 Release Message (REL)

Table 88 shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

Table 88 Q.767 ->UCP parameters in message REL

Q767 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Automatic congestion level	O	Discard
User-to-user information	O	Discard
End of optional parameters	O	Tandem

Table 89 shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received

Table 89 Q.767 ->UCP parameters in message REL

Q767 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Automatic congestion level	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.1.9 Suspend/Resume Message (SUS/RES)

Suspend and resume messages are tandemed to UCP trunk.

Table 90 Q.767 -> UCP parameters in message RES and SUS

Q767 Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

109.23.2 Parameters interworking for messages from UCP to Q.767

Reference feature document AD9067‘Support for User to User Parameter’ for proper requirements when mapping of the User to User parameter is required.

109.23.2.1 Initial Address Message (IAM)

Table 91 shows the tandeming and discarding of parameters from a UCP to Q.767 IAM.

Table 91 UCP -> Q767 parameters in the IAM message

UCP Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process
Calling Party's Category	F	Process
User service information	F	Mapped
Called Party Number	V	Process
Calling Party Number	O	Process
Carrier Identification	O	Discard

Table 91 UCP -> Q767 parameters in the IAM message

UCP Parameter	Type	Action
Carrier Selection	O	Discard
Charge Number	O	Discard
Channel Assignment Map	O	Discard
Generic Address	O	Discard
Generic Digits	O	Discard
Jurisdiction Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Network Specific Facilities	O	Discard
Network-Specific IAM	O	Discard
Operator Information	O	Discard
Operator Service Indicator	O	Discard
Originating Line Information	O	Discard
Remote Operations	O	Discard
Supplementary Line Information	O	Discard
Transit network selection	O	Discard
User service information (mandatory variable length parameter in UCP protocol)	O	Process
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.2.2 Address Complete Message (ACM)

Table 92 shows the tandeming and discarding of parameters from a UCP to Q.767 ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to ‘Y’.

Table 92 UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	discard
Cause indicators	O	Tandem
Network specific information	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Table 93 shows the tandeming and discarding of parameters from a UCP to Q.767 ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to ‘Y’.

Table 93 UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard
Cause indicators	O	Tandem
Network specific information	O	Discard
User-to-user indicators	O	Tandem

Table 93 UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.2.3 Answer Message (ANM)

Table 94 shows the tandeming and discarding of parameters from a UCP to Q.767 ANM.

Table 94 UCP -> Q767parameters in the ANM message

UCP Parameter	Type	Action
Message type	F	Tandem
Call reference	O	Discard
Carrier Selection	O	Discard
Internetwork Specific ANM	O	Discard
Intranetwork Specific ANM	O	Discard
Network Specific Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Operator Information	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.2.4 Call Progress Message (CPG)

Table 95 shows the tandeming and discarding of parameters from a UCP to Q.767 CPG.

Table 95 UCP -> Q767 parameters in the CPG message

UCP Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Cause indicators	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.2.5 Pass Along Message (PAM)

Table 96 shows the tandeming and discarding of parameters from a UCP to Q.767 PAM.

Table 96 UCP -> Q767 parameters in message PAM

UCP Parameter	Type	Action
Message type	F	Tandem

109.23.2.6 Release Message (REL)

Table 97 shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

Table 97 UCP -> Q767 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem

Table 97 UCP -> Q767 parameters in message REL

UCP Parameter	Type	Action
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

Table 98 shows the tandeming and discarding of parameters in REL message when a cause value of Normal Call Clearing is received.

Table 98 UCP -> Q767 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

109.23.2.7 Suspend/Resume Message (SUS/RES)

Table 99 shows the tandeming and discarding of parameter in the SUS and RES messages from a UCP trunk to Q.767 trunk.

Table 99 UCP -> Q767 parameters in message RES and SUS

UCP Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

109.23.3 Parameter interworking for messages from ISUP92 to UCP

109.23.3.1 Initial Address Message (IAM)

Table 100 shows the tandeming and discarding of parameters from a ISUP92 trunk to UCP trunk.

Table 100 ISUP92 ->UCP parameters in the IAM message

ISUP92 Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process
Calling Party's Category	F	Process
Transmission Medium Requirement (TMR)	F	Mapped
Called Party Number	V	Process
Access Transport	O	Tandem
Calling Party Number	O	Process
Closed User Group Interlock Code	O	Tandem
Optional Forward Call Indicators	O	Tandem
User service information	O	Process
User-to-user information	O	Tandem
Original Called Number	O	Tandem
Redirecting Number	O	Tandem
Redirection Information	O	Tandem
User to User Indicators	O	Tandem
End of optional parameters	O	Tandem

109.23.3.2 Address Complete Message

Table 101 shows the discarding and tandeming of parameters for a ISUP92 to UCP ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to ‘Y’.

Table 101 ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Access delivery information	O	Discard
Call diversion information	O	Discard
Cause indicators	O	Tandem
Echo control information	O	Discard
Generic notification indicator	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Table 102 shows the discarding and tandeming of parameters in ISUP92 to UCP ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to ‘Y’.

Table 102 ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Access delivery information	O	Tandem
Call diversion information	O	Tandem
Cause indicators	O	Tandem
Echo control information	O	Tandem
Generic notification indicator	O	Tandem
Optional backward call indicators	O	Tandem
Parameter compatibility information	O	Tandem
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.3.3 Answer Message (ANM)

Table 103 shows the tendeming and discarding of parameters for a ISUP92 to UCP ANM.

Table 103 ISUP92 ->UCP parameters in the ANM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Access delivery information	O	Discard
Access transport	O	Tandem
Backward call indicators	O	Tandem
Call history information	O	Discard
Connected number	O	Tandem
Echo control information	O	Discard
Generic notification indicator	O	Discard
Generic address	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.3.4 Call Progress Message (CPG)

Table 104 shows the tandmenig and discarding of parameters in the ISUP92 to UCP message.

Table 104 ISUP92 -> UCP parameters in the CPG message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Access delivery information	O	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Call diversion information	O	Tandem
Cause indicators	O	Tandem
Generic notification indicator	O	Tandem
Optional backward call indicators	O	Tandem
Parameter compatibility information	O	Tandem
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.3.5 Connect Message (CON)

CON message is not supported in UCP protocol. Table 105 shows the parameters which will be tandemed and discarded while sending an ANM to the UCP trunk.

Table 105 ISUP92 -> UCP parameters in the CON message

ISUP92 Parameter	Type	Action
Message type	F	Mapped
Backward call indicators	F	Tandem
Access delivery information	O	Discard
Access transport	O	Tandem
Call history information	O	Discard
Connected number	O	Tandem
Echo control information	O	Discard
Generic notification indicator	O	Discard
Generic address	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.3.6 Continuity Test Message (COT)

As shown in table 106 this message is tandemed to the UCP trunk.

Table 106 ISUP92 -> UCP parameters in Message COT

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

109.23.3.7 Forward Transfer Message (FOT)

As shown in table 107 FOT message is tandemed to the UCP trunk.

Table 107 ISUP92 -> UCP parameters in message FOT

ISUP92 Parameter	Type	Action
Message type	F	Tandem
End of optional parameters	O	Tandem

109.23.3.8 Release Message (REL)

Table 108 shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

Table 108 ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Access delivery information	O	Discard
Access transport	O	Discard
Automatic congestion level	O	Discard
Parameter compatibility information	O	Discard
Redirection number restriction	O	Discard
User-to-user information	O	Discard

Table 108 ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

Table 109 shows the tandeming and discarding of parameters in REL message when a cause value of Normal call Clearing is received.

Table 109 ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Access delivery information	O	Tandem
Access transport	O	Tandem
Automatic congestion level	O	Discard
Parameter compatibility information	O	Tandem
Redirection number restriction	O	Tandem
User-to-user information	O	Tandem
User-to-user indicators	O	Tandem
End of optional parameters	O	Tandem

109.23.3.9 Suspend/Resume Message (SUS/RES)

These messages are tandemed as shown in table 110.

Table 110 ISUP92 -> UCP parameters in message RES and SUS

ISUP92 Parameter	Type	Action
Message type	F	Tandem

Table 110 ISUP92 -> UCP parameters in message RES and SUS

ISUP92 Parameter	Type	Action
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

109.23.4 Parameter mapping for messages from UCP to ISUP92

This section shows the parameter tandeming and discarding for the messages coming on the UCP trunk and going to the ISUP92 trunk.

Reference feature document AD9067‘Support for User to User Parameter’ for proper requirements when mapping of the User to User parameter is required.

109.23.4.1 Initail Address Message (IAM)

Parameter tandeming and discarding for the IAM is shown in table 111.

Table 111 UCP -> ISUP92 parameters in the IAM message

UCP Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process
Calling Party's Category	F	Process
User service information	F	Mapped
Called Party Number	V	Process
Calling Party Number	O	Process
Carrier Identification	O	Discard
Carrier Selection	O	Discard
Charge Number	O	Discard
Channel Assignment Map	O	Discard
Generic Address	O	Discard
Generic Digits	O	Discard

Table 111 UCP -> ISUP92 parameters in the IAM message

UCP Parameter	Type	Action
Jurisdiction Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Network Specific Facilities	O	Discard
Network-Specific IAM	O	Discard
Operator Information	O	Discard
Operator Service Indicator	O	Discard
Originating Line Information	O	Discard
Remote Operations	O	Discard
Supplementary Line Information	O	Discard
Transit network selection	O	Discard
User service information (mandatory variable length parameter in UCP protocol)	O	Process
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.4.2 Address Complete Message (ACM)

Table 112 shows the discarding and tandeming of parameters for a UCP to ISUP92ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to ‘Y’.

Table 112 UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard

Table 112 UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
Cause indicators	O	Tandem
Network specific facility	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Table 113 shows the discarding and tandeming of parameters in UCP to ISUP92 ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to ‘Y’.

Table 113 UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard
Cause indicators	O	Tandem
Network specific facility	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.4.3 Answer Message (ANM)

Parameter tandeming and discarding for ANM message form UCP to ISUP92 are shown in table 114.

Table 114 UCP -> ISUP92parameters in the ANM message

UCP Parameter	Type	Action
Message type	F	Tandem
Call reference	O	Discard

Table 114 UCP -> ISUP92parameters in the ANM message

UCP Parameter	Type	Action
Carrier Selection	O	Discard
Internetwork Specific ANM	O	Discard
Intranetwork Specific ANM	O	Discard
Network Specific Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Operator Information	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.4.4 Call Progress Message (CPG)

Parameter tandeming and discarding for CPG message form UCP to ISUP92 are shown in table 115.

Table 115 UCP -> ISUP92 parameters in the CPG message

UCP Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Cause indicators	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

109.23.4.5 Continuity Test Message (COT)

Parameter tandeming and discarding for COT message form UCP to ISUP92 are shown in table 116.

Table 116 UCP -> ISUP92 parameters in Message COT

UCP Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

109.23.4.6 Pass Along Message (PAM)

Parameter tandeming and discarding for PAM message form UCP to ISUP92 are shown in table 117.

Table 117 UCP -> ISUP92 parameters in message PAM

UCP Parameter	Type	Action
Message type	F	Tandem

109.23.4.7 Release Message (REL)

Table 118 shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

Table 118 UCP -> ISUP92 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

Table 119 shows the tandeming and discarding of parameters in REL message when a cause value of Normal call Clearing is received.

Table 119 UCP -> ISUP92 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

109.23.4.8 Suspend/Resume Message (SUS)

Table 120 shows the tandeming and discarding of parameters in SUS/RES message.

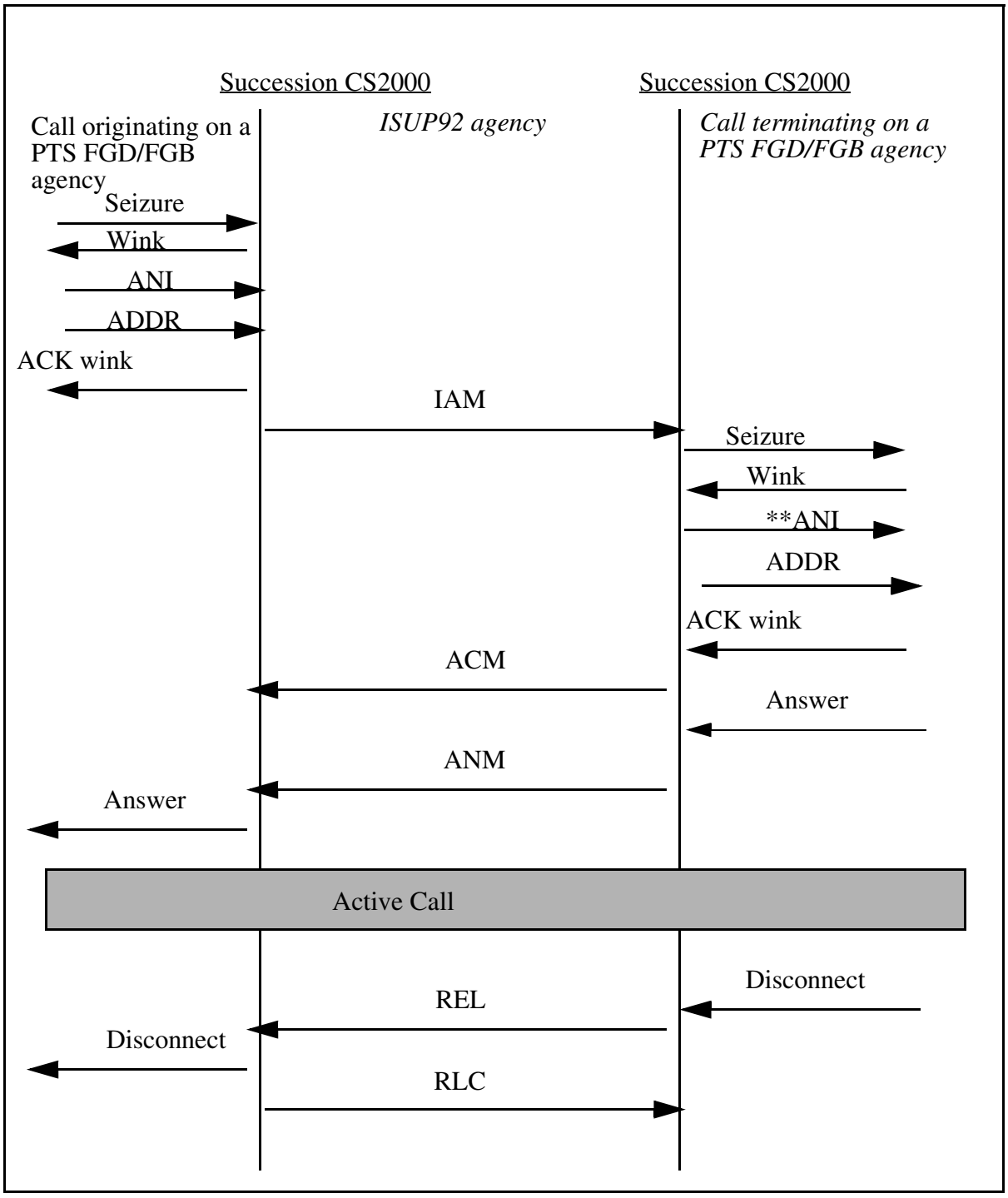
Table 120 UCP -> ISUP92 parameters in message RES and SUS

UCP Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

109.24 Appendix L: Interworking of ISUP92/Q.767 with PTS agents

The following diagram depicts the signal flow for a call originating and terminating on an ISUP92/Q.767 agent from a PTS FGD/FGB.

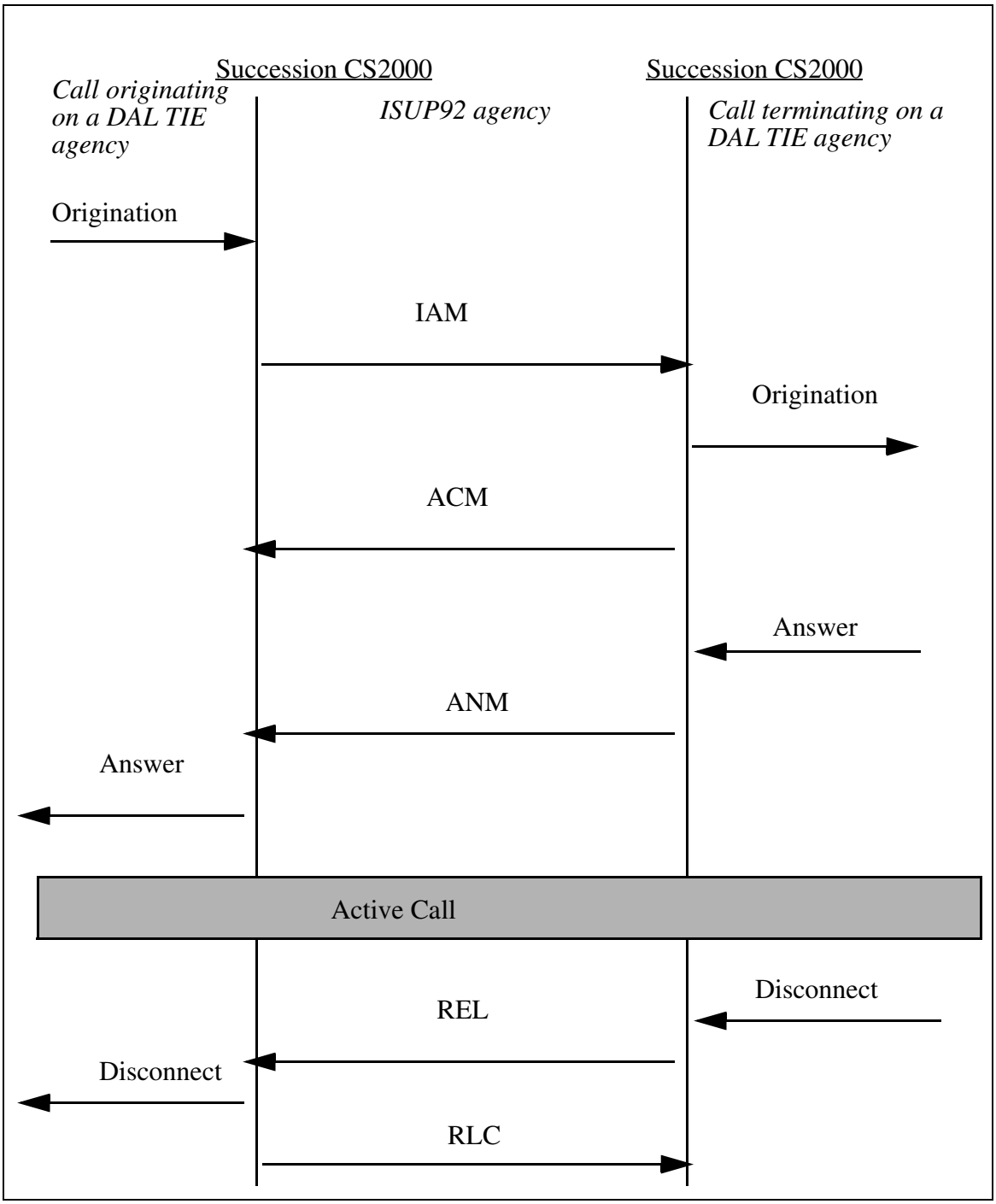
Figure 28 Interworking between ISUP92/Q.767 and PTS FGB/FGD agent.



** In case of FGB, ANI delivery is optional.

The following diagram depicts the signal flow for a call originating and terminating on an ISUP92/Q.767 agent from a DAL TIE.

Figure 29 Interworking between ISUP92/Q.767 and DAL-TIE agents



The following table illustrates the message mapping between the ISUP92/ Q.767 messages and the FGB/FGD messages.

Table 121 ISUP92/Q.767 --> FGB/FGD messages mapping

ISUP92/Q.767 Message	FGB/FGD Message
IAM	Seized message is sent and wink is received after address digits are outpulsed
SAM	**
ACM	--
ANM	Answer message is received.
REL	On-Hook message is received
RLC	--

Note:

*** If Overlap sending is allowed, then Seized message is sent to DAL TIE only after SAM is received.*

The following table explain the mappings between the ISUP92/Q.767 messages and the corresponding DAL TIE messages.

Table 122 ISUP92/Q.767 --> DAL TIE message mapping

Messages	**DAL TIE messages**
IAM	Seized message is sent and wink is received.
SAM	**
ACM	---
ANM	Answer message is received
REL	On-hook message is received
RLC	---

Note:

*** If Overlap sending is allowed, then Seized message is sent to DAL TIE only after SAM is received*

For PTS originations and ISUP92/Q.767 terminations, the default values of parameters in IAM are given below.

Table 123 PTS-> ISUP92/Q.767, value of ISUP Parameter 'Called Party Number' in IAM

ISUP Parameter Field	ISUP value
Nature of Address	National number (0000011)[a]
Numbering Plan Indicator	ISDN (telephony) Numbering Plan (Recommendation E.164) (001)
Odd/Even Indicator	odd (1)- if odd number of digits in the called party, even (0)-if even number of digits in called party

a. The value of this parameter depends on the translation system used in the call.

Table 124 PTS-> ISUP92/Q.767, value of ISUP Parameter 'Nature of Connection Indicators' in IAM

ISUP Parameter Field	ISUP value
Satellite Indicator	Datafill dependant[a]
Continuity Check Indicator	Datafill dependent[b]
Echo Control Device Indicator	Datafill dependent

a. The value of this field depends on the SAT field of table TRKSGRP
b. The value of this field depends on the CONTCHK field of table TRKSGRP

Table 125 PTS-> ISUP92/Q.767, values for ISUP Parameter 'Forward Call Indicator' in IAM

ISUP Parameter Field	ISUP value
National / International Call Indicator	Call to be treated as National (0)
End to End Method Indicator	No end to end method available(00)
Interworking Indicator	Interworking encountered (1)
End to End Information Indicator	No end to end information available (0)
ISDN User Part Indicator	ISDN User part not used all the way (0)
ISDN User Part Preference Indicator	ISDN user part not required all the way (01)
ISDN Access Indicator	Originating access non-ISDN (0)
Trans_called_Num_Ind	Number_Not_Translated
Routing_attempt_Ind	No_routing_attempt(0000000)

Table 126 PTS-> ISUP92/Q.767, values for ISUP Parameter 'Calling Party Category' in IAM

ISUP Parameter Field	ISUP value
Calling Party Category	ordinary subscriber (00001010)

Table 127 Default values for ISUP Parameter 'Transmission Medium Requirement' in ISUP92/Q.767 IAM

ISUP Parameter Field	ISUP value
Transmission Medium Requirement	3.1 Khz audio(00000011)[a]

a. The value of this field depends upon the BCNAME field of table TRKGRP.

Table 128 Default values User Service Information parameter in IAM

ISUP Parameter Field	ISUP value
Coding standards	CCITT (00)

Table 128 Default values User Service Information parameter in IAM

ISUP Parameter Field	ISUP value
Information transfer rate	64_KBits/S (10000)
Information transfer mode	Circuit mode (00)
Information transfer capability	3.1Khz Audio (10000)
Layer1 Identification	Layer1_G711_ALaw(00011)
User Rate	User Rate Nil(00000)
Synchronization	Synchrone(0)
Negotiation	Negot_not_inband(0)

The default values of BCI in ACM is given below for ISUP92/Q.767 to PTS interworking.

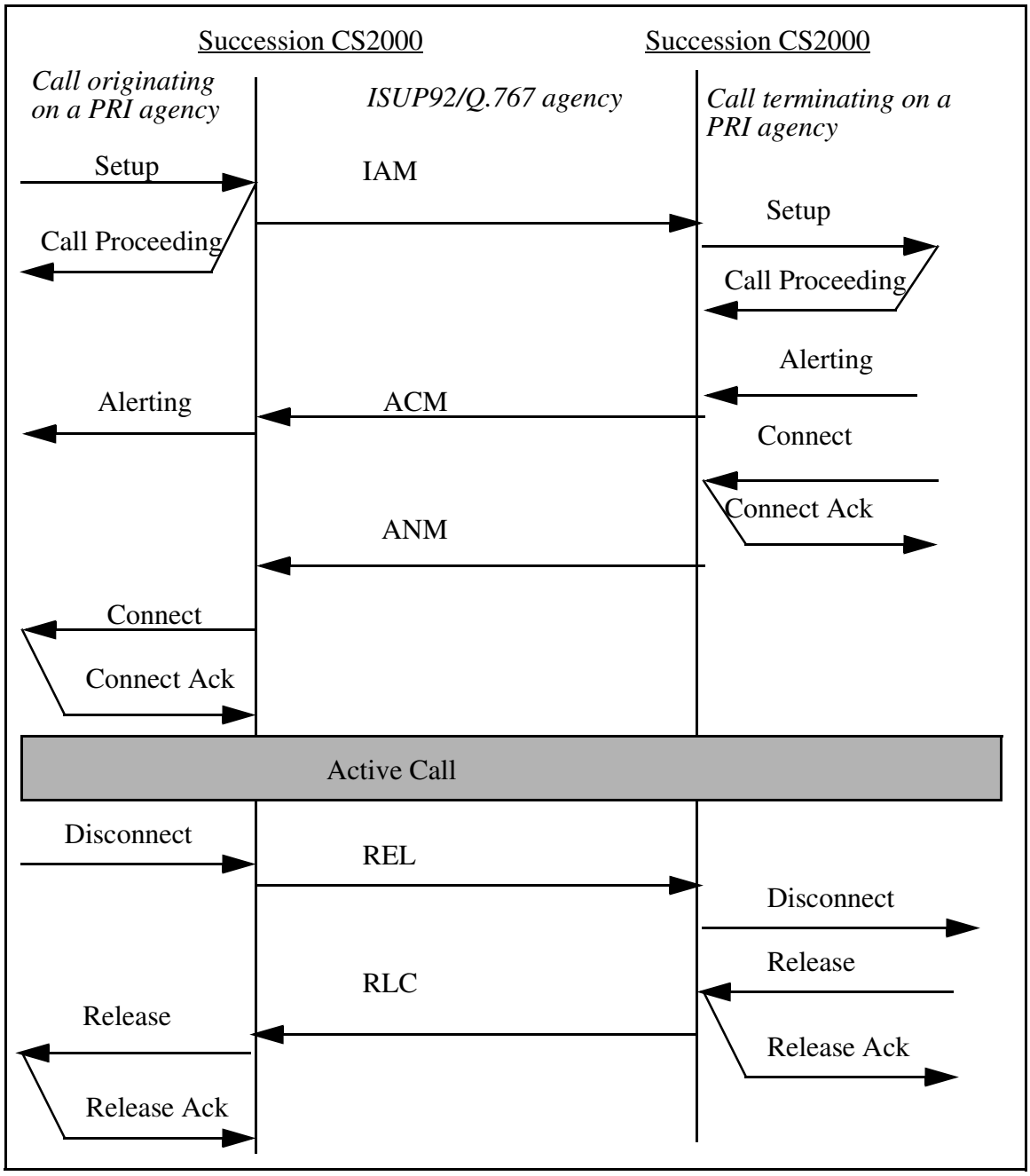
Table 129 Default BCI field values in ACM for ISUP92/Q.767 origination and PTS termination.

Field name	**Default value**
Charge Indicator	10 “Charge”
Called party’s status	No indication (00)
Called party’s category	No indication (00)
End-End_Method indicator	No end-end method available (00)
Interworking indicator	Interworking encountered (1)
End-End information Indicator	No end to end information available (0)
ISUP indicator	ISUP not used all the way (0)
Holding indicator	Holding not requested (0)
ISDN access indicator	terminating access non ISDN (0)
Echo control device indicator	incoming half echo control device not included (0)
SCCP method indicator	No SCCP indication (00)

109.25 Appendix N: Interworking between ISUP92/Q.767 and UCS PRI

The following message sequence diagram depicts the signal flow for a call originating from and terminating on a ISUP92 agent from a PRI agent.

Figure 30 Interworking Between ISUP92/Q.767 and PRI Agents



The following table illustrates the message mapping between the isup92/q767 messages and the corresponding PRI messages:

Table 130 UCS PRI to ISUP92/Q767 Message Mapping[a]

UCS PRI Messages	ISUP Messages
ALERTING*	ACM
CONNECT	CON (if ACM has not been sent) ANM (if ACM has been sent)
DISCONNECT	REL
PROGRESS*	ACM
RELEASE	REL
RELEASE COMPLETE	REL
RESTART	REL
SETUP	IAM

* If ALERT is received, interwoking indicator of BCI in ACM is set to ‘no interworking encountered’. If PROGRESS is received, it is set to ‘interworking encountered’.

a. The ISDNXFER option of table TRKGRP for terminating ISUP agency controls the support of ISDN services, when the originating agency is a PRI trunk. It is recommended to use this option when the entire call path is predetermined to be all the way ISDN user part(all the way ISDN and SS7). If the entire call path is not ISUP all the way, then this option need not be selected. This way, we can avoid unwanted packets(ISDN options which carry services) to be sent over the network.

Table 131 ISUP92/Q.767 to UCS PRI Message Mapping

ISUP Messages	UCS PRI Messages
ACM	ALERT (if Backward Call Indicator bit is set to ‘no interworking encountered’) PROGRESS (if Backward Call Indicator bit is set to ‘ interworking encountered’)
ANM	CONNECT
IAM	SETUP
REL	DISCONNECT

109.25.1 ISUP92/Q.767 and UCS PRI Message Mapping

Table 132 Mapping of SETUP message to IAM message

UCS PRI IEs	ISUP parameter
Bearer Capability (M)	User Service Info/Transmission Medium Requirement
Called Party Number (M)	Called Party Number
Called Party Subaddress (O)	Access Transport*
Calling Party Number (O)	Calling Party Number
Calling Party Subaddress (O)	Access Transport*
Low Layer Compatiblity (O)	Access Transport*
High Layer Compatibility (O)	Access Transport*
Progress Indicator (O)	Forward Call Indicators
User to User (O)	User to User Info
* The IAM Message contains a maximum of one Access Transport parameter, containing UCS PRI IEs as required. The ATP mapping is subject to the datafill in Table ISDNPARM.	

Table 133 Mapping of IAM -> SETUP

ISUP parameter	UCS PRI IEs
Transmission Medium Requirement (V)	Bearer Capability
User Service Information (O)	Bearer Capability
Called Party Number (V)	Called Party Number
Access Transport (O)	*
Calling Party Number (O)	Calling Party Number
Forward Call Indicators (F)	Progress Indicator
User to User Info (O)	User to User Info
* Access Transport parameter contains one or more of: HLC, LLC, Called Party Subaddress, Calling Party subaddress, Display, Facility. These are inserted in the setup message in accordance with UCS PRI encoding rules.	

Table 134 Mapping of ALERT -> ACM[a]

UCS PRI IEs	ISUP parameter
Progress Indicator (O)	No Mapping
User to User Info(O)	User to User Info

a. If an ALERT message is received, an ACM with BCI set to ‘no interworking required’ and ‘ISUP all the way’ is sent on the ISUP side.

Table 135 Mapping of PROGRESS -> ACM[a]

UCS PRI IEs	ISUP parameter
Progress Indicator (F)	No Mapping

a. If an PROGRESS message is received, an ACM with BCI set to ‘interworking required’ and ‘Not ISUP all the way’ is sent on the ISUP side.

Table 136 Mapping of ACM -> ALERT / PROGRESS

ISUP parameter	UCS PRI IEs
Backward Call Indicators (F)	No Mapping
User to User Info (O)*	User to User Info
* UUI mapping happens only for the case of ACM to ALERT. This is because UUI mapping is defined only for non-interworking scenarios.	

Table 137 Mapping of CONNECT -> ANM/CON

UCS PRI IEs	ISUP parameter
User to User Info(O)	User to User Info

Table 138 Mapping of ANM/CON -> CONNECT

ISUP parameter	UCS PRI IEs
User to User Info (O)*	User to User Info

Table 139 Mapping of DISCONNECT -> REL

UCS PRI IEs	ISUP parameter
Cause (V) *[a]	Cause Indicator
User to User Info(O)	User to User Info
*Mandatory in the first call clearing message.	

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Table 140 Mapping of RELEASE / RELEASE COMPLETE -> REL

UCS PRI IEs	ISUP parameter
Cause (O) *[a]	Cause Indicator
User to User Info(O)	User to User Info
* Mandatory in the first call clearing message.	

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Table 141 Mapping of REL -> DISCONNECT

ISUP parameter	UCS PRI IEs
Cause Indicator (V)[a]	Cause

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Note: Reference feature document AD9067 'Support for User to User Parameter' for proper datfill requirements when mapping of the User to User parameter is required.

109.25.1.1 Information Elements and Parameters Mapping

109.25.1.1.1 Bearer Capability <-> User Service Info The following mapping for Bearer Capability and User Service Information is based on different call scenarios. It is not mapped octet by octet since some octet contents may affect the other octet's existence.

109.25.1.1.2 56K Data[1] Call:

Table 142 ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	**Octet 3, Coding Standard** 00 CCITT
Octet 1 Information Transfer Capability[a] 01000 unrestricted digital info	**Octet 3, Information Transfer Capability** 01000 unrestricted digital info
Octet 2, Transfer Mode 00 Circuit Mode	**Octet 4, Transfer Mode** 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	**Octet 4, Information Transfer Rate** 10000 64 kbits/s
Octet 3, User Information layer 1 protocol 00001 Layer 1 Rate Adaption	**Octet 5, Bearer Capability Multiplier** 00001 CCITT Standardized rate adaption
Octet 3a, User Rate 01111 56kbits/s	**Octet 5a, Access Data Rate** 01111 56kbits/s

a. For all calls Bearer capability screening is done. This is to ensure that unsupported BC values are not sent on any trunk. Refer to feature AD9582 for details on Bearer capability screening.

Table 143 ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000010 unrestricted digital info	**Information Transfer Capability:** 01000 unrestricted digital info.

Table 144 UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	**Octet 1, Coding Standard** 00 CCITT
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	**Octet 1 Information Transfer Capability** 01000 unrestricted digital info

[1]A call is termed as a Data Call if the Transmission Medium Requirement is 64 Kbps Unrestricted. If the User rate is 56kbits/s then it is a 56K Data Call. If there is no user rate then it is a 64kbits/s Data Call.

Table 144 UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 4, Transfer Mode 00 Circuit Mode	**Octet 2, Transfer Mode** 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbits/s	**Octet 2, Information Transfer Rate** 10000 64 kbits/s
Octet 5, Bearer Capability Multiplier 00001 CCITT Standardized rate adaption	**Octet 3, User Information layer 1 protocol** 00001 Layer 1 Rate Adaption
Octet 5a, Access Data Rate 01111 56kbits/s	**Octet 3a, User Rate** 01111 56kbits/s

Table 145 UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP92/Q.767 Transmission Medium Requirement
Octet 3, Information Transfer Capability	
01000 unrestricted digital info.	00000010 unrestricted digital info
01001 restricted digital info	00000010 unrestricted digital info

109.25.1.1.3 64K Data Call

Table 146 ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	**Octet 3, Coding Standard** 00 CCITT
Octet 1 Information Transfer Capability 01000 unrestricted digital info	**Octet 3, Information Transfer Capability** 01000 unrestricted digital info.
Octet 2, Transfer Mode 00 Circuit Mode	**Octet 4, Transfer Mode** 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	**Octet 4, Information Transfer Rate** 10000 64 kbits/s

Table 147 ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000010 unrestricted digital info	**Information Transfer Capability:** 01000 unrestricted digital info.

Table 148 UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	**Octet 1, Coding Standard** 00 CCITT
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	**Octet 1 Information Transfer Capability** 01000 unrestricted digital info
Octet 4, Transfer Mode 00 Circuit Mode	**Octet 2, Transfer Mode** 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbits/s	**Octet 2, Information Transfer Rate** 10000 64 kbits/s

Table 149 UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP Transmission Medium Requirement
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	00000010 unrestricted digital info

109.25.1.1.4 Voice Call[1]

Table 150 ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	**Octet 3, Coding Standard** 00 CCITT

[1]A Call is termed as a voice call if the TMR is either 3.1 Khz Audio or Speech.

Table 150 ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 1 Information Transfer Capability 00000 Speech 10000 3.1Khz audio	**Octet 3, Information Transfer Capability** Based on the TMR Value
Octet 2, Transfer Mode 00 Circuit Mode	**Octet 4, Transfer Mode** 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	**Octet 4, Information Transfer Rate** 10000 64 kbits/s
Octet 3, User Information layer 1 protocol 00010 Recommendation G.711 A-law	**Octet 5, User Information Layer 1 Protocol** 00010 Recommendation G.711 Mu-law Speech

Table 151 ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000000 Speech 00000011 3.1KHz Audio	**Octet 3, Information Transfer Capability** 00000 Speech 10000 3.1Khz audio

Table 152 UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	**Octet 1, Coding Standard** 00 CCITT
Octet 3, Information Transfer Capability [a] 00000 Speech 10000 3.1KHz Audio	**Octet 1 Information Transfer Capability** 00000 Speech 10000 3.1KHz Audio
Octet 4, Transfer Mode 00 Circuit Mode	**Octet 2, Transfer Mode** 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbits/s	**Octet 2, Information Transfer Rate** 10000 64 kbits/s

Table 152 UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 5, User Information Layer 1 Protocol 00010 Recommendation G.711 Mu-law Speech	**Octet 3, User Information layer 1 protocol** 00011 Recommendation G.711 A-law

a. In order to ensure the PRI bearer compatibility information is properly propogated to the terminating gateway IMT, the ISDNXFER option should be provisioned on the terminating ISUP trunk.

Table 153 UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP Transmission Medium Requirement
Octet 3, Information Transfer Capability	
00000 speech	00000000 speech
10000 3.1KHz Audio	00000011 3.1KHz Audio

109.25.1.2 Default Values of ISUP Backward Call Indicator

Table 154 Default Values of ISUP Backward Call Indicator

ISUP Backward Call Indicator
Charge Indicator - Charge
Called Party Status Indicator - Subscriber Free
Called Party Category - Ordinary Subscriber
End To End Method - No End To End Method Available
Interworking Indicator- Depends on the Backward Message from PRI (See *Note 1*)
End To End Information Indicator- No End To End Information Available
ISUP Indicator - Depends on the Backward Message from PRI (See *Note 1*)

Table 154 Default Values of ISUP Backward Call Indicator

ISUP Backward Call Indicator
Reverse Holding Indicator -Not Required
ISDN Access Indicator - Access ISDN
Echo Control Device Indicator - Echo Control Device Not Included
SCCP Method Indicator - Connection less and Connection Oriented Methods Available
Notes: Note 1: If an ALERTING message comes from the PRI side, the Interworking Indicator in the BCI is set to 'No interworking' and the ISUP Indicator is set to 'ISUP all the way'. If an PROGRESS message comes from the PRI side, the Interworking Indicator in the BCI is set to 'Interworking encountered' the ISUP Indicator is set to 'Not ISUP all the way'.

109.25.1.3 UCS PRI Calling Party Number -> ISUP92/Q.767 Calling Party Number[1]

Table 155 UCS PRI Calling Party Number <-> ISUP92/Q.767 CPN

UCS PRI CPN	ISUP CPN
Type of Address, Octet 3	**Nature of Address, Octet 1**
001 International Number	0000100 International Number
010 National Number	0000100 International Number
Numbering Plan Identification, octet 3	**Numbering Plan Indicator, Octet 2**
0001 ISDN/Telephony numbering plan	001 ISDN/Telephonny Numbering Plan
others	001 ISDN/Telephonny Numbering Plan
Presentation Indicator, Octet 3a	**Address presentation, octet 2**
00 Presentation allowed	00 presentation allowed
01 Presentation restricted	01 presentation restricted
10 Number not available due to interworking	00 presentation allowed
Screening Indicator, Octet 3a*	**Screening Indicator, Octet 2**
11 network provided	11 network provided
others	CPN discarded*
* If CPN is received with Screening Indicator as "User provided, not screened(00)", "user provided, verified and passed(01)" or "user provided, verified and failed(10)", then CPN is not mapped.	

1. The ISDNXFER option of table TRKGRP for terminating ISUP trunk is required to be present for the delivery of CPN when the originating agency is a PRI trunk. Otherwise the CPN parameter is not sent in the outgoing IAM.

109.25.1.4 ISUP92/Q767 CPN -> UCS PRI CPN

Table 156 ISUP92/Q.767 CPN -> UCS PRI CPN

ISUP CPN	UCS PRI CPN
Nature of Address, Octet 1 0000100 International Number	**Type of Address, Octet 3** 001 International Number
Incomplete Indicator(NI), Octet 2 0 Complete 1 Incomplete	 Not mapped. CPN discarded.
Numbering Plan Indicator, Octet 2 001 ISDN/Telephonny Numbering Plan	**Numbering Plan Identification, octet 3** 0001 ISDN/Telephony numbering plan
Address presentation, octet 2 00 presentation allowed 01 presentation restricted others	**Presentation Indicator, Octet 3a** 00 Presentation allowed 01 Presentation restricted 01 Presentation restricted
Screening Indicator, Octet 2 01 User provided, verified and passed 11 Network provided others	**Screening Indicator, Octet 3a*** 01 User provided, verified and passed 11 Network provided 00 User provided, not screened

109.25.1.5 ISUP92/Q.767 Cause Indicator -> UCS PRI Cause

Table 157 ISUP92/Q.767 Cause Indicator <-> UCS PRI Cause Indicator

ISUP Cause	UCS PRI Cause
Location, Octet 1 0111 International Network	**Location, Octet 3** Based on Location field of TRKSGRP datafill.
Coding Standard, Octet 1 00 CCITT standard (Default)	**Coding Standard, Octet 3** 00 CCITT standard (Default)
Diagnostics, Octet 3-n Not mapped	**Diagnostics, Octet 5-5b** Not mapped

If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP (Treatment to Cause Mapping) and CSEMAP (Cause to Treatment mapping) are used and the mappings are done as per the datafill in these Tables.

109.25.1.6 UCS PRI Cause -> ISUP92/Q.767 Cause Indicator

Table 158 UCS PRI Cause <-> ISUP92/Q.767 Cause Indicator

PRI Cause	ISUP Cause Indicator
Location, Octet 1 0000 User 0001 Local Private Network 0010 Local Network 0011 Transit Network (Default) 0100 Public network serving the remote user 0101 Private Network serving the remote user 0111 International Network	**Location, Octet 3** 0111 International Network
Coding Standard, Octet 1 00 CCITT standard (Default) 10 National standard	**Coding Standard, Octet 3** 00 CCITT standard (Default)
Diagnostics, Octet 3-n Not mapped	**Diagnostics, Octet 5-5b** Not mapped

Table 159 ISUP Forward Call Indicator <-> UCS PRI Progress Indicator

ISUP Forward Call Indicator	PRI Progress Indicator
Interworking indicator	**Progress Description**[a]
Interworking encountered	Call is not end to end ISDN

a. If there is no Progress Indicator then the Interworking indicator of ISUP FCI is set to the default value of 'No Interworking Encountered'

Table 160 Default values of Forward Call Indicator[1]

ISUP Forward Call Indicator
National/International call indicator - Dependent on call type
End to end method indicator - No end to end method available
Interworking indicator - No Interworking encountered

Table 160 Default values of Forward Call Indicator[1]

ISUP Forward Call Indicator
End to end information indicator - No end to end information available
ISDN user part indicator- ISDN user part used all the way
ISDN user part preference indicator- ISDN user part preferred all the way
ISDN access indicator - Originating access ISDN
SCCP method indicator - No indication

1. The ISDNXFER option of table TRKGRP for terminating ISUP trunk is required to be present for the support of ISDN services, when the originating agency is a PRI trunk. Otherwise the PRA-ISUP call supports only the mandatory parameters and the FCI is sent as per the table below.

Table 161 Default values of Forward Call Indicator

ISUP Forward Call Indicator
National/International call indicator - Dependent on call type
End to end method indicator - No end to end method available
Interworking indicator - Interworking encountered
End to end information indicator - No end to end information available
ISDN user part indicator- ISDN user part not used all the way
ISDN user part preference indicator- ISDN user part not required
ISDN access indicator - Originating access non ISDN
SCCP method indicator - No indication

110: Functional Description (FN): A00003717

110.1 Feature name

A00003717 - CICM Flow Through Provisioning, CICM Component

110.2 Description

This document describes the CICM component of new SUCCESSION functionality, providing support for the flow through of line and user provisioning data between the SESM OSSGate provisioning interface and the CICM platform.

Prior to the CICM 7.10 and SUCCESSION SN07 product releases, any provisioning requests targeted at the CICM platform would have been duplicated in 2 separate locations, the SESM OSSGate interface and subsequently the CICM Element Manager, so increasing the complexity of the provisioning operation and correspondingly increasing the possibility of service mismatches occurring due to human error.

As this document is specific to the CICM functionality, it is recommended that it be read with the corresponding SESM documentation, to gain a full understanding - please refer to cross references [1] and [2] on page 1271.

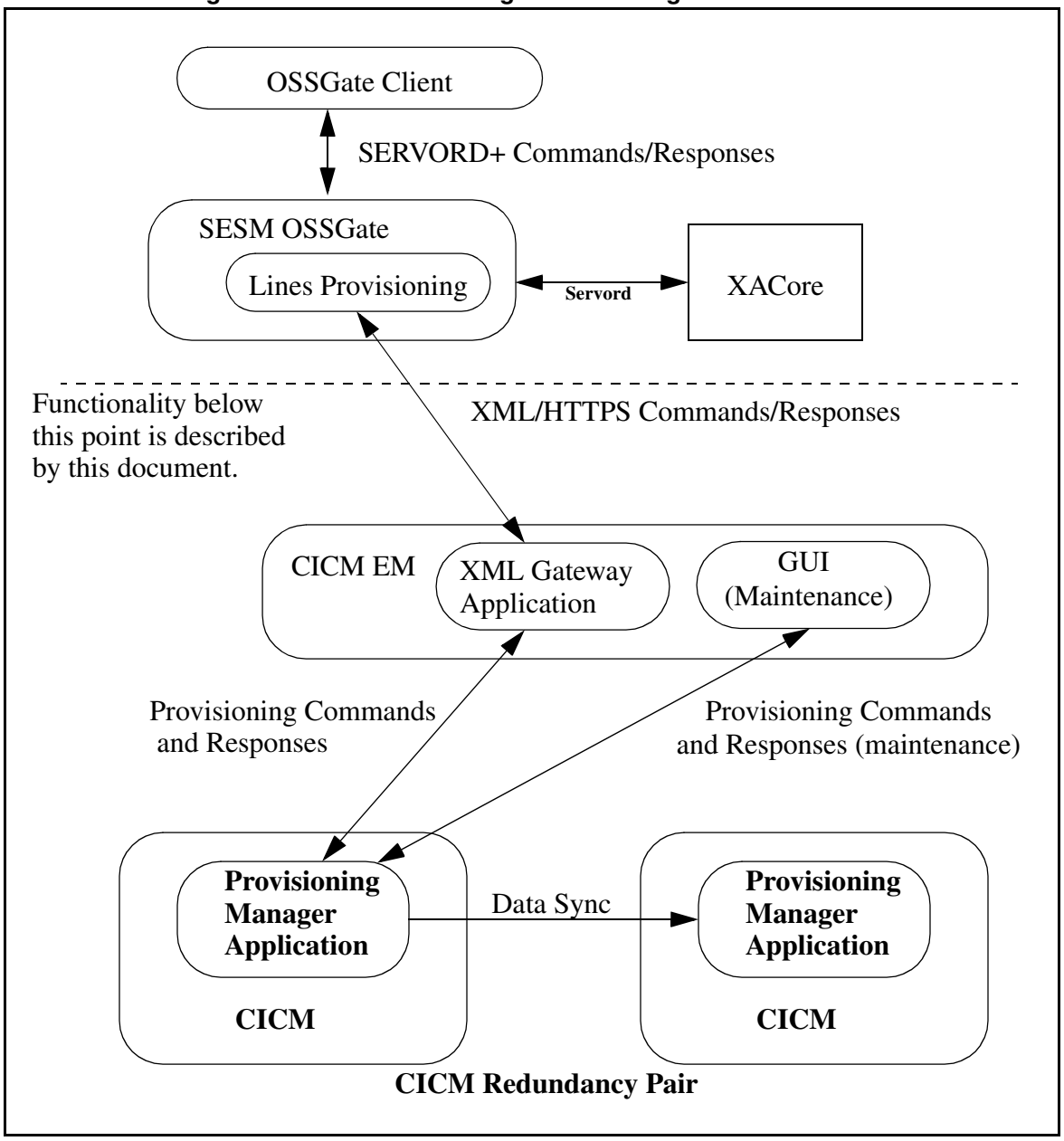
110.3 Document Change History

Table 1 Table Change History

Name	Modifications	Date	Issue
Peter Mitchell	First draft	10/02/2004	AA01
Peter Mitchell Richard Medhurst	Released prior to review	11/02/2004	AA02
Peter Mitchell Richard Medhurst	Incorporated review comments	11/03/2004	AA03
Richard Medhurst	Removed SDN feature Removed EffectiveFeatures Section. Added Undelete Section	17/03/2004	AA04
Richard Medhurst	Removed Undelete user pages from the GUI	22/04/2004	AA05

110.4 High Level Flow Through Provisioning Architecture

Figure 1 CICM Flow Through Provisioning For Succession



110.5 Support For Pre-Provisioned Lines

Changes will be made as part of this activity to support the introduction of pre-provisioned lines (feature key data). The modeling of feature key settings for the CICM lines is modified such that feature key settings are now stored against the line in question, as opposed to any user provisioned against that line. The modeling of lines at the SESM, CS2K and GWC components is also updated by related features to introduce pre-provisioned line support for CICM.

These changes have the following functional implications:

- Line data fill always in existence at the SESM, CS2K and GWC platforms.
- Feature key settings being stored against the line, will survive any operations resulting in the deletion or replacement of a user entity, so allowing. This allows the CICM to remain in sync with the equivalent data fill present at the CS2K.

110.6 Feature Key Parameter Support

As the flow through provisioning activity requires that feature key settings are setup from the SESM OSSGate interface, this activity will ensure parity of support with provided at the CS2K. These changes involve the addition of missing feature key types, and the enforcement of equivalent rules at the flow through provisioning interface as are present at the CS2K.

Prior to this release, when setting up feature key options the options would need to be provisioned in two separate locations. Firstly from the OSSGate interface to provision the feature keys on the CM, and secondly from the CICM EM to ensure that the appropriate CICM node is aware of the feature key settings. With the previous release only a subset of the possible feature key settings were made known to the CICM EM, even though they represent functionality legally supported by the CICM nodes. This anomaly would be worked around by setting the appropriate feature key to the “Unknown” state indicating the presence of an unmappable feature key setting.

The flow through provisioning feature requires that CM feature key settings map correctly to those supported by the CICM EM and CICM. Hence those feature key settings missing from the earlier releases are added as part of this feature to ensure parity. These new mappings are represented by Table 3 and Table 4. These do not represent new functionality, rather the correct modeling of existing functionality.

The following table describes the current feature key support. Where a CICM feature is shown with multiple SESM feature codes, this indicates multiple options applied against that key, with a single option being dominant from a CICM perspective.

Table 2 Feature Key Settings - Existing Pre-CICM 7.10 Mappings

CICM Feature Code	SESM Feature Code	Description
Unassigned		No feature assigned to key
CFU	CFU	Call Forward
MWT	MWT	Message Waiting
CXR	CXR	Transfer
RAG	RAG	Ring Again
SCL	SCL	Speed Call
PDN	PDN	Primary DN
QTD	QTD	Time and date
AGN	INCALLS + DN	ACD Incalls (handled as INCALLS key)
DN	DN	Directory Number
ACDMSB	MSB	ACD make set busy
3WC	3WC	3 way call
DCPK	DCPK	Directed call
ACDNR	ACDNR	ACD not ready
ACDEMR	EMR	ACD answer emergency
SPV	SUPR + DN	ACD incalls supervisor (handled as Supervisor key)
ACDCALLSUP	CLSUP + DN	ACD call supervisor
ACDEMRANS	AEMK + DN	ACD answer emergency
ACDAGNANS	AAK + DN	ACD answer agent
ACDAGNSTA	ASL	ACD agent status
ACDAGNOBS	OBS	ACD observe agent
C06	CNF	6 party conference
AUD	AUD	Auto dial
PRK	PRK	Non directed call
FXR	FXR	Fast transfer
CPU	CPU	Call pickup
ICM	ICM	Intercom (business sets)
CWT	CWT	Call waiting
QBS	QBS	Query busy station

Table 2 Feature Key Settings - Existing Pre-CICM 7.10 Mappings

CICM Feature Code	SESM Feature Code	Description
DASK	DASK	ACD display agent summary
DQS	DQS	ACD display queue status
DQT	DQT	ACD display queue threshold
FAA	FAA	ACD forced agent availability
CIF	CIF	ACD Controlled interflow
NGTSRVCE	NGTSRVCE	ACD supervisor control of night service
LOB	LOB	ACD line of business
CAG	CAG + DN	ACD call agent
CALLFORCE	FORCING	ACD Call Agent with Call Forcing

The following table describes the additional feature key support for this release (excluding ACD DN related functionality).

Table 3 Feature Key Settings - CICM 7.10 Mappings Extensions

CICM Feature Code	SESM Feature Code	Description
AAB	AAB	Automatic Answer Back
ACB	ACB	Automatic Callback
BLF	BLF	Busy lamp field
CCBS	CCBS	Call Completion To Busy Subscriber
CCV	CCV	Call Covering
COT	COT	Customer originated trace
CWD	CWD	Dial call waiting
EBO	EBO	Executive Busy Override
EMW	EMW	Executive message waiting
INSPECT	INSPECT	Calling Name Inspect Key
LVM	LVM	Leave message
MCH	MCH	Malicious call hold
MRFM	MRFM	Multiple Appearance DN Ring Forward
MSBI	MSBI	Make Set Busy Intragroup
MWIDC	MWIDC	Message Waiting Indication
MWQRY	MWQRY	Message waiting query
PRL	PRL	Privacy release

Table 3 Feature Key Settings - CICM 7.10 Mappings Extensions

CICM Feature Code	SESM Feature Code	Description
PRV	PRV	Privacy
SCS	SCS	Speed calling short list
SLQ	SLQ	Single line queuing
UCDLG	UCDLG	Uniform call distribution login
GIAC	GIAC	Group intercom all calls
GIC	GIC	Group intercom
QCK	QCK	Quick conference key
SUBCOM	SUBCOM	Sub community route for emergency calls

The following table indicates those feature codes being added to support ACD DN type functionality. It is possible for multiple feature key settings to be provisioned against a line, and these options may be added or removed individually from the OSSGate interface, however a single dominant feature is always assumed to take precedence from a CICM perspective. The subordinate states are encoded so that CICM may correctly move between feature key settings on the individual options being added or removed.

Table 4 Feature Key Settings - CICM 7.10 ACD DN Mapping Extensions

CICM Feature Code	SESM Feature Code	Description
SPVAGNDN	SUPR + INCALLS + DN	Supervisor key with subordinate INCALLS and DN options (Handled as Supervisor Key)
SPVAGNPDN	SUPR + INCALLS + PDN	Supervisor key with subordinate INCALLS and DN options (Handled as Supervisor key)
SPVPDN	SUPR + PDN	Supervisor key with subordinate PDN option (Handled as Supervisor key)
AGNPDN	INCALLS + PDN	Incalls key with subordinate PDN option (Handled as Incalls key)

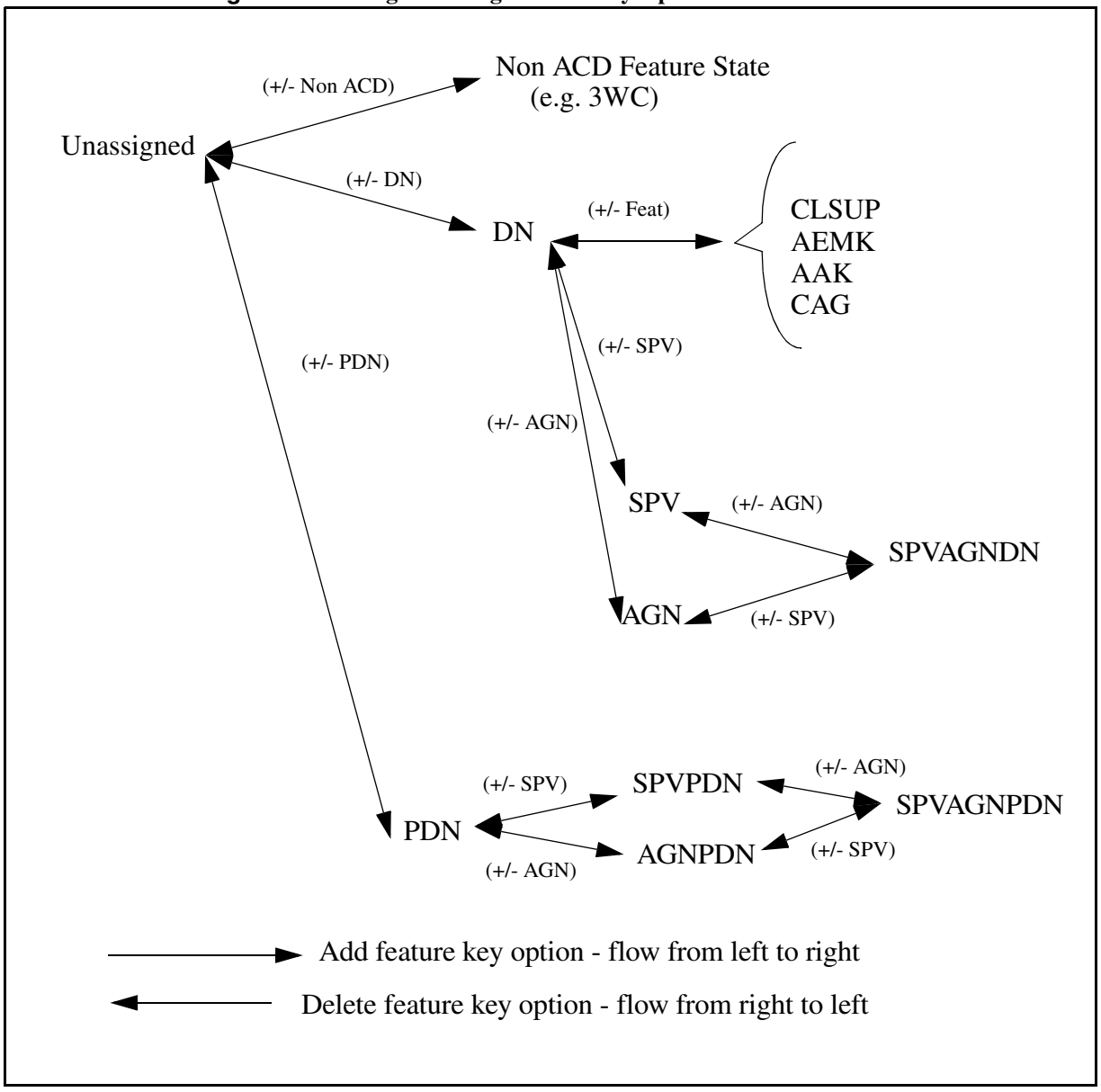
Note: Multiple SESM feature codes indicate that functionality is additive. Order of precedence runs from left to right, with that option listed first being dominant.

110.7 Flow Through Provisioning Interface Supported Operations

Flow Through Provisioning is driven on demand by SESM OSSGate. The usage of OSSGate is beyond the scope of this document, however what is documented in the following sections is a brief overview of the functionality provided on behalf of OSSGate. The relevant SESM documentation should be read to gain an understanding of how to drive that interface - see references [1] and [2] on page 1271.

The diagram shown in Figure 2 shows the valid transition states for adding and deleting feature key settings using the flow through addition and deletion functionality describes in sections 110.7.1 and 110.7.2.

Figure 2 Adding / Deleting Feature Key Options



110.7.1 Feature Key Setting Addition

Feature key settings may be added incrementally against a valid CICM line feature key. The CICM platform will enforce the same rules that the CS2K applies when validating requests to add a feature to a feature key - specifically the translation from the original state to the new state must be valid.

Generically with the exception of ACD functionality this requires a feature key to move from the unassigned state to a new valid state.

Feature key addition will occur as a result of a OSSGate NEW or ADO command line option for ACD type functionality.

110.7.2 Feature Key Setting Deletion

Feature key settings may be deleted consecutively from a valid CICM line feature key. Performing a deletion will remove that option from the key in question, resulting the key moving into a new valid state. Typically this involves the key moving to the unassigned state - or potentially in the case of ACD functionality, to a new valid ACD state.

Feature key deletion will occur as a result of an OSSGate DEO command line option for ACD type functionality.

110.7.3 Feature Key Setting Updating

Feature key settings may be updated or overridden. This forces the feature key into a new state directly, regardless of any feature key setting previously in place. This allows the SESM OSSGate to directly set a feature key without needing to understand its previous state, which would impose additional overhead on the provisioning operation.

Feature key updating will occur as a result of an OSSGate NEW, ADO, DEO or CHF type operation for non ACD type functionality.

110.7.4 Line Outage

Flow through provisioning allows for a line to be reset to its original unassigned state. This has the immediate affect of deleting any user present on that line, and removing any provisioned feature key settings. This would occur if an OUT operation is invoked from OSSGate.

110.7.5 M522 Feature Key Extension Box Updating

Flow through provisioning allows the number of M522 extension boxes provisioned against a CICM line to be manipulated from OSSGate - so ensuring that an identical number of extension boxes are provisioned at the CICM and the CS2K, within the range 0 - 2 extension boxes.

110.7.6 User Creation

Flow through provisioning allows for CICM Users to be created on demand by the OSSGate interface. The presence of a valid User is a pre-requisite for a CICM line to become active as the data fill associated with the user is required for login purposes.

110.7.7 User Deletion

Flow through provisioning allows for the deletion of CICM users on demand by the OSSGate interface. Deletion of a CICM User effectively disables the line associated with that User as it will no longer be possible to log in.

110.7.8 User Updating

Flow through provisioning allows for the manipulation of selected parameters associated with a User. The users Password and/or Profile settings may be manipulated at the request of SESM OSSGate.

110.8 Flow Through Provisioning Order Of Data Fill

For the CICM 7.10 release, line feature key data fill and user data fill have been decoupled in-order to support pre-provisioned lines.

There is no imposed ordering to the order of data fill - feature keys may be setup against a line prior to a User entity being created or vise versa.

As the User entity is created on demand, the User password or profile settings may not be set in advance of creation.

Feature key settings will survive any deletion of an existing User, so allowing a new User to adopt the assigned settings for the line in question.

It is not possible for a line to go in service prior to the creation of a User entity as no mechanism exists for a handset to login exists without a valid User to associate against.

110.9 Provisioning Data Rollback

Flow Through Provisioning request from SESM OSSGate impact many functional components. As an example the setting of a group of feature keys in response to a Servord ADO command, results in provisioning requests being sent to both CICM and the XACORE. The potential exists for a request to fail either partially or completely at either the CICM or the XACORE.

Upon a failure being reported to SESM, the line provisioning application will request that all successful operations be rolled back to the previous state. This helps to maintain data consistency between the various SUCCESSION components.

Should it prove impossible to successfully perform a rollback of the CICM, the CICM EM GUI may be used to perform any manual corrections that are required.

110.10 Security And Access To Flow Through Provisioning

Access to the Flow Through Provisioning interface requires the presence of HTTPS security certificates at both the SESM and the CICM EM platforms.

These security certificates will be provided as part of the installation procedure, however should it be desired to provide alternative certificates, this will be supported.

110.11 Backwards Compatibility

Due to data fill changes required to support pre-provisioned CICM lines, the SESM platform will only provide Flow Through provisioning support for CICMs of vintage 7.10 or later. Any provisioning operation impacting a CICM running the 6.12 release or earlier must therefore be provisioned separately at the OSSGate interface and then subsequently at the CICM EM. This is due to there being no linkage between the SESM box and the CICM XML Gateway application.

This restriction is based on the vintage of the CICM box and not the managing CICM EM box, therefore the same restrictions apply to an installation running CICM EM release 7.10 with subtended CICM 6.12.

No support will be provided by the SESM OSSGate interface for TDM CICM installations.

110.12 Upgrade Considerations

Data fill changes at the CS2K XACore make it difficult to automate an upgrade between CICM 6.12 and CICM 7.10. No upgrade mechanism is therefore provided. Upgrading should be by means of a migration of service from a CICM running release 6.12 and CICM 7.10

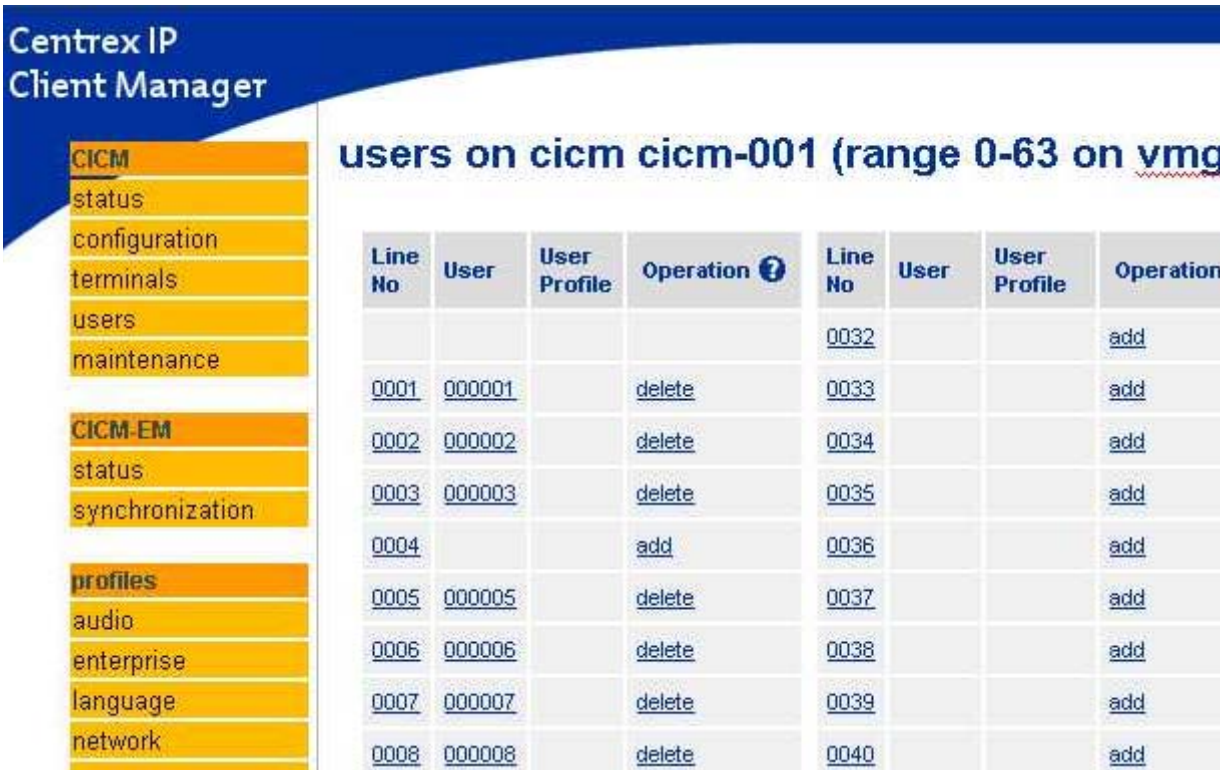
The CS2K XACore load will support existing CICM 6.12 nodes and new CICM 7.10 nodes. Migration of service from CICM 6.12 to CICM 7.10 will be via means of the upgrade procedure described by reference [4] on page 1272.

110.13 User interface changes to the CICM EM GUI

Flow through provisioning changes the location of the feature key data from being held against a user, to being held against a line. This results in changes to the EM pages when managing a 7.10 (of higher) CICM. These changes are detailed in this section.

110.13.1 Editing line feature data

The existing browse users page is modified to provide a link to edit the data associated with a line. Note the additional hyperlink under the “Line No” column



Clicking the hyperlink will load the page where the features can be corrected. In practise this page should not normally be used as the data should be provided by flow through provisioning. However should a mismatch occur, it can be corrected on this page.

110.13.2 Line Feature data entry page

On this page the user may enter the feature data filled against the Line.

110.13.3 Changes to the user and profile pages

The feature key data is no longer stored within the profile or user override portions of the MIB, these page have been altered such that the feature key cannot be set. Instead for a user override the feature key from the line data is displayed along with the user override information. This can be seen in the next diagram. For profile pages no feature key data is displayed.

110.14 Hardware Requirements or Dependencies

Hardware requirements as per a standard CICM installation. No special requirements exist for this functionality.

110.15 Software Requirements or Dependencies

Software must be aligned at the SN07 release at all SUCCESION components.

Specifically:

- CS2K XACORE - CS2M0007 FCS
- CS2K SESM - SESM_7 FCS
- GWC - GN070 FCS
- CICM EM - 7.10 FCS

- CICM - 7.10 FCS

110.16 Limitations and restrictions

The following functional restrictions are imposed by the SESM platform:

- No mechanism to audit the CICM data fill against the SESM and CS2K XACORE.
- No mechanism to query CICM specific data fill from the SESM OSSGate interface (QLEN, QDN and related query operations). However CICM line data can be queried from the CS2K XACore via OSSGate.
- Provisioning requests that require SESM interaction with the CS2K XACORE will not flow through to the CICM. For example the provisioning of Hunt Groups.
- No support for CICM Release 6.12 or earlier.
- No support for TDM CICM releases as this is a SUCCESSION only delivery.

Note: Lack of Hunt Group provisioning flow through may result in a feature key assignment mismatch for those lines forming part of a hunt group. As the CS2K XACore data fill will be correct, this will manifest itself as a labelling mismatch. The outcome of selecting a mismatched feature key will be correct. The CICM EM GUI may be used to correct any mismatches, should this be desired.

110.17 Interactions

Flow through provisioning will interact with the SESM CICM OSSGate interface. This will manifest itself as an extension to the functionality available from OSSGate.

110.18 Applicable customer facing sections

Fault Management

Logs	___N/A___
Alarms	___N/A___

Configuration

Data Schema	___N/A___
User Interface	___110.13__
Element Management	___N/A___
Security	___110.10___
Service Order	___N/A___

Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

110.19 Glossary

Term	Description
ACD	Call centre (administrative center) feature key functionality
ADO	Add Option (OSSGate / Servord)
CHF	Change Feature (OSSGate / Servord)
CICM	Centrex IP Client Manager
CICM EM	CICM Element Manager
CS2K	Nortel VoIP switch core (XACore)
DN	Directory Number
DEO	Delete Option (OSSGate / Servord)
FCS	Final Compile Ship
GWC	Gateway controller
HUNT Group	Grouping of 1 or more LENs / DNs into a functional group
LEN	Line Entity
NEW	Create new line (OSSGate / Servord)
OSSGate	SESM Northbound OSS interface for Line Provisioning
OUT	Remove line (OSSGate / Servord)
QDN	Query DN (OSSGate / Servord)
QLEN	Query Line Entity (OSSGate / Servord)
SERVORD	XACore line provisioning interface
SESM	Succession Element and Sub Element Manager
XACORE	Nortel switch core - CS2K

110.20 Cross References

[1] A00003717, Centrex IP Flow-Through Provisioning FN, SESM Component.

[2] A00001935, SESM Provisioning Support For Centrex IP Nodes And Lines

[3] A00003950, CICM Security Support

[4] CICM 6.12 To 7.10 Upgrade Procedure, David Tubb.

111: Functional Description (FN): A00003718-3719

111.1 Feature name

This document contains the functional description for the Alarms, Logs and Performance feature for the SN07 release of the Centrex IP Client Manager (CICM). The Actid for this feature is A00003718.

111.2 Description

Fault and performance management is an important component of any Network Element in Succession. The ability for operators to detect, monitor and correct erroneous behaviour and hardware outages is key to maintaining Quality of Service in a Succession network.

This feature will revisit the existing fault generation, logging and performance management capability of the CICM system. A new interface has been introduced to the Succession network that will manage the output used by external OSSs to monitor the network element and, for example, detect alarm conditions. This new interface is called the Integrated Element Manager System (IEMS). The IEMS can be accessed using a Graphical User Interface which will give access to the alarms and logs for a network element. This will also interact with the Element Manager GUI.

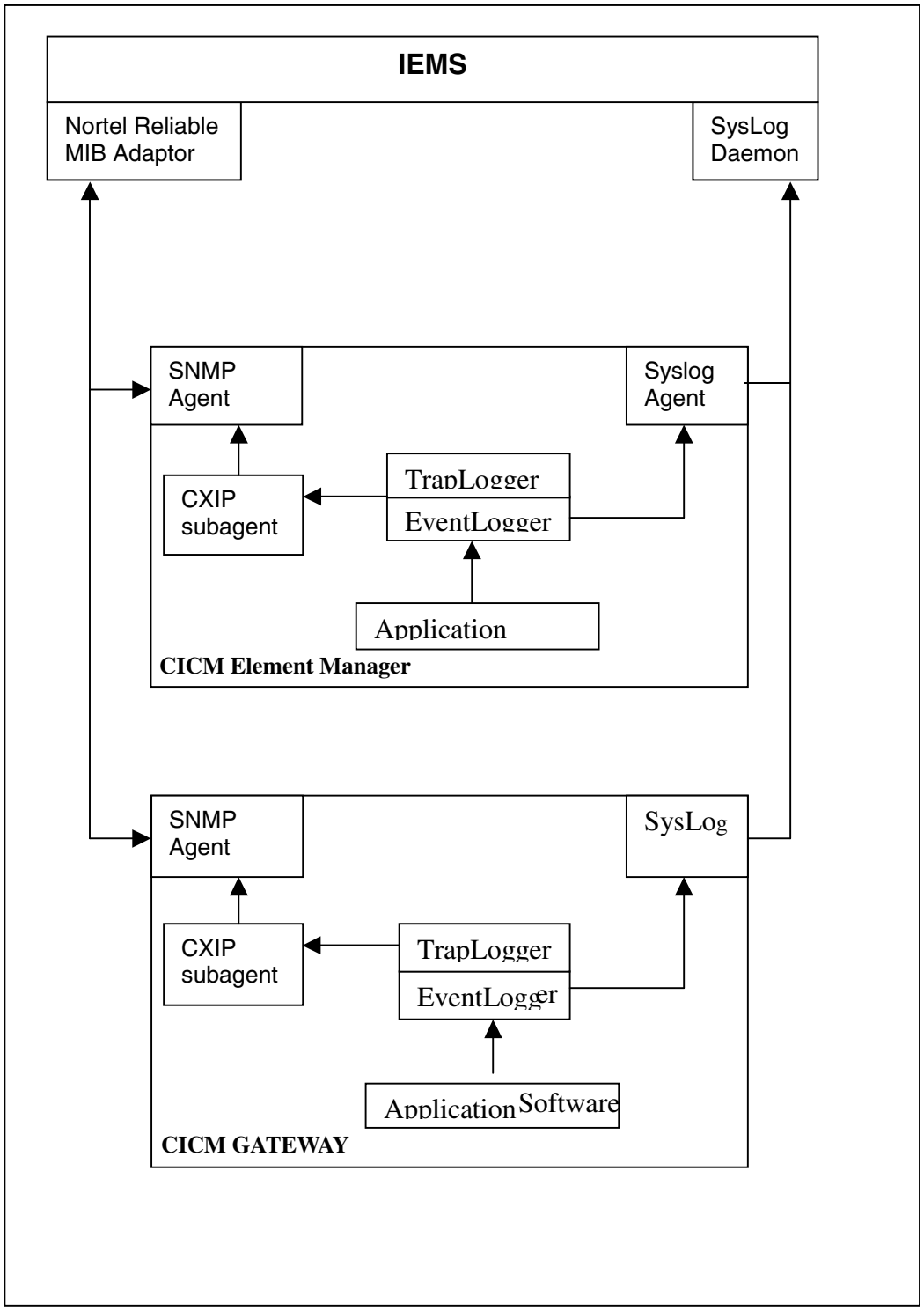
The CICM must integrate with the IEMS. Work needs to be done in this feature to raise alarms, logs and performance metrics in a suitable format that the IEMS can read.

There are two parts of the CICM system that can raise alarms and faults to the IEMS namely the CICM and the CICM Element Manager. The Element manager will raise alarms associated with the Element Manager Platform (e.g. memory shortage) and communication with the CICMs that it manages and will not have knowledge of the alarms and faults generated by the CICM. The CICM will send alarms as SNMP traps directly to the IEMS.

Logs are currently stored locally in debug and event Log files. Pertinent Event Logs must be sent to the OSS using Syslog formatted in the Custlog Format to aid debugging of alarms.

The following figure shows the overall intended system architecture for Faults and Logs.

Figure 1: CICM Fault Architecture

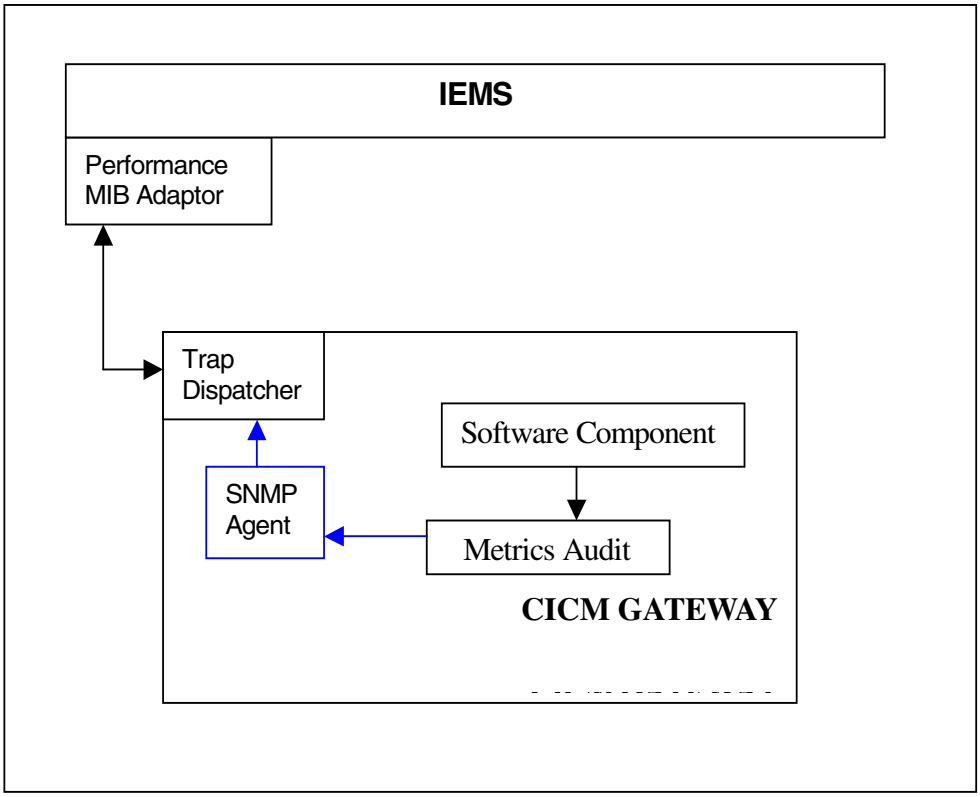


Performance management is a required part of any Succession system. A network element must be able to gather and provide statistical performance data to enable

customers to evaluate the system and gauge where improvements would be most beneficial.

Figure 2 shows the overall intended Architecture for the Performance system.

Figure 2: CICM Performance Architecture



It should be noted that there is no TDM support in this feature. Additional work will be required in order to support TDM within the new architecture. The nature of this extra work is to define and integrate the TDM specific cards into the architecture.

111.3Applicable customer facing sections

111.3.1 Alarms

All alarms are sent to the IEMS as an SNMP trap (to the Nortel Notifications MIB within the Nortel Reliable MIB, see “Nortel Notifications MIB” on page

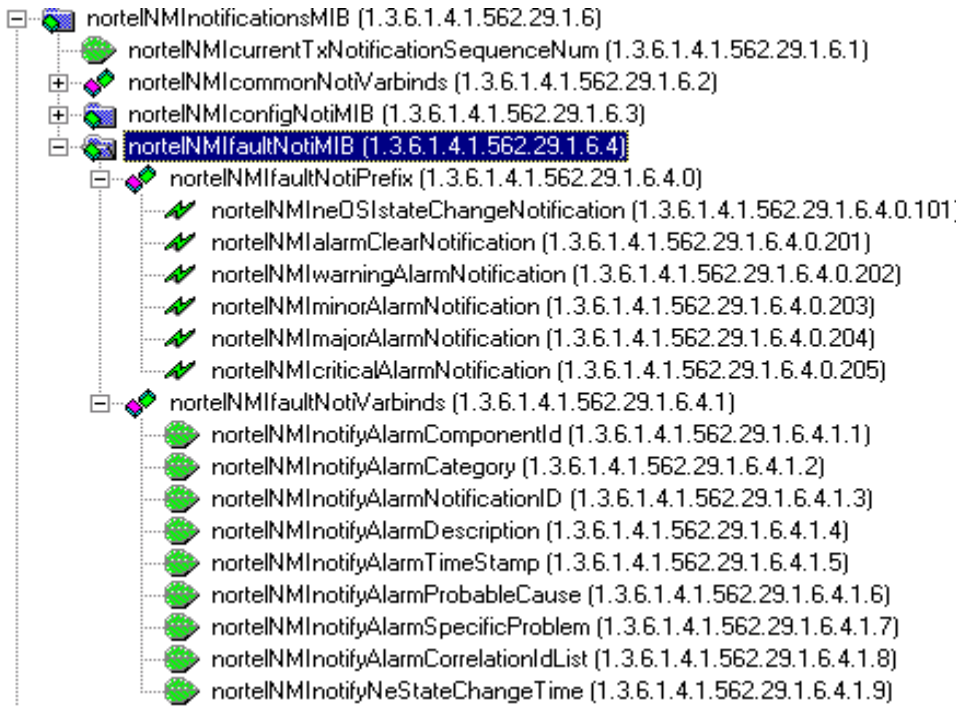
1277) and as a log (to SYSlog, see section “Syslog Details”). Each trap sent from the gateway will incorporate the following details:

- Sequence number.
- Severity indicator (see Table 1).
- Component ID – The distinguished name ID of the component in the Network element that the alarm was raised against (see section 0).
- Category – The category of the Alarm (communications, quality of service, processing error, equipment or environment).
- Notification ID – Unique ID generated from the process number and sequence number combined.
- Description – The description text of the particular alarm.
- Time Stamp – The time the alarm was raised in UTC time.
- Probable Cause – An enum representing one of the most likely causes of the fault as defined in ITU-T X733 & X736.
- Specific problem – A refinement of the probable cause.
- Correlation ID list – To link this alarm with previous alarms and effectively override (clear) those alarms.

Table 1 Alarm severity

	Critical	Major	Minor	Warning
Service Affecting	Yes	Yes	No (or few affected)	No
Action required	Yes	Yes	Yes	No
Recommended Timeliness of Action	Immediately – drop everything	Rapidly – in next work shift	Soon – could be delayed until next day	Later – investigate if reoccurrence
Target Reporting time	Within 2 Sec	Within 30 Sec	Within 2 Min	Within 5 Min

Nortel Notifications MIB



Please refer to the following table for a list of supported alarms.

Alarms

Object	Severity	probable cause
Element Manager		
Comunication failure with gateway Node	Major	44 - responseTimeExcessive
loss of connection with gateway Node	Major	42 - remoteNodeTransmissionError
Loss of communication with both Nodes	Major	44 - responseTimeExcessive
CICM node		
endpoint registration failure		46 - softwareError
max call threshold exceeded	Major	51 - threshold crossed
VMG GWC connection loss	Critical	42 - remoteNodeTransmissionError
VMG max call threshold exceeded	Major	51 - threshold crossed
VMG BHCA threshold exceeded	Major	51 - threshold crossed
network messaging threshold reached	Major	43 - resourceAtOrNearingCapacity
network max connections reached	Major	43 - resourceAtOrNearingCapacity
network transmission failure/ packet loss	Major	54 - transmitFailure
terminal SW update failure	Warning	115 - procedural error
terminal security problem	Minor	116 - UnathorisedAccessAttempt
terminal max no of connections reached	Major	51 - threshold crossed
Platform		
connectivity (Pam) failure	Major	42 - remoteNodeTransmissionError
mate node communication loss	Major	44 - responseTimeExcessive
mate node connection loss	Major	42 - remoteNodeTransmissionError
SW version mismatch between nodes	Minor	57 - version mismatch
Syslog communication failure	Major	6 - communicationsSubsystemFailure
network connection not responding	Critical	6 - communicationsSubsystemFailure
chassis fan failure	Major	21 - heatingorventilationorcoolingsyster
chassis PSU failure	Major	35 - power problem
sw upgrade failure	Minor	115 - procedural error
software component failure	Critical	2 - ApplicationSubSytemFailure
sam 21 version mismatch	Minor	57 - version mismatch
card OOS	Critical	114 - out ofService
Link OOS	Major	114 - Out of Service
host resources fault	Major	43 - resourceAtOrNearingCapacity
Configuration database read/write failure	Critical	46 - softwareError

111.3.2 Component ID's

The CICM is divided into three objects for the purpose of reporting alarms, the CICM element manager, a CICM node and the platform which the EM and the CICM use. These objects contain sub-objects which appended together with the alarm type to form the Component Id.

Table 3: Component ID's

Object	Sub Object	Component Id
CICM element manager	Node (CICM)	CICM=<CICM ID>;NODETYPE=cicmEm
CICM node	Terminal	CICM=<Cicm ID>;Nodetype=Cicm;Component=Terminals;terminal=<terminal ID>
	Cards	CICM=<Cicm ID>;Nodetype=Platform;Component=Card;Card=<card id>
CICM platform	Software Component	CICM=<Cicm ID>;Nodetype=Platform;SoftwareComponent=<component id >

111.3.2.1 Alarm Examples

Major Alarm Notification on Node A:
Component Id: CICM=CICM100A; Nodetype=CICM;User=000001
Category: 1 (communications)
Notification ID: 2
Description: Password Lockout
Probable cause: 101 (authentication Failure)
Specific Problem: user <userID> exceeded failed attempt threshold.
CorrelationId list: (list of alarms relating to other login attempt failures.)

Critical Alarm Notification on node B:
Component Id: CICM=CICM100B;Nodetype=Cicm;Component=chassis
Category: 4 (equipment)
Notification ID: 34
Description: Fan Overheating
Probable cause:21– heatingOrCoolingOrVentilationProblem
Specific Problem:
CorrelationId list: (none)

Minor Alarm Notification on Node B:
Component Id:
Cicm=CICM100B;Nodetype=Cicm;Component=Card;CARD=<card number>
Category: 1 (communications)
Notification ID: 45
Description: Link OOS
Probable cause: 114 (out of Service)
Specific Problem:

CorrelationId list: (none)

Major Alarm Notification on node B:
Component Id: Cicm=CICM100B;Nodetype=Cicm;Component=CARD
Category: 1 (communications)
Notification ID: nnnn:nnnn
Description: Link group alarm - too many links OOS.
Probable cause: 51 (threshold exceeded)
Specific Problem:
CorrelationId list: (list of individual Link OOS alarms)

111.3.2.2 Alarm Throttling

The IEMS can receive logs at a maximum overall network rate. The CICM alarm generation rate must therefore keep within certain bounds in order to not exceed that IEMS rate. To solve this a throttling capability is required.

The alarm manager will meet this requirement by having separate buffers for each severity of alarm. This will enable the critical alarms to be sent immediately and for major, minor and warning alarms to be prioritized in order that they are sent within the required time periods as specified in “Alarm severity” on page 1276, but at a controllable rate. The rate of alarms being raised should be configured in the CICM registry MIB.

111.3.2.3 Alarm Provisioning

The CICM must be provisioned with the data it requires to determine whether it is to send traps and logs to an IEMS. A number of provisioning steps have been added to the preboot provoisioning sequence to allow this. These steps are executed when the CICM load is first installed.
The following questions are asked relating to Alarms:

A prompt is made for an SNMP V1 and/or an SNMP V2c Trap destination as before:
Next, specify the IP addresses of the SNMP management stations that should receive traps and (alarm) notifications from this system.
Enter [list of] SNMP V1 Trap receiver address[es]:
>
Enter [list of] SNMP V2C Notification receiver address[es]:
>

If an IEMS is to be used the ip address of the IEMS should be provisioned in one of the above.

The next question confirms whether the IEMS is to be used.

Are the Above IP addresses IEMS Destinations? [Y\N, default=Y]
>

The next question asks about the Log destination. There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage. Invalid IP addresses including 0.0.0.0 and 255.255.255.255 will not be allowed.

111.4 Logs

This section describes the changes in logging functionality for both the CICM and the CICM element manager. Both the element manager and the CICM will be responsible for sending its own logs to the IEMS. Logs will not be exchanged between the CICM and element manager. The desired behavior for Logs is that they are sent to the IEMS using CUSTLOG or security log formats via a syslog agent. Three log streams will be used to send logs to up to three different syslog daemons (i.e. IEMS). This is an enhancement of the current functionality where all logs are stored on the CICM. Logs will still be stored on the CICM and the CICM will, in addition, send logs to custlog, audit log and security log streams. Each log must be formatted correctly for that particular stream.

The CICM will produce logs in the custlog or security log formats. This information will then be stored in the IEMS.

For this section the term CICM applies to both the CICM network element and the CICM element manager.

111.4.1 Syslog Details

The CICM will use the syslog protocol to send the logs to the IEMS. The CICM and CICM element manager will both act as senders. They will only be able to create and send syslog messages, they will not be able to receive or relay syslog messages. The CICM will conform to RFC 3164 The BSD syslog protocol [1].

As with most syslog applications UDP port 514 (the syslog port) will be used to send the syslog messages to the IEMS. The total length of the entire packet must not be greater than 1024 bytes. The CICM will not create a log that will exceed this limit.

To successfully send syslog packets to the IEMS the CICM needs to correctly format a syslog packet. The syslog packet can be split into three parts. The first, named the PRI is a number that contains the syslog facility and severity. This number is enclosed in less than and greater than symbols < >.

The syslog facility is used to identify which process is responsible for raising the log. Below are two tables which show the facility and severity values that will be used by the CICM.

Table 4: List of possible syslog facilities.

Code	Facility	Log Stream
0	kernel messages	
1	user-level messages	
2	mail system	
3	system daemons	
4	security/authorization messages	
5	messages generated internally by syslogd	
6	line printer subsystem	
7	network news subsystem	
8	UUCP subsystem	
9	clock daemon	
10	security/authorization messages	
11	FTP daemon	
12	NTP subsystem	
13	log audit	
14	log alert	
15	clock daemon	
16	Local use 0	
17	Local use 1	Custlog
18	Local use 2	
19	Local use 3	Audit log
20	Local use 4	
21	Local use 5	
22	Local use 6	Security log

Table 5: Syslog packet severities

Code	Severity	Mapping custlog values
0	Emergency: system is unusable	
1	Alert: action must be taken immediately	Critical
2	Critical: critical conditions	Major
3	Error: error conditions	Minor
4	Warning: warning conditions	Minor
5	Notice: normal but significant condition	No alarm
6	Information	
7	Debug	

All logs sent to the IEMS must have a severity of 5 – Notice to enable the IEMS to differentiate between the logs and alarms.

The facility and severity fields will be used by the IEMS or another SYSlog daemon to sort the different logs into different problem areas and to highlight significant issues quickly.

The remainder of the syslog message is the MSG part. The MSG part has two fields known as the TAG field and the CONTENT field. The value in the TAG field will be the name of the program which generated the message, i.e. CICM. The CONTENT field contains the log in one of the supported formats, please see below.

Example of a syslog PRI and header.

```
<34>Oct 11 22:14:15 47.34.234.1 XX: Log contents
       PRI  Timestamp         Host IP       process
```

The CICM will send log file header information after a system restart or whenever connection is opened the IEMS.

111.4.1.1Syslog failure.

If the CICM detects that a log stream has collapsed for any reason a SNMP trap will be sent to the IEMS. If the CICM cannot send any logs they will be buffered up to a point until the stream is operational. Please see section on throttling for details of buffer restrictions. If a problem occurs with the IEMS the CICM will not detect this and continue to send logs. These logs may become lost. The CICM will still store a local copy, which can be accessed via the CICM element manager. The CICM offers no guarantee that the log will be seen by the IEMS.

111.4.2Custlog details

The CICM will log the following events using the custlog format and output the logs to the custlog stream.

- Service affecting state changes
- Specific customer/blm requested events
- Data corruptions/data mismatches

The custlog will contain the following information:

Node id is the name of the network element reporting the log. In this case it will be the name of the CICM gateway or element manager, e.g. CICM-100.

Hostname is the name or IP address of the element reporting the problem. In this case it will be the name of the side of active gateway or element manager, e.g. CICM100A

Application name is the type of network element reporting the log. In this case CICM.

Sequence number is a number applied each time the log is outpulsed. It is incremented by one for each log sent out on a particular stream. It is this mechanism that allows the IEMS to detect if it has missed a log. Valid sequence numbers are from 0 to 999. When 999 has been reached the number will be reset.

Report Name is a 4 char string representing the application that the log is being generated for (not the application doing the logging), e.g. CICM

ReportNum is a 3-digit number which ranges specify certain log categories.

Applications that generate new log reports must use the following log numbering scheme. Do not use the range 100-299 unless the log category does not fit into one of the standard categories.

Table 6: Log Categories

Log Category Log	Number Range:
Trouble	300 to 399
Service summary	400 to 499
State Change	500 to 599
Information	600 to 799
Threshold	800 to 899
Expert	900 to 999

Alarm Value is one of: NONE, WARNING, MINOR, MAJOR, CRITICAL All logs will have the value of NONE.

Event Type is one of: CBSY, EXC, FAIL, FLT, INFO, INIT, LO, MANB, OFFL, PASS, PBSY, RTS, SUMM, SYSB, TBL, TRAN, TRAP, UNEQ, THR

Label is a string indicating the type of the log (perhaps identifying a subsystem) Label must not be “instance specific” – i.e. it is the same for all occurrences of log, e.g. Login failure

TextFormat is a string detailing the log information – can be no longer than 860 chars. The following subfields are included in the test format:-

Location is the identifier of the machine sending the log.
Time is the time the error occurred.
ComponentID is an identifer of the system component that is sending the log. For more details see the alarm section.
Description is used to further describe the problem.

Required Syslog message format

May 24 00:02:00 rtpssdm oamp:
| Date, time, hostname, & Application generated by Syslog|

_V2_~I=CICM-130~H=CICM-130A~A=CICM~S=0001~~
| *Node id* || Host Name || Application ||Sequence Number|

CICM 675 NONE INFO SDM OM FILE RETENTION
| Report name|| report no || alarm value ||Event Type ||_____Label_____|

Breakdown of text format sub components.

Location: CICM-130-A^M
| Location |

Time: Fri Jun 04 17:18:56 2004^M
| Time |

ComponentID: CICM=CICM-130-A;NodeType=Cicm;Component=Card;Card=7^M
| Component ID |

Description: terminal id:7 Card 7 is INSV.
| Description |

For further details on field ranges and log reporting guidelines see Appendix A of the DID or http://sdm.ca.nortel.com/vr23/resources/iempg.af05.pdf

The logs should be indented by 8 characters and should be a maximum of 1000 characters. Every log should end with the ^M character.

111.4.3 Security log details

The CICM will log the following events using the security log format and output the logs to the security log stream.

- Unsuccessful terminal logins
- Successful terminal logins
- Unsuccessful PAM authentication
- Successful PAM authentication

Security logs will begin with a field identifying the class of log. For security this field value is class_security.vers01.

A security log will contain the following information. Other optional fields are supported by the log format but are not used by the CICM in this feature.

DST This is the address of the destination, e.g. the IEMS

DOC The document (DOC) field is the name of an accessed resource, e.g. CICM100A.

STAT The STAT field describes the state or status of the designed process. Possible values for this field may include “Failure”, “Success”, “Start”, “End”.

MID The Message Identifier allows message text to change, for translation to other language or to fix a typo, without affecting analysis tools. Another benefit of this would be saving bandwidth by not having to send the message itself. The value MUST be a unique string. The MID values would be stored at each sender, and the actual message templates would be stored at the collectors. This means that each sender (product) must submit to the collector/ analyzer, message template files defining its’ MIDs. Separate template files would be required for each language. The collectors would need to be configured to a certain language. The format of these message template files is defined in Ref 3 Section 3.2, “MID Message Template Format”.

This field is currently not supported by the CICM or the IEMS. A value of 0 will be used.

SRC.OFFENDThe offending source field is the address of the originating packet, which triggered a security audit event. For this feature it will be the IP address of the CICM. If omitted it implies it is the same as the source address.

Optional fields
SRC.USR User name or user id.

EVNT.TYPE The event type field specifies the type or classification of the event, e.g. login.

HOST The name of the host issuing the log.

CMD This field is used to supply a little more information on the security breach. For example in the case of a terminal login failure the field will include the terminal ID and the login the person used.

111.4.4 Audit logs

The following actions will be logged to the audit stream:

- Addition or removal of CICMs from a CICM EM.
- Addition or removal of a profile from either a CICM or a CICM EM (controlled from the EM web pages).
- Any action using flow through provisioning e.g adding/deleting a user.

The audit logs will be in the same format as the security logs.

111.4.4.1 Debug log

Debug logs are logs that are not of interest to Nortel customers, e.g. swerrs should be classed as a debug log. No work will be done to enhance the debug logs. Currently debug logs are viewed via the CICM EM. Debug logs will not be sent via syslog to the IEMS. Any log or notification that is sent to the IEMS will be copied into the debug stream.

111.4.5 Log Throttling

There is an overall maximum rate that the IEMS can receive logs. The CICM logging device will contribute to that overall log rate; so it must therefore keep within certain bounds in order to meet that IEMS rate. To solve this problem a throttling capability is needed. The customer should be able to set the number of logs that can be sent over a specified time frame. When the rate of logs being produced exceeds the threshold the remaining logs will be buffered until a time when they can be sent. If logs are being buffered for an extended period of time it will be possible to fill the buffer. In this scenario logs will be lost. Each log stream will have its own log buffer.

Debug logs will not be throttled as they are simply output to a file and not transmitted to the IEMS. A copy all logs and notifications will be sent to the debug stream even though they may have been buffered and lost. Therefore it should always be possible to get copies of lost logs or notifications.

111.4.6 Log Viewing

The logs which are stored on the CICM will be viewable from a page on the CICM EM. The EM will request the log files from the CICM and display them using a web page. This functionality is not part of this activity.

111.4.7 Log Provisioning

The CICM must be provisioned with the data it requires to determine whether it is to send traps and logs to an IEMS. A number of provisioning steps have been added to the preboot provoisioning sequence to allow this. These steps are executed when the CICM load is first installed.
The following questions are asked for provisioning Logs:
This step follows on from the provisioning of trap information.

The following questions are asked:

Are Logs to be sent to Syslog stream destinations? [Y\N, default=N]
>

Next the ipaddresses of the three syslog destinations are required, A prompt is made for CustomerLog, SecurityLog and Audit Log destinations in turn.

Next, specify the IP addresses of the Syslog management stations that should receive Customer, Security and Audit logs from this system. Enter each IP addresses in dotted form.:

Enter the network address of the Syslog destination for Custlogs:
>

Enter the network address of the Syslog destination for Security Logs:
>

Enter the network address of the Syslog destination for Audit Logs:
>

This Question is followed by the Performance provisioning Step (see Section 2.5.3.1). There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage. Invalid IP addresses including 0.0.0.0 and 255.255.255.255 will not be allowed.

111.5 Performance

Performance management is an important component of any Network Element in Succession.

A network element must be able to gather and provide statistical performance data to enable third parties to evaluate the system and gauge where improvements would be most beneficial. The ability for operators to monitor behaviour and trends is key to maintaining Quality of Service in a Succession network.

This feature will revisit the existing performance management capability of the CICM system. A new interface has been introduced to the Succession network that will manage the output used by external OSSs to monitor CICM network elements. This new interface is called the Integrated Element Manager System (IEMS).

The CICM and CICM-EM network elements must integrate with the IEMS. Work will be done in this feature to make available performance metrics in a suitable format that the IEMS can read.

Currently a number of performance metrics are gathered in the CICM System and are logged and recorded.

The Performance metrics currently gathered are:

- Percentage Memory usage
- Number of Active Users
- Number of Active connections
- Percentage CPU Usage

Additional metrics that will be gathered include the following:

- Number of Busy hour call attempts
- Number of logged in users
- Number of Logs sent.
- Transmitted bytes/sec
- Received bytes/sec.

Each of these metrics will be collected, averaged over a specific time interval and stored in the MIB.

Within the CICM software an audit function will collect each metric after a specified time interval has elapsed.

Some measurements (those relating to call traffic) will be taken every 5 minutes. Other measurements will be collected and averaged over either 15 or 30 minute intervals. There are no 5 minute interval metrics planned in the CICM. The 15 or 30 minute interval will be configured in the registry MIB. On installation of a new load the user will be prompted to select either 15 or 30 minute data for all metrics, given the number of metrics provided this will be the only method of configuration. The interval selected will apply to all metrics.

The metrics will be stored in the performance MIB and will be collected at intervals by the IEMS.

111.5.1 Performance Metric Provisioning

The CICM must be provisioned with the data it requires to determine the interval over which performance metrics are to be collected. A provisioning step has been added to the preboot provoisioning sequence to allow this. This step are executed when the CICM load is first installed.
The following question is asked for provisioning performance metrics:
This step follows on from the provisioning of log information.

The following question is asked:

Enter the time interval over which performance metrics will be measured [15/30]:
>

There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage.

111.6 Data schema (DS)

A new MIB has been created as the key for this feature. There is a CICM MIB which makes performance data available to registered Trap listeners. This interface will be unaffected in the SN07 release. The performance data will still be made available via the existing interface for TDM implementations.

The new MIB interface has been created to integrate with the concept of a Nortel standard Performance MIB. The performance MIB has a number of fields for each performance Metric as follows:

- index - unique numeric key for each metric on a CICM basis
- metric name – text describing the name of the metric
- metric value type (counter or gauge)
- metric range - max & min

- metric gauge usage (average or peak)
- metric value holding registers (4 registers)
- metric current value - or
- metric current value OID - if the current value is kept in another MIB.

At the time of writing the MIB interface definition has not been completed, but will be finished in time for this development.

111.7 Hardware Requirements or Dependencies

The following is a list of the minimum hardware required for this feature:

- One CS2K
- One GWC with a CICM profile
- One CICM-EM
- One CICM
- CICM Ethersets
- One IEMS platform

111.8 Software Requirements or Dependencies

Integrated Element Manager System (IEMS) Software is the recommended tool to be used in order to be able to access the output of this feature (loadname and firmware load).

111.9 Limitations and restrictions

The CICM will not guarantee that the IEMS will receive and logs or traps that it sent.

Each CICM can only datafill three log streams. It is possible to create a stream to three different IEMS.

This feature does not support TDM platforms for this release. Only the succession platform is supported. The existing TDM implementation will function as before however this feature is not intended for a TDM release and the necessary TDM components are not supported.

Changing the severity of an alarm, once set, is not supported.

111.10 Interactions

111.11 Glossary

Term	Description
CICM	CentrexIP Client Manager
CICM EM	CentrexIP Client Element manager
MIB	Managed information Base
VoIP	Voice over IP
XPM	eXtended Peripheral Module

111.12 References

[1] The BSD syslog Protocol RFC 3164
[2] Log Strategy for non-core Succession NEs v4.8
[3] OA&M Security Audit Log Format SRD Issue 1.1.doc

112: Functional Description (FN): A00003720

112.1 Feature name

Compact Call Server Hybrid Asynchronous Transfer Mode Processor Mezzanine Card Replacement

112.2 Description

This feature is to add support for the new ATM PMC hardware for the Hybrid Compact Call Server, as the old PMC is no longer being fabricated.

There are no customer-visible changes in the operation of the new hardware.

112.3 Hardware Requirements or Dependencies

This feature adds support for the Interphase 4576 ATM PMC to the Compact Call Server hybrid.

With this feature, the MC cards in the hybrid solution will support either a pair of IDT 77252 cards, or a pair of Interphase 4576 cards. Mixed configurations (i.e. where the two ATM PMC cards are not identical) are not supported and the mcblade will not boot.

The MC card with the IDT PMC from Motorola corresponds to a PEC code of NTRX51GY (this includes the base card and the two PMCs).

For the IDT PMC only the PEC code is A0998974

The MC card with the new Interphase PMC from corresponds to PEC code NTRX51HY (including the base card and the two PMCs).

The Interphase PMC by itself is PEC code A0539541.

112.4 Software Requirements or Dependencies

To run the MC cards with the Interphase PMCs, the MC load from SN07 or later must be loaded on the SDM and used by the MC cards.

112.5 Limitations and restrictions

ATM PMC cards of different models may not be placed on the same MC card.

112.6 Interactions

No customer-visible interactions with existing features.

112.7 Applicable customer facing sections

Fault Management

- Logs _n/a_____
- Alarms __n/a_____

Configuration

- Data Schema ___n/a____
- User Interface __n/a_____
- Element Management _n/a_____
- Security _n/a_____
- Service Order __n/a_____
- Office Parameters __n/a_____

Accounting (includes AMA billing) __n/a_____

Performance (includes operational measurements) _n/a_____

112.8 Glossary

Term	Description
New term	Definition
ATM	Asynchronous Transfer Mode
PMC	Processor Mezzanine Card
MC	Message Controller

113: Functional Description (FN): A00003767

113.1 Feature name

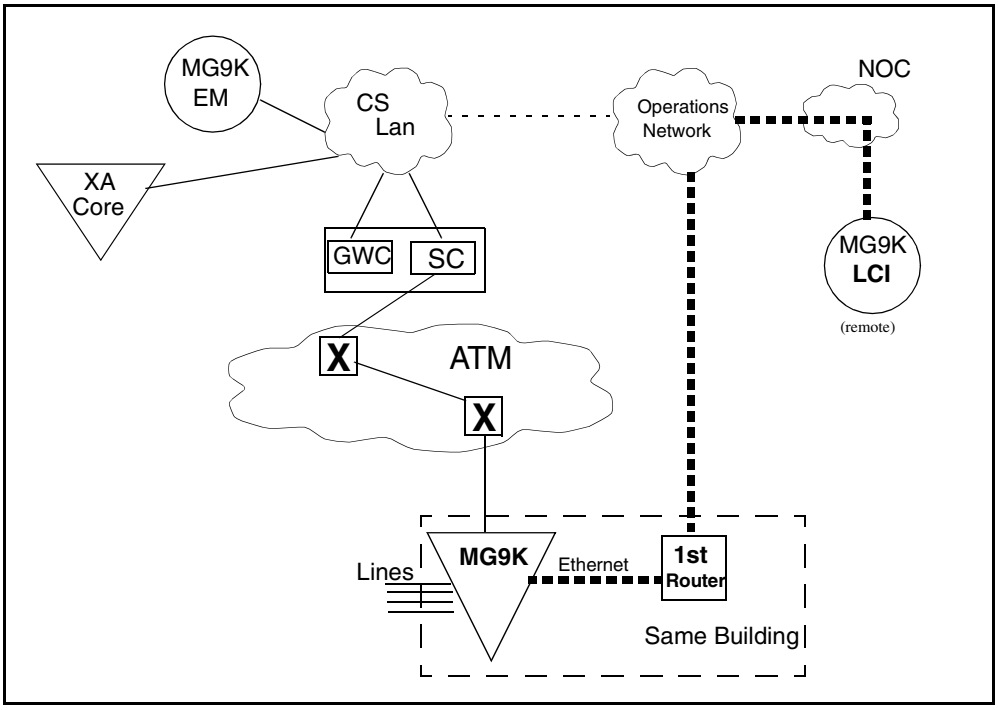
A00003737: LCI Remote Access, Enhancements and MG9000 Security

113.2 Description

Feature A00003737 supplys the MG9K customer with a means for querying the ESA state and the SNMP alarm log history for a node that has lost Element Manager connectivity. The Element Manager remains as the master interface for maintaining the MG9000, with this newly added backup functionality being made available from the Local Craft Interface
The customer requested remote access to the MG9000 LCI. Feature A00003737 provides this new functionality by allowing the ethernet addresses on the DCC cards to be provisionable. Thus, if they choose to support remote access, integrating the newly assigned address into their operations network.

As a result of adding remote access, interfaces (FTP, Telnet, Web Access) into the MG9k need to be secured using the Secure Sockets Layer.

The diagram below provides a simplified overview highlighting the location of the MG9k and its access points (atm/ethernet) within the Succession network.



113.3 Hardware Requirements or Dependencies

NA

113.4 Software Requirements or Dependencies

FTP, used for collecting Operational Measurement files and pushing down provisioning data for configuring ESA, has been replaced with Secure Shell FTP (SSH FTP). Any FTP requests into the MG9K will be required to use a Secure FTP client that supports the behavior as described by the IETF document “SSH File Transfer Protocol.”

Currently the webserver running on the controller cards (DCC), uses HTTP (not secure) for the trasmission of web content between the MG and a web client. Instead of HTTP, HTTPS will be used. This is the secure and encrypted transmission of the web content between the user’s client and the webserver (DCC). The Local Craft Interface will use this protocol for all of it’s actions (commissioning, debug, password maintenance, dual homing management, ESA status’). All MG9K supported web browsers already include support for HTTPS - no customer change required.

FOR GNPS (support) ONLY:

Remote Telnet access has been disabled as a result of the Security portion of this feature. Instead, support groups are to use a Secure Shell client for accessing Dsh. SSH works (from a users stand point) just like telnet. Run the SSH client command at the prompt on a computer that is connected to the same network as the node you are trying to access. All client-server communication is encrypted. Previously telnet allowed anonymous user access; SSH requires userid and password authentication. This is either the default password all MG9000 loads are shipped with, or a customer provisioned password. Once a user has ssh'd into the DCC card, they can telnet internally just as before. Also, SSH clients automatically try to connect to port 22 (default ssh port). The MG9K ssh server is running on port 24. This must be specified by the user of the client. Example (using openSSH client): ssh -l admin -p 24 47.1.1.1

Here we are attempting to ssh to "47.1.1.1" to port 24 as user "admin".

113.5 Limitations and restrictions

No new limitations/restrictions other than the secure client usage mentioned throughout the document.

113.6 Interactions

In previous releases, FTP and LCI communication was not secure. Now, using SSL, these data transmissions are secured. Regardless, the customer interface's look and feel remain unchanged. Required additional user-machine interactions are described in the subsequent sections.

113.7 Applicable customer facing sections

Fault Management	
Logs	___NA___
Alarms	___NA__
Configuration	
Data Schema	___NA___
User Interface	___NA___
Element Management	___X___
Security	___X___
Service Order	___NA___
Office Parameters	___NA___
Accounting (includes AMA billing)	__NA____

Performance (includes operational measurements) __NA____

113.8 Glossary

Term	Description
SSL	Secure Socket Layer
HTTPS	Hypertext Transfer Protocol Secured
SSH	Secure Shell -an open protocol for securing network communications
SSH FTP	SSH File Transfer protocol - secured file transfers

114: Functional Description (FN): A00003767

114.1 Feature name

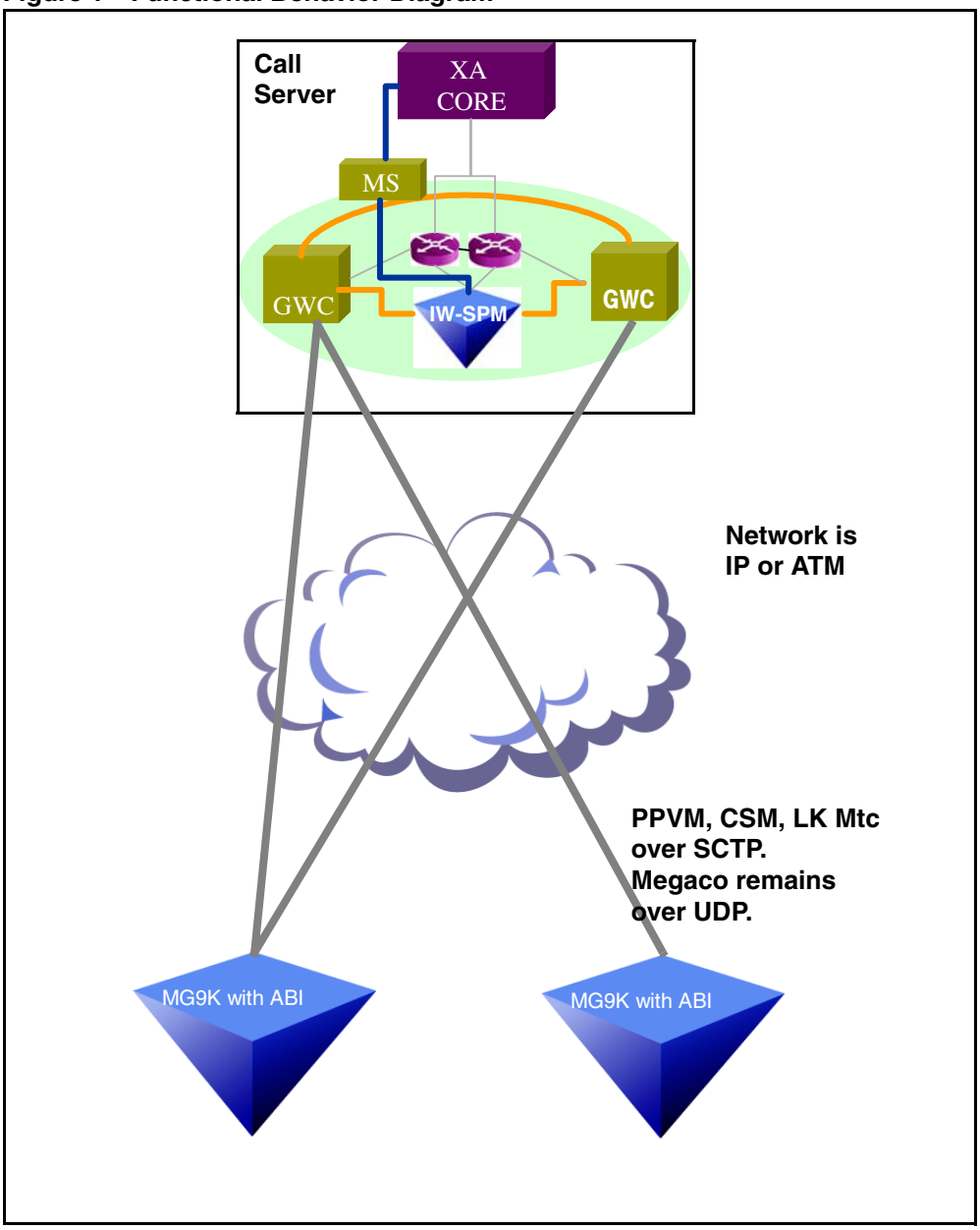
IP ABI PPVM Robustness & Msg Loss Alarms.

This feature would be better named “SCTP for ABI messaging”

114.2 Description

This activity introduces SCTP (Stream Control Transmission Protocol) for messaging transport between a Succession GWC (gateway controller) and MG9K ABI (DS-512) cards. SCTP is used for three of the Nortel proprietary protocols: PPVM (XPM supervision), CSM (Channel Supervision Message), and DS-512 link maintenance.

Figure 1 Functional Behavior Diagram



SCTP is introduced here to provide the customer with a more reliable messaging link between the GWC and ABI cards compared with the existing UDP transport. SCTP is supported on both the IP and ATM network fabrics.

SCTP provides the ability to retransmit lost messages and to ensure that the messages arrive in order. Additionally, SCTP provides alarms when message retransmits or loss get high or when a messaging link is lost. This provides the customer with the ability to find and solve network messaging problems quickly.

SCTP seamlessly and automatically upgrades and downgrades in a customer installation. The customer is not required to provide any configuration information.

When both the GWC and ABI network components are upgraded to SN07, the components will discover that they both support SCTP and will start using SCTP. If only one or neither component supports SCTP, then the existing UDP protocol will continue to be used.

114.3 Hardware Requirements or Dependencies

This activity is compatible with existing GWC and ABI hardware, including ABI hardware introduced in SN07.

114.4 Software Requirements or Dependencies

Requires gateway controller software loads of GC070 or higher.

Requires DMS-100 core loads of SNNCSH07 or higher.

Requires ABI loads of SN07 or higher.

114.5 Limitations and restrictions

None.

114.6 Interactions

None

114.7 Applicable customer facing sections

Fault Management	
Logs	__X__
Alarms	__X__
Configuration	
Data Schema	__X___
User Interface	__X___
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____

Performance (includes operational measurements) __X__

114.8 Glossary

Term	Description
SCTP	Stream Control Transmission Protocol

115: Functional Description (FN): A00003773

115.1 Feature name

ACT: A00003773, Trunk Group Based Quality of Service (QOS) Operational Measurement (OM) support for MG4K-IP

115.2 Description

The activity A89007725 in SN06, '*Trunk Group based QoS OM'* provided a new trunk group based operational measurement group (TRKQOSOM) on the Succession Call Server. The operational measurement values record instances in which QOS threshold values have been exceeded for calls handled by GWC based TDM trunk group.

This feature A00003773 '*OM FOR TRKQOS FOR MG4K IP'*, extends trunk group based QoS OM support to MG4K-IP. As part of this activity, the operational measurement values record instances in which QOS threshold values have been exceeded for calls handled by MG4K-IP based TDM trunk group.

The QOS statistics that are included in the OM for each MG4K-IP and GWC trunk group are packet loss, jitter, and delay (latency).

When MG4K-IP based trunk calls are released, the QOS statistics for that call are compared to the QOS OM threshold values. If a statistic for the call exceeds the QOS OM threshold value, the OM value for that statistic on the MG4K-IP based trunk group will be incremented.

The OM group will contain entries for each MG4K-IP based TDM trunk group datafilled on the Call Server. In order for the trunk group to appear in the OM group at least one member of the trunk group must be datafilled to reside on a MG4K-IP node via table TRKMEM.

Each entry in the OM group will contain a CLLI and threshold-crossing counters for packet loss, jitter, and delay (latency).

The active registers will contain data for the current reporting interval. The holding registers will contain data for the previous reporting period. The interval for OM peg count transfer from the active to holding registers is controlled by the OM system. Refer to the OM system documentation for details on the available intervals for active to holding transfer.

In SN06, the activity A89007725 introduced a new office parameter *PACKET_QOS_OM_THRESHOLDS* to define QOS OM threshold values for GWC. The same QOS OM threshold values

(PACKET_QOS_OM_THRESHOLDS) defined in table OFCVAR will be applied to all MG4K-IP nodes datafilled on the Call Server. The values may be changed at any time without the need for Call Server/MG4K-IP restart.

The Table 1, “PACKET_QOS_OM_THRESHOLDS Office Parameter,” on page 1304 describes the range of values possible for each QOS OM threshold office parameter datafilled in table OFCVAR.

Table 1 PACKET_QOS_OM_THRESHOLDS Office Parameter

Parameter	Field		Range	Units
PACKET_QOS_OM_THRESHOLDS	Enabled		Y/N	
	Jitter		0 TO 100	Milliseconds (ms)
	Delay		0 TO 500	Milliseconds (ms)
	Loss	Whole	0 TO 9	% packet loss range from 0 TO 9.999999%
		Fraction	0 TO 999999	

The threshold values may be set in table OFCVAR by positioning on and changing the appropriate threshold as shown in Figure 1, "Commands to set threshold values in table OFCVAR":

Figure 1 Commands to set threshold values in table OFCVAR

```
TABLE: OFCVAR
>pos packet_qos_om_thresholds
     PACKET_QOS_OM_THRESHOLDS                    N  1  2  3 4
>change
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: N  1  2  3 4
>Y 10 30 4 5
TUPLE TO BE CHANGED:
     PACKET_QOS_OM_THRESHOLDS                    Y 10 30 4 5
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Jitter Threshold : 10 milliseconds
Delay Threshold : 30 milliseconds
Loss  Threshold : 4.500000 %
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

In the above example, the QOS OM threshold reporting was changed such that the reporting is active and the thresholds were set (jitter=10 ms, delay= 30 ms, Packet Loss= 4.5%).

The default values for the OM thresholds will be set to the maximums and the enabled value will be set to N (No).

In order to view the QOS OM threshold crossing data, access the TRKQOSOM group via OMSHOW as shown in Figure 2, "Commands to view the QOS OM threshold crossing data" follows:

Figure 2 Commands to view the QOS OM threshold crossing data

```
>omshow trkqosom active(or holding for previous interval)
TRKQOSOM

CLASS: ACTIVE
START:2002/07/22 12:50:00 MON; STOP: 2002/07/22 12:53:44 MON;
SLOWSAMPLES:        3 ; FASTSAMPLES:        22 ;

     KEY (COMMON_LANGUAGE_NAME)
       PKTLOSS    JITTER     DELAY

     64 IP01S7ITW2
           0        1                0
     65 COMPISUP_OG
           0        0                0
     66 IPD1ITSIMTS7
           0     0                   0

.............................
```

The data presented will include an entry for each MG4K-IP based TDM trunk group datafilled on the Call Server. For each entry, the CLLI will be presented with the PKTLOSS, JITTER, and DELAY threshold crossing data.

Definitions for Packet Loss, Delay and Jitter registers are as follows:

Packet loss rate is calculated in percentage as:
[RtpCumulativeLostPackets *100] / [RtpPacketsReceived + RtpCumulativeLostPackets]

Where, RtpPacketsReceived - The number of the RTP packets received from the IP network.
RtpCumulativeLostPackets - The number of lost RTP packets in the receiving direction. The count represents the Cumulative Number of Packets Lost field that is inserted in to the RTCP reception blocks.

Interarrival time jitter is an estimate of the statistical variance of RTP data packet interarrival times. The Jitter value calculated as the smoothed mean absolute value of the difference between the sending interval at a source and the interarrival time at a receiver. It is a running filtered average, basically a low pass filter with a 1/16 contribution each sample.

$jitter_{new} = jitter_{old} + [(instantaneous\ jitter - jitter_{old}) / 16]$

Where, instantaneous jitter = | [rec_i – rec_{i-1})] – [$sent_i$ – $sent_{i-1}$] |
rec_i / $sent_i$ = Time when i^{th} data packet is received/sent.

The round-trip delay is calculated when a RTCP reception report is received. The Delay (latency) is smoothed as,
$delay_{new}$ = $delay_{old}$ + [(instantaneous delay– $delay_{old}$) / 16]

Where instantaneous delay = | A - LSR - DLSR |
A = time a source received this reception report
LSR = last Send Report timestamp received field
DLSR = delay since last Send Report field

115.3 Hardware Requirements or Dependencies

None

115.4 Software Requirements or Dependencies

This functionality requires SN07 load in the Call Server, and SN07.1 or higher load in the MG4K-IP CEM and GEM RM.

115.5 Limitations and Restrictions

The intent of this activity is to provide an indication of QOS on the Call Server for each MG4K-IP based trunk group. As such, the activity does not attempt to record every violation of the QOS OM threshold. Rather, for the trunk group as a whole, a general indication of QOS health will be provided.

OM peg counts stored in the MG4K-IP that have not been reported to the Call Server will not be maintained over MG4K-IP GEM Sparing and Restarts.

TRKQOSOM OM group shall not be supported for IW-IP nodes.

115.6 Interactions

None

115.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A

Service Order	N/A
Office Parameters	X
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	X

115.8 Glossary

Term	Description
MG4K-IP	Multi-Service Gateway 4000-Internet Protocol.
GWC	Gateway Controller
Jitter	The Jitter value calculated as the smoothed mean absolute value of the difference between the sending interval at a source and the interarrival time at a receiver.
Delay (Latency)	Total time difference between the time a packet is sent and the time a corresponding reply packet is received. This delay refers to network delay only and does not include packetization/codec delay etc.
Loss	This is the percentage of packets lost over duration of the call.
OM	Operational Measurement
DPT	Dynamic Packet Trunk
QOS	Quality Of Service
RTCP	Real Time Control Protocol

116: Functional Description (FN): A00003789

116.1 Feature name

SN07: A00003789 - INTRA IMT CAUSE Enhancements

116.2 Description

This feature introduces the capability for originating INTRA IMT trunks to route advance on four specific CAUSE values:

- CAUSE 42 - Switch Equipment Congestion (SWEQCONG)
- CAUSE 47 - Resources Unavailable (RESUNAV)
- CAUSE 51 - This is a non standardized “Service” related CAUSE (CSE_51) utilized by the customer in their own network.
- CAUSE 34 - No Circuits Available (NOCIRCAV)

This feature introduces a new office parmater RTE_ADVANCE_FOR_INTRA_IMT_NCRT in table OFCVAR which controls the optionality to route advance on CAUSE 34 - No Circuit Available (NOCIRCAV). Cause values 42, 47 and 51 are not affected by the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT.

PTS and SS7 INTRA IMT originators are supported and must terminate to an SS7 EANT or IMT terminator for the described CAUSE enhancements to take place.

Specifically for SS7 INTRA IMT originators this feature enables CAUSE handling in the CM with existing optional table CSEMAP for all CAUSE values in addition to the specified functionary for CAUSE 34, 42, 47 and 51.

The INTRA IMT CAUSE enhancement capability is controlled on a per trunk group basis using a new option in table TRKOPTS called INTRACSE. **NOTE: Patch SBB41 introduced the TRKOPTS option as INTRA_CSE (w/ underscore) and this activity removes the underscore for TRKOPTS option consistency and ease of use.** The INTRACSE TRKOPTS option can only be assigned to originating (IC, 2W) IMT Trunks with TRKGRP field NETWKSPC set to INTRA. The INTRACSE option contains a “route advance choice” field that can be set to Y or N.

This capability interacts with optional table CSEMAP but does not have a dependency on table CSEMAP. For more information see “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1311.

This capability is under Software Optionality Control (SOC). The SOC order code is NSER0005.

Please refer to the following sections for detailed information on this capability:

- Background Information
- Software Optionality Control NSER0005
- Table TRKOPTS option INTRACSE
- Table OFCVAR Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT
- Call Processing CAUSE Handling

116.2.1 Background Information

It is important to understand the default or existing CAUSE handling behavior for both PTS and SS7 INTRA IMT originators prior to this activity.

PTS INTRA IMT originators that terminate to SS7 EANT and IMT trunks always perform CAUSE handling in the CM as the CAUSE value cannot be passed to the adjacent office due to interworking (PTS to SS7). Therefore "default" CAUSE handling for PTS INTRA IMT originators already exists. The specific CAUSE values impacted by this feature have a default functionality for PTS INTRA IMT originators as follows:

- CAUSE 34, 42 and 47 all route advance by default and can be overridden by associated CSEMAP entries to not route advance or to go to a different treatment. Reference Table 1 below.
- CAUSE 51 is an undefined CAUSE value and by default goes to (RODR) treatment. CSE_51 can be overridden by a CSEMAP entry to route advance or go to a different treatment. Reference Table 1 for details.

Table 1 Default PTS INTRA IMT CAUSE Handling Behavior

CSEMAP	CAUSE 34, 42, 47 Default Result	CAUSE 51 Default Result
No Entry	Route Advance (Default)	TRTMT (Default - RODR)
RTE ADV - N	CSEMAP TRTMT	CSEMAP TRTMT
RTE ADV - Y	Route Advance (CSEMAP)	Route Advance (CSEMAP)

SS7 INTRA IMT originators that terminate to SS7 EANT and IMT trunks do not perform CAUSE handling in the CM prior to this feature. The CAUSE values are passed (bounced) to the adjacent office without any CM interaction.

This activity, when active, will impact both SS7 and PTS INTRA IMT originators in the same way as described in section “116.2.4 Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1311. When inactive, the default behavior will be as described in this section "Background Information" .

116.2.2 Software Optionality Control (SOC) NSER0005

The new SOC order code NSER0005 - Intra IMT Cause Enhancements is introduced by this feature. When the NSER0005 SOC state is IDLE, CAUSE handling behavior is unchanged for calls with INTRA IMT originators. The new TRKOPTS option INTRACSE can be data filled when the SOC state is IDLE or ON. The new office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT can also be changed when the SOC state is set to IDLE or ON.

The new SOC NSER0005 - Intra IMT Cause Enhancements is dependant upon SOC NSER0003 - Inter/Intra IMT for the described functionality to be active.

Changing the NSER0005 SOC state to ON does not in itself enable any new functionality. NSER0005 SOC in conjunction with the INTRACSE TRKOPTS option, enables the CAUSE Enhancements capability described in this document. For more information see “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1311.

116.2.3 Table TRKOPTS option INTRACSE

A new TRKOPTS option called INTRACSE is introduced by this feature. The INTRACSE option contains a field called RTE_ADV_CHOICE that must be data filled to Y or N to select the route advance capabilities described in section “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1311.

Figure 1 shows an example entry of the INTRACSE option data filled on a trunk CLLI in table TRKOPTS.

Figure 1 TRKOPTS option INTRACSE Example Entry

```
TABLE: TRKOPTS
 -------------------------
TRKCLLI   INTRACSE   INTRACSE  RTE_ADV_CHOICE  Y
```

The CAUSE Enhancement capability is dependant on the the originating trunk and therefore The INTRACSE option can only be assigned to IC or 2W INTRA IMT trunks. The option can be assigned to both SS7 and PTS INTRA IMT signaling trunks. The option allows the customer to activate the CAUSE enhancements capability on a per trunk group basis. INTRA IMT originators with this option assigned must terminate to an SS7 terminating trunk to enable the CAUSE Enhancement capability.

Various error messages occur during datafill if the INTRACSE option is assigned to something other than the specified trunk data. Figure 2 below illustrates the error messages associated with the INTRACSE option.

Figure 2 TRKOPTS INTRACSE Datafill Error Messages

Attempts to datafill the INTRACSE option on a trunk type other than IMT, results in the following error message:

'INTRACSE option is supported only for IMT trunk types'

Attempts to datafill the INTRACSE option on an IMT trunk with a NETWKSPC value other than INTRA, results in following error message

'INTRACSE option requires NETWKSPC to be INTRA'

Attempts to datafill the INTRACSE option on an outgoing (OG) trunk, result in the following error message:

'INTRACSE option supports IC and 2W direction only.'

116.2.4 Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT

A new office paramater RTE_ADVANCE_FOR_INTRA_IMT_NCRT is added to table OFCVAR to control the route advance behavior of CAUSE 34 in conjunction with the INTRACSE TRKOPTS option. The functionality of this parameter does not affect the route advance capability of cause values 42, 47 and 51. The values for the parm are {N,Y} and are immediately activated when changed.

The functionality of this office parameter is further explained in the section “CAUSE Processing CAUSE Handling”.

Figure 3 shows an example entry of the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT in table OFCVAR.

Figure 3 OFCVAR Office Parameter Example Entry

```
TABLE: OFCVAR
 ------------------------
RTE_ADVANCE_FOR_INTRA_IMT_NCRT  Y
```

116.2.5 Call Processing CAUSE Handling

The CAUSE enhancements capability for this activity is described in "Table 2 INTRA IMT CAUSE Handling Matrix" on page 1313. There are several variables that determine the CAUSE handling behavior for INTRA IMT originators. The variables are summarized as follows:

- SOC NSER0003 - Inter/Intra IMT must be ON. For "Table 2 INTRA IMT CAUSE Handling Matrix" on page 1313 this variable is not listed and the SOC is assumed to be ON.
- SOC NSER0005 - Intra IMT Cause enhancements - IDLE / ON status indicates optionality status. IDLE implies default or existing behavior prior to this activity.
- TRKOPTS option INTRACSE. The presence of the option for a particular trunk allows two things to occur:
  - — Enables CAUSE handling in the CM for INTRA IMT SS7 originators for all CAUSE values in addition to the functionality described in this document for CAUSE values 34, 42, 47 and 51.
  - — Checks the status of office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT and determines whether to enable or disable CAUSE 34 from route advancing for SS7 and PTS INTRA IMT trunks. However a CSEMAP entry for CAUSE 34 can be used to provide route advance capabilities or change the treatment handling.
- INTRACSE RTE_ADV_CHOICE Y/N - this field impacts CAUSE values 34, 42, 47 and 51 only and when set to Y enables route advance with or without CSEMAP interaction. When set to N default treatment is used or CSEMAP entries can allow route advance or change the treatment.
- CSEMAP entries for CAUSE values 42, 47 and 51. With INTRACSE RTE_ADV_CHOICE = N, the CSEMAP entries determine route advance or treatment CAUSE handling. With INTRACSE RTE_ADV_CHOICE = Y, the call always route advances regardless of CSEMAP entry.

- CSEMAP entry for CAUSE 34. If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT = Y and INTRACSE RTE_ADV_CHOICE = N, the CSEMAP entry determines route advance or treatment CAUSE handling. With INTRACSE RTE_ADV_CHOICE = Y, the call always route advances regardless of CSEMAP entry. If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT = N, INTRACSE RTE_ADV_CHOICE subfield has no impact on CAUSE handling for CAUSE 34. The presence of the INTRACSE option forces the call to go to treatment (NCRT). However a CSEMAP entry for CAUSE 34 can change the treatment or set the route advance bool and the call routes accordingly.

Table 2, "INTRA IMT CAUSE Handling Matrix," on page 1313 describes the CAUSE Enhancement behavior provided by this activity.

Table 2 INTRA IMT CAUSE Handling Matrix

SOC NSER0005	TRKOPTS INTRACSE	CSEMAP	CAUSE 42,47 and 51 Result	CAUSE 34 Result when RTE_ADVANCE_FOR_INTRA_IMT_NCRT=N	CAUSE 34 Result when RTE_ADVANCE_FOR_INTRA_IMT_NCRT=Y
IDLE	N/A	N/A	Default CAUSE Behavior[a]	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	No Entry	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	RTE ADV - N	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	RTE ADV - Y	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	RTE ADV - N	No Entry	Default TRTMT[b]	Default TRTMT	Default TRTMT
ON	RTE ADV - N	RTE ADV - N	CSEMAP TRTMT	CSEMAP TRTMT	CSEMAP TRTMT
ON	RTE ADV - N	RTE ADV - Y	Route Advance (CSEMAP)	Route Advance (CSEMAP)	Route Advance (CSEMAP)
ON	RTE ADV - Y	No Entry	Route Advance (INTRACSE)	Default TRTMT (NCRT)	Route Advance (INTRACSE)
ON	RTE ADV - Y	RTE ADV - N	Route Advance (INTRACSE)	CSEMAP TRTMT	Route Advance (INTRACSE)
ON	RTE ADV - Y	RTE ADV - Y	Route Advance (INTRACSE)	Route Advance (CSEMAP)	Route Advance (INTRACSE)

a. Default CAUSE Behavior is different for SS7 and PTS See "Background Information" on page 1309. for specific details
b. Default TRTMT for CAUSE 34 is NCRT, CAUSE 42 is NBLH, CAUSE 47 is GNCT, and CAUSE 51 is RODR

116.3 Hardware Requirements or Dependencies

None

116.4 Software Requirements or Dependencies

SOC NSER0005 is dependant on SOC NSER0003 - Inter/Intra IMT. SOC NSER0003 must be ON before SOC NSER0005 call processing capabilities become active.

116.5 Limitations and restrictions

From a Table Control perspective the TRKOPTS option INTRA _CSE can only be assigned to:

- INTRA IMT (IC or 2W) PTS Trunks
- INTRA IMT (IC or 2W) SS7 Trunks

From a Call processing perspective CAUSE handling requires terminations from INTRA IMT trunk originators to EANT or IMT (INTRA or INTER) SS7 trunk terminators.

116.6 Interactions

This capability interacts with optional Table CSEMAP but is not dependant nor does it change the behavior of the CSEMAP table. For details reference Table 2, “INTRA IMT CAUSE Handling Matrix,” on page 1313.

116.7 Applicable customer facing sections

Fault Management	
Logs	___N/A___
Alarms	___N/A___
Configuration	
Data Schema	___X___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

116.8 Glossary

Term	Description
AMA	Automatic Message Accounting
EANT	Equal Access Network Trunk
IMT	Inter Machine Trunk
PTS	Per Trunk Signaling
SOC	Software Optionality Control
SS7	Signaling System #7

117: Functional Description (FN): A00003905

117.1 Feature name

DIRP ENHANCEMENTS FOR BILLING

117.2 Description

Feature A00003905 increases the number of DIRP volumes in table DIRPPOOL from 24 to 72.

The feature uses SOC to restrict provisioning more than 24 volumes per DIRP pool if the SOC state is IDLE. Rejection messages indicate that this feature is inactive.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

117.3 Hardware Requirements or Dependencies

Feature A00003905 works in conjunction with feature A00002186 to realize 4G of storage capacity for a DIRP subsystem. Feature A00002186 increase DDU storage capacity from 1G to 4G. However, for any feature functionality to be active, 4G DDUs must be present in the switch with the appropriate IOM load.

117.4 Software Requirements or Dependencies

To achieve 4G of DIRP DDU storage capacity, both features A00003905 and A00002186 must be present and active. Both features are enabled and disabled via SOC. IOM load XXXYYYZZZ is required.

117.5 Limitations and restrictions

None.

117.6 Interactions

Feature A00003905 impacts table control for table DIRPPOOL. Expanding the number of volumes per pool necessitated a change in how table DIRPPOOL is manually provisioned. Volumes are no longer provisioned as individual fields but are provisioned in groups of three. Using DIRP MNT to provision volumes is unaffected.

117.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema __X__
- User Interface __X__
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

117.8 Glossary

Term	Description
New term	Definition
DIRP MNT	MAPCI; MTC; IOD; DIRP; MNT

118: Functional Description (FN): A00003923

118.1 Feature name

CTX / RES SCAI Redirection

118.2 Description

Intelligent Call Management (ICM) also known as CompuCall (for X.25 transport) provides communications channel between a computer and a switch that allows a telephone company to provide coordinated switch-based services to applications residing on a customers host computer.

Currently ACD Call Redirection[1] is assigned as an option (SCAIREDIR) to an ACD Group in table ACDGRP on the DMS. Once assigned, incoming calls to the ACD Group generate a DV-Call-Received-C message to the ICM Host computer. Included in this message are the Called Number, Calling Number and Charge Number. If the ICM Host computer wishes to redirect the call, it sends a DV-Call-Redirect message to the DMS switch including the Redirecting DN. If the Host computer does not wish to redirect the call, it sends a Return-Result as the acknowledgement for the DV-Call-Recieved-C message. The Host computer must receive an acknowledgement for the DV-Call-Redirect message before it sends an acknowledgement for the DV-Call-Received-C.

This activity will enhance the ACD Call Redirection feature[1] and extend it's functionality beyond ACD Groups making it available for use on CENTREX and Residential lines.

The option SCAIRDIR will be assignable to any (non-ACD) CENTREX or Residential line as a sub-option to the Extended Call Management (ECM) option. ECM is a required option as it provides the neccessary access to SCAI messaging and capabilities in the (non-ACD) CENTREX or Residential environment. Once assigned, incoming calls to the line will generate redirection messaging that follows the same sequence of events as described above, allowing the ICM Host computer to redirect the call if it wishes to.

[1] *AG2195 - ECM Inbound Redirection & AR0048 - Call Redirection to Specific Line*

118.2.1 Application Logon SCAI Service Version

The dv-Appl-Logon message contains a parameter, Service Version, which uniquely identifies the version of messages which will be used for the session.

This activity requires the use of a Service Version of 09 or newer[2]. Service

Version 09 was developed in CCM07, since the Service Version is upward compatible, all previous Service Version functionality is provided with the latest Service Version[2].

A Service Version of 09 or newer[2] must be specified in the dv-Appl-Logon message in order for the host application to generate and/or recognize the DV-Call-Received-C and DV-Call-Redirect messages for Centrex or Residential lines.

118.2.2 Subscription to SCAI messages

This activity requires subscription to the ROUTING and either RESEVENT or CTXEVENT sub-services found in table SCAISSRV. The default tuple of ROUTING34$ and either RESEVENT07$ or CTXEVENT34$ or newer[3] is required in order to have access to the DV-Call-Received-C and DV-Call-Redirect messages for Centrex or Residential lines.

118.2.3 CTX and Residential SCAIRDIR Line Option

A new option SCAIRDIR will be created as a sub-option to the Extended Call Management (ECM) option[4]. The sub-option SCAIRDIR will have a sub-field called MSGTO that has a range between 1 and 30 seconds. Once assigned, incoming calls to the line will generate DV-Call-Received-C messaging which can be acted upon by the ICM Host computer to redirect the call if desired. The new SCAIRDIR sub-option will be assignable via SERVORD as follows:

```
>SERVORD
SO: ADO $ 05 00 00 05
OPTION: ECM
CALL_EVENTS: Y
MAKECALL: Y
CONF_XFER: Y
MSG_WAIT: Y
SCAICC: Y
CHKLOPT: Y
NETICM: Y
SCAIRDIR: Y
    MSGTO: 30
OPTION: $
```

[2] *As of this document the latest SCAI Service Version was SCAI18*

[3] *As of this document the latest default tuples where ROUTING15$, RESEVENT13$ and CTXEVENT13$*

[4] *ECM is required as it provides the access to SCAI capabilities in the non-ACD CTX and RES environment*

118.2.4 Phone Set Compatibility

The new sub-option SCAIRDIR will be applicable to the same sets as the ECM Line Option[5]. This includes sets that are Meridian Business Set (MBS), 500/2500 IBN and Meridian Feature Transparency (MFT) sets, including EtherSets.

Only single DN apperance per line will be supported by this activity. Lines with features such as Multiple Appearance Directory Number (MADN), Hunt Groups, UCD etc. are not supported

118.2.5 CTX / RES SCAIRDIR Functionality

The DMS sends the dv-Call-Received-C message[6] to the host when a call is received for a CTX/RES line with the SCAIRDIR sub-option and that CTX/RES line belongs to an associated environment with which the host has established a session.

The host must send an acknowledgment back to the DMS within 1 to 30 seconds (as determined by the MSGTO sub-field of the SCAIRDIR sub-option). The host responds to the dv-Call-Received-C in one of the following ways:

- dv-Call-Redirect message[7]
  - — If the host determines the call should be redirected, it responds with a dv-Call-Redirect message
- Return Result
  - — If the host determines call redirection is not required, it responds with a Return-Result message, in which case the call will continue to route to the destDN. The Return-Result message has no parameters.
- Return Error
  - — If the host responds with a Return-Error message, the call will continue to route to the destDN.
- Reject
  - — If the host responds with a Reject message, indicating a protocol error or a message received out of sequence, the call will continue to route to the destDN.
- No Response from Host
  - — If the host does not respond to a dv-Call-Received-C message within a predetermined time period (MSGTO sub-field of SCAIRDIR sub-option) , the call will continue to route to the destDN.
- Response Received Out of Sequence
  - — Any out of sequence messages of this type are treated as extraneous and the DMS responds to the host with a Reject message.

[5] *Reference AR0046 - ECM / SCAI Support for Non-ACD*

[6] *A call to an ECM associated CTX/RES line WITHOUT the SCAIRDIR sub-option will generate the normal dv-Call-Offered-U message*

[7] *Reference AG2195 - ECM Inbound Redirection & AR0048 - Call Redirection to Specific Line*

118.2.6 CTX / RES SCAIRDIR Setup and Validation

For proper CTX/RES SCAIRDIR operation, the following setup and conditions must be met:

1. The SCAI Service Version is at least 09 (SECTION 2.2.1)

2. An ICM switch-host session is established. A successful dv-Appl-Logon request was sent by the host computer.
3. The switch-host session is subscribed to a ROUTING and RESEVENT or CTXEVENT sub-service and the DV-Call-Received-C and DV-Call-Redirect messages within ROUTING. (SECTION 2.2.2).
4. The Centrex/Res line must have the line option ECM with sub-option SCAIRDIR set to 'Y' and the MSGTO sub-field set between 1 and 30 seconds. (SECTION 2.2.3)
5. The line which the host application is monitoring must be associated to the session via dv-DN-Associate.

118.2.7 Message Protocol

The ASN.1 notations for the DV_CALL_RECEIVED_C message are shown in this section. A sample X.209 hex encoding has been provided here. The length fields are variable because the length depends on the variable content. The tag values are taken from the ROSE protocols.

118.2.7.1 CTX / RES dv-Call-Received-C ASN.1 Encoding

```
dv-Call-Received-C          OPERATION
                            ARGUMENT    CallReceivedArgument
                            RESULT
                            ERRORS      {Call-Received-Error}
                            LINKED      {DV-CALL-REDIRECT}
                            ::= 10

CallReceivedArgument            ::=  SEQUENCE
    {   networkCallID           [0]  IMPLICIT SEQUENCE
        {  networkNodeID             [0]  IMPLICIT INTEGER      OPTIONAL,
           localCallID               [1]  IMPLICIT INTEGER      OPTIONAL }
                                                                OPTIONAL,
        destDN                  [1]  IMPLICIT OCTET STRING     OPTIONAL,
        origCallingNumber       [2]  IMPLICIT OCTET STRING     OPTIONAL,
        origChargeNumber        [3]  IMPLICIT OCTET STRING     OPTIONAL,
        callHistoryInfo         [4]  IMPLICIT SEQUENCE
           {  callType                  [0]  IMPLICIT ENUMERATED
              {  callTransferred             (1),
                 callOverflowed              (2),
                 callRedirected              (3),
                 callForwarded               (4),
                 callConsult                 (5),
                 callConference              (6),
                 callReturnedToQueue         (7),
                 callRouted                  (8) }              OPTIONAL,
              origInboundDN     [1]  IMPLICIT OCTET STRING     OPTIONAL,
              prevApplicationID [2]  IMPLICIT INTEGER          OPTIONAL,
              hostCallData      [3]  IMPLICIT OCTET STRING     OPTIONAL}
```

```
                                                                    OPTIONAL,
        forwardingParty         [6]  ForwardingPartyType            OPTIONAL,
        cpadigs                 [7]  IMPLICIT OCTET STRING          OPTIONAL}

AddressType                     ::=  CHOICE
    {   positionID              [0]  IMPLICIT INTEGER,
        dialedDigits            [1]  IMPLICIT IA5String,
        stationNumber           [2]  IMPLICIT OCTET STRING,
        q.931Address            [3]  Q.931AddressType }

Q931AddressType                 ::=  SEQUENCE
    { numberTypeNumberPlan           [0]  OCTET STRING              OPTIONAL,
      presentationScreeningIndicator [1]  OCTET STRING              OPTIONAL,
      digits                         [2]  IA5 STRING                OPTIONAL}


ForwardingPartyType             ::=  IMPLICIT SEQUENCE
    {   firstFwdNumber               [0]  Address Type              OPTIONAL,
        firstFwdReason               [1]  IMPLICIT ENUMERATED
          {  unknown                      (0),
             userBusy                     (1),
             noReply                      (2),
             unconditional                (3) }                     OPTIONAL,
        lastFwdNumber                [2]  Address Type              OPTIONAL,
        lastFwdReason                [3]  IMPLICIT ENUMERATED
          {  unknown                      (0),
             userBusy                     (1),
             noReply                      (2),
             unconditional                (3) }                     OPTIONAL}


call-Received-Error             ERROR    ::=    0
```

118.2.7.2 CTX / RES dv-Call-Received-C Coded Example

The DMS receives a call initiated by the OrigCallingNumber 9192466001 for the destDN of 9194815200 and assigns the call a LocalCallId = 4. The DMS sends a dv-Call-Received-C message to the host who responds with a Return Result message in which case the DMS would continue to route the call to destDN. If the host determined the call should be redirected, it would respond with a dv-Call-Redirect message. If the host determined that there was an error, it would respond with a Return Error message.

INVOKE **DMS ===> HOST**

Table 1: CTX / RES dv-Call-Received-C Coded Example

Hex Dump			Information Element	Comments
Tag	**Len**	**Content**		
A1	2B		INVOKE	this message is 43 bytes decimal
02	02	03 F9	InvokeID	the Invoke ID is decimal 1017
02	01	0A	Operation	the operation is dv-Call-Received-C [10] decimal
30	22		Argument	CallReceived argument is of sequence type and is 34 bytes long decimal
A0	06		NetworkCallId	the NetworkCallId is a constructor 6 bytes
80	01	00	NetworkNodeId	the NetworkNodeId is 0
81	01	04	LocalCallId	the LocalCallId is 4
81	0A	39 31 39 34 38 31 35 32 30 30	destDN	the called DN is 9194815200
82	0C	00 83 39 31 39 32 34 36 36 30 30 31	OrigCallNumber	the first two bytes are fixed and presently unused. The OrigCallNumber is 9192466001
Hex Dump = A1 39 02 02 03 F9 02 01 0A 30 22 A0 06 80 01 00 81 01 04 81 0A 39 31 39 34 38 31 35 32 30 30 82 0C 00 83 39 31 39 32 34 36 36 30 30 31				

RETURN-RESULT **DMS <=== HOST**

Table 2: CTX / RES dv-Call-Received-C Return Result Coded Example

Hex Dump			Information Element	Comments
Tag	Len	Content		
A2	04		RETURN RESULT	the message is 3 bytes long decimal
02	02	03 F9	InvokeID	the Invoke ID is 1017 decimal
Hex dump = A2 04 02 02 03 F9				

.

RETURN-ERROR **DMS <=== HOST**

Table 3: CTX / RES dv-Call-Received-C Return Error Coded Example

Hex Dump			Information Element	Comments
Tag	Len	Content		
A3	07		RETURN ERROR	the message length is 7 bytes decimal
02	02	03 F9	InvokeID	the Invoke ID is decimal 1017
02	01	00	Error Value	the Error Value is Call-Received-Error (0).
Hex dump =A3 07 02 02 03 F9 02 01 00				

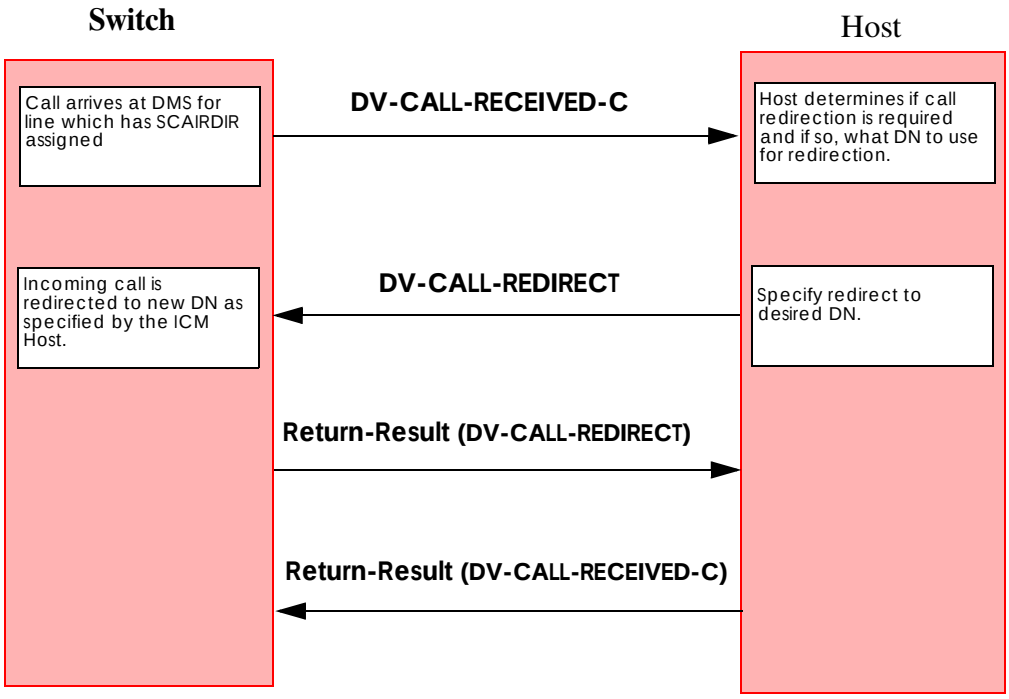
118.2.8 CTX / RES SCAIRDIR Message Flow Example

The following two message flow examples demonstrate basic messaging between the DMS and host computer for:

1. A CTX / RES line that has SCAIRDIR assigned and the incoming call to that line is redirected.
2. A CTX / RES line that has SCAIRDIR assigned and the incoming call to that line routes to the line.

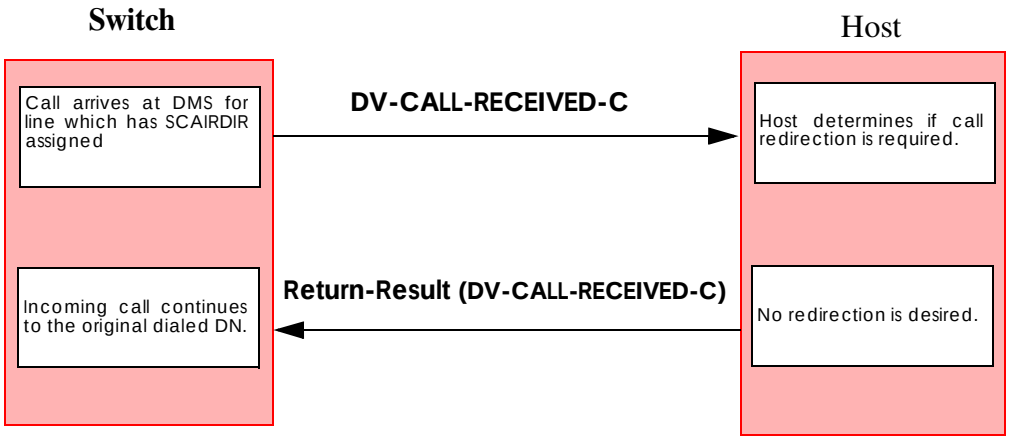
Message Flow for A Redirected Call

Incoming call to a CTX/RES line which has SCAIRDIR assigned and the ICM Host redirects the call to a different DN.



Message Flow for A Non-Redirected Call

Incoming call to a CTX/RES line which has SCAIRDIR assigned and the ICM Host does NOT redirect the call. Call is presented to original DN.



118.3 Hardware Requirements or Dependencies

Not Applicable

118.4 Software Requirements or Dependencies

Not Applicable

118.5 Limitations and restrictions

- This feature *A00003923 - CTX / RES SCAI Redirection* is not compatible with Call Waiting (CWT) or Call Waiting Intra-group (CWI) see Section 2.6 - Interactions.
- The limitations and restrictions that apply to ECM line option, *AR0046 - ECM / SCAI Support for Non-ACD,* will apply to this feature as well.
- Where applicable, the limitations and restrictions of ACD Call Redirection, *AG2195 - ECM Inbound Redirection,* will apply to this feature as well.

118.6 Interactions

- This feature *A00003923 - CTX / RES SCAI Redirection* is not compatible with Call Waiting (CWT) or Call Waiting Intra-group (CWI). If SCAIRDIR has been assigned and activated (via SOC) and CWT / CWI has also been assigned, the originator of a call to the busy set will receive NACK treatment and the busy set will not be presented with Call Waiting tone. It is recommended that CWT/CTI and SCAIRDIR not be assigned to the same phone set.

This activity provides the ways and means for a dv-Call-Received-C message to be generated for a compatible CTX/RES line, the actual redirection of the call is executed via the dv-Call-Redirect message which is not enhanced by this activity. Reference AG2195 - ECM Inbound Redirection & AR0048 - Call Redirection to Specific Line for detailed information on the dv-Call-Redirect message.

118.7 Applicable customer facing sections

Fault Management

Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	__X__
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	__X__
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

118.8 Glossary

Term	Description
ACD	Automatic Call Distribution
ASN	Abstract Syntax Notation
BCS	Batch Change Supplement
CTI	Computer Telephone Integration
CTX	Centrex
DN	Directory Number
ICM	Intelligent Call Management
IBN	Integrated Business Network
MBS	Meridian Business Set
MDC	Meridian Digital Centrex
RES	Residential Enhanced Services
SCAICC	Switch Computer Application Interface Call Control
SCAISSRV	Switch Computer Application Interface SCAI Service

119: Functional Description (FN): A00003933

119.1 Feature name

Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application

This activity delivers an RFC 3261 Compliant Interface for the CS 2000 enabling open interoperability with call servers, application servers, and proxy servers using the Session Initiation Protocol (SIP).

The Session Server Manager and SIP Gateway application are part of the SN07 release.

119.2 Feature Synopsis

119.2.1Activity List

Activity A00003933 is the repository for all the FN information associated with the Session Server Manager - SIP Gateway application. The list of activities addressed by this FN includes:

- A00003270 SIP Open Interop Call Processing
- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003281 SIP on Session Server Call Audit
- A00003933 SIP on Session Server ICAF
- A00003277 Session Server OM Subsystem
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003282 SIP on Session Server Datasync

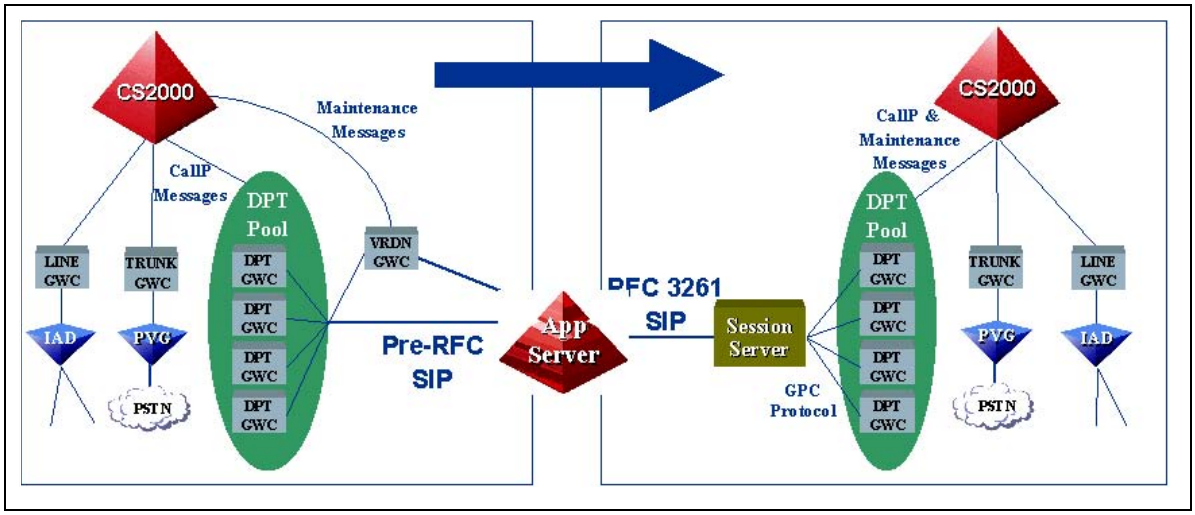
- A00003934 Session Server Project ICAF
- A00004271 SIP App Server SOC
- A00004414 SIP Call Server SOC

119.3 Project Background

SIP is a protocol designed for multimedia communication. The current SCS 2000 SIP offering is a proprietary implementation of SIP for Telephones (SIPT) based on earlier drafts of the SIP specifications. The SCS 2000 SIP implementation was developed to communicate between two CS 2000s and to the Multi-Media Communication Server (MCS). This implementation was available in SN04.

Market drivers are pushing the implementation of SIP to an open interoperability (interop) standard. To meet this requirement, the Session Server Manager is being developed to convert open interop SIP messaging into messages understandable by the CS 2000.

Figure 1 SIP on CS 2000 Evolution



119.3.1 Pre-SN04 VRDN SCTP architecture

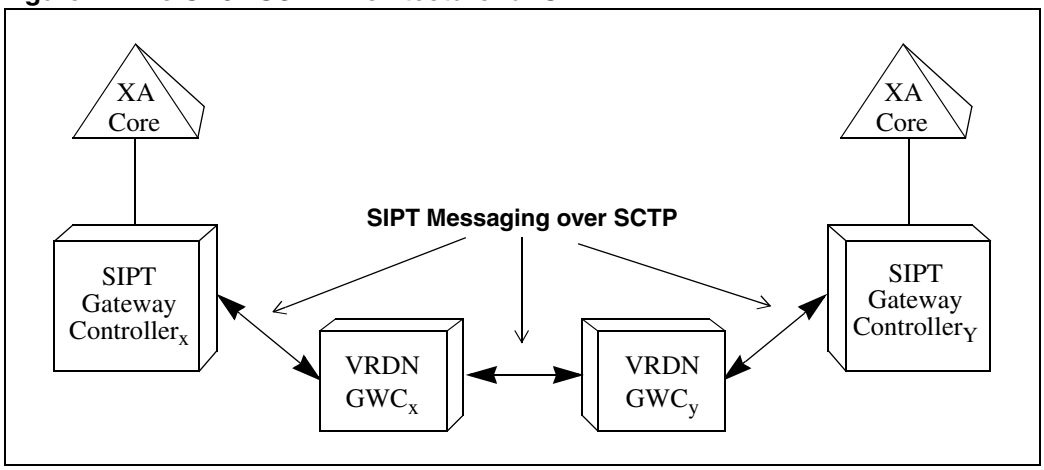
In the initial implementation of SIPT for GWC, signaling path established calls from the VRDN to the remote node. The nodes included SIPT and VRDN gateway controllers. The SIPT gateway controller's function is to process the call while the VRDN is responsible for routing the call. A signaling path exists between the SIPT Gateway Controllers and the VRDN, and between the VRDN and the remote Call Server. Call State is maintained in the VRDN.

The VRDN architecture dynamic packet trunking (DPT) call traverses the following four node types. A visual representation of this architecture is shown in Figure 2, "Pre-SN04 SCTP Architecture for SIPT".

— local SIPT and VRDN gateway controller

— remote VRDN and SIPT gateway controller

Figure 2 Pre-SN04 SCTP Architecture for SIPT



A quick summary of the steps in figure 2 are as follows:

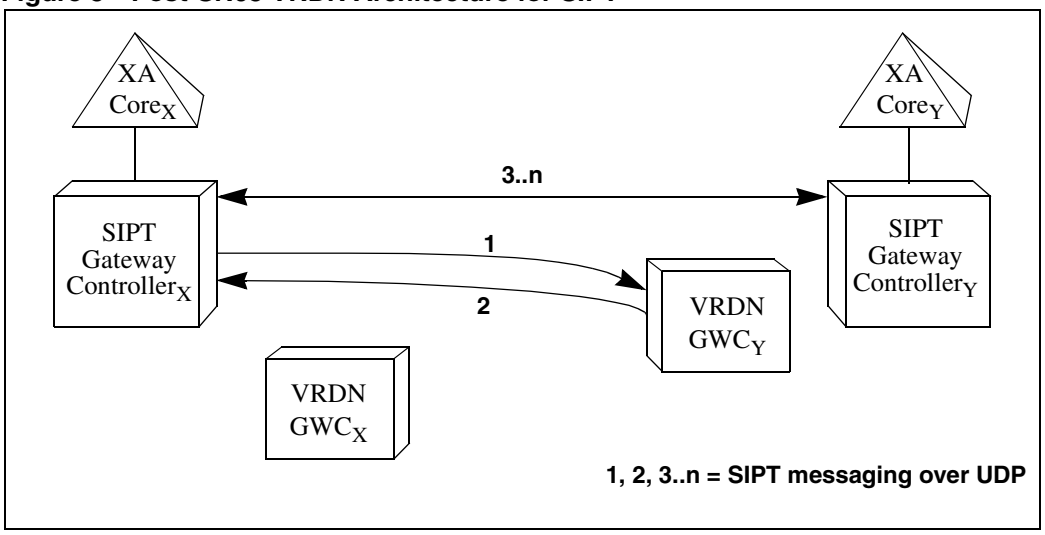
- GWC_X composes an INVITE message and sends it to a local VRDN.
- Local $VRDN_X$ determines which remote VRDN is applicable and then forwards the INVITE.
- Remote $VRDN_Y$ receives the INVITE and determines which of its SIPT gateway controllers should receive the INVITE message. The INVITE message is then sent to that SIPT gateway controller (GWC_Y).

119.3.2Post-SN03 VRDN architecture

In order to overcome limitations when using the previous architecture, a new SIPT architecture was introduced in SN04 (i.e. GWC07). Activity A59034776: “VRDN Capacity Enhancements” provides the majority of the functionality. The purpose of the new architecture was to decrease dependency on the local and remote VRDN.

In the previous architecture, a call from an originating SIPT GWC traverses local and remote VRDN before reaching the destination SIPT gateway controller. With the new architecture, the originating SIPT GWC sends its INVITE directly to the remote VRDN. The remote VRDN replies to the originating SIPT GWC with a 302-Temporarily Moved instead of forwarding the INVITE to the remote SIPT GWC. The 302 message contains the necessary information to contact the remote SIPT GWC. After receiving the 302, the local SIPT GWC sends the INVITE directly to the remote SIPT GWC. A diagram of the new architecture is shown below.

Figure 3 Post-SN03 VRDN Architecture for SIPT



A quick summary of the steps shown in figure 3 are as follows. Note the local VRDN for XA-Core$_X$ is still utilized when call originates from the remote XA-Core.

- Based on MGCINV datafill, a remote VRDN is selected. An INVITE message is sent to that MGC.
- The VRDN on the remote replies with a 302-Temporary Moved message indicating a SIPT GWC for the remote XA-Core. The contact header in the 302 contains the necessary information to reach GWC$_Y$.
- After receiving the 302 message, SIPT GWC$_X$ sends an INVITE to GWC$_Y$, which decides it will accept the call. Standard SIP messaging for call setup is performed. Once the call is complete, it is taken down via the standard SIP mechanisms.

119.3.3VRDN Architecture Limitations

In the VRDN architectures, the SIP stack resides in the gateway controllers and is not compliant to RFC 3261.

In order to move forward in terms of supporting SIP compliancy and greater call volume, a new SIP architecture needs to be created. Hence, the origination of the Session Server Manager platform.

119.3.4Pre-Session Server Manager OAMP Relationships

Before discussing the Session Server Manager platform, the current OAMP component relationship is presented so an understanding of the current scenario exists.

119.3.4.1 Component Relationships

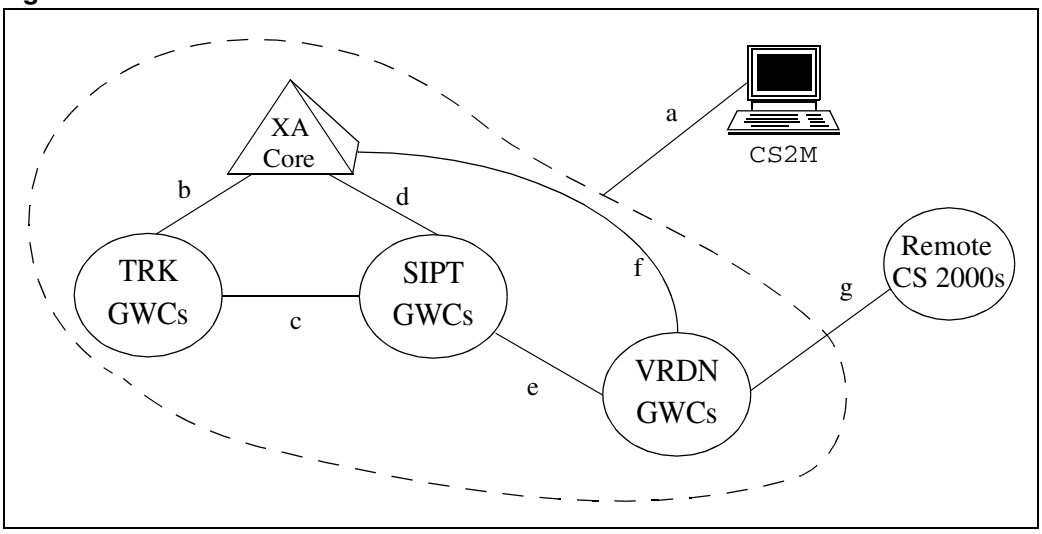
The main components with respect to SIPT call processing are shown and described briefly.

Table 1 SIPT call processing components

Node	Function
XA-Core	General call processing engine of the CS 2000. The XA-Core connects to the IP network via the HIOP and the SDM. SDM is used by CS2M (formerly known as SESM) and the HIOP is used for GWC communications.
TRK GWCs	Functions as the interface between the XA-Core and gateways such as the PVG.
SIPT GWCs	Functions as interface between TRK GWC and the VRDN. Contains SIP call processing functions.
VRDN GWCs	Functions as the "router" to direct incoming/outgoing calls to the appropriate local or remote GWC.
CS2M	General OAM&P platform for most CS 2000 peripherals. Formerly known as SESM.

The figure and follow-on explanation shows and explains at a high level the relationships between each CS 2000 node.

Figure 4 CS 2000 Architecture



a. CS2M provides OAM&P functions for the GWC and Core in the CS 2000 network. CS2M's interaction with the core consists of provisioning datafill such as certain pieces of gateway controller data (e.g. table SERVRINV). CS2M is the main OAM&P component for gateway controllers. OAM&P functions include node and unit provisioning, maintenance, and reporting of performance metrics, logs, and alarms.

b. While CS2M provides most of the OAM&P functions for the trunking GWC, core tables are also utilized for call processing. These tables include SERVRINV, TRKMEM, and TRKSGRP.

c. Only a CallP relationship exists here. This interaction consists of peer messaging in support of outgoing DPT call being routed to, or coming from, a SIPT gateway controller.

d. The local call server uses the SIPT gateway controller to handle DPT calls. Outgoing calls destined for a remote call server are routed through a SIPT gateway controller. For the outgoing call, the core sends the trunk profile index with the IAM which maps to a destination MGC and Telephony Profile in the SIPT GWC. This information determines the remote destination MGC.

   The SIPT gateway controller performs SIP processing and sends out a SIP Invite to the remote MGC. If SCPT is the transport protocol, a local VRDN is utilized. Incoming calls to the SIPT GWC originate from the local VRDN or remote MGC depending on the transport protocol used.

   Datafill from tables SERVRINV, SERVSINV, MGCINV, TELEPROF, TRKSGRP, DPTRKMEM, and TRKOPTS are utilized to perform call processing for the incoming and outgoing call.

e. From an OAM&P perspective, datafill in MGCINV and VRDNINV indicate the MGC for a remote call server. The local call server utilizes the VRDN to route the outgoing call to the remote call server. For an incoming call, the VRDN picks a local SIPT gateway controller to handle the incoming call.

f. Represents maintenance interactions.

g. Represents an outgoing call to remote SIP node or an incoming call.

119.3.4.2 Provisioning

On the core, the below figure illustrates the table control relationships for gateway controllers followed by a brief description of each table. Not every possible table is shown and described.

Figure 5 GWC Table Control Hierarchy

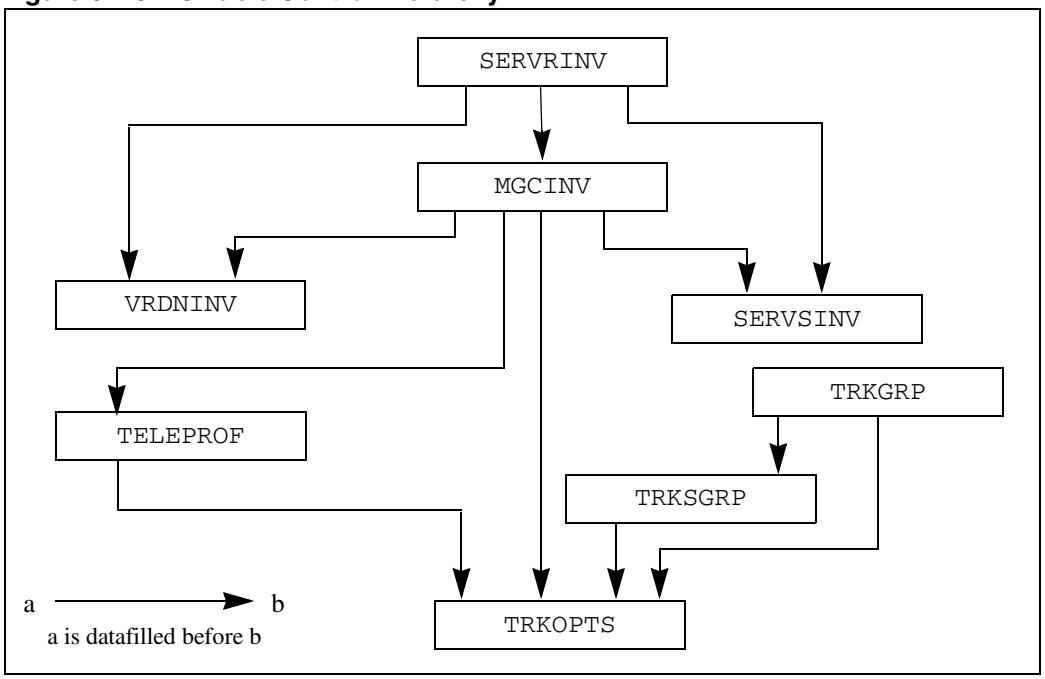


Table 2 Pre-Session Server Manager GWC table descriptions

Table	Description
SERVRINV	Stores provisioned data for gateway controllers including IP addresses, exec information, etc. Gateway controllers are provisioned in CS2M, and then the system automatically enters required datafill in SERVRINV.
MGCINV	Defines remote media gateway controllers for other Call Servers and their associated IP addresses, related virtual router distribution nodes, and connection protocols.
VRDNINV	Defines the locations of the VRDNs and the remote MGCs, which they serve. A VRDN is a dual-purpose device that handles outgoing routing and incoming distribution.
SERVSINV	Contains the names of the server subtending nodes and their associated gateways. The subtending nodes are the Audio Controller and the Dynamic Packet Trunk (DPT).
TELEPROF	Defines the link between a telephony profile and a destination media gateway controller (MGC).
TRKGRP	Contains customer-defined data for each trunk group that exists in the switch.
TRKSGRP	Lists the supplementary information for each subgroup that is assigned to one of the trunk groups listed in table TRKGRP.
TRKOPTS	Provisions special options on trunk groups. For our case, that option is dynamic and the signaling type is SIPT

When utilizing a Session Server Manager-only architecture, many of the above tables may be obsolete. Refer to upcoming sections for complete details.

119.4 Session Server Manager Description and Overview

The Session Server Manager is a platform for delivery of multiple applications. The Session Server Manager consists of a NEBS Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. The SIP Gateway application is the initial application for the Session Server Manager platform.

119.4.1Hardware

The hardware platform for the Session Server Manager is the Hewlett Packard HP-CC3310. Components include:

- Dual Intel 2.4 GHz P4 Xeon Processors
- Up to 12 GB RAM (Session Server is 4 GB)
- Memory Speed – 266 MHz DDR
- Local Disk – Dual 73GB or 146GB disk drives (Session Server is 73 GB)
- Multiple GigE copper interfaces (2 on-board plus 2 per NIC)

- 2U Form Factor

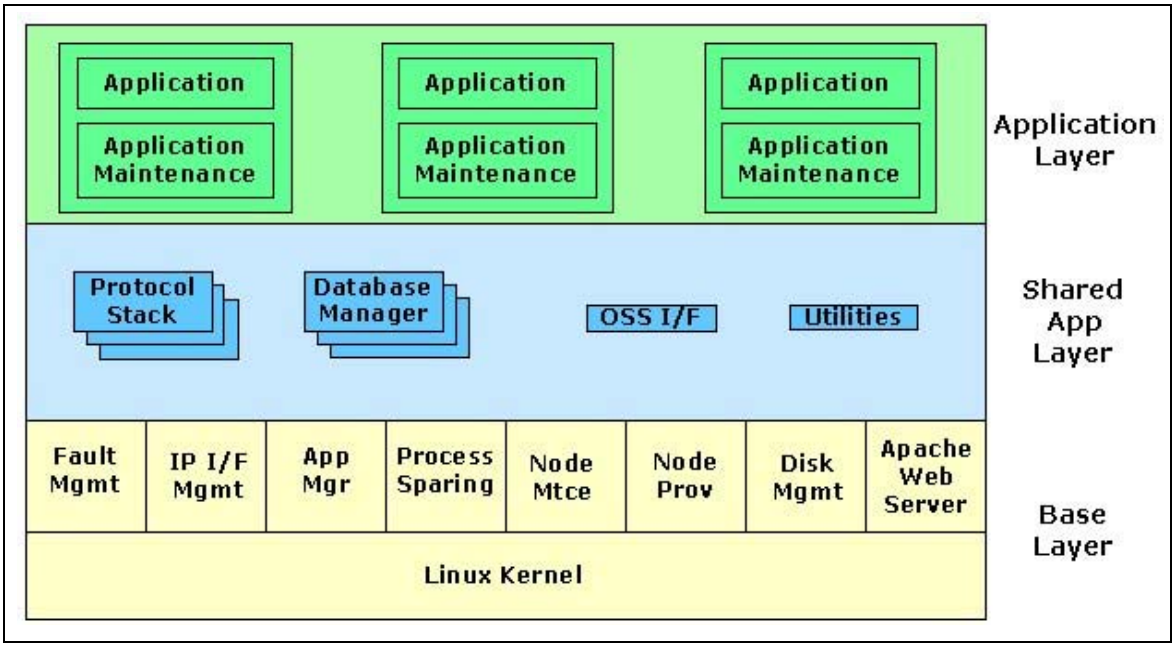
The HP-CC3310 provides processing, memory, and disk capacity for Storage Management (STORM), SIP, and planned SIP applications

119.4.2Software

The Session Server Manager Software has a layered architecture, which consists of the following:

- **The base layer**, which includes the Linux kernel along with a carrier-grade platform for fault management, sparing, and application initialization
- **A shared application layer**, which contains re-usable components that can be integrated as needed into higher level applications
- **An application layer** that includes a maintenance process for each application, which manages the associated processes.

Figure 6 Session Server Manager Software Architecture



119.4.2.1 Session Server Manager Base Layer

The base layer uses Linux version 2.4.22. This base layer provides Carrier Grade capabilities.

Note: This section represents an SN07 view.

Fault/SWACT Management

- Detects hardware faults on the platform
- Monitors for conditions that should prompt an activity switch
- Arbitrates failure requests from applications that need to initiate a SWACT.

IP Interface Management

- Maintains Gigabit Ethernet interfaces on the platform
- Allocates bandwidth to maintenance and application tasks
- Participates in the IP address takeover during an activity switch.

Application Manager

- Provides an interface for applications to bind their maintenance processes into the system
- Monitors and re-initiates application maintenance process as needed
- Provides a possible re-use of SDM application manager software platform.

Node Maintenance

- Provides interfaces for bringing the node into service and initiating application start-up
- Provides a craftsperson interface via a Web Server
- Supports manual and autonomous maintenance actions
- Monitors between active and inactive nodes to that insure failover can be initiated when running in synchronization.

Node Provisioning

- Provides a provisioning interface via Web Server for platform configuration parameters.

Disk Management

- Provides interfaces for disk access
- Supports the STORM application in CS 2000-Compact configurations.

Apache Web System

- Consists of Apache, Apache Tomcat, and Java Runtime environment
- Provides web-based interface for provisioning and maintenance
- Presents an integrated view for all applications running on the platform.

119.4.2.2 Session Server Manager Share Layer

The share layer contains reusable components that are independent of the applications using them.

Note: This section represents an SN07 view.

Application Data Synchronization

- Allows applications to checkpoint data between the active and inactive units at specific points in time.
- Supports variable length buffers that can be refined and versioned by the application

SIP Stack

- Provides an RFC-3261 compliant SIP interface, which can be incorporated into any application running on the platform
- Allows APIs and callback interfaces that permit applications to implement state machines based on event notifications.

Database Manager

- Provides persistent data storage for each application
- Introduces a SQL based database, which is accessed through ODBC and JDBC interfaces, that isolates each application from the underlying database product
- Supports data replication between active and inactive units, and ultimately between multiple active units.

Downstream Interfaces to Billing and OMs/Statistics

- Provides a collection point for billing, and OM data for the system
- Stores information to local disk, which can be accessed via maintenance interfaces
- Opens downstream feeds, in CS 2000 configurations, to SDM for billing and IEMS (Integrated Element Management System) for logs, alarms, and statistics.

Application-specific processes

These applications-specific processes include:

- An application maintenance process
  - — Initiates and then monitored by the base layer application manager
  - — Creates all other processes associated with the application
  - — Provides maintenance actions to transition the application in and out of service.
- Call/Transaction Processing process(es)
  - — Initiates and then monitored by base layer application manager
  - — Creates all other processes associated with the application
  - — Provides maintenance actions to transition the application in and out of service.

119.4.2.3 Session Server Manager Application Layer

The Application Layer consists of a set of applications. The applications may or may not communicate with each other. Each application includes a maintenance application used for monitoring and interacting with the application. The SIP Gateway is the initial application delivered on the Session Server Manager.

119.4.3CS 2000 Architecture with Session Server Manager

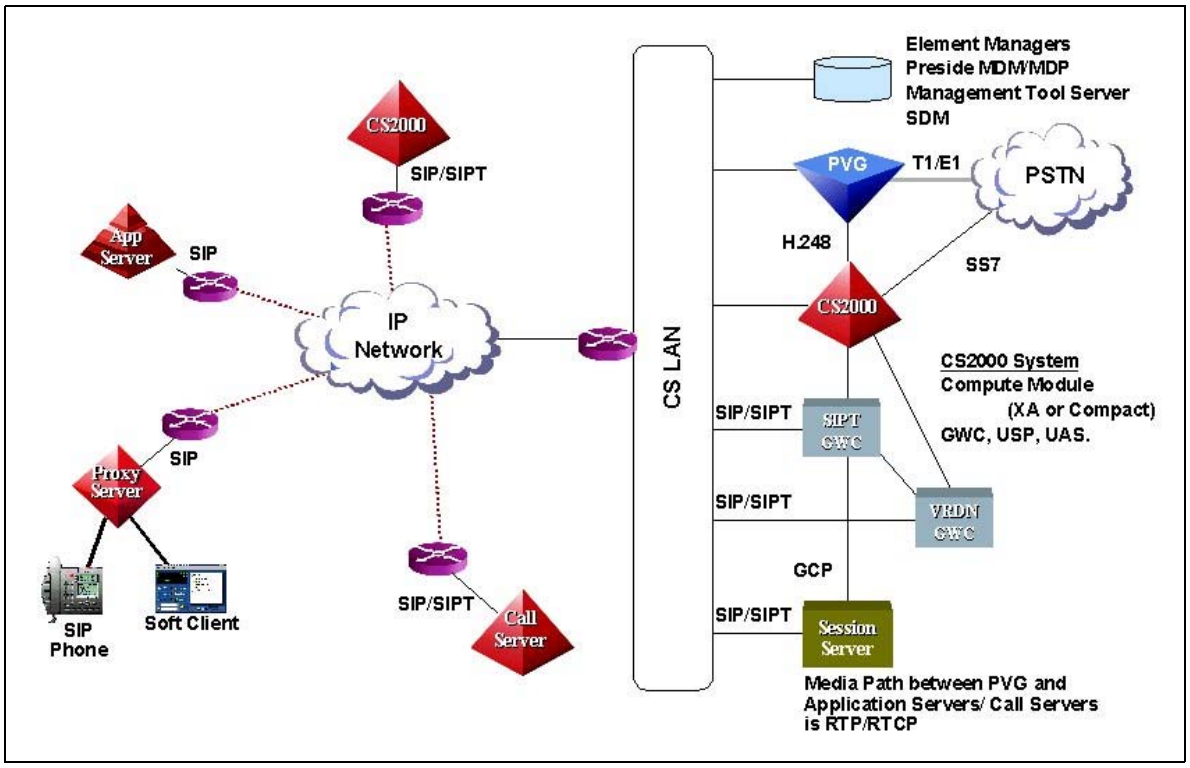
119.4.3.1 VRDN Present

With the Virtual Router Distribution Node (VRDN) present, the Session Server Manager is a peer to the VRDN. The SIPT Gateway Controller will maintain current calls through the VRDN, but will establish new calls through the Session Server Manager. Once the Session Server Manager is providing the SIP Call Processing function and no calls are left on the VRDN, the VRDN can be removed.

Note 1: Installation of the Session Server Manager at the Near End Call Server, requires actions at the Far End Call Server. These actions are addressed in the upgrade section.

Note 2: Once the Session Server Manager is installed in a SCS 2000, the VRDN is to be removed. A configuration with Session Server Manager and VRDN in the same SCS 2000, is only supported as an upgrade path.

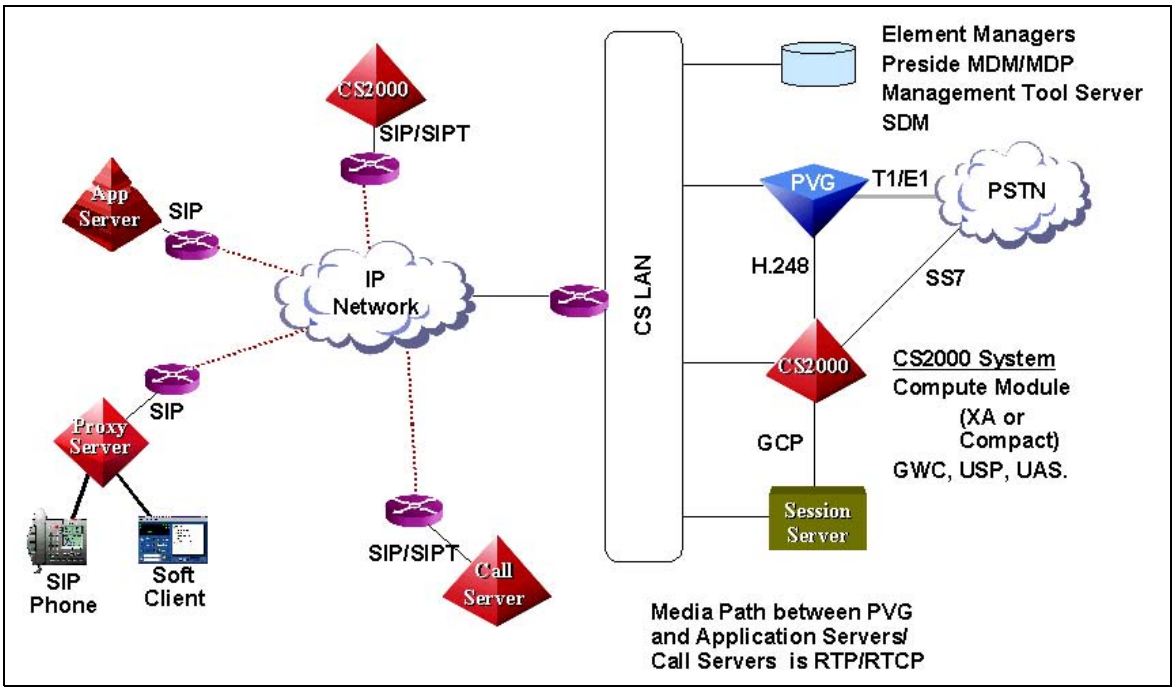
Figure 7 Session Server Manager with the VRDN present



119.4.3.2 VRDN not Present

When the VRDN is not present, the SIPT Gateway Controller establishes all calls throughout the Session Server Manager.

Figure 8 Session Server Manager with the VRDN not present



119.4.4Services and Features

The Session Server Manager interoperates with User Agents on the SIP Network.

- Calling Number Delivery / Blocking
- Calling Name Delivery / Blocking
- Suspend / Resume Handling

119.4.4.1 SIGNALING INTEROPERABILITY

- TDM signaling
  - — ANSI ISUP
  - — ANSI PRI
- Variants

  SIP Signaling from the Session Server Manager is tunneled into the CS 2000 as Dynamic Packet Trunks (DPT). The DPT trunk datafill in the CS 2000 DPT Trunks are provisioned as ISUP trunks. For the SIPT implementation, any variant is allowed for the DPT trunks. SIPT allows

transport of the ISUP payload in the SIP message. Transport is in accordance with the T1S1.7/2003-179R2 - T1.SIP Interworking Output Baseline Document.

SIP Gateways may not support SIPT and not provide an ISUP payload in the SIP message. When communicating with a SIP Gateway that does not provide ISUP payload in the SIP message, the CS 2000 can generate an ISUP payload; however, the payload will be based on the variant type of the DPT trunk. The SIP implementation can only generate ISUP payload for IBNT2 (for NA loads), IBN7 (for International loads), or IT.

Note: DPT trunks to SIP gateways can only be provisioned as IBNT2/ IBN7 or IT.

119.4.4.2 BEARER INTEROPERABILITY

- Media
  - — Fax -G3, T.38
  - — DTMF- In-band G.711, Out-of-band RFC2833
  - — CODEC -G.711 A/u-law, G.729a/b, codec negotiation
  - — H.248

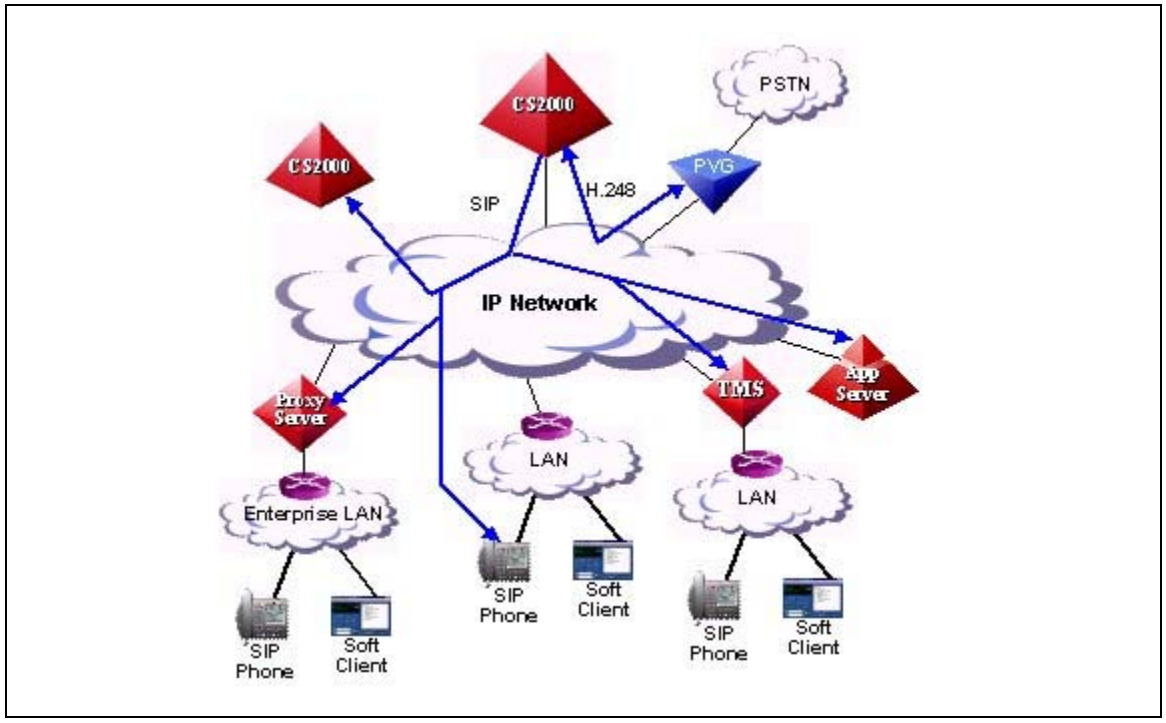
119.4.4.3 MCS & CS 2000 INTEROPERABILITY

- All SIPT supported services and functionality carried over from SN06 are supported on the Session Server Manager
- Backward SIPT compatibility with previous release
- CS 2000 with SN07 is supported with MCS 3.0.

119.5 SIP Compliancy

The initial offering is to allow interoperability with third party proxy servers and application servers. This implementation will update Nortel's compliance to the current IETF standards and drafts.

Figure 9 SIP Standards Compliance



The solution will provide support for (but not limited to) the following standards and drafts:

- RFC 3261[1] - SIP: Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3326 - SIP Reason Header
- RFC 2976 - The SIP INFO Method
- RFC 3264[2] - An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265 – Specific Event Notification (SUBSCRIBE/NOTIFY)

[1]Session Server Manager commits to those requirements pertinent to a User Agent Client. Session Server Manager is not a User Agent Server, nor a Back to Back User Agent in SN07.
[2]For SIP to SIP calls, as a B2BUA, we are compliant with RFC 3264.
For SIP to H.248 calls, as a terminating gateway, we are partially compliant due to incompatibilities between the specifications.

- RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- Referred-by Mechanism – draft-ietf-sip-referredby-02
- Q.1912.5 - Interworking Between Session Initiated Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part
- SIP Replaces Header – draft-ietf-sip-replaces-03
- SIP Call Control Transfer – draft-ietf-sipping-cc-transfer
- T1S1.7/2003-179R2 - T1.SIP Interworking Output Baseline Document

119.6 SIP Call Processing

In the SN07 release of the Session Server Manager platform, the SIP Gateway application is the only application supported. This section discusses high-level details about this application, and the differences between the Session Server Manager- and GWC-based SIP call processing.

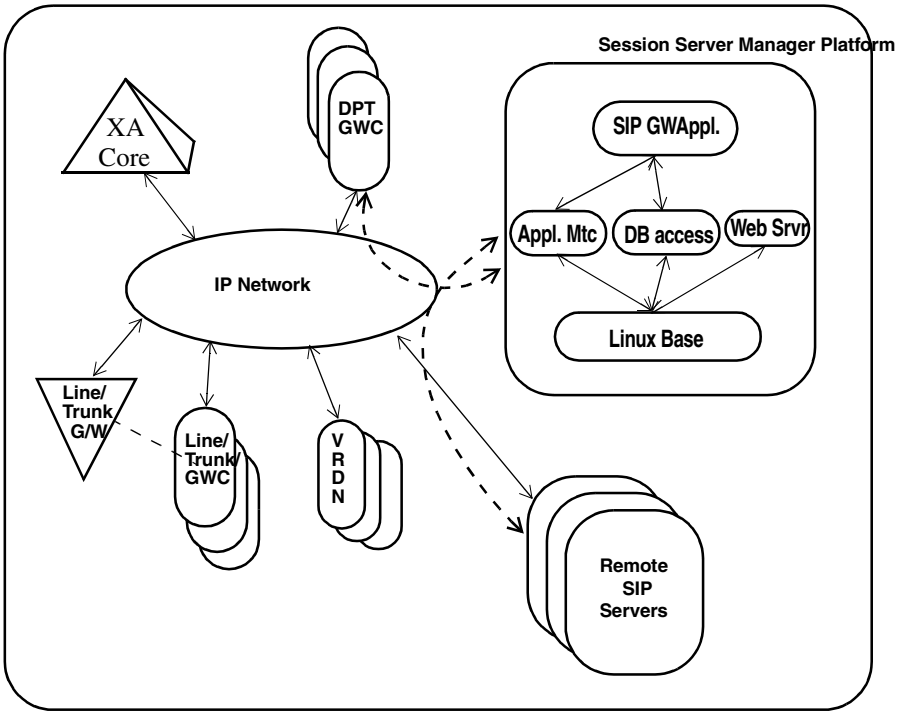
Also presented are example call flows for an incoming and outgoing SIP call.

119.6.1 Description and Overview

The SIP Gateway application on the Session Server Manager platform is the entity primarily responsible to set-up and tear-down calls, maintain accessibility to DPT GWCs and remote SIP servers, and other functions. The SIP Gateway application provides an RFC 3261 compliant SIP interface for interworking. This application also provides the necessary support to be compliant with other RFCs including 3262 (Reliability of Provisional Responses in SIP), and 3264 (SIP Event Notification Mechanism).

Figure 10 illustrates a high-level view of the Session Server Manager when placed within a SCS 2000 SIP solution.

Figure 10 Session Server High-Level view



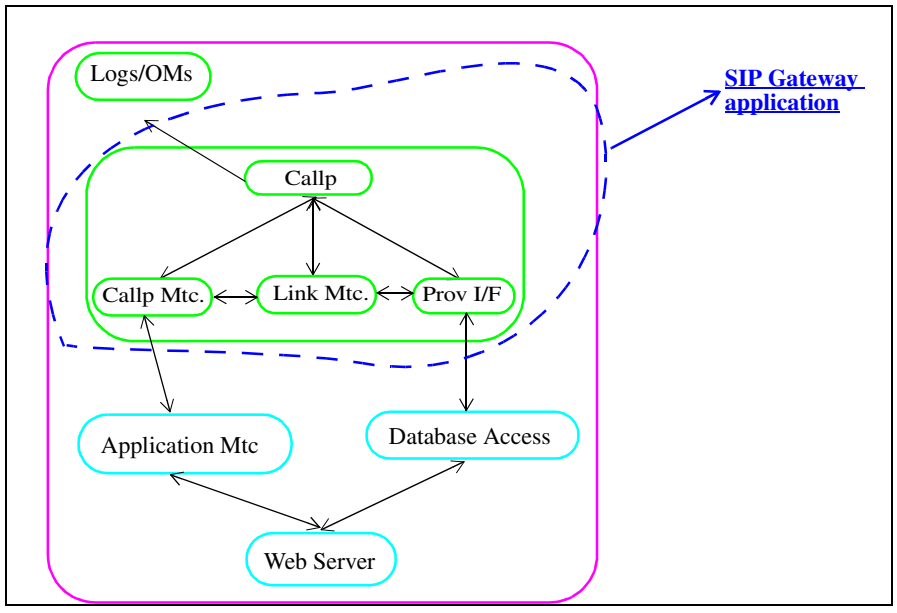
With the new platform, SIP call processing is done within the call processing application in the Session Server Manager. The Session Server Manager communicates with the DPT GWC in a generic call control/maintenance protocol, which will trigger the usage of Dynamic Packet Trunking (DPT) infrastructure to setup and tear-down calls.

As illustrated in Figure 10, "Session Server High-Level view", the Session Server Manager communicates with all the DPT GWCs as well as with remote SIP servers. In this model, all SIP-specific behavior is performed on the Session Server Manager as opposed to the GWC. CS 2000 SIP solution with a Session Server Manager does not require a VRDN, and the tasks originally performed by the VRDN are moved into the Session Server Manager.

Additionally, numerous configuration/maintenance capabilities are also provided within the Session Server Manager and are discussed in subsequent sections of this document.

The SIP Gateway application in the Session Server Manager interworks with different logical components, including call setup, maintenance, and provisioning, to satisfy different roles and responsibilities. Figure 11, "Session Server SIP Gateway application Logical View" illustrates the different logical components that constitute a SIP Gateway application.

Figure 11 Session Server SIP Gateway application Logical View



- **Call Processing Application:** This is the main component responsible for integrating different logical components to enable setup/tear-down of calls. It is responsible to send/receive incoming SIP messages, parse/analyze the message, and take appropriate action. It maintains a call state machine and

generates OMs and logs whenever necessary. It also triggers a billing application to generate a billing record for calls.

- **Call Processing Maintenance**: This component provides the interface for interworking with an application maintenance entity to perform maintenance activities on the SIP Gateway application. When a craftsperson performs a maintenance action, this component is ultimately notified and performs the necessary action. Please see “119.8.2.5 SIP Gateway application maintenance” on page 1406 for additional information.
- **Link Maintenance**: This component is responsible for maintaining the availability of remote SIP servers as well as the availability of SIP GWCs. When bringing the SIP Gateway application into the server, this component discovers and maintains the list of SIPT GWCs available for call processing. In addition, this component is also responsible for maintaining a list of remote SIP servers that are available for communication.
- **Provisioning Interface**: This component provides the call processing entity access to all the provisioned data. Call processing queries this component at various points, including startup, take-down, and call setup, to determine the course of action to be taken.
- **OMs/Logs**: Different components interact with OM/log subsystem to generate logs and OMs. Please refer to sections “119.8.2.7 Logs” on page 1413 and “119.8.2.8 Operational Measurements” on page 1415 for additional information.

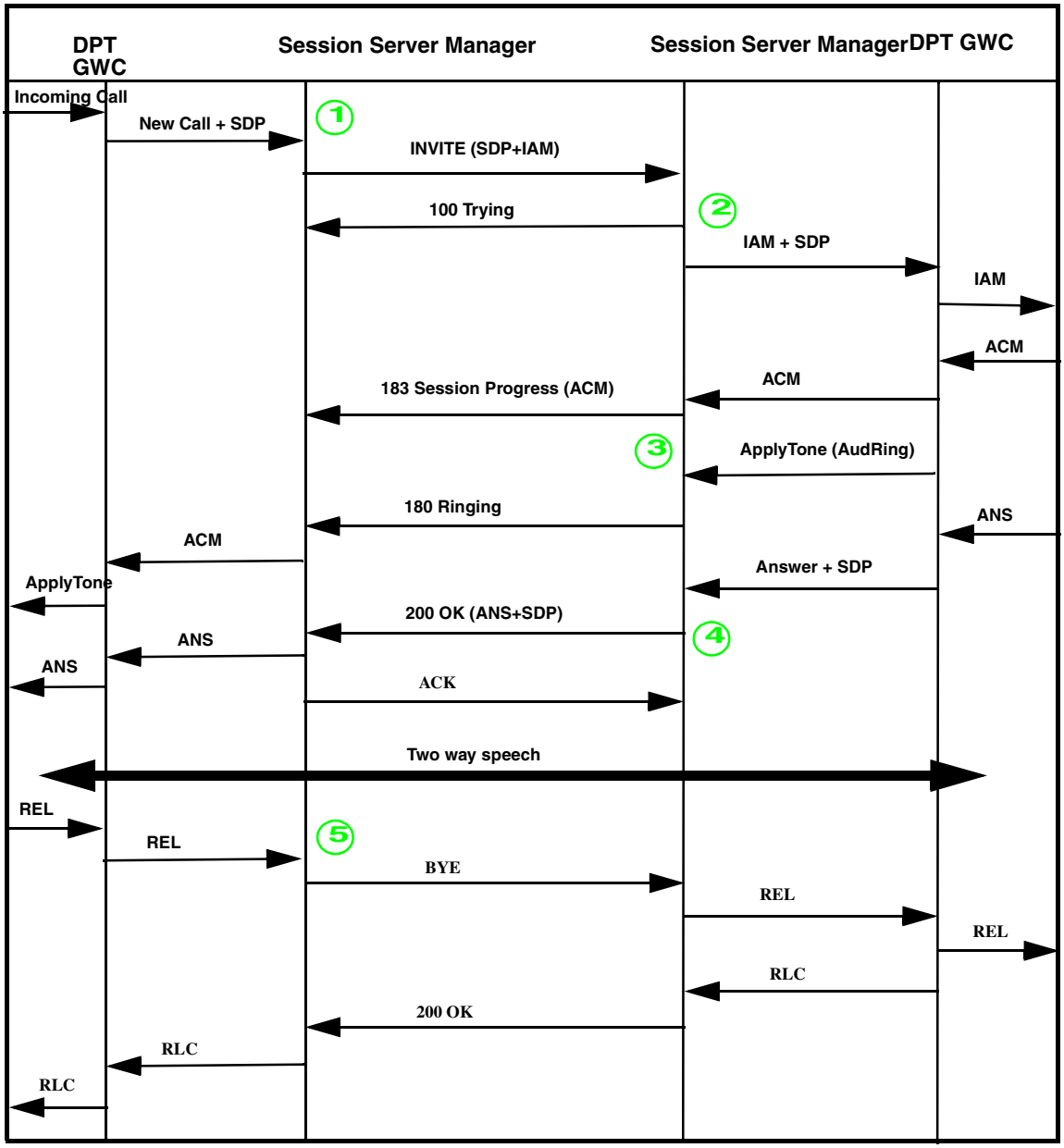
119.6.2Call Flows

Both incoming and outgoing calls between SIP and the Session Server Manager make use of table SIPLINK that is datafilled in the core. SIP Access Link name information from table SIPLINK is downloaded to the Session Server Manager during the DPT GWC discovery process. In order to have successful call processing with a remote SIP server, each remote SIP server must be associated with SIP Access Link name. The SIP Access Link name is uniquely associated with a trunk group in the Core which in-turn is used for set-up of translations for various call-types.

Please refer to configuration section of this document for more information on table SIPLINK.

Figure 12, "Sample Session Server Manager SIP Call Flow" captures a sample call flow for a SIP bridging scenario with Session Server Manager on both sides. Key points on the incoming and outgoing side of the call are discussed.

Figure 12 Sample Session Server Manager SIP Call Flow



For the purpose of this call flow, it is assumed that the core is already set up with translations to route the call over appropriate SIP trunk. A trunk is considered a SIP trunk if it is datafilled as SIPT in table TRKOPTS.

Also, it is assumed that the call flow is happening on a reliable transport protocol like TCP.

1. The core selects one DPT GWC to process the outgoing call. If there is more than one DPT GWC, then the core employs a round-robin algorithm to determine the GWC to which to present the call.

On receipt of the IAM message, the DPT GWC on receipt of the IAM message does the following:

a. Extracts the trunk information and determines if a SIP Access Link is associated with this trunk.

b. If a SIP Access Link is not associated with this call, the call is setup as a pre-Session Server Manager SIP call.

c. If a SIP Access Link is associated with this call, the IP address of the Session Server Manager is retrieved and the IAM is forwarded to the Session Server Manager. (The IP address of the Session Server Manager is sent to the GWC as part of the GWC discovery process. This is discussed in the configuration section).

d. The Session Server Manager then extracts the SIP Access information and retrieves information regarding the remote SIP server to which the call is intended.

e. The SIP INVITE message is constructed with appropriate headers, session description, and payloads (if applicable) and is sent to the remote SIP server.

A sample INVITE message is shown below:

```
INVITE sip:2461803@47.174.73.242 SIP/2.0
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
User-agent: CS2000/7.0
Mime-Version: 1.0
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,NOTIFY,REFER
Via: SIP/2.0/TCP 47.142.210.200:5060;branch=z9hG4bK-3f7776e3-160d-11156ea5
Contact: <sip:9192461802@47.142.210.200>
Content-Type: multipart/mixed ;boundary=unique-boundary-1
Content-Length:358

--unique-boundary-1
c: application/SDP ;charset=ISO-10646
v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

--unique-boundary-1
c: application/ISUP ;version=gr394 ;base=gr394

"
```

2. On receipt of an incoming SIP call, the Session Server Manager sends back a 100 Trying message to the sending entity while the INVITE is processed. A call processing application retrieves the host or IP address information from the header information to determine the characteristics of the sending entity.

Once the remote server profile is retrieved, the SIPLINK name associated with the remote SIP server is retrieved. The ISUP IAM payload, if any, is also retrieved and forwarded to the DPT GWC along with the SIPLINK information.

The DPT GWC gets the SIP LINK information from the Session Server Manager and determines the trunk, on which the incoming call is processed.

A sample SIP 100 Trying message:

```
SIP/2.0 100 Trying
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/TCP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Length:0
```

3. Once the incoming INVITE is processed, the remote SIP server can send any number of provisional responses (18X). ISUP payloads, such as ACM or CPG, are encapsulated in an appropriate provisional response if the remote server is capable of handling ISUP messages.

It is also possible that the provisional responses are used to apply local ringing and/or pass any media information to which the terminating side would like the originating side to hear.

A sample 183 Session Progress and 180 Ringing messages are as follows:

180 Ringing:

```
SIP/2.0 180 Ringing
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Length:0
```

183 Session Progress:

```
SIP/2.0 183 Session Progress
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
```

```
CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Type: application/SDP ;charset=ISO-10646
Content-Length:171

v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5006 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

4. When the terminating side answers the call, it forwards the ANS ISUP message (if applicable) along with its session description in a 200 OK message to the originating side.

The originating side extracts the relevant information and forwards the terminating SDP to the appropriate endpoint. It also returns a SIP ACK request to the terminating SIP server to complete the three-way hand-shake.

A sample 200 OK and ACK messages are as follows:

200 OK

```
SIP/2.0 200 OK
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Content-Transfer-Encoding: binary
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Type: multipart/mixed ;boundary=unique-boundary-1
Content-Length:2
--unique-boundary-1
c: application/SDP ;charset=ISO-10646
v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

--unique-boundary-1
c: application/ISUP ;version=gr394 ;base=gr394
```

ACK:

```
ACK sip:2461803@47.174.73.242 SIP/2.0
From: <sip:919246180247.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 ACK
User-agent: CS2000/7.0
Max-Forwards: 70
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
```

```
Via: SIP/2.0/UDP 47.142.210.200:5060;branch=z9hG4bK-3f7776e4-1a39-4674927a
Contact: <sip:9192461802@47.142.210.200>
Content-Length:0
```

5. When either the originating or terminating sides ends the call, the ISUP REL message is forwarded to the Session Server Manager. The Session Server Manager then builds a SIP BYE message, encapsulates the ISUP message, if applicable, and sends it to the remote SIP server.

The remote SIP server on receipt of the BYE message, extracts the ISUP message, if applicable, and forwards to the DPT GWC on its way to the core. It also responds to the BYE with a 200 OK and encapsulates the ISUP RLC whenever applicable.

A sample BYE and 200 OK are as shown:

```
BYE sip:2461803@47.174.73.242 SIP/2.0
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f774d15-1d8b-7effbf92
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f774966-1453-43179ce
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 4 BYE
User-agent: CS2000/7.0
Content-Transfer-Encoding: binary
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
4d31-8bca-68dc7389
Content-Type: application/ISUP ;version=gr394 ;base=gr394
Content-Length:6
```

200 OK for BYE:

```
SIP/2.0 200 OK
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f774d15-1d8b-7effbf92
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f774966-1453-43179ce
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 4 BYE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
4d31-8bca-68dc7389
Content-Length:0
```

119.7 Carrier Grade Topics

This section describes various aspects of the Session Server Manager platform that contribute to making it a carrier grade product.

119.7.1Call Audits

The Session Server Manager platform provides a secondary call auditing capability for cleaning up stranded calls and reclaiming any call processing resources on the Session Server Manager not associated with valid calls. During normal operation, Session Server Manager calls will be cleaned up properly on call takedown or when a maintenance action results in calls being ended. The call audit assures that the calls are not left up indefinitely due to some type of lost message or other error condition.

Session Server Manager calls are audited in two directions. One audit is between the Session Server Manager and the DPT GWC associated with the call. A second audit is between the Session Server Manager and the remote SIP server associated with the call. Calls are terminated whenever any of three components (Session Server Manager, DPT GWC, or remote SIP server) do not recognize the call being audited.

Call audits between the Session Server Manager and the remote SIP server can be configured to on a per SIP server basis, using either a SIP Info message or a SIP re-invite. When provisioning the Remote SIP Server, the “Use Info for Long Call Audit” parameter can be set to Yes or No to indicate whether to use the “SIP Info message” or not. Refer to “119.8.2.4.2 Remote SIP Servers” on page 1379 for details on provisioning or modifying Remote SIP Server datafill.

If the SIP Info audit method is specified, the Session Server Manager will send a SIP Info message to the SIP server destination at regular intervals. If no response is received on two successive audit attempts or if an error response is received, the call will be taken down.

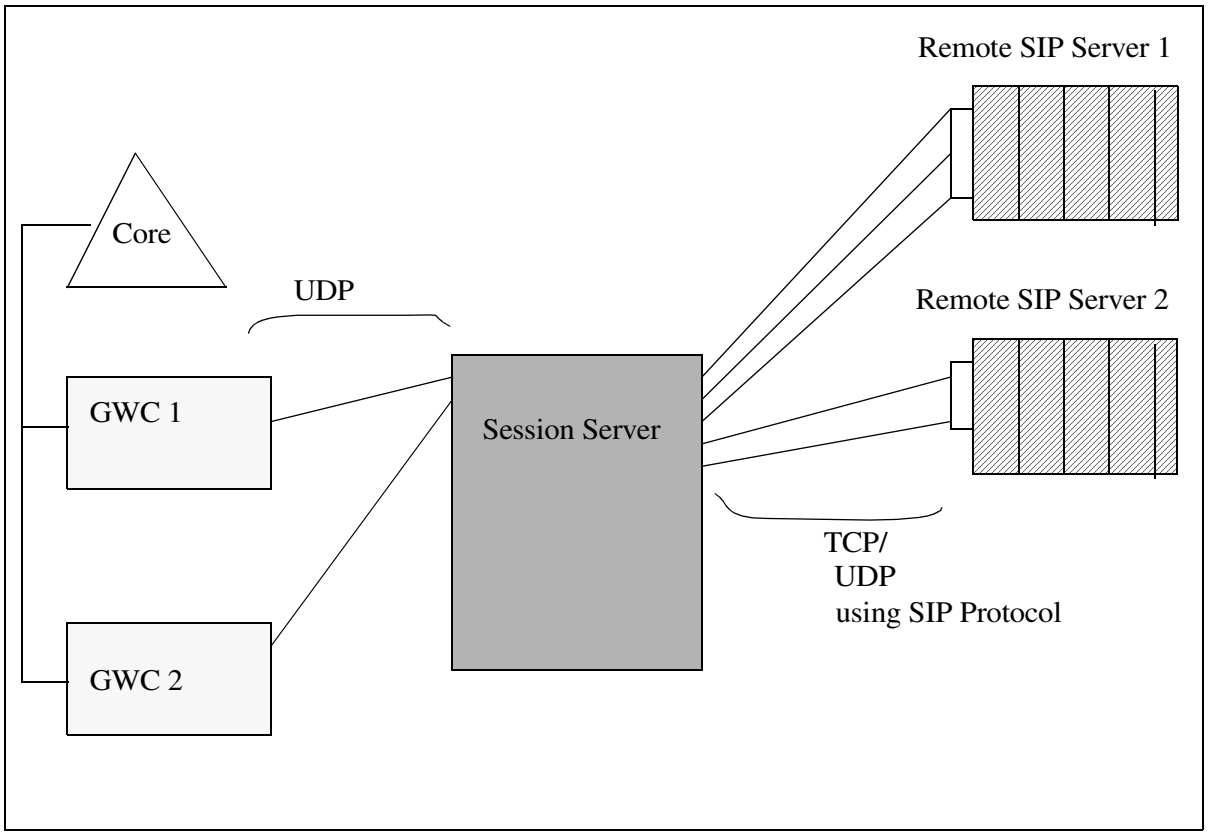
If the remote SIP server does not support the SIP Info message for this purpose, the SIP server must be configured to use the SIP re-invite method for auditing. If this approach is selected, a SIP Invite will be sent at regular intervals for a call once it is answered. Again, successive failures or no response results in the call being taken down. If the call is not answered after multiple audit intervals, the call will be taken down.

119.7.2Link failover mechanism

The link failover mechanism involves routing calls and verifying connectivity between the Gateway Controller (GWC) and the Session Server Manager platform and between the remote Media Gateway Controller (MGC) and the Session Server Manager. The remote SIP server could be a proxy server or a final destination.

Communication between the GWC and the Session Server Manager is accomplished with a normalized proprietary protocol using UDP as the transport medium. Communication between the Session Server Manager and the remote SIP server is through SIP or SIPT with a transport medium of either UDP or TCP. The diagram below illustrates the connectivity between the different entities.

Figure 13 Component Connectivity



To ensure that the remote SIP server is ready to receive messages from the Session Server Manager, an audit mechanism is optionally established between the Session Server Manager and its associated remote servers. The audit mechanism is accomplished by the Session Server Manager sending the SIP OPTIONS request message to the SIP servers upon a consistent interval and waiting for the response. This ability will be configurable per remote server.

When provisioning the Remote SIP Server, the "Options Supported" parameter can be set to Yes or No to indicate whether to use the "Options Supported message" or not. Refer to "119.8.2.4.2 Remote SIP Servers" on page 1379 for details on provisioning or modifying Remote SIP Server datafill.

When the Session Server Manager sends out a SIP OPTIONS message, if a time-out occurs or any failure causes the server using that IP address to be unreachable, the failure count is updated for that IP address. Whenever a message is received on

that IP address, the failure count is reset. If the failure count reaches a specified threshold, the IP address is marked as inactive. If a new message is received on the inactive IP address, it is then reset to ACTIVE.

When all the IP addresses for a particular remote server are marked as inactive, each GWC is sent an access link status message indicating that the link is down. Additionally, an alarm will be raised on the Session Server Manager indicating the SIP-Server message path failure. When at least one IP address for that server becomes responsive, each GWC is sent an access link status message indicating that the link is up.

If a particular server does not care to support the OPTIONS message exchange capability, then its associated access links may appear to be always active. However, if repeated attempts to send SIP messages to a particular destination on a given IP corridor consistently result in failure, then once a threshold of failure has been attained, the access link will be considered out of service. As in the OPTIONS scenario, this results in the transmission of an access link status message to the GWC/Core to indicate the change in status. The access link will be returned to service upon receiving a new call from the IP address in question. In addition, the failed link will periodically be retried for call processing to determine if the link has become active again. If the link continues to fail on these retries, the link will remain out of service and any other IP routes provisioned for the destination SIP server will be used to complete the call.

Additionally, if a particular access link has been orphaned from its server destination, i.e., provisioning has removed a particular access link's remote server association, then this will be treated in the same manner as an audit failure.

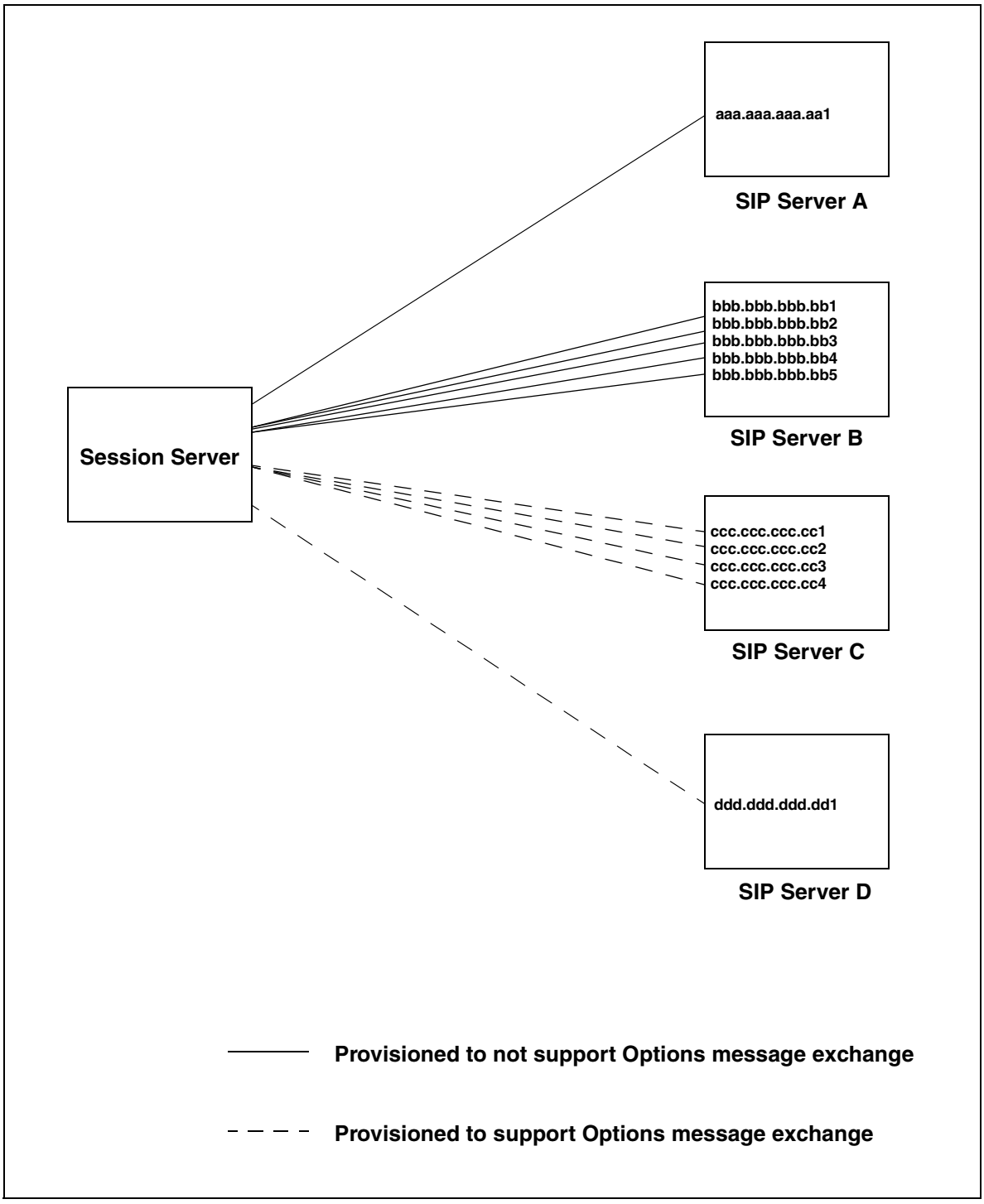
The Session Server Manager is also responsible for responding to SIP OPTIONS messages sent from remote SIP servers. Depending on the maintenance state of the Session Server Manager, it will either respond with a 200 OK (Session Server is in service) or with a 503 (Session Server is in deload or BSY state). When the Session Server Manager is in the deload or BSY state, it will not send SIP OPTIONS messages at each audit interval.

To summarize, link viability to a remote SIP server may be maintained in various different ways based on provisioning and network configuration.

1. Server A in Figure 14 depicts an access link with a singular IP presence may be configured to disable the OPTIONS message exchange mechanism. From the Session Server Manager viewpoint, this connection is always active regardless of the actual transport status, until it achieves a specific level of consistent failure. At this point the access link will be removed from service.

2. As shown in Figure 14 by server B, an access link provisioned to not support OPTIONS messages may consist of multiple IP address destinations. These multiple IP addresses are progressively stepped through service calls bound for the remote SIP server on the given access link. In this setup, if some transport layer problem is encountered, the next IP destination in the list may be attempted until all possible routes are exhausted. Again, if all routes surpass the send failure threshold, the access link will be removed from service.
3. In the figure, the access link to server D is comprised of a single IP address configured to support OPTIONS messages. With the OPTIONS messaging ensuring a valid network connection to the server, any call that reaches the Session Server Manager bound for server D is much more likely to find its intended IP tunnel open. However, as in the server A configuration, if some transient network fault occurs that was not detected by the audit mechanism prior to an attempted message transmission on the link, there is no further fallback mechanism.
4. The final permutation of OPTIONS support and IP presence is embodied in the server C connection. This setup ensures messaging link integrity while also providing the ability to round-robin through the suite of possible destinations to the server if a transient network failure is encountered.

Figure 14 Maintaining SIP Server Links from the Session Server Manager



119.7.3Link Status in the CM

In the CM, the status of an access link can be monitored by posting the associated SIPT trunk group[1] at the MAPCI;MTC;TRKS;DPTRKS level of the MAP. Since the CM has no direct communication with the Session Server, it is dependent on receiving link status information from the SIPT gateway controllers, who receive Access Link Status messages from the Session Server and pass them on to the core.

The status of the access link on the Session Server is determined using the strategy discussed in the previous section (Link Failover Mechanisms). Any change in a link's status detected by the Session Server is immediately propagated to each SIPT gateway controller, then to the core. As long as there is stable communication between the core and at least one SIPT gateway controller and the session server, the status of a SIPT trunk in the CM should mirror that of its associated access link.

For a trunk to be INS at the DPTRKS MAP level, the following conditions must exist:

- On the Session Server, the access link associated with the trunk must be mapped to a Remote SIP Server.
- On the Session Server, the associated Remote SIP Server must have at least one active IP connection. An active connection is defined as one of the following:
  - For a Remote SIP Server configured to support SIP OPTIONS messaging for heartbeats, a connection is active if the Session Server is receiving timely 200 OK responses to its SIP OPTIONS requests on at least one of the IP connections to the remote server.
  - For a Remote SIP Server that doesn't support OPTIONS for heartbeats, a connection is active if the Session Server is successfully sending and/or receiving SIP messages at a level above the failed message threshold on at least one of the IP connections to the remote server. Note that by default the connection is considered active until proven otherwise by exceeding the failed message threshold during call processing.
- The Session Server application must be UNLOCKED.
- In the CM, at least one SIPT GWC must be in-service at the MAPCI;MTC;TRKS;DPTTRM level of the MAP.

When the last of these conditions is met, the Session Server sends an Access Link Status message indicating the link is up to each SIPT GWC. The gateway controllers then propagate the message to the CM, resulting in the state of the trunk group changing to INS.

[1]The association of the trunk group to an access link is defined in CM table SIPLINK.

Once a trunk group is INS, a failure of any of the first three conditions will cause the Session Server to send an Access Link Status message indicating the link is down to each SIPT GWC. The gateway controllers then propagate the message to the CM and the CM changes the status to SYS.

If a situation occurs where there are no longer any in-service SIPT GWCs, the CM changes the state of the trunk to SYS. This is the only time the CM undertakes unsolicited action to remove a link from service; otherwise, link status in the core is totally under the control of the Session Server. In other words, when at least one SIPT GWC is in-service at the DPTTRM level, the only way the trunk group's state can be changed (other than by manual intervention) is if the Session Server sends an Access Link Status message to report the state change.

If the Session Server goes out of service due to a system failure or because of improper shutdown (which would disrupt the ability to send the Access Link Status message to the gateway controllers), all INS SIPT trunks associated with any access links on the Session Server will remain INS.

119.7.4Scalability and Load Balancing

In the initial release of the Session Server Manager product, a single redundant pair of Session Server boxes will satisfy the call volume requirements. If call volume requirements increase in the future, later releases of the Session Server Manager product will address the need to expand the network to include multiple redundant pairings of Session Servers.

If additional DPT GWCs are required to handle increased call volume, they can be introduced without any impact to call processing. In addition to the normal commissioning and provisioning required to add a new DPT GWC, the IP address of the GWC(s) must be added to the list of GWCs connected to the Session Server Manager. This change is done through the web provisioning interface on the Session Server Manager and it can be made while the Session Server box is in service. The new GWC(s) will be used for call processing once they are brought in service. The Session Server Manager uses a simple round-robin scheme to distribute incoming calls across all in-service DPT GWCs.

119.7.5Performance

The committed performance of the Session Server Manager, in SN07, is to meet VRDN equivalency. The VRDN currently supports a call rate of 900K Busy Hour Half Call Attempts (A half call is either the originating leg of a call, or the terminating leg).

The Session Server Manager will support up to 37,5000 simultaneous calls. Given a call model of 2 minute hold time and 30 second intercall delay, this provides a capacity of 900K BHHCA.

119.7.6Upgrades

This section describes the upgrade procedures for offices that want to introduce the Session Server Manager platform into their network. Procedures vary depending on whether the office was previously running SIPT traffic using the VRDN architecture or not. The following topics are covered in this section:

- Upgrading an SCS 2000 office to include the Session Server Manager when SIPT traffic was not previously handled in the office.
- Upgrading an SCS 2000 office to include the Session Server Manager and migrating existing SIPT traffic from the VRDN architecture to the Session Server Manager platform.
- Upgrading the Session Server Manager with new software loads and/or maintenance releases (MRs).

119.7.6.1 Upgrading to Session Server Manager without VRDNs

This section is for offices that did not have SIPT traffic prior to introducing the Session Server Manager platform. Before the Session Server can be inserted in the network, the CS 2000 must first be upgraded to an SN07 or later release. Adding the Session Server Manager is a completely separate step from upgrading the office and sufficient soak time should be employed after the upgrade to SN07 or later, before the Session Server Manager platform is introduced.

The normal upgrades steps should be followed for upgrading the CS 2000, including upgrading peripherals and the DMS core. In addition to requiring an SN07 or later core release, the Session Server Manager platform also requires that all DPT GWC peripherals be at an SN07 or later release. Since the office was not previously running SIPT traffic, DPT GWCs may need to be added or existing TDM GWCs need to be converted to DPT GWCs. The normal procedures for adding or converting to DPT GWCs should be followed, there are no new commissioning or provisioning steps required for the DPT GWCs in order to have them work with the Session Server Manager platform.

Once the upgrade is complete and the DPT GWCs are in place, the following steps should be followed to add the Session Server Manager platform:

- Connect the Session Server Manager hardware platform to the CS 2000 LAN.
  Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for connection information.
- Commission the Session Server Manager platform.
  Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for commissioning information.
- Provision core tables to add DPT trunks (TRKGRP, TRKSGRP, and TRKOPTS) and to map the new DPT trunks to SIP access link names in

new table SIPLINK. For more information see “CS 2000 OAMP” on page 1366. In a later step, the SIP access links will be mapped to remote SIP server destinations through the Session Server Manager web interface.

- Provision the Session Server Manager platform using the web interface. For more information see “Session Server Manager OAMP” on page 1368.
- Bring DPT GWCs and DPT TIDs in service, if that hasn’t been done already. This is done using normal procedures for DPT GWCs.
- Bring the CSC 2000 - SIP Gateway application in service using the web interface. For more information see “SIP Gateway application maintenance” on page 1406.
- Once all components (DPT GWCs and Session Server application) are in service, access link names provisioned in core table SIPLINK are transferred to the Session Server Manager and can be seen through the web interface. Complete the Session Server Manager provisioning by mapping the access link names to remote SIP server destinations. For more information see “CS 2000 OAMP” on page 1366.
- Change DMS translations as appropriate to make use of the new DPT trunks for both incoming and outgoing calls. Once the translations changes are made, SIP traffic can begin to flow through the Session Server Manager platform. Customers may choose to route only a small set of test traffic through the Session Server Manager at first, before completing translations changes to include all the desired SIP/SIPT traffic.

119.7.6.2 Upgrading to Session Server Manager with VRDNs

This section is for offices that have existing SIPT traffic using the VRDN architecture and the Session Server Manager is being introduced as a replacement for the VRDNs. With the SN07 release of the Session Server Manager product, SCTP is not a supported transport protocol for SIPT traffic. Therefore, existing SIPT traffic through VRDNs using SCTP cannot be migrated to the Session Server Manager. If UDP is used for the SIPT traffic through the VRDN, that traffic can be migrated to the Session Server Manager using the procedures defined in this section.

Before the Session Server Manager is introduced, the office must first be upgraded to an SN07 or later release. During and immediately after the upgrade, SIPT traffic will continue to flow through the VRDNs. DPT GWCs with an SN07 or later load are capable of handling both traffic through VRDNs and traffic through the Session Server Manager at the same time.

Other than upgrading the DPT GWCs to an SN07 or later release as part of the upgrade process, no additional provisioning changes are needed to make the DPT GWCs work with the Session Server Manager.

Once the CS 2000 upgrade is complete and sufficient soak time has passed to ensure that the upgrade was successful, the Session Server Manager platform can be introduced. The following steps should be followed to add the Session Server Manager and migrate SIPT traffic from the VRDNs to the Session Server Manager:

- Before installing the Session Server on the SN07 CS2K that is being upgraded, be sure that all SN06 CS2Ks that exchange SIP-T traffic with this office have the appropriate core and GWC patches applied. SN06 core patches ATM83P2F and ATM84P2P must be applied to allow the destination IP address of the SN07 CS2K to be changed in table MGCINV. Do not make this configuration change at this time, just make sure the patches are applied. GWC patch XZB41GZU must be applied to all DPT and VRDN GWCs at the SN06 switches to allow them to receive SIP traffic from the Session Server.
- Connect the Session Server Manager hardware platform to the CS 2000 LAN.
  Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for connection information.
- Commission the Session Server Manager platform.
  Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for commissioning information.
- Provision new core table SIPLINK with SIP access link names. SIP access links are mapped to SIP server destinations through the Session Server Manager web interface in a later step. In this step, DO NOT provision any DPT trunks against the SIP access link names in table SIPLINK. Instead, use '$' when provisioning the DPT trunk in table SIPLINK. Table SIPLINK will be revisited at a later step to add the trunk-to-link mapping when it is time to actually swing outgoing traffic from the VRDN to the Session Server Manager.
- Provision the Session Server Manager platform using the web interface. For more information see "Session Server Manager OAMP" on page 1368.
- Bring the SCS 2000 - SIP Gateway application in service using the web interface. For more information see "SIP Gateway application maintenance" on page 1406.
- Once all components (DPT GWCs and Session Server Manager application) are in service, access link names provisioned in core table SIPLINK are transferred to the Session Server Manager and can be seen through the web interface. Complete the Session Server Manager provisioning by mapping the access link names to remote SIP server destinations. For more information see "Session Server Manager OAMP" on page 1368.
- At the beginning of this step, all incoming and outgoing SIPT traffic continues to flow through the VRDNs. To swing outgoing SIPT traffic

from the VRDN to the Session Server Manager, revisit core table SIPLINK and change the tuples to include the appropriate DPT trunks against the appropriate access link names. Customers may choose to swing only one trunk at first to test the Session Server Manager, perhaps even adding a new DPT test trunk for this purpose. Note that the remote SIP server provisioning done through the web interface on the Session Server Manager should point to the VRDNs on remote CS2Ks. The remote VRDNs are capable of receiving SIPT traffic from DPT GWCs (pre-migration, if UDP transport is used), or from a Session Server Manager (once a trunk is migrated). Once table SIPLINK is changed, new outgoing calls on the affected DPT trunk will route through the Session Server Manager while existing calls finish up through the VRDN.

- To route new incoming calls through the Session Server Manager, the SN06 core and GWC patches mentioned earlier should have been applied on all CS2Ks that send SIPT traffic to the office being upgraded. Assuming the patches are applied, change the destination IP address in table MGCINV for the switch that has been upgraded. The IP address used to be the IP address of the VRDN on the upgraded switch and it must now be changed to be the IP address of the Session Server Manager. Note that the patches are only required if the remote CS 2000 is not being upgraded to SN07. With an SN07 or later load in the remote CS 2000, the IP address can be changed in table MGCINV without needing a patch. Also, the customer can skip the IP address change altogether if the remote CS 2000 is also being upgraded to include a Session Server Manager. In that case, the DPT trunks can be migrated to the Session Server Manager, which will be configured to send calls to the Session Server Manager on the other switch. Note that VRDNs are required at an office until all incoming and outgoing traffic have been migrated to the Session Server Manager. It should also be noted that the destination IP address for a SIP server configured in the Session Server Manager can be changed on the fly. This is required if the Session Server Manager was sending calls to a remote VRDN and then that remote office is upgraded to use the Session Server Manager.
- In addition to remote CS2Ks, it is possible that the upgraded CS 2000 was also receiving incoming SIP traffic from an IMS. In that case, the IMS configuration data must also be changed to send calls to the Session Server Manager instead of sending calls to the VRDN.
- Once all incoming and outgoing traffic has been migrated from the VRDN to the Session Server Manager, the VRDN GWCs can be removed or converted to another type of GWC.

119.7.6.3 Electronic Software Delivery

Session Server Manager software loads can be delivered by CD or electronically. To deliver the SIP Gateway application electronically, follow these steps:

- First, be sure that the NCGL platform software is installed on the Session Server Manager. Please refer to feature A00004005, Nortel Carrier Grade Linux (NCGL) platform "Session Server" for installation information.
- Transfer the ISO image containing the SIP Gateway application load to the /opt/swd directory on the Session Server Manager. Note that this directory has a size of 1GB and can contain no more than four SIP Gateway loads at once. Be sure to delete old loads to make room for the new load being delivered.

  e.g.: scp <iso image> mtc@<Session Server IP addr>:/opt/swd
- Log into the command line on the Session Server Manager as root.
- Verify that the /cdrom device is not currently mounted by typing:

  umount /cdrom
- Mount the ISO image that was transferred electronically to the /cdrom device:

  mount -o loop /opt/swd/<ISO image> /cdrom
- Follow the instructions below to upgrade or install the SIP Gateway application.

119.7.6.4 Upgrading a Session Server Manager load

Upgrading a Session Server Manager with a new software release or a maintenance release is very much like upgrading any other DMS component. Session Server Managers are deployed in redundant pairs, one box acting as the active unit and another box acting as a hot standby (the inactive unit).

Use the following steps to upgrade:

- Deliver the software load to the inactive unit to be upgraded:

  Note 1:The software load may be delivered by CD or electronically. For instructions on electronic deliver, please refer to section119.7.6.3.

  Note 2:For CD delivery, insert the CD in the CDROM drive and type "mount/cdrom" at the command line.
- Install the SIP Gateway application from the command line.
  Note: The user must be logged in as root.

  Type:

  — cd/cdrom

  — ./InstallApps (or just type cd/cdrom/InstallApps)

  InstallApps will prompt the user to proceed with the upgrade.

- Once the InstallApps script is finished, the SIP Gateway application should come in-service automatically if it is in-service on the active unit.
- Swact the Session Server Manager using the web interface. For more information see “SIP Gateway application maintenance” on page 1406.
- Repeat the procedures for the previously active unit, which is now inactive.

119.8 OAMP

This section describes the Operations, Administration, Maintenance, and Provisioning functionality when utilizing a Session Server Manager architecture. While a majority of the OAMP functions now reside on the Session Server Manager itself, the Call Server 2000 (CS 2000) core does have OAMP changes.

This OAMP section focuses heavily on the first application to be deployed on the Session Server Manager. This application, also referred to as the SIP Gateway, should be assumed to be the main topic of discussion with respect to Session Server Manager operations, administration, maintenance, and provisioning.

119.8.1CS 2000 OAMP

Call Server 2000 Core OAMP changes revolve around new table SIPLINK, which is the trigger point for calls utilizing the Session Server Manager platform as opposed to the VRDN. Also, part of the CS 2000 OAMP changes for an Session Server Manager-only environment involve the retirement of several media gateway controller related tables

The below figure illustrates the table control relationships for gateway controllers in a Session Server-only environment. This is followed by a brief description of each table. Not every possible DMS table is shown and described.

Figure 15 Core OAMP hierarchy with Session Server Manager

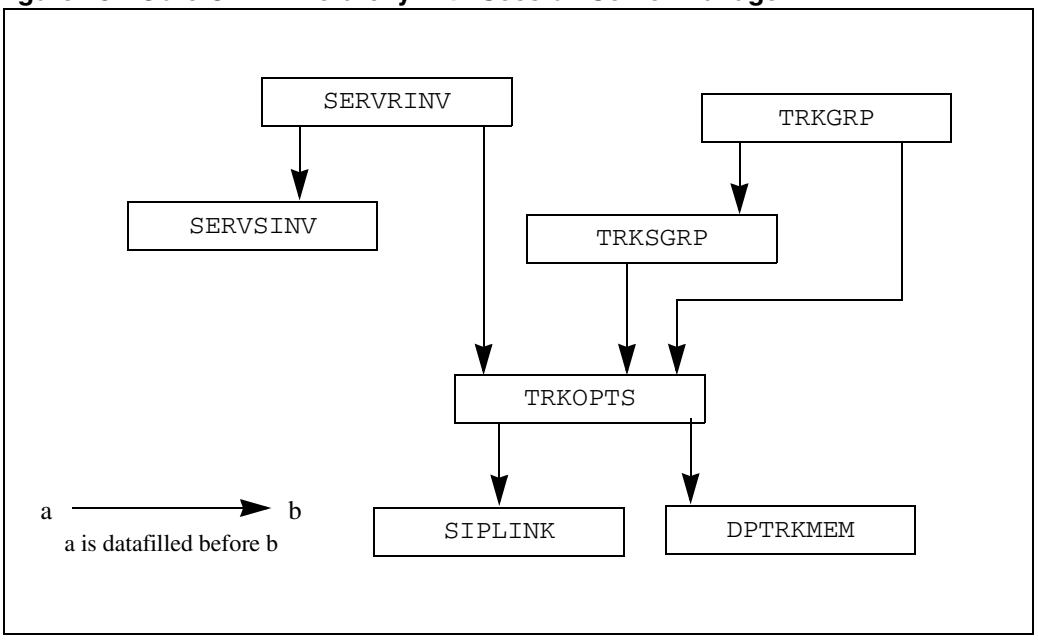


Table 3 Table Descriptions

Table	Description
SERVRINV	Stores provisioned data for gateway controllers including IP addresses, exec information, etc. Gateway controllers are provisioned in CS2M and then the system automatically enters required datafilled in SERVRINV
SERVSINV	Contains the names of the server subtending nodes and their associated gateways. The subtending nodes are the Audio Controller and the Dynamic Packet Trunk (DPT).
SIPLINK	Contains the access link information that is used to direct calls to the appropriate SIP server. This information is also used by Session Server devices for mapping incoming calls.
TRKGRP	Contains customer-defined data associated with each trunk group that exists in the switch.
TRKSGRP	List the supplementary information for each subgroup that is assigned to one of the trunk groups listed in table TRKGRP.
TRKOPTS	Provisions special options on trunk groups. For the Session Server Manager, that option is dynamic and the signaling type is SIPT.
DPTRKMEM	Used to provision ISDN User Part and SIP trunks dynamically for both ATM and IP networks.

The major differences between the old and new data models with respect to core provisioning are as follows:

- Retirement of tables VRDNINV, MGCINV, and TELEPROF. These three table are unnecessary when Session Server Manager functionality is utilized.
- Table SIPLINK is added to contain the access link information.
- Tables TRKGRP, TRKSGRP, TRKOPTS, DPTRKMEM, SERVSINV, and SERVRINV remain unchanged.

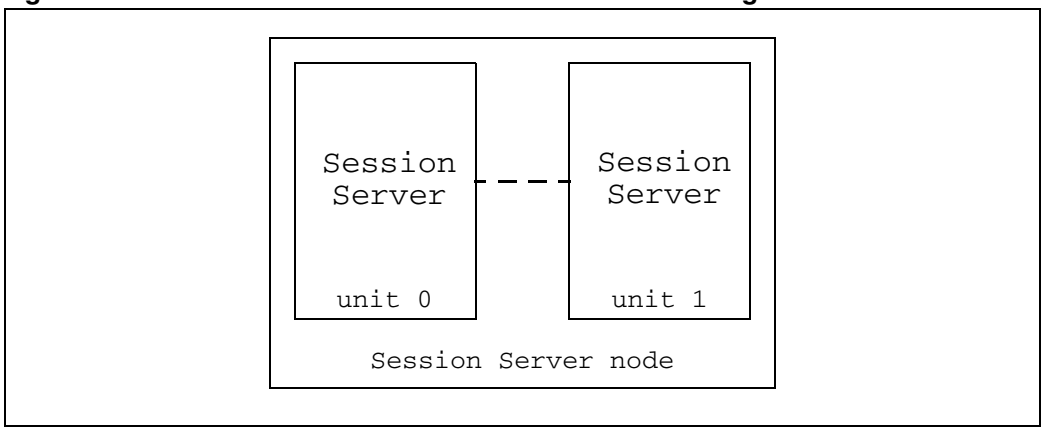
119.8.2Session Server Manager OAMP

This section discusses Operations, Administration, Maintenance, and Provisioning (OAM&P) topics for the new Session Server Manager platform. Topics discussed include the following:

— OAM&P Overview
— Node Provisioning
— Node Maintenance
— SIP Gateway Provisioning
— SIP Gateway Maintenance
— Alarms
— Logs
— Operational Measurements

Before jumping into the sections mention above, a distinction should be made with respect to the Session Server Manager product release and this document. In the SN07 release, the architecture for the Session Server Manager will consist of a dual unit configuration similar to that of gateway controllers. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server Manager that is interconnected via a gigabit ethernet LAN.

Figure 16 SN07 Architecture for the Session Server Manager



119.8.2.1 Overview

For the SN07 release of the Session Server Manager, there are four major OAMP areas to discuss. Those areas are as follows:

— Web Based OAM&P
— Provisioning Framework
— Application Maintenance
— Alarms, Logs, and OMs

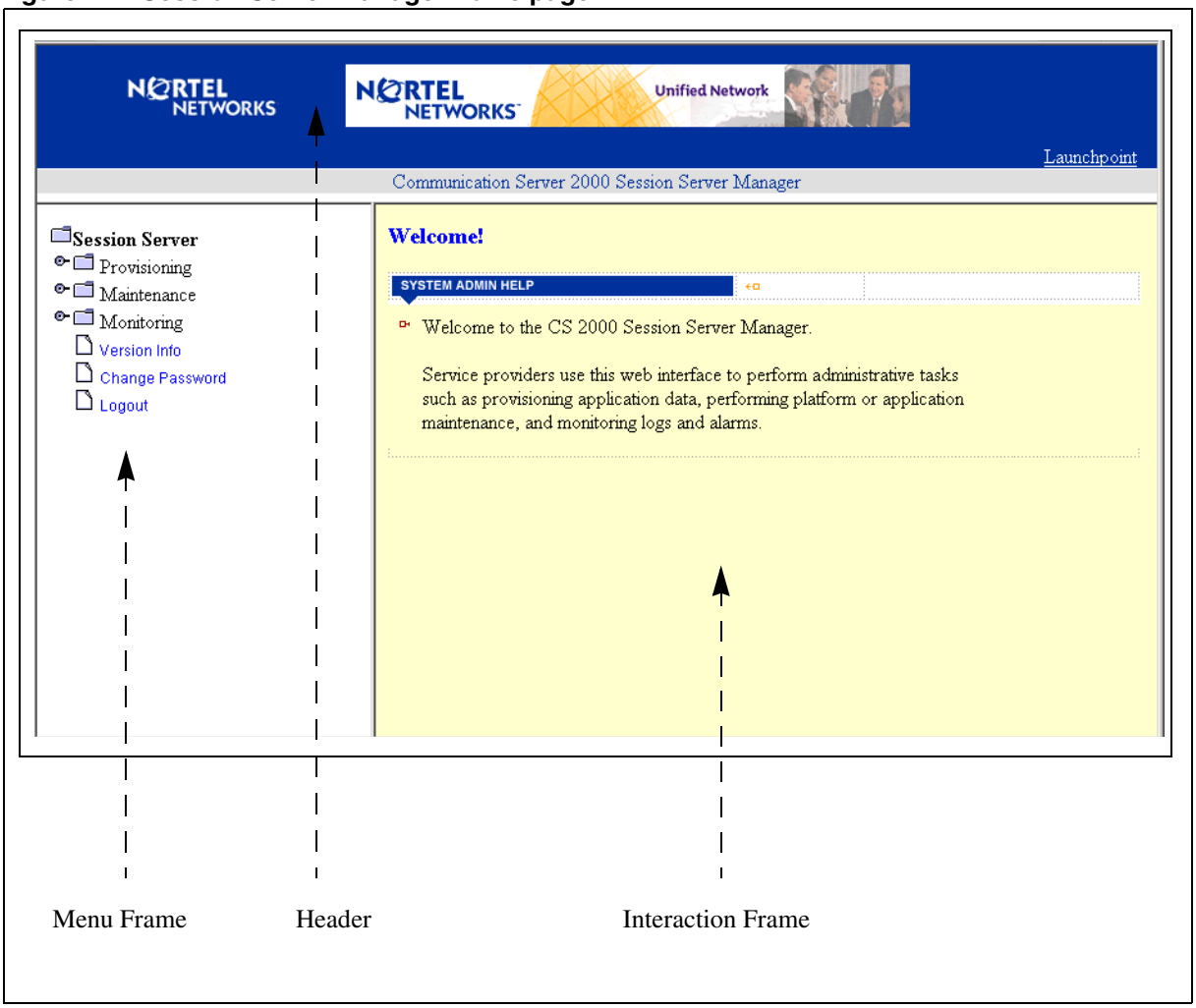
119.8.2.1.1 Web Based OAM&P

One paradigm shift to note is that the Session Server Manager functions as its own element manager. This means that provisioning for a Session Server Manager takes place on the Session Server itself. Additionally, maintenance type activities also take place on the Session Server Manager.

The craftsperson uses a web based interface to perform the provisioning and maintenance activities. This interface consists of a web system[1] running on the Session Server Manager that provides provisioning web pages as well as maintenance related web pages. Please refer to activity A00004005: *NCGL Support for SAM-XTS and Session Server* for details on logging on via the web interface.

An example of the Session Server Manager home page is shown in Figure 17.

Figure 17 Session Server Manager home page



[1]Consists of Apache, Apache Tomcat, and Java Runtime environment.

All Session Server Manager web pages are divided into three areas:

- **Header**
  The area with the Nortel logo and the “Home” and “Help” tags.
- **Menu Frame**
  The user uses the menu bar on the left to locate the proper function in the web page hierarchy.
- **Interaction Frame**
  This area is where a user fills in forms, performs maintenance actions, and obtains relevant information.

119.8.2.1.2 Provisioning Framework

As mentioned before, the Session Server Manager is its own element manager. That also means provisioned data is stored on the Session Server Manager itself. The storage mechanism is an on-board standard query language (SQL) database. Data in this database survives scenarios such as dead office recovery.

119.8.2.1.3 Application Maintenance

In the initial release, only the SIP Gateway application exists on the Session Server Manager. That application is managed via an Application Maintenance entity known as SIP Gateway Maintenance. Again, the web based interface is the craftsperson's way to interact with SIP Gateway Maintenance as described in "119.8.2.5 SIP Gateway application maintenance" on page 1406.

119.8.2.1.4 Alarms, Logs, and OMs

An application on the Session Server Manager, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OM).

119.8.2.2 Platform Commissioning

Platform provisioning for the Session Server Manager takes places during the commissioning phase when the software is installed for the first time. Initial commissioning is not done via the web based interface. Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for complete commissioning information.

A quick overview of this commissioning phase is detailed below. These steps are meant as an example only.

- Power on (or reset) the Session Server Manager.
- Insert the Session Server Manager installation CD/DVD into the CDROM drive.
- Eventually the user is taken to an initial commissioning screen. Here initial commissioning prompts the user to enter the following data items for initial node provisioning:
  - Hostname - Hostname for this particular Session Server Manager unit. (e.g. "NGSS-Unit0)
  - Unit IP Address - IP Address of this particular Session Server Manager unit.
  - Subnet Mask - Subnet mask for the Session Server Manager.
  - Timezone - The timezone of the Session Server Manager (e.g. EST)
  - One or More NTP Servers - At least one Network Time Protocol server must be datafilled.

- Log Server IP Address [optional] - IP Address of a remote log server if Session Server Manager customer logs are to be reported to a far end entity. If no far end log server is being utilized, this field should remain empty.
- Network Monitor IP Address (mandatory) - Datafill with a network node that can always pinged from the Session Server. It is recommended that you specify the IP address of a highly available node on the network.
- Core IP Address [optional] - Datafilled with the IP address of the Core. This optional field is for future use.
- Web Proxy IP Address [optional] -If the Session Server Manager is to be accessed via a Web Proxy, the web proxy IP address is datafilled. For example, in the Succession environment, this would likely be the SSPFS proxy server.
  If a web proxy is not going to be used, this optional field should be left blank.
- Session Server Manager Location - A text string indicating the location of the Session Server Manager.
- SNMP Trap Destination [optional] - IP Address of the far end node to receive SNMP traps from this Session Server Manager unit. If SNMP traps are not to be reported to a far end node, this optional field should remain blank.

Once the commissioning steps are complete, the Session Server Manager should fully initialize and the craftsperson has access to the on-board web system.

119.8.2.3 Node Maintenance

Please refer to A00004005: *NCGL Support for SAM-XTS and Session Server* for a complete list and description of Session Server Manager Node Maintenance type functions available. A quick summary of some of those functions include:

— Lock/Unlock Node

This provides for the ability to bring a Session Server unit into service.

— Duplex Activities

This provides for the ability for Session Server Manager to SWACT from the Active/Enabled unit to its mate unit.

— System Info

Provides information such as the date, time since last reboot, IP address of the system, and IP address of the web browser looking at the System Info page.

— System Status

Provides CPU, Process, and Memory information

— Connectivity

  Allow the user to setup and monitor a remote host via pings.

— Storage

  Allows a view of file system data includes partition specific data such as total space, used and available space, and the ability to set alarm thresholds based on the amount of space utilized

— Services

  Displays NFS, TFTP, and active remote session status information. e.g. if two SSH sessions are in progress, the active remote session indicates “2”.

— Admin

  Allows the user to perform administrative tasks related to the system. For example the user can reboot the Session Server Manager from this menu.

— Alarms

  Provides the ability to view alarm information which consists of type, id, timestamp, severity, and description.

— Logs

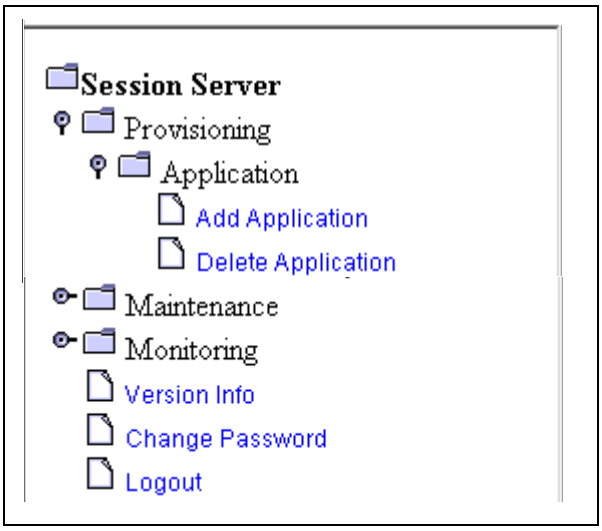
  Provides the ability to view customer related logs that are not application related.

119.8.2.4 SIP Gateway application provisioning

This section describes the provisionable data related to the SIP Gateway application. All SIP Gateway provisioning is performed via the Session Server Manager web interface.

The first provisioning step is to enable the SIP Gateway application if it is not already listed. This is a one time step, but it is required at the outset. When the Application folder in the menu frame is opened the first time, the SIP Gateway application is not listed as shown below.

Figure 18 No SIP Gateway application

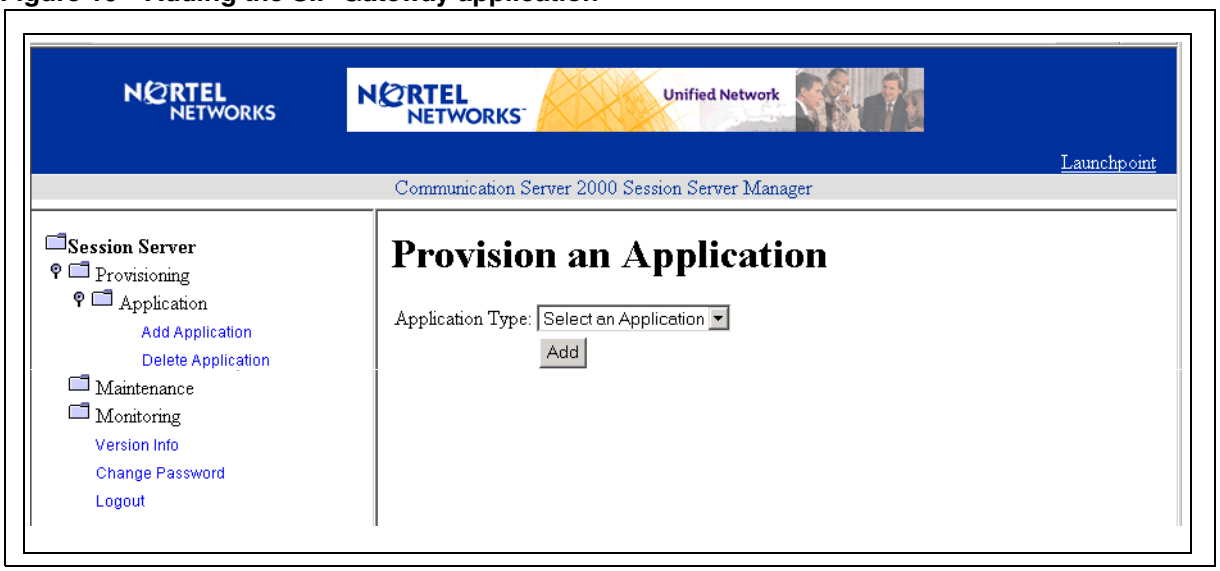


To add the SIP Gateway application, the craftsperson clicks on “Add Application” link and is presented with the **Provision an Application** web form as shown in “Figure 19 Adding the SIP Gateway application” on page 1375. From this point, the craftsperson selects “SIP Gateway” and clicks on “Add” to add the application.

Note: If the SIP Gateway application is already listed, there is no need to provision it.

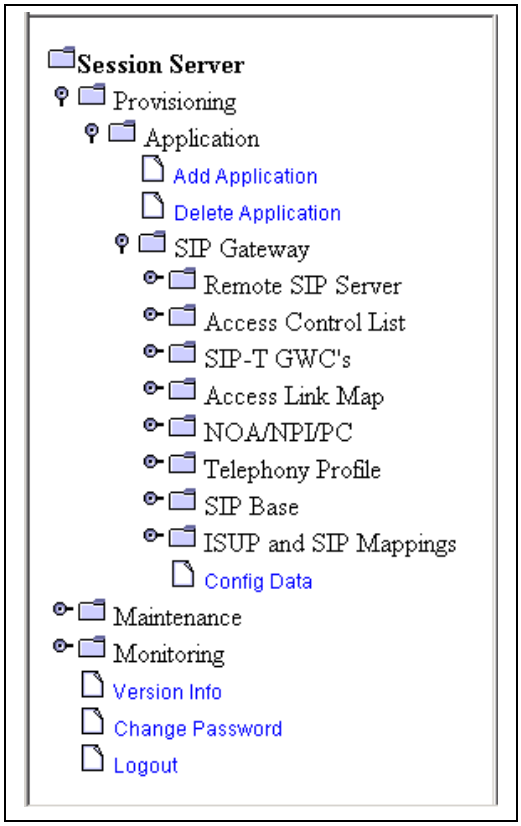
Note: If the SIP Gateway application is already listed and it is added again, that operation does not perform a second add. Also, it does not have a negative impact on the existing SIP Gateway application.

Figure 19 Adding the SIP Gateway application



After adding the application, the craftsperson should close and open the Application folder and the SIP Gateway application will be present. Next, the craftsperson uses the "SIP Gateway" level to perform provisioning.

Figure 20 SIP Gateway provisioning



In the Session Server menu on the left of the page, the following is performed.

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder

The provisionable items for the SIP Gateway application consist of required and optional datafill. Certain datafill is optional because either defaults exist or that datafill is not required.

Required Datafill	Optional Datafill[a]
Config Data	Access Control List
Remote SIP Servers	NOA/NPI/PC
SIP-T Gateway Controllers	SIP Base
Telephony Profile	ISUP to SIP Cause Code Map
Access Link Map	SIP to ISUP Response Code Map
ISUP Variant Map[b]	SIP Redirection Map

a. All of the optional datafill items exist in the Mappings sub-folder with the exception of “SIP Base”, which is under the “SIP Gateway” folder.
b. The SIP Base item seen in Figure 20 relates to the ISUP Variant mapping datafill in the Mappings sub-folder.

119.8.2.4.1 Config Data

Before the SIP Gateway application is brought into service, four base configuration parameters should be modified to appropriate values.

LocalTcp

The IP address should be datafilled to match the IP address of the Session Server Manager. The port should be datafilled to 5060.

LocalUdp

The IP address should be datafilled to match the IP address of the Session Server Manager. The port should be datafilled to 5060.

MgcHostName

This parameter should be datafilled to match parameter HOST_MGCNAME in table OFCENG in the local CS 2000 Core.

An example of HOST_MGCNAME in the local CS 2000 core is as follows:

```
TABLE: OFCENG
                        PARMNAME                                        PARMVAL
-------------------------------------------------------------------------------
                    HOST_MGCNAME                                          MGCA
```

In the above scenario, parameter MgcHostName on the Session Server Manager should be datafilled to be MGCA.

If the Session Server Manager is being used to communicate with other CS2Ks that have VRDNs, then it is very important that the MgcHostName parameter match the HOST_MGCNAME parameter in table OFCENG. If it does not match, DPT trunks at the far end CS 2000 will transition to a SYSB state and call processing between the CS2Ks will be halted.

Note: The string associated with the MgcHostName parm will be used to populate the Via Header of the SIP INVITE message. See section “119.6.2 Call Flows” for additional information.

maxCallLegs

This parameter determines the maximum amount of simultaneous SIP transactions. The default setting is 1000.

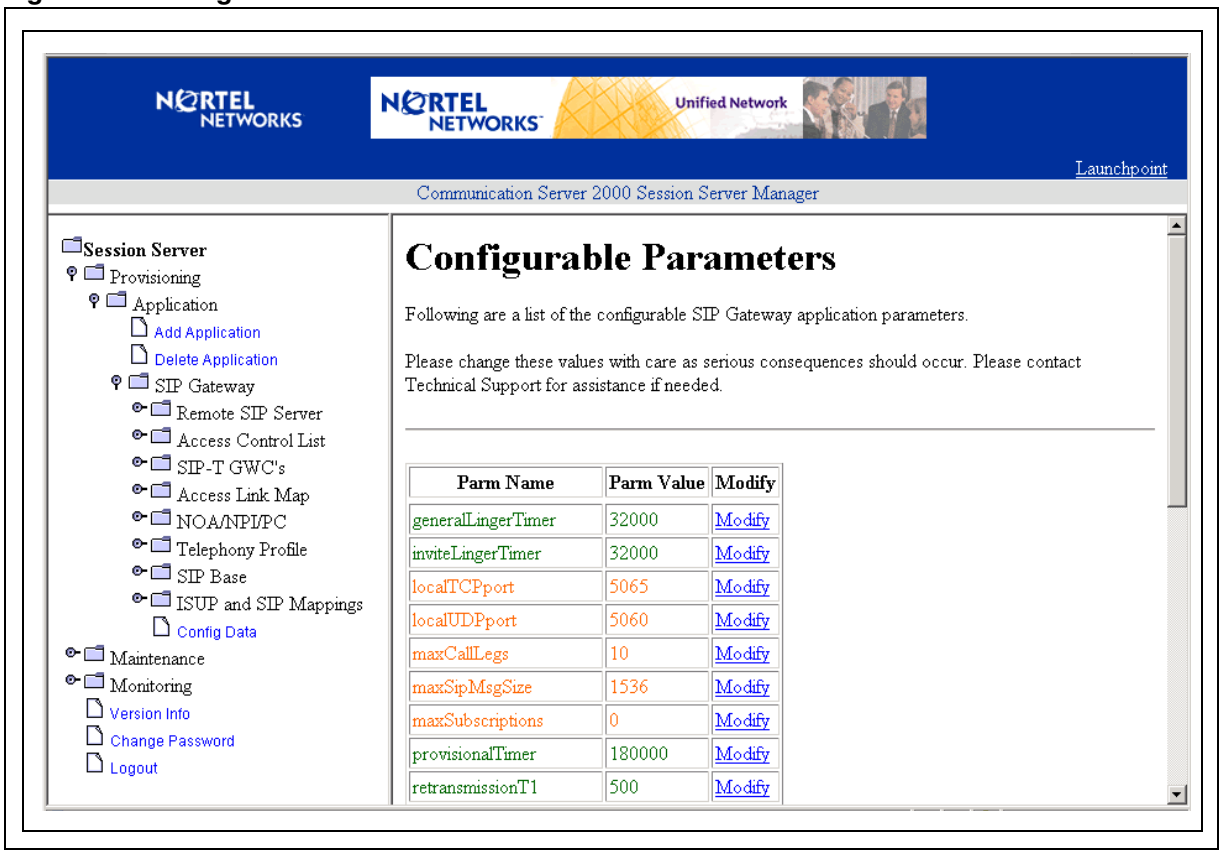
If the SIP Gateway application is in-service when the above values are changed, it must be taken out of service and brought back in-service for the new parameter values to take effect. Details on this may be found in “119.8.2.5 SIP Gateway application maintenance” on page 1406. Next, while many parameters exist on the “Config Data” page, **care** must be taken when changing any of them.

All the configurable parameters are found on the **Configurable Parameters** page. That page is reached from the Session Server Manager main page via:

— Click on the Provisioning folder
— Click on the Application folder
— Click on the SIP Gateway folder
— Click on **Config Data**

An example of the Config Data page can be found in “Figure 21 Configurable Parameters” on page 1378.

Figure 21 Configurable Parameters



The range of values for the configuration parameters are:

- generalLingerTimer 0 - 60000
- inviteLingerTimer 0 - 60000
- maxCallLegs 0 - 40000
- maxSubscriptions 0 - 100000
- provisionalTimer 0 - 540000
- retransmissionT1 0 - 60000
- retransmissionT2 0 - 60000
- retransmissionT4 0 - 60000

119.8.2.4.2 Remote SIP Servers

A remote SIP Server is a remote SIP device that the Session Server Manager communicates with via the session initiation protocol. Two examples are other Call Server 2000s or a Multimedia Communication Server (MCS).

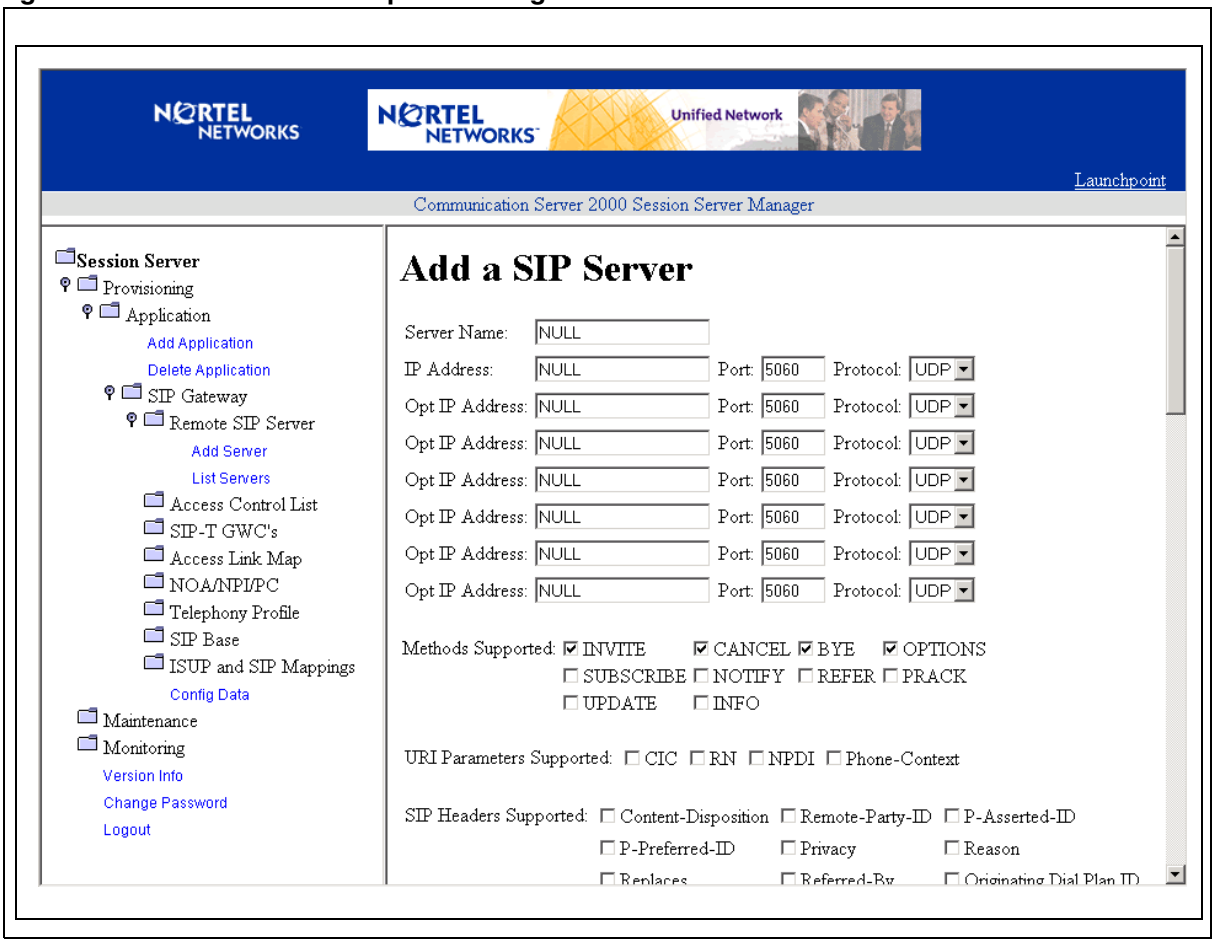
SIP Gateway remote SIP server provisioning is performed by opening the "Remote SIP Server" folder in the left menu. Once there, the following may be performed:

— Remote SIP Server datafill may be added by clicking on the "Add Server" link. Figure 22 shows an example of the page presented to the user after this.

— Remote SIP Servers may also be listed by clicking on "List Servers".

— After listing the Remote SIP servers, the user may choose to delete a particular remote SIP server or modify the data for a particular SIP server.

Figure 22 Remote SIP Server provisioning



Datafill for a remote SIP server consists of the following items:

Table 4 Remote SIP Server Data

Title	Description	Default
Server Name	Character string name for the remote server. ***Note***: Use DNS naming conventions when naming your server.	N/A
IP Address, Port, and Protocol	An IP addresses list that represents the Remote SIP Server. Up to 7 IP addresses and Ports are supported. At least one IP address must be entered. ***Note***: If used for loop-around calls, the IP address for the active Session Server node should be entered.	N/A for IP, 5060 for Ports, and UDP for Protocols
Optional IP Addresses, Ports, and Protocols	Up to 6 additional IP addresses are supported for each remote SIP Server.	N/A for IP, 5060 for Ports, and UDP for Protocols
Server Methods • Invite • Cancel • Bye • Prack • Subscribe • Notify • Refer • Options • Update • Info	• Click on the methods that are supported by the Remote Server	All False
URI Parameters Supported • CIC • RN • NPDI • Phone-Context	• Click on appropriate parameter if it is supported. • CIC parameter carries Carrier Identification Parameter from SIP to ISUP and vice-versa. • Redirect Number is used in LNP scenarios • NPDI indicates the number in Request-Uri is ported • Phone-Context indicates the context of the called party number in the Request-Uri	All False

Table 4 Remote SIP Server Data

Title	Description	Default
SIP Headers Supported • Content-Disposition • Remote-Party-ID • P-Asserted-ID • P-Preferred-ID • Privacy • Reason • Replaces • Referred-By • Originating Dial Plan ID • Billing Number • Rate Plan • Terminating Dial Plan ID • Diversion	• Click appropriate headers that are supported by remote server	All False
ISUP-SIP Cause Map	Contains the name of the mapping table for ISUP Release Cause to SIP response code.	N/A
SIP-ISUP Cause Map	Contains the name of the mapping table for SIP Response code to ISUP Release Cause.	N/A
SIP Redirection Map	Contains the name of the mapping table for redirection mapping.	N/A
ISUP Variant to SIP Version Mapping	Contains the name of the mapping table for ISUP Variant to SIP Version Mapping.	N/A
NOA/NPI to Phone Context Map	Only selectable if URI Parameter-Phone Context is selected. Contains the name of the mapping table for NOA/NPI to Phone Context Mapping.	N/A
SIP Cause Precedence Priority	A list of precedence rules and their respective priority.	Ordered as Listed
APN Representation	Contains the choices for Action Point Number Representation	N/A
BCI Data	Includes: • Interworking indication • ISUP/BICC indicator • ISDN Access Indicator	N/A

Table 4 Remote SIP Server Data

Title	Description	Default
FCI Data	Includes: • Domestic/International Call indication • Interworking indicator • ISDN User Part Indicator • ISUP/BICC Preference indicator • ISDN Access Indicator	N/A
SIP Header Format	Supports the compact or long form of SIP headers.	Compact
Options for Heartbeat	Indicates if SIP Options method is used to determine accessibility of the SIP server.	Yes
Telephony profile Support	An indication of whether or not the Session Server Manager will send the X-Nortel_profile header to this remote SIP Server. ***Note:*** Datafill with "No" when the Remote SIP Server does not support receiving the X-Nortel-Profile header in the SIP message.	Yes
Use Info for Long Call Audit	Long call audit provisioning.	No
Map Non-Screened RPI To Calling #	Whether or not to include RPI header for clg number when building outgoing INVITEs	No
Accept Early SDP	Determines if Early Session Description Protocol are allowed by the remote server	Yes
Accept Invite without SDP	Indicates whether or not to accept an Invite without the SDP and proceed with the call and return a 488 Not Accepted Here error message.	Yes
E.164 Format Allowed	Indicated if the E.164 format is supported. ***Note***: To derives ETSI ISUP message utilizing SIP instead of SIP-T, the value must be set to No.	No
Enforce CODEC- Compatibility	Indicates whether support for other codec is supported. If Yes, then at least one of the codec fields must be set to yes in the Config Data web page.	No
Accepts Encapsulated ISUP	Indicates whether to perform ISUP encapsulation or not.	Yes
Country Code Support	Indicates if country code screening is supported. If yes a country code must be datafilled.	No
Country Code	Indicates if Country Code is supported, then datafill 3 digit Country Code if Country Code Support is set to Yes.	N/A

Table 4 Remote SIP Server Data

Title	Description	Default
Hop-Counter Factor	Set the typical number of HOPS to account for when adjusting for call latency. ***Note***: Hop-Counter Factor is used to derive the Hop-Counter. As specified in the Q1912 Standard, Table 11/ Q19125, the Hop-Counter value = Integer part of (Max-Forwards value / Hop-Counter Factor), where the factor is constructed according to the following principles: • Hop-Counter for a given message should never increase and should decrease by at least 1 with each successive visit to an interworking unit regardless of intervening interworking, and similarly for Max-Forwards in the SIP domain. • The initial and successively mapped values of Hop-Counter should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.	7
Out of Band DTMF Payload	Indicates the Out of Band DTMF payload monitor/ detection mechanism to use	N/A
Agent Representation	Indicates agent supported ISUP/PRI/Line.	ISUP
“unknown” header	Indicates the String to use when Presentation indication is Unknown	NULL
“anonymous” header	Indicates the String to use when Presentation indication is restricted	NULL

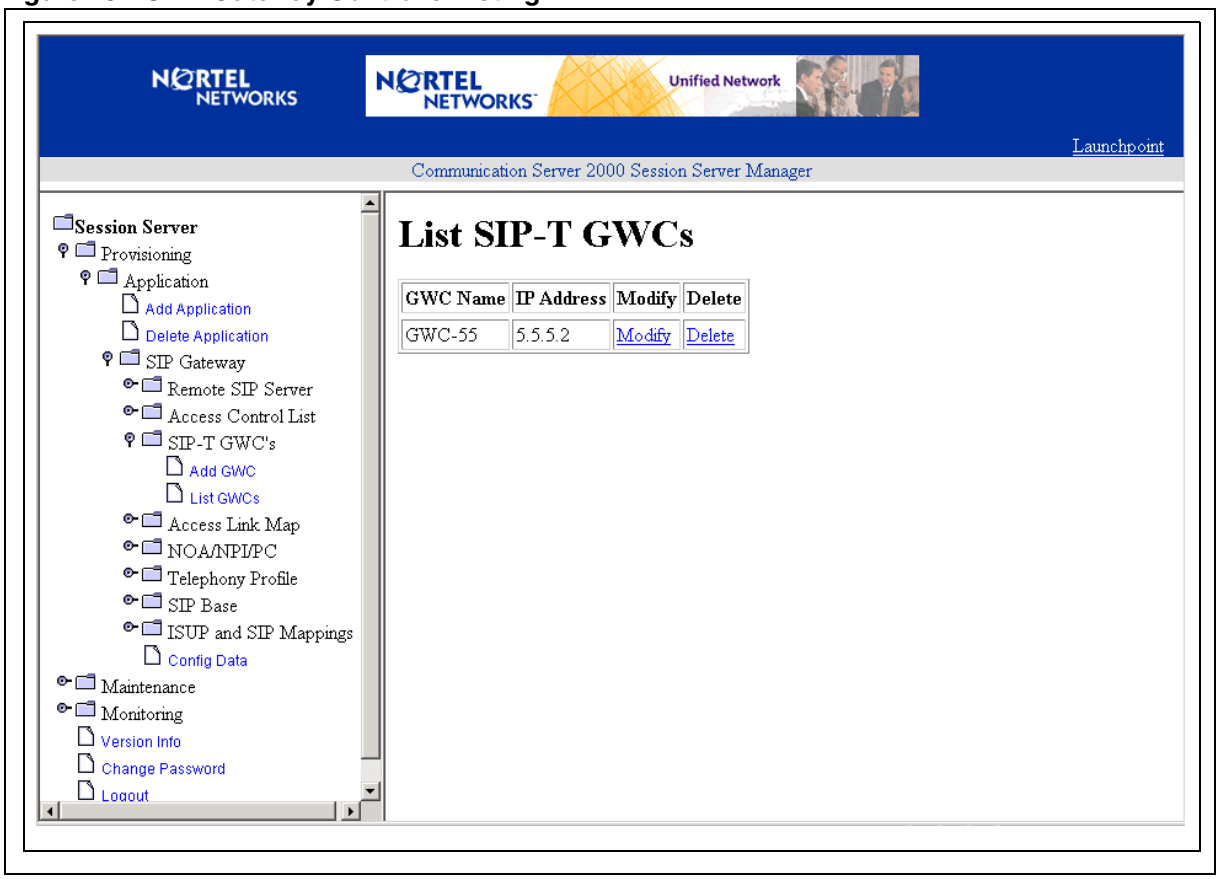
119.8.2.4.3 SIP-T Gateway Controllers[1]

This area of datafill consists of a list of local SIP-T[2] gateway controllers that are used for dynamic packet trunking calls for the SIP Gateway application. SIP Gateway SIP-T GWC provisioning is performed via the following.

- In the SIP gateway provisioning menu, gateway controller datafill may be added using the "Add GWC" link in the SIP-T GWC folder
- It may also be listed by clicking on "List GWC". Once the GWCs are listed, the user may choose to delete a GWC or modify the IP address for a particular GWC.

Datafill for a gateway controller consists of a gateway controller name and its IP address. The IP address should point to the active unit. An example of the craftsperson clicking on "List GWC" is shown in the below figure.

Figure 23 SIPT Gateway Controller listing



[1]All GWCs are still provisioned maintained via CS2M. Datafilling a GWC in the Session Server Manager only indicates that the Session Server Manager will be communicating with that GWC.
[2]SIP-T and DPT gateway controllers are one in the same with respect to the Session Server Manager.

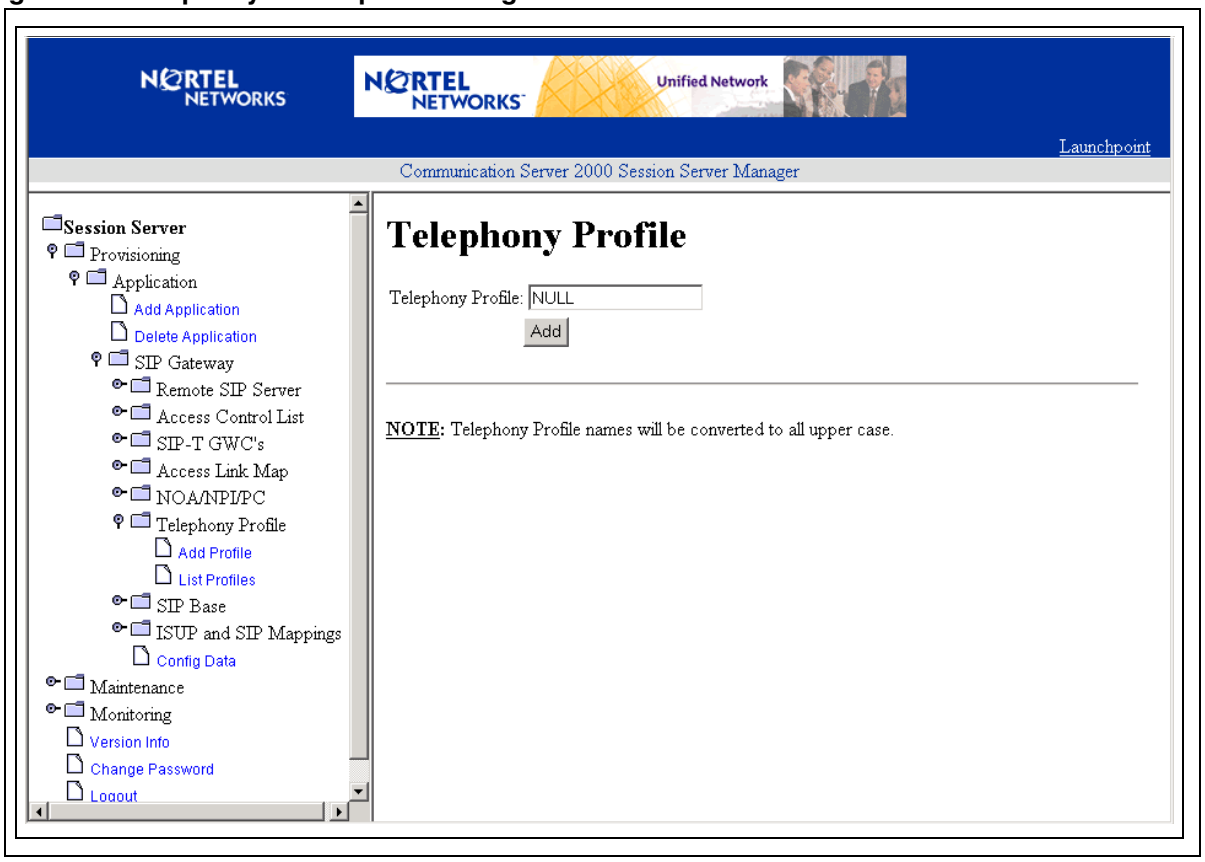
119.8.2.4.4 Telephony Profile

A telephony profile is a simple character string that is mapped to a SIP Access Link and Remote SIP Server pair described in section "119.8.2.4.5 Access Link Map" on page 1386. Telephony Profile provisioning is performed via the following:

- In the SIP gateway provisioning menu, telephony profile datafill may be added using the "Add Profile" link in the Telephony Profile folder.
- It may also be listed by clicking on "List Profiles". Once the profiles are listed, the user may choose to delete a particular one if it is not being used in any Access Link Mappings. Note that modifications on a profile are not allowed whether or not it is being used elsewhere.

An example of a user that is about add a new telephony profile is shown in the figure below.

Figure 24 Telephony Profile provisioning



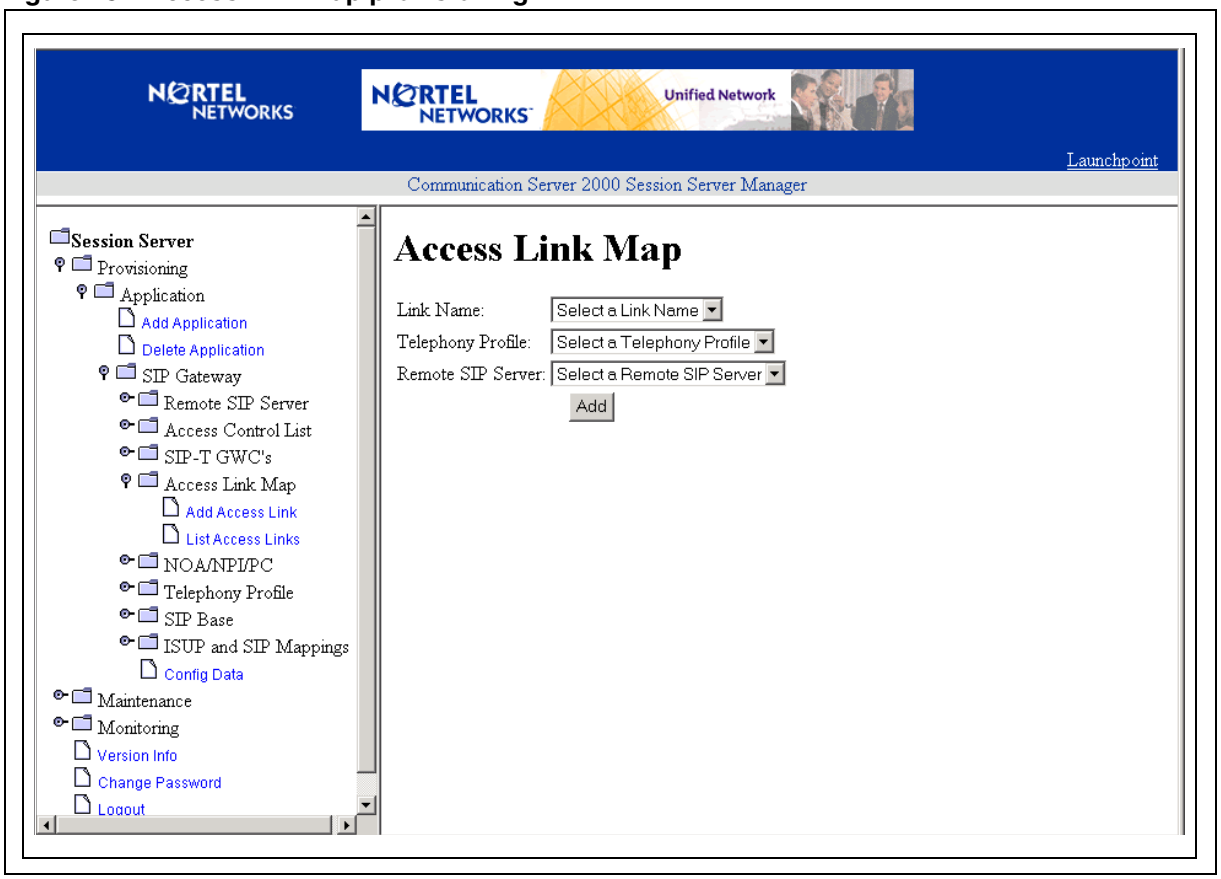
119.8.2.4.5 Access Link Map

An Access Link Map provides the customer with a mechanism to determine the routing of outgoing and incoming SIP calls.

- In the SIP gateway provisioning menu, Access Link Map datafill may be added using the “Add Access Link” link in the Access Link Map folder.
- Access Link mappings can also be listed by clicking on “List Access Links”. Once the access link mappings are listed, the user may choose to delete a particular mapping. Modifications to existing mappings are not allowed.

An example of a user that is about to add a new access link mapping is shown below. An access link mapping consists of an Access Link, Telephony Profile, and a Remote SIP Server.

Figure 25 Access Link Map provisioning



119.8.2.4.6 ISUP Variant Map

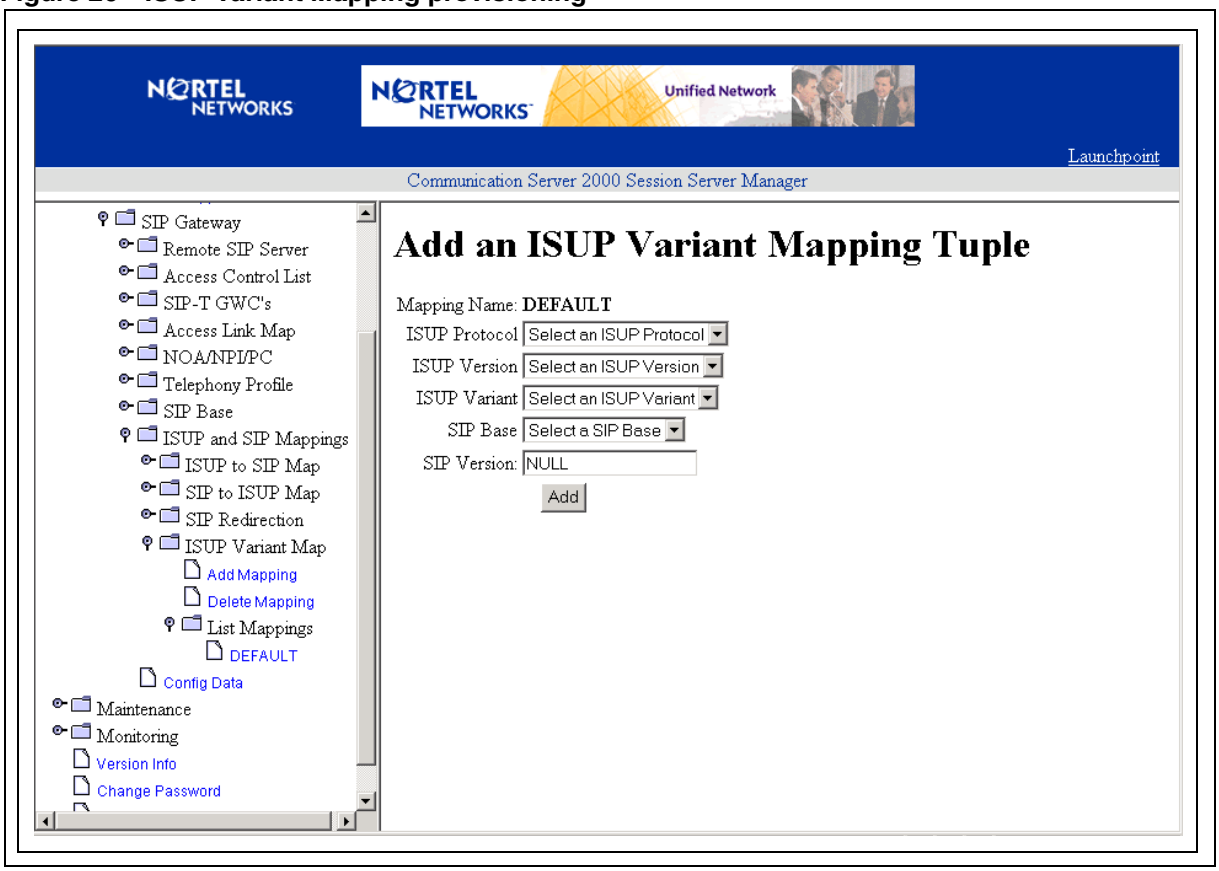
This mapping table provides a mechanism to map ISUP Protocol, Version, and Variant to a SIP Base and Version. Example mappings are shown below.

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q764			ANSI88	<user defined string>
UCP			ANSI88	<user defined string>

When adding the remote SIP servers, if you plan to select a custom mapping value for ‘ISUP Variant to SIP Ver Map’, then add a new variant mapping table using the steps in Figure 26. If DEFAULT was selected for ‘ISUP Variant to SIP Ver Map’ when adding the remote SIP server, the only additional step required is to add a tuple to the DEFAULT mapping table within the ISUP Variant Map folder using the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the ISUP and SIP Mappings folder
- Click on the **ISUP Variant Map** sub-folder
- Click on List Mappings
- Click on DEFAULT
- In the frame on the right, click Add.
- See “ISUP Variant to SIP Version Mapping information” on page 1428 as a guide for datafill rules.

Figure 26 ISUP Variant Mapping provisioning



At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs.

Once successfully added, the craftsperson may chose to add, modify, or delete tuples in their mapping or even delete their newly added mapping table. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "ISUP Variant Map" sub-folder. In order to modify a mapping, the craftsperson clicks on "List Mappings" and then clicks on the mapping they wish to modify.

Like other mapping tables, a default mapping table exists called DEFAULT. However this table is different in the fact that it is empty. Also this default table may have tuples added, modified or deleted.

Tuples within an ISUP to SIP Variant mapping table that are added or modified must adhere to specific datafill rules. The legal combination for the columns in a tuple are listed in the appendix in "119.17.1 ISUP Variant to SIP Version Mapping information" on page 1428.

119.8.2.4.7 Access Control List [optional]

In certain scenarios it may be desirable to restrict which far-end nodes are allowed to initiate call processing with SIP Gateway application. The ability to create these restrictions exist in the form of an Access Control List (ACL)[1].

- ACL functionality is optional and can be enabled/disabled by the users. Default value is disabled. ACL is enabled/disabled under system configuration menu of SIP gateway application.
- If ACL is disabled, all incoming SIP messages are accepted.
- Remote SIP servers are automatically included in the ACL list for screening, hence Remote SIP server IP addresses are not required to be provisioned again in the ACL list.
- With ACL enabled, SIP messages only from the list of servers provisioned in ACL list or listed in Remote SIP Server IP list are accepted.
- Please note that all the remote servers/gateways which can talk to NGSS SIP application must be datafilled in ACL, if enabled. For e.g if the remote server is a VRDN, it not sufficient to just datafill VRDN IP address, all SIPT GWCs also need to be included in the ACL, as SIPT GWCs will send SIP messages directly to NGSS.
- If ACL is enabled while both ACL list and Remote Server IP address list are empty, all incoming messages will be dropped. Hence before enabling ACL, care should be taken to properly provision Remote SIP server and/or ACL list.
- In the SIP gateway provisioning menu, access control list datafill may be added using the “Add IP Range” link in the Access Control List folder.

  When the “Add IP Range” link is clicked, the user is prompted for an IP address and a network mask. The range of IP addresses to allow is calculated based on a combination of the IP address and network mask entered.
- Provisioned servers may be listed by clicking on “List IP Ranges”. Once the IP ranges are listed, the user may choose to delete a particular IP range.

[1]Datafill added to the access control list under SIP Gateway provisioning only affects the SIP Gateway application. Other application which exist on the Session Server Manager are not impacted by this datafill.

Note that Remote Server IP address are not listed in this list though they are included in screening the incoming SIP messages.

- To modify an IP address range it must be deleted and re-added. It cannot be modified.
- A range of 0.0.0.0 is not supported because it is the default address if no address has been assigned yet.

A few examples of the IP/mask algorithm include:

10.1.1.1/255.255.255.255 means only one host 10.1.1.1.

10.1.1.1/255/255/255.0 means all host in the range 10.1.1.0 to 10.1.1.255

Figure 27 Access Control List - Adding a New IP Address

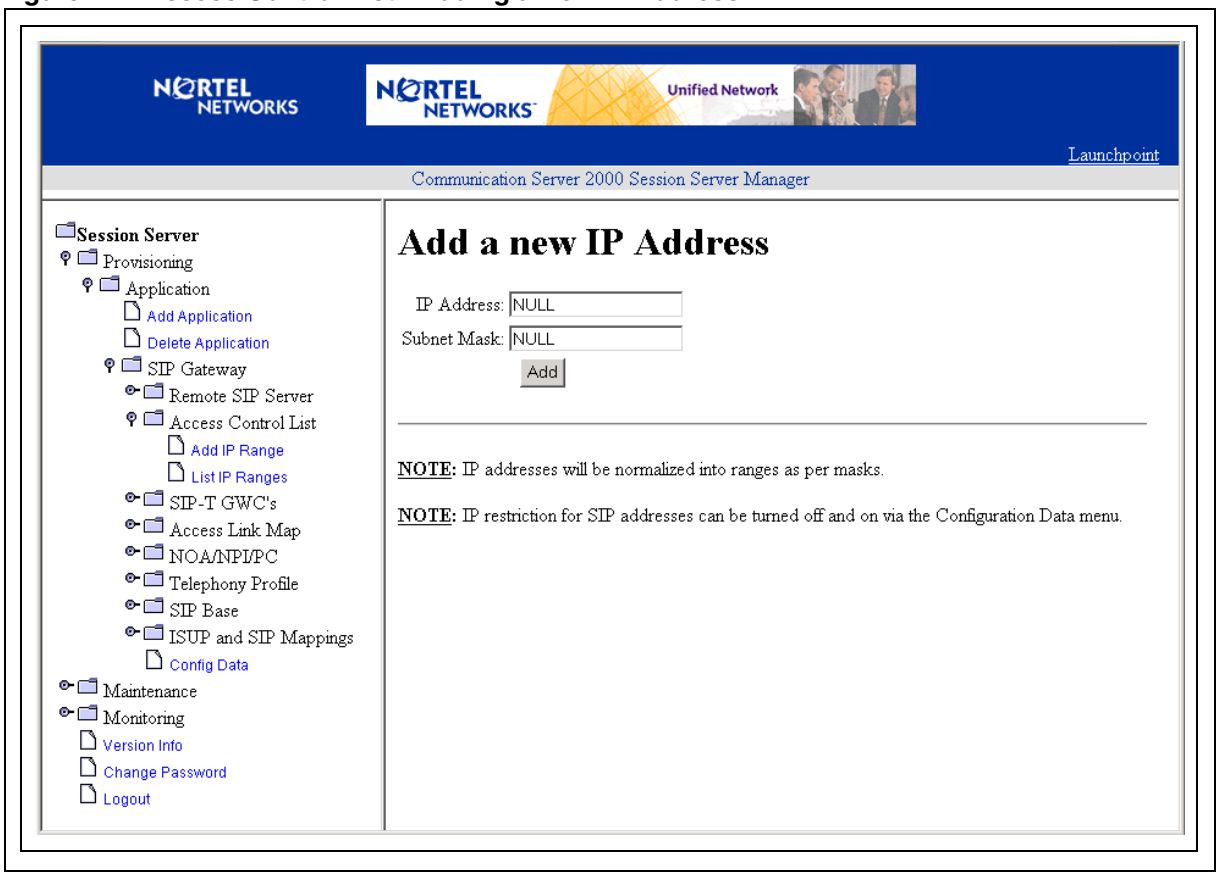
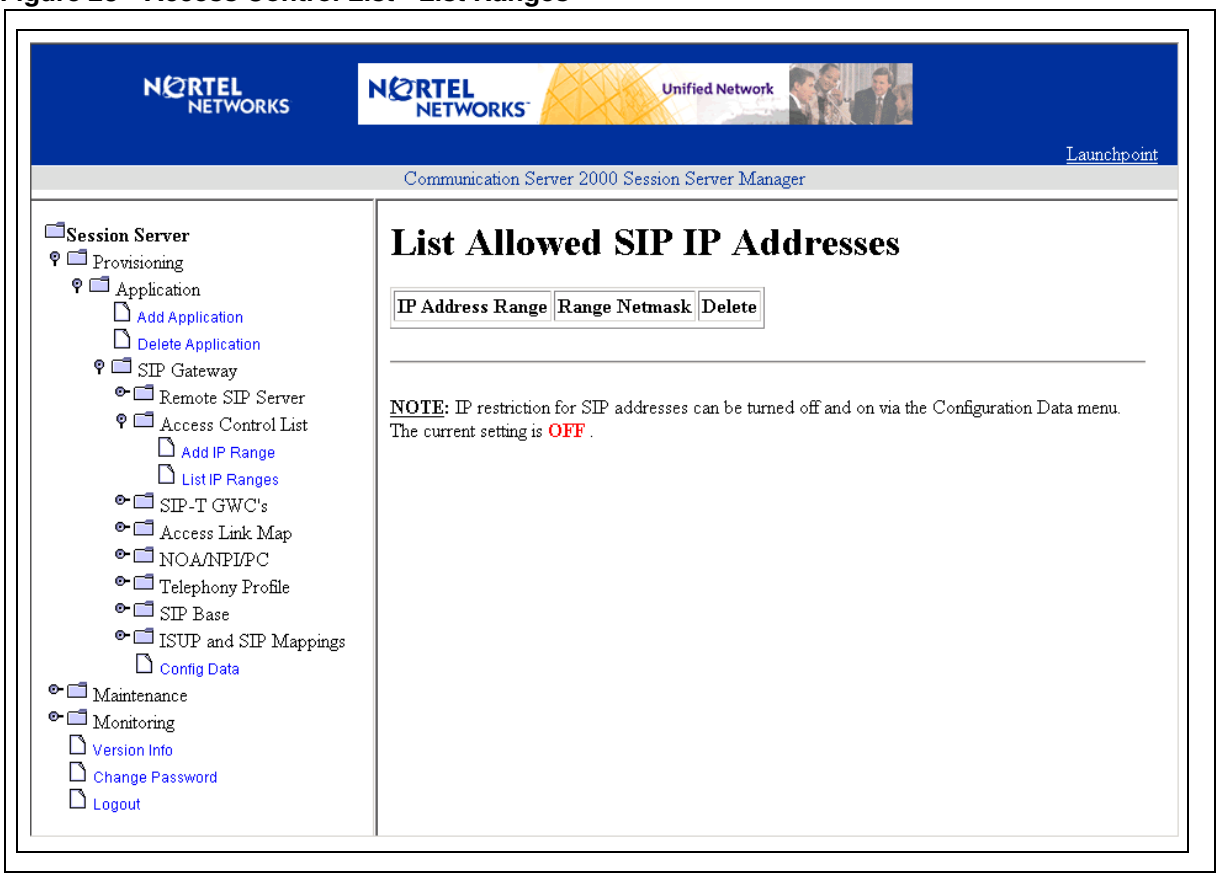


Figure 28 Access Control List - List Ranges



119.8.2.4.8 NOA/NPI/PC Indicator mapping [optional]

The NOA/NPI/PC Indicator mapping represents the Nature of Address/ Numbering Plan to Phone Context Indicator mapping.

When selecting the NOA/NPI/PC folder, three options are available: Add NOA, List NOA, or a subfolder NOA/NPI/PC mapping.

The Add and List pages allow for the addition or deletion of "Nature of Address" values. These entries have been preloaded with standard values.

Figure 29 Adding an NOA

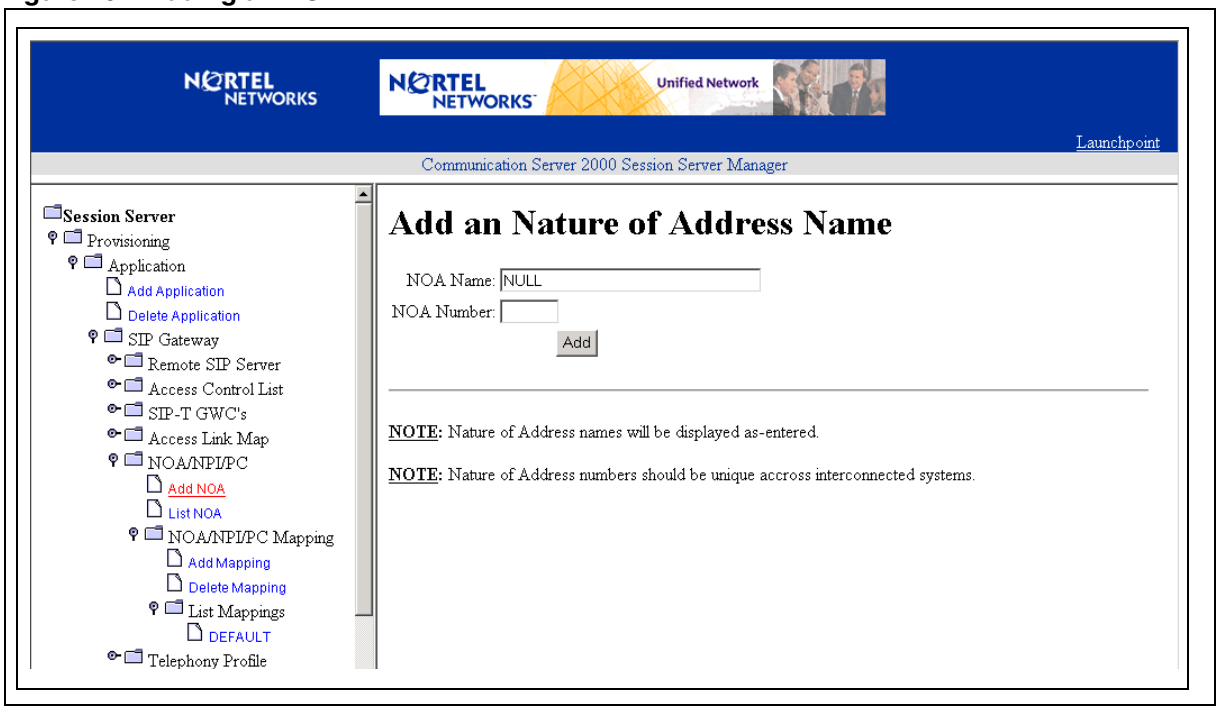
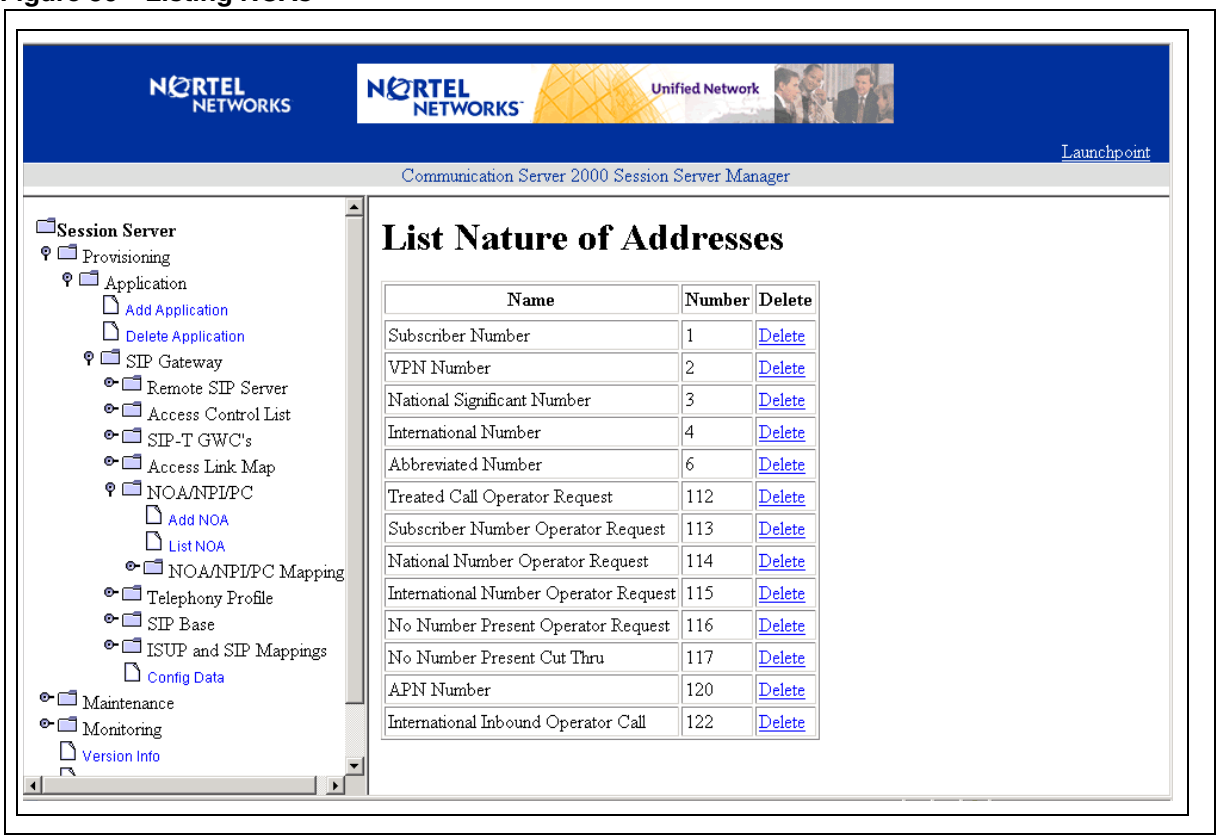


Figure 30 Listing NOAs



NOA/NPI/PC Mapping subfolder includes options to Add Mapping, Delete Mapping, and List Mappings.

When a call is originated this value will be added to the originating URI to indicate the context or origin of the call. For numbers like 411 and 911 this is necessary in that the number does not by itself identify the geographical origin of the call.

Either the default mapping may be changed to support such a feature or new mapping tables may be created.

Figure 31 Add an NOA to Phone-Context Mapping

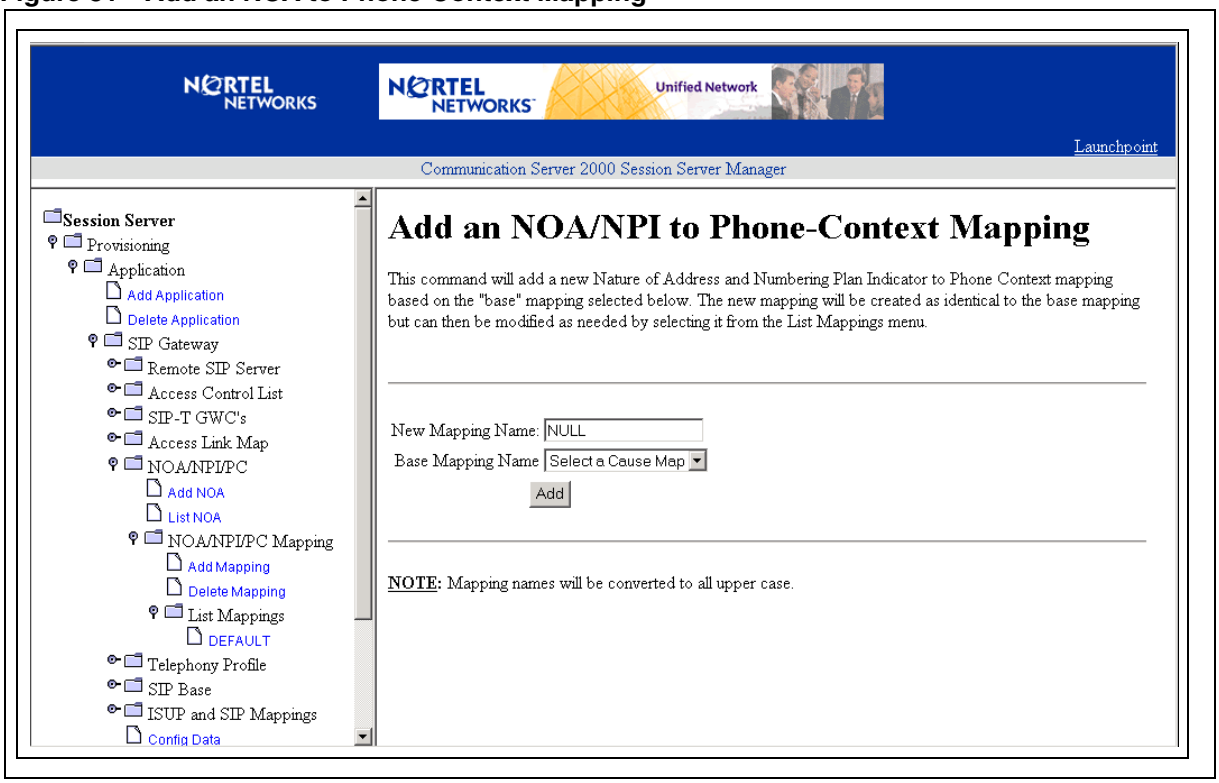


Figure 32 New NOA to Phone-Context Mapping

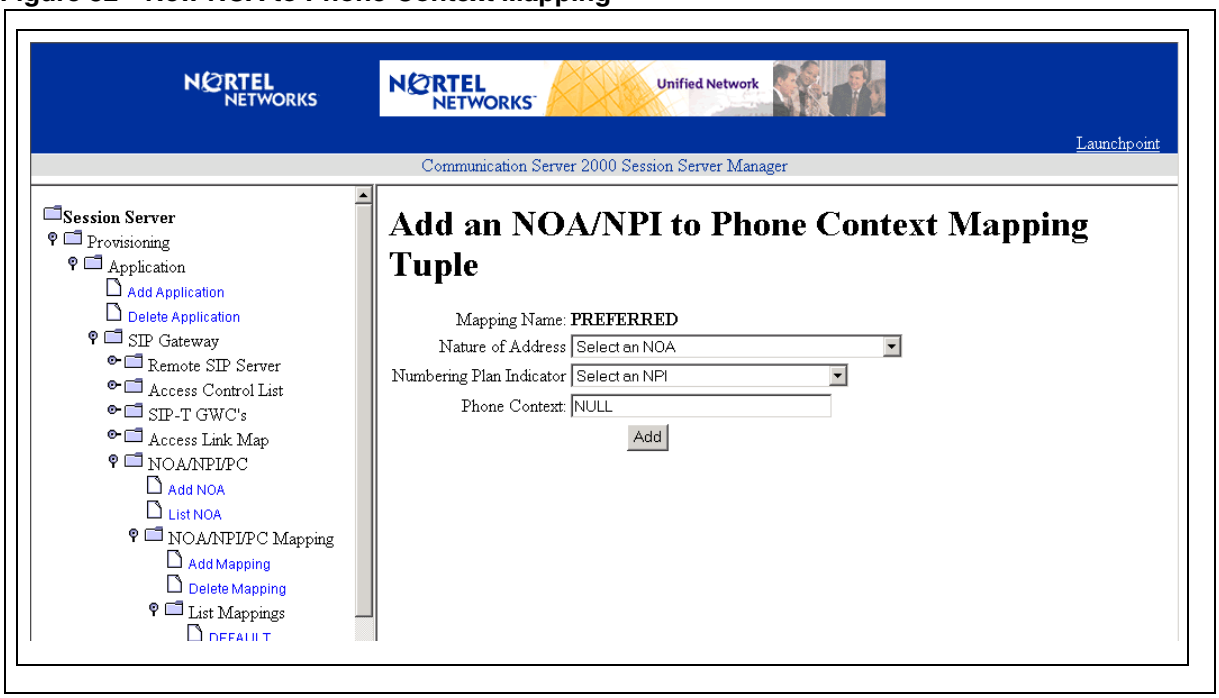


Figure 33 Delete an NOA/NPI to Phone Context Map

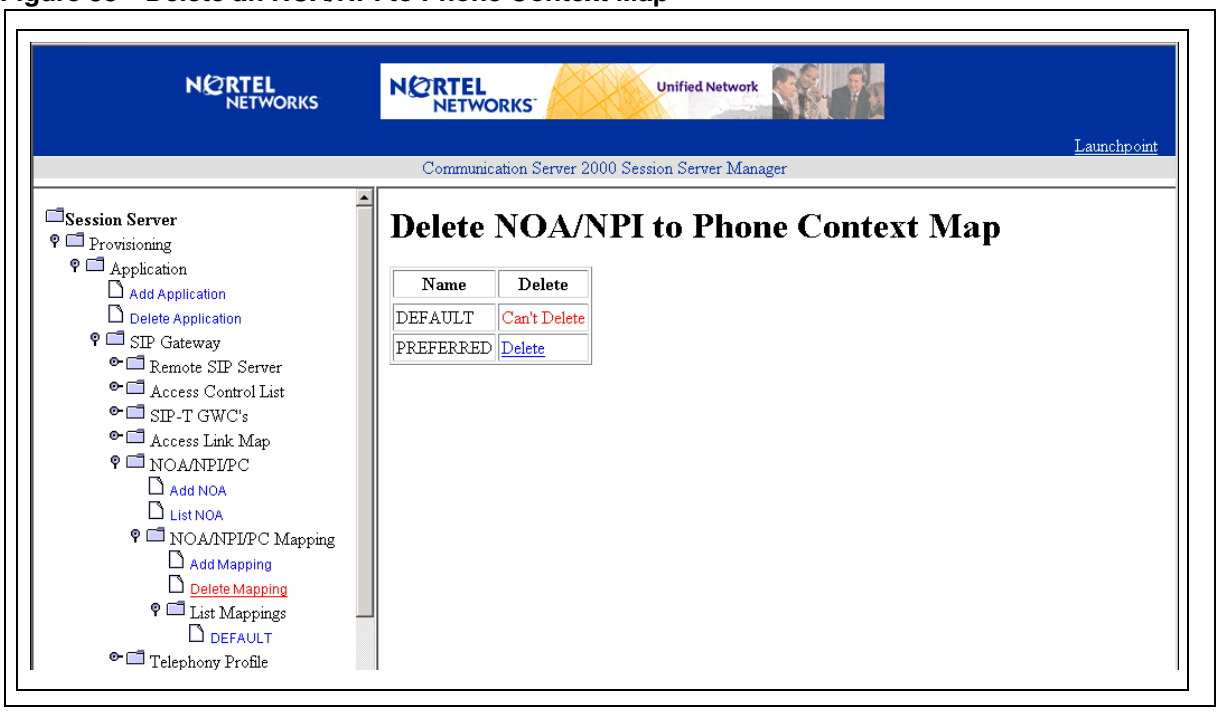
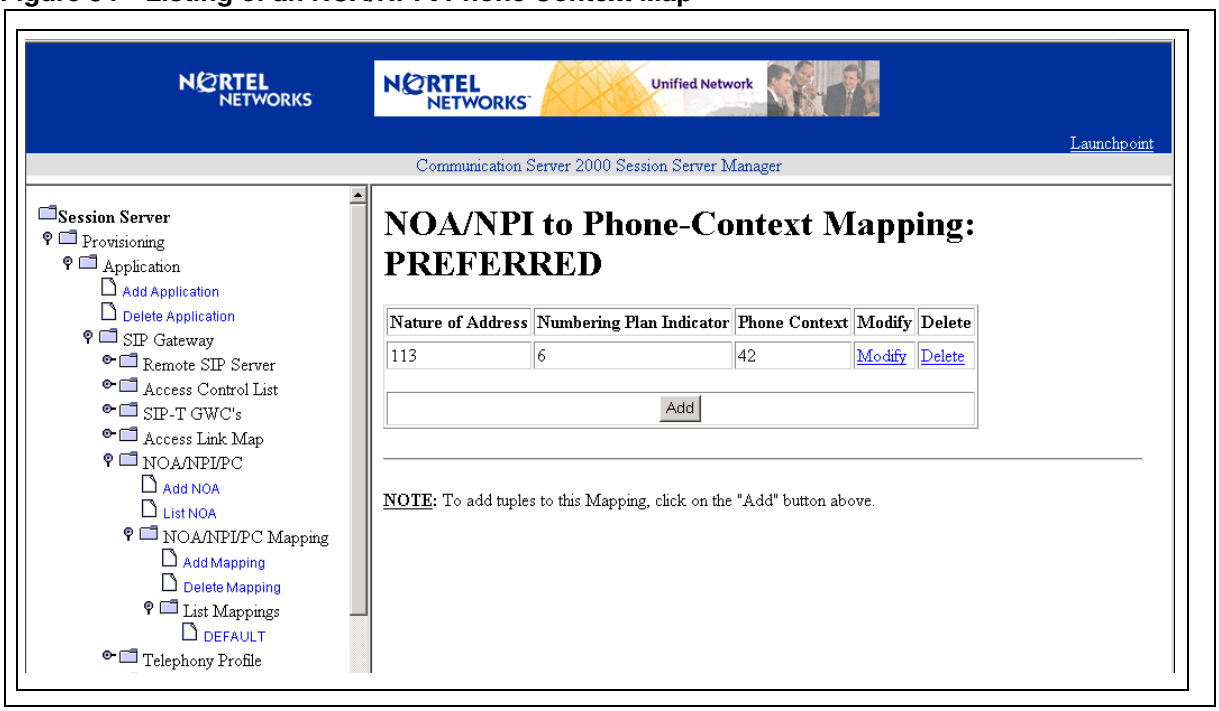


Figure 34 Listing of an NOA/NPI t Phone Context Map



119.8.2.4.9 ISUP Cause to SIP Response code mapping [optional]

An ISUP Cause to SIP Response code mapping table maps an ISUP Release Cause to a SIP Response code. For example, the ISUP release cause value of 17, indicating user busy, might be mapped to a SIP response code value 486 indicating busy.

A single ISUP Cause to SIP Response mapping table consists of nearly eighty ISUP Release Causes mapped to SIP response codes. Along with each mapping is a SIP Text Reason Phrase and an ISUP Text Reason Phrase. See Table 5, "ISUP Release Cause to SIP Response Code mapping" for a partial mapping.

Table 5 ISUP Release Cause to SIP Response Code mapping

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
.. ..			
4	487	Request Terminated	Send Special Tone Information
5	404	Not Found	Misdialled trunk prefix
6	480	Temporarily Unavailable	Channel Unacceptable
7	487	Request Terminated	Call awarded and being delivered in an established channel
8	487	Request Terminated	Preemption
9	487	Request Terminated	Preemption-circuit reserved for use
16	487	Request Terminated	Normal call clearing
17	486	Busy Here	User busy
.. ..			

The ISUP Cause to SIP Response mapping is termed optional datafill since a pre-defined mapping table exists in the system. This mapping table is called "DEFAULT". This predefined default mapping table may be selected when provisioning a Remote SIP Server described in "119.8.2.4.2 Remote SIP Servers" on page 1379. Note that this pre-defined mapping table cannot be modified.

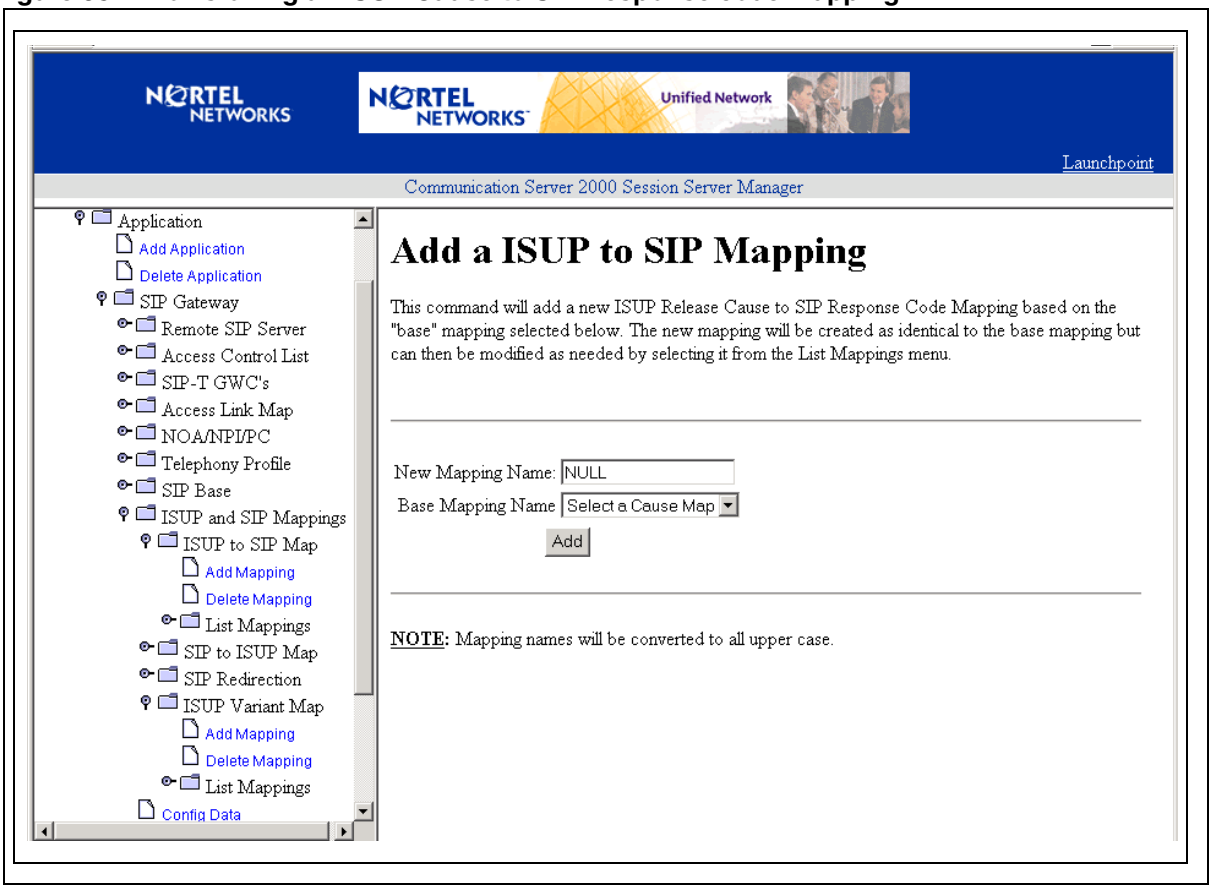
Although a pre-defined mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the “ISUP to SIP Map” sub-folder from the main Session Server Manager menu via the following commands:

— Click on the Provisioning folder
— Click on the Application folder
— Click on the SIP Gateway folder
— Click on the Mappings folder
— Click on the **ISUP to SIP Map** sub-folder
— Click on Add Mapping.

After clicking on “Add Mapping”, Figure 35 shows what a craftsperson sees in the web browser.

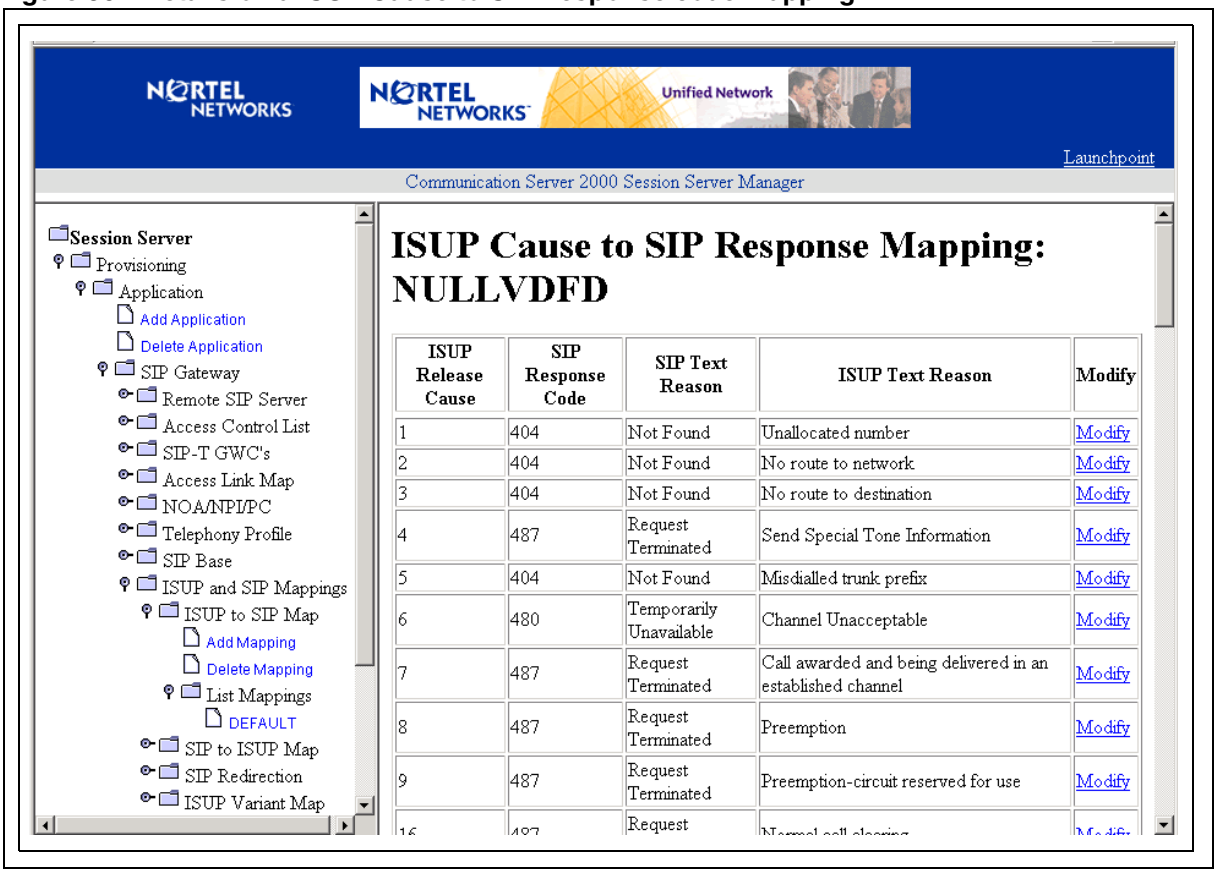
Figure 35 Provisioning an ISUP Cause to SIP Response code mapping



At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created, it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user’s call processing needs. The clone procedure exists so that a user does not have to enter the nearly eighty mappings to complete an ISUP Release Cause to SIP Response Code mapping table. A user is allowed to clone from any of the existing ISUP Release Cause to SIP Response Code mappings.

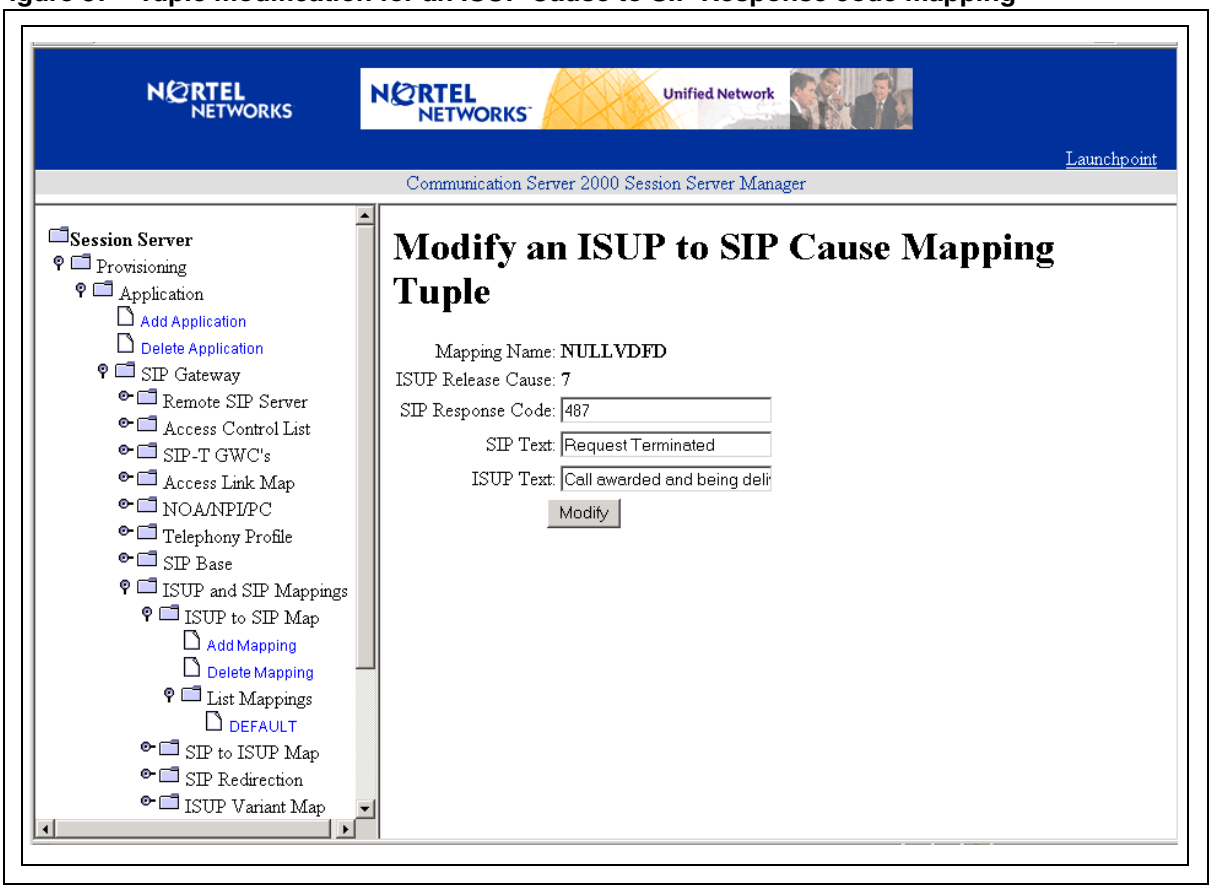
For the previous example, assume that the craftsperson entered a mapping name of MAP123. The mappings that exist in the system may be displayed by clicking on “List Mappings” within the “ISUP to SIP Map” sub-folder. In Figure 36, five mappings exist including the one just created by the craftsperson. Assuming the craftsperson wants to examine or modify the new mapping table, they simply click on the “MAP123” link.

Figure 36 Details on a ISUP Cause to SIP Response code mapping



Once clicked the mapping table is presented in the Interaction Frame. If the craftsperson then wants to modify a single tuple within that mapping table, they simply click on the “Modify” link and a tuple modify screen comes up in the Interaction Frame as shown in Figure 37, on page 1399 .

Figure 37 Tuple modification for an ISUP Cause to SIP Response code mapping



In Figure 37, the craftsperson chose to modify the tuple with the ISUP Release Cause of 5. They are then allowed to modify the SIP Response Code, SIP Text, and ISUP Text.

Existing mapping tables may be deleted by clicking on the “Delete Mapping” link within the “ISUP to SIP Map” sub-folder. When “Delete Mapping” is clicked, the user is presented with a selection of all mapping tables. Note the default mapping cannot be deleted. Finally, if the user attempts to delete a mapping that is in use by a Remote SIP Server, the request is denied.

119.8.2.4.10 SIP Response Code to ISUP Cause mapping [optional]

A SIP Response Code to ISUP Release Cause mapping table maps an SIP Response Codes to ISUP Release Causes. For example, the SIP Response Code of 404 may be mapped to the ISUP Release Cause of 41.

A single SIP Response to ISUP Cause mapping table consists of nearly forty SIP Response Codes mapped to ISUP Release Causes. See Table 6, "SIP Response Code to ISUP Release Cause mapping" for an example of this mapping:

Table 6 SIP Response Code to ISUP Release Cause mapping

SIP Response Code	ISUP Release Cause
400	41
401	21
402	21
403	21
404	1
.. .. ..	.. .. ..

The SIP Response Code to ISUP Release Cause mapping is termed optional datafill since a pre-defined mapping table exists in the system. This mapping table is called "DEFAULT". This predefined default mapping table may be selected when provisioning a Remote SIP Server described in "119.8.2.4.2 Remote SIP Servers" on page 1379. Note this pre-defined mapping table cannot be modified.

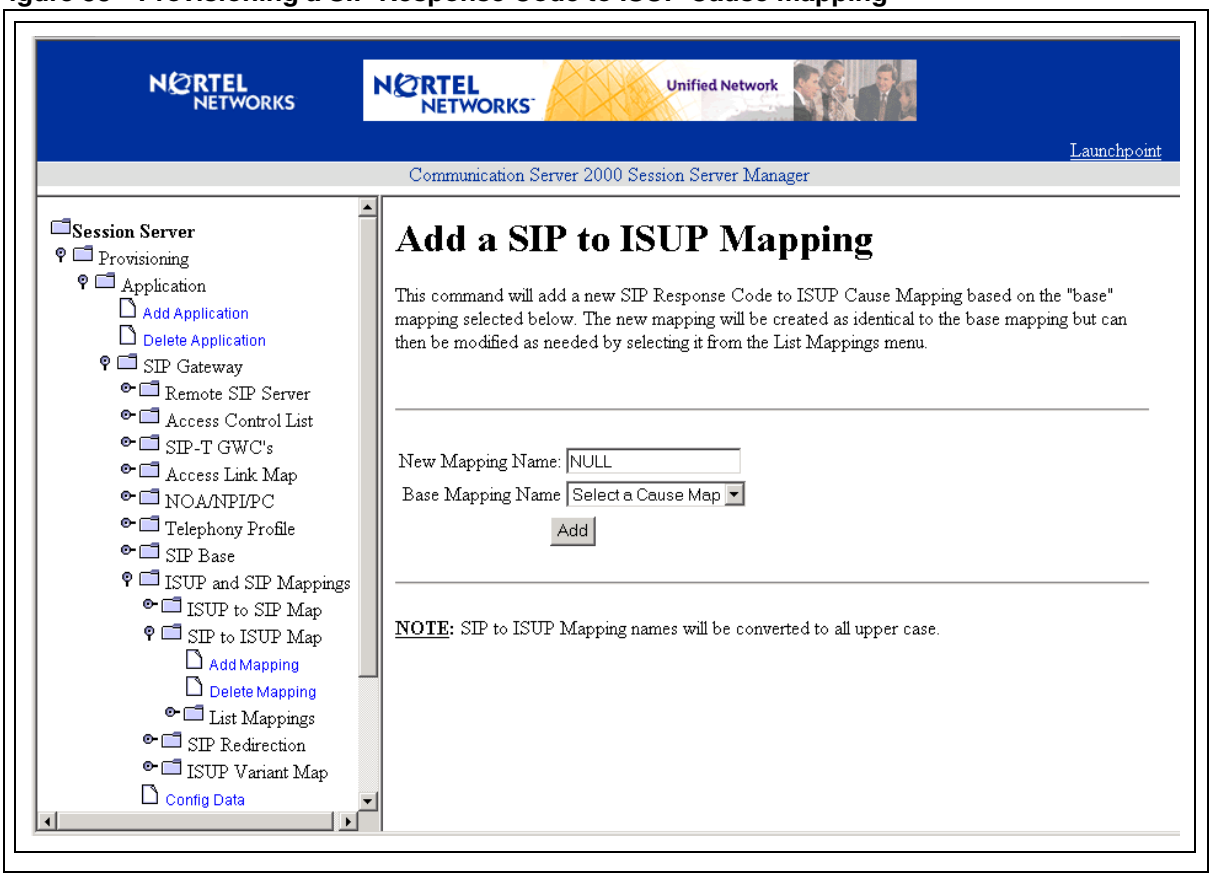
Although a pre-defined mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the "SIP to ISUP Ma" sub-folder from the main Session Server Manager menu via the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the Mappings folder
- Click on the **SIP to ISUP Map** folder
- Click on Add Mapping

After clicking on "Add Mapping", Figure 38, on page 1401 shows what a craftsperson sees in the web browser.

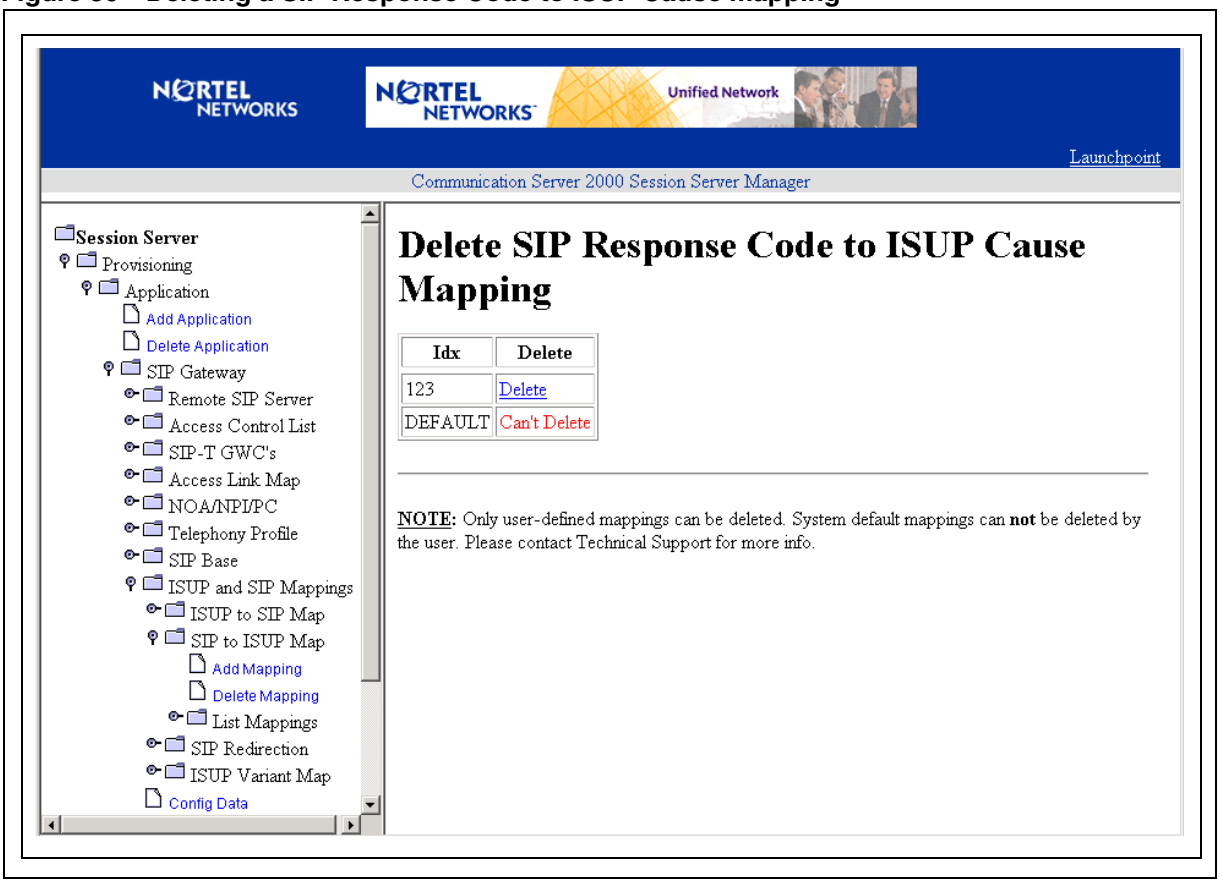
Figure 38 Provisioning a SIP Response Code to ISUP Cause mapping



At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created, it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs. This clone procedure exists so that a user does not have to enter the nearly forty mappings to complete a SIP Response Code to ISUP Release Cause mapping table. Note a user may clone from any of the existing SIP Response Code to ISUP Release Cause mappings.

Once successfully added, the craftsperson may chose to modify tuples in their mapping or even delete the newly added mapping table. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "SIP to ISUP" sub-folder. Figure 39, on page 1402 shows an example of what is presented to the craftsperson in such a scenario.

Figure 39 Deleting a SIP Response Code to ISUP Cause mapping



119.8.2.4.11 SIP Redirection Mapping [optional]

SIP Redirection Mapping is a mapping of 3xx SIP redirection response messages to an associated 300-699 response codes. This mapping allows the customer to configure a call receiving a 3XX redirection message to be processed as a 300 or 699 related value. An example of the redirection mapping defaults are shown in Table 7, “Redirection mapping defaults”.

Table 7 Redirection mapping defaults

SIP Redirection code	Response Code
300	300
301	301
302	302
305	305
380	380

SIP Redirection Mapping datafill is optional if the customer does not wish to change any of the above pre-defined defaults.

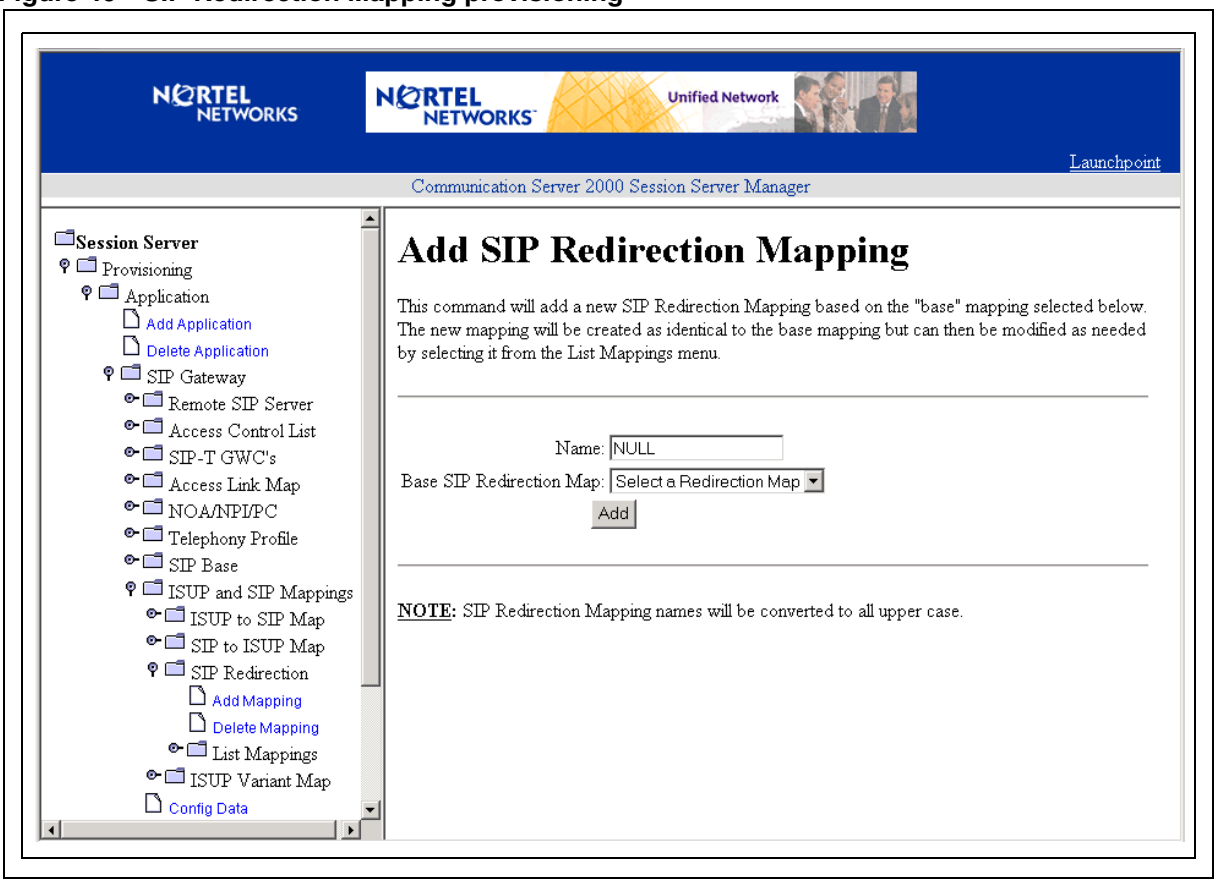
Although the pre-defined default mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the “ISUP to SIP Map” sub-folder from the main Session Server Manager menu via the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the Mappings folder
- Click on the **SIP Redirection** folder
- Click on Add Mapping

After clicking on “Add Mapping”, Figure 40, on page 1404 shows what a craftsperson sees in the web browser.

Figure 40 SIP Redirection Mapping provisioning



At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs.

Once successfully added, the craftsperson may chose to modify tuples in their mapping or even delete their newly added mapping. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "SIP Redirection" sub-folder. In order to modify a mapping, the craftsperson clicks on "List Mappings" and then clicks on the mapping they wish to modify.

119.8.2.4.12 SIP Base [optional]

A SIP Base is a simple character string that represents base protocols utilized when provisioning ISUP to SIP Variants described in an section 119.8.2.5. In order to provision a new SIP base, the following is done:

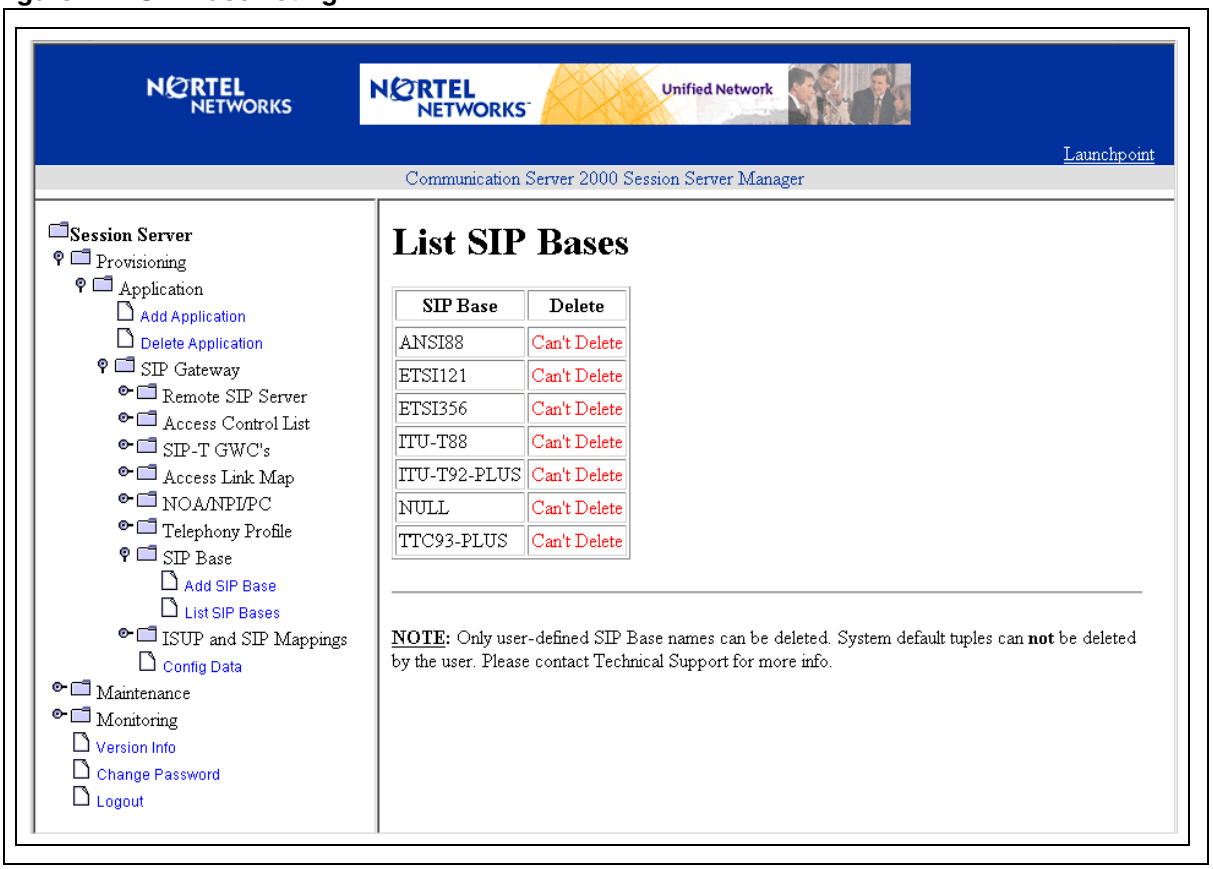
- In the SIP Gateway provisioning menu, SIP Base datafill may be added using the “Add SIP Base” link in the SIP Base folder.
- It may also be listed by clicking on “List SIP Base”. Once the values are listed, the user may choose to delete a particular one if it is not being used in any datafilled tuples in the ISUP Variant Mapping table. Deletions on system defaults are not allowed.

Six protocol defaults exist. Those pre-defined defaults are:

ANSI88	ITU-T92-PLUS	ETSI356
ITU-T88	ETSI121	TTC93-PLUS

An example of a user listing all the SIP Base values in the system is as follows:

Figure 41 SIP Base listing



119.8.2.5 SIP Gateway application maintenance

In previous sections, the functionality of the SIP Gateway application, which resides on the Session Server Manager was described in detail. For the SIP Gateway application to function properly, certain actions must be performed by SIP Gateway maintenance.

Note this section is written with the assumption that the Session Server Manager's unit status is active and enabled. Refer to section "119.8.2.5.2 Unit Status" on page 1411 for allowed maintenance actions when the unit is either not active or not enabled.

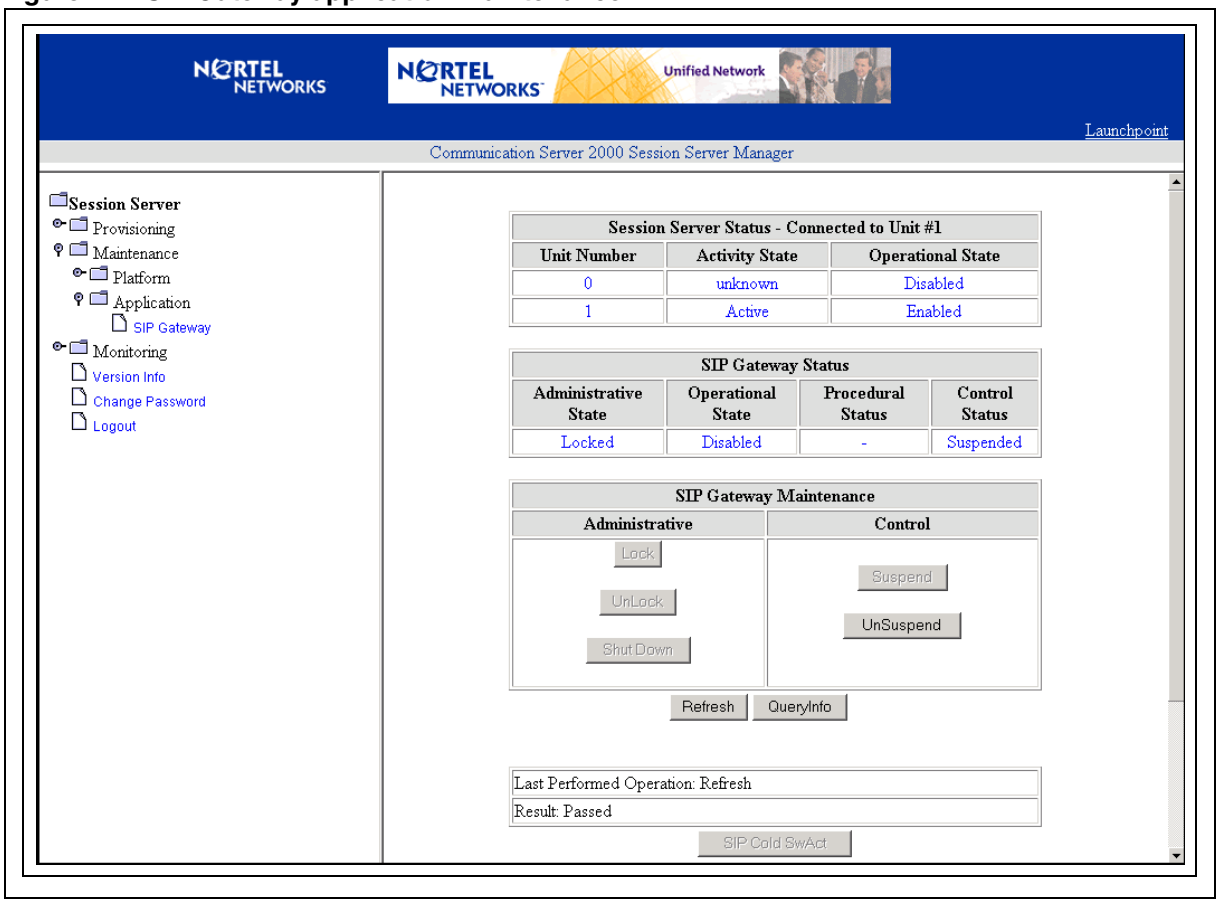
Access the SIP Gateway maintenance section of the web page by going to:

— Click on Maintenance folder

— Click on the Application folder

— Click on SIP Gateway

Figure 42 SIP Gateway application maintenance



Before performing maintenance actions, a basic outline on how to bring the SIP Gateway application into service and out of service is as follows:

Taking the application from out of service to in-service

— Unsuspend followed by Unlock

Taking the application from in-service to out of service

— Lock followed by Suspend

SIP Gateway maintenance utilizes the CCITT X.731 state and status attributes as well as X.731 commands. This is different than the standard DMS Core commands (e.g. BSY, RTS) and state (e.g. INSV), but it is consistent with recent Succession platform additions. The following table shows the four fields that comprise the CCITT X.731 state of the SIP Gateway application. The last column in the table is shown to provide a mapping to old-style DMS states to aid in understanding[1].

Table 8 SIP Gateway application states

Administrative State	Operational State	Procedural Status	Control Status	DMS Style States
Locked	Disabled	-	Suspended	OFFL
Locked	Enabled	-	-	MANB
Locked	Enabled	Terminating	-	MANBP
Unlocked	Enabled	-	-	INSV
Unlocked	Disabled	-	-	SYSB
Shutting Down	Enabled	-	-	INSVD

From the web interface, the above states may be changed via the following maintenance commands. Each of the five maintenance control items are represented by clickable buttons on the web page.

- Administrative State Control- The user can select from the following:
  - — Lock
  - — Unlock
  - — Shut Down
- Control Status Control - The user can select from the following:
  - — Suspend
  - — Unsuspend

[1]The DMS style states are not shown on the SIP Gateway maintenance web page. It is shown above only for understanding.

Depending on the current state, the user is not always allowed access to all of the maintenance control options.

The table below explains what controls are allowed depending on the current Admin State, Operational State, and Procedural Status. Again, DMS Style representation is shown in parenthesized italics to aid in understanding.

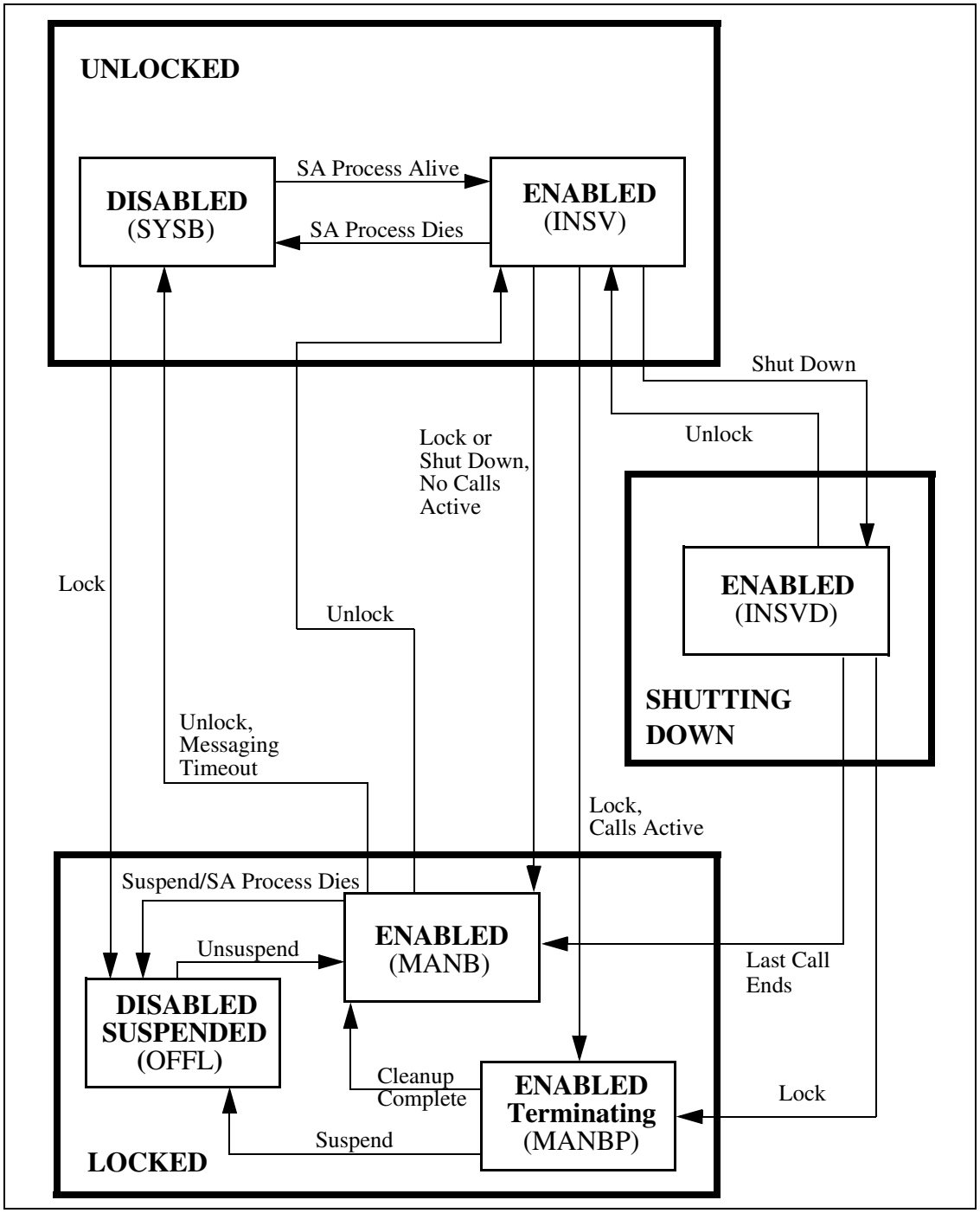
Table 9 SIP Gateway Maintenance External Controls Allowed

Admin State	Operational State	Procedural Status	Control Status	Allowed Controls DMS Style Commands in ()'s
Locked	Disabled	-	Suspended	Admin Control None Control Status Unsuspend (*BSY*)
Locked	Enabled	-	-	Admin Control Unlock (RTS) Control Status Suspend (*OFFL*)
Locked	Enabled	Terminating	-	Admin Control None Control Status: Suspend (*OFFL*)
Unlocked	Enabled	-	-	Admin Control Lock (*BSYFORCE*) Shut Down (*BSY*) Control Status None
Unlocked	Disabled	-	-	Admin Control Lock (*OFFL*[a]) Control Status None
Shutting Down	Enabled	-	-	Admin Control Lock (*BSYFORCE*) Unlock (*RTS*) Control Status None

a. From a DMS perspective, this is a non-standard command. In the DMS model you would expect to do a BSY command, and then an OFFL command to get from the SYSB to OFFL state. However, for the SIP Gateway maintenance state model, SYSB is an error condition where the SIP Gateway process has died due to some error. MANB is a state where the SIP Gateway process should be up and running. Thus, it is more applicable when manually taking the SIP Gateway out of service from the SYSB command to go directly to OFFL (as opposed to first going MANB), as both are states where the SIP Gateway process is not running.

Finally, a maintenance state is presented. DMS system commands are shown in parentheses to aid in understanding. However, DMS style commands are not shown on the web page since CCITT X.731 commands and controls are utilized.

Figure 43 SIP Gateway Maintenance State Diagram



119.8.2.5.1 Application Cold Swact

On the SIP Gateway Application maintenance page, the SIP Cold SWACT button allows users to perform an application cold switch of activity (SWACT) if the Session Server Manager platform is active and enabled. If the unit is not active, the button is not allowed to be pressed.

Assuming the Session Server Manager unit activity status is active and the operational state is enabled, the craftsperson can click the button to perform an application cold SWACT.

Note: From the active unit web page, the unit must be active, enabled, and the mate unit must be on standby and enabled in order to access the SIP Cold SWACT button.

If the user clicks the SIP Cold SWACT button, a dialog box appears to verify that the user wants to proceed with a SIP Gateway cold SWACT. The consequences of performing a SIP Gateway cold SWACT include the following:

- All currently active SIP Gateway calls will be taken down.
- A Session Server Manager force SWACT will then occur.

Note: This is not the normal interface to request a platform SWACT. Only proceed with the SIP Gateway cold SWACT if a platform SWACT has already taken place, and a problem has been detected with SIP Gateway call processing.

119.8.2.5.2 Unit Status

The previous SIP Gateway maintenance sections made the assumptions that the Session Server Manager unit's activity state was active and the operational state was enabled. If unit activity state is not active or the operation state is not enabled, maintenance actions on the SIP Gateway application are not allowed. The only buttons available for use on the SIP Gateway application maintenance page are the refresh and the QueryInfo buttons.

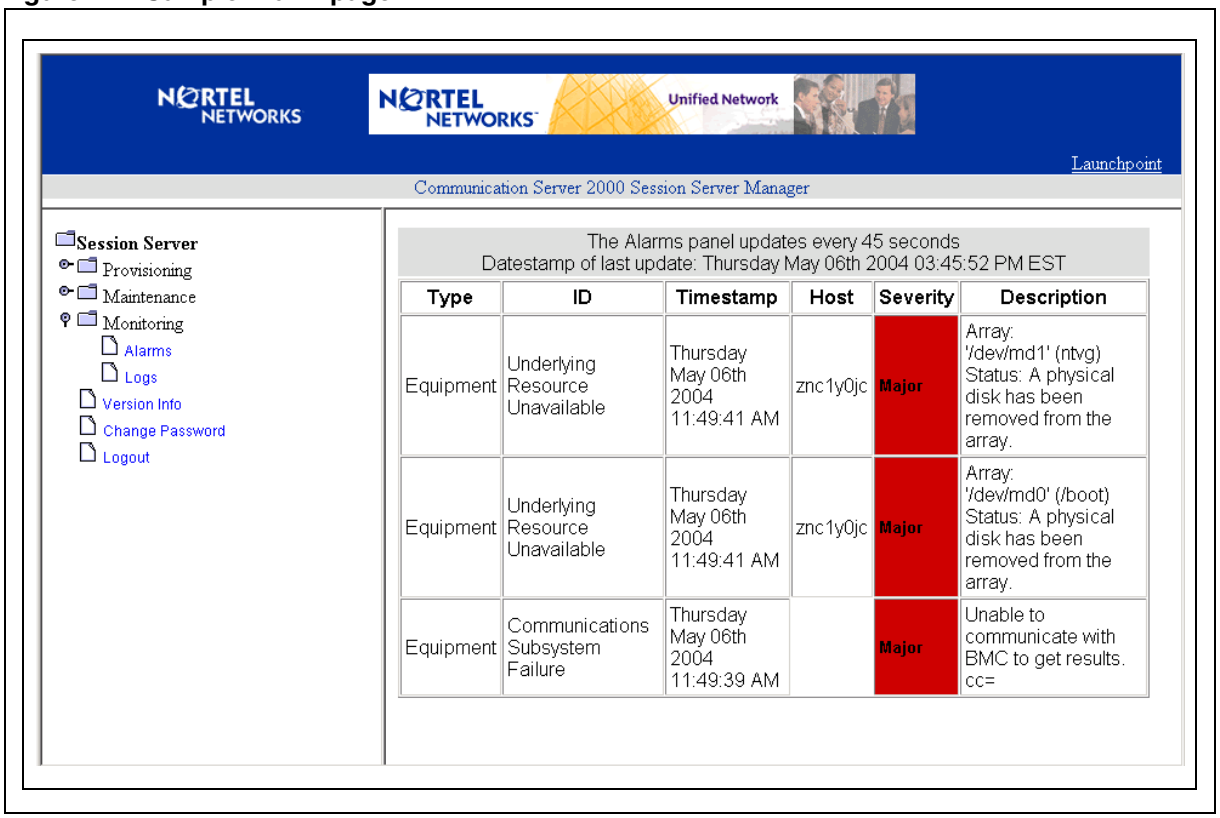
119.8.2.6 Alarms

The Session Server Manager has the capability for applications or the system itself to generate alarms. These alarms can be viewed on the Session Server Manager's Alarm web page. Information shown about particular alarms include the type, identifier, time-stamp, host (unit from which the alarm was raised), severity, and a description of the alarm.

The user may view alarms by going to the alarms web page. The alarm web page is located in the Monitoring menu folder.

Once the craftsperson clicks on Alarms, the alarm web page is presented in the right frame with the current alarm list. The alarm web page updates every 30 seconds and the user also has the option of invoking a re-query of alarms. This is similar to the Alarm implementation for the Storm system.

Figure 44 Sample Alarm page



119.8.2.7 Logs

The Session Server Manager has the capability for applications or the system itself to generate logs. These logs can be viewed on the Session Server Manager's log web page. Information shown about a particular log includes:

- Timestamp
- Session Server device name
- Process that generates the log
- Log ID and number
- Alarm severity
- Log type
- Log label
- Additional information

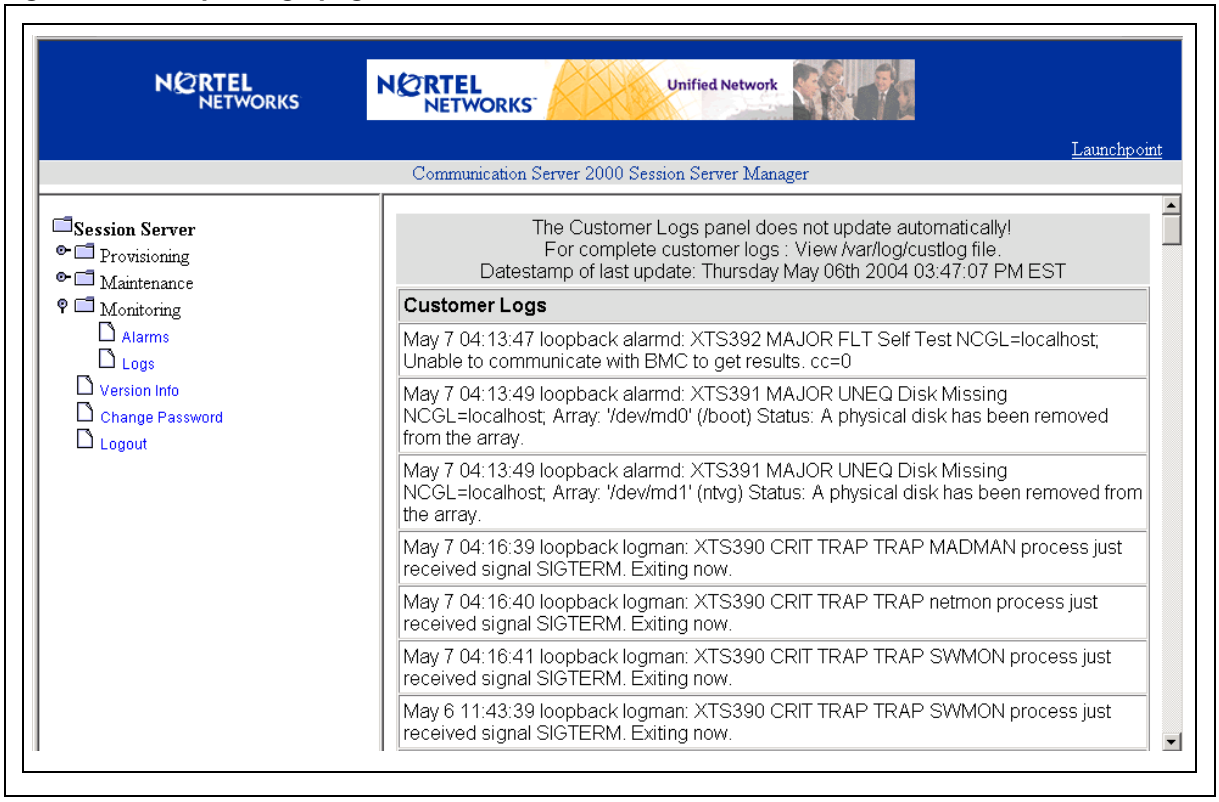
The user may view logs by going to the logs web page located in the Monitoring menu folder.

Note 1: The body of log formats shown in this document are the formats for Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server Web Interface. However the content of the logs will not differ, only the formatting.

Note 2: When viewing logs from an IEMS, log headers may differ slightly from what is shown in this document.

Once the craftsperson click on Logs, the log web page is presented in the right frame with the current log list. A sample log web page is shown below.

Figure 45 Sample Logs page



119.8.2.8 Operational Measurements

Like other Call Server platforms, the Session Server Manager records operational measurements (OMs) for various performance related data items. The OM subsystem is similar to the OM subsystem but is different in some aspects. The majority of OMs pegged in SN07 are directly related to the SIP Gateway application. Also, OMs that are pegged can be viewed via a command line user interface (CLUI) after using secure shell (SSH) to login to the Session Server Manager.

After logging in to the Session Server via SSH to an account such as “mtc”, the user may issue commands such as the help command:

```
[mtc@sserv-unit0 mtc]$ omshow help

        Please select from the following options.

        omshow help
        omshow all active
        omshow all holding
        omshow all lastfive
        omshow <omgroup> active
        omshow <omgroup> holding
        omshow <omgroup> lastfive
        omshow all zero
        omshow <omgroup> zero
        omshow holdingperiod 30
        omshow holdingperiod 15
```

A brief description of the above commands are as follows:

`omshow help` - Print out the commands as shown above.

`omshow all active` - Print out all the OM groups and their associated active registers.

`omshow all holding` - Print out all the OM groups and their associated holding registers.

`omshow all lastfive` - Print out all the OM groups and their register values for the past five minutes.

`omshow <omgroup> active` - Print out the active registers for a particular OM group.

`omshow <omgroup> holding` - Print out the holding registers for a particular OM group.

`omshow all zero` - Zero the active registers for all OM groups.

`omshow <omgroup> zero` - Zero the registers for a particular OM group.

`omshow holdingperiod 30` - Set the holding period to 30 minutes.

`omshow holdingperiod 15` - Set the holding period to 15 minutes.

Operational Measurements are kept in two primary formats for a particular holding period. For example lets assume the holding period time is 30 minutes and the current time is 4:50 PM. The active registers represent 4:30-4:50 PM and the holding registers represent 4:00-4:30 PM. Finally at 5:00PM the active registers are copied to the holding registers. The possible holding periods for the Session Server are 15 and 30 minutes. The default holding period time is 15 minutes.

In addition to the above, the values of OM groups and registers can be output for the current five minute interval. For example, if the current time is 4:04:39 PM, the register values for the last 4 minutes and 39 seconds can be output via the “lastfive” selection.

Note OM values pegged in an application such as the SIP Gateway application may not reach the OM subsystem for a full minute. This can impact what is displayed when the omshow command is used since omshow pulls values from the OM subsystem.

Finally OM group register data pegged on one unit of a Session Server is completely independent of register data on its mate unit. Register data is not transferred from one unit to another.

119.8.2.8.1 Operational Measurements

This section contains a list of three OM groups and registers that are supported in SN07 on the Session Server. OMs on the Session Server are not in any related to operational measurements on the Core. Also, OMs generated on the Session Server are not sent to the CS2K Core.

Table 10 OM Group: SIPGW_CALLP

Register Name	Description
IC_CALL_ATTEMPTS	Total number of incoming call attempts
OG_CALL_ATTEMPTS	Total number of outgoing call attempts
CALLS_ANSWERED	Total number of calls answered
CALLS_ABANDONED	Total number of calls abandoned
CALLS_REJECTED	Total number of calls rejected
CALLS_REDIRECTED	Total number of calls redirected

Table 11 OM Group: SIPGW_SERVICES

Register Name	Description
REFER_ATTEMPTS	Total number of refer attempts[a]
REFER_SUCCESS	Total number of successful refers
IC_DTMF_SUBSCRIBES	Total number of incoming DTMF subscribes
OG_DTMF_SUBSCRIBES	Total number of outgoing DTMF subscribes
IC_DTMF_NOTIFYS	Total number of incoming DTMF notifies
OG_DTMF_NOTIFYS	Total number of outgoing DTMF notifies
IC_FAX_SUBSCRIBES	Total number of incoming fax subscribes
OG_FAX_SUBSCRIBES	Total number of outgoing fax subscribes
IC_FAX_NOTIFYS	Total number of incoming fax notifies
OG_FAX_NOTIFYS	Total number of outgoing fax notifies

a. Registers IC_FAX_SUBSCRIBES, OG_FAX_SUBSCRIBES, IC_FAX_NOTIFYS, and OG_FAX_NOTIFYS exist but are not supported in the SN07 release.

Table 12 OM Group: SIPGW_MISC

Register Name	Description[a]
TCP_CALLS	Total number of TCP Calls
UDP_CALLS	Total number of UDP calls
SIP_MSG_SEND_FAILURES	Total number of SIP Msg Send Failures
INCOMING_SDP_INCOMPATIBLE	Total number of incompatible SDPs received from remote SIP servers
OUTGOING_SDP_INCOMPATIBLE	Total number of incompatible SDPs received from local gateways.

a. Register SIP_MSG_SEND_FAILURES exists but is not supported in the SN07 release.

119.8.2.8.2 CSV files

While the OMSHOW function provides near term information, it does not save performance info after a set period in time. In certain scenarios this historical information may prove to be valuable. Therefore OM information is also saved to comma separated value (CSV) files. Two sets of comma separated files are created.

Short Term

These six comma separated value files represents the last 30 minutes worth of information. Each file consists of a particular five minute interval within the thirty minute timeframe.

Long Term

The long term history represents the last 24 hours worth of information. If the OM collection interval is 15 minutes, then a total of 96 files are kept representing the last 24 hours. However if the collection interval is 30 minutes, 48 files are kept.

Please refer to “119.24 Appendix D: CSV file information” on page 1438 for detailed information on the CSV file locations and the file format.

119.9 Software Optionality Control (SOC)

There are two new core usage SOC options that are used to limit the maximum number of simultaneous calls allowed through the Session Server Manager at any given time. Without one or both of the new SOC options, no call processing can take place using the Session Server Manager. Before discussing the new SOC options, it is important to understand the relationship between the new SOC options and the existing DPT SOC option in the core.

119.9.1Existing DPT SOC option CS2B0005

Calls using the SIPT Gateway application on the Session Server Manager are considered to be DPT (Dynamic Packet Trunking) calls and are therefore limited by the base DPT SOC, CS2B0005. Before Session Server Manager calls can be made, the base DPT SOC must be purchased. This existing DPT SOC option is a usage based SOC and it specifies the maximum number of DPT ports that can be used simultaneously for processing all DPT calls.

Although DPT SOC option CS2B0005 specifies the maximum possible number of DPT ports that can be used in the office, the actual maximum for the office is governed by the office parameter DPT_MAX_PORTS in table OFCVAR. The DPT_MAX_PORTS parm can be set to any value equal to or less than the CS2B0005 SOC option and it allows fine tuning of DPT traffic limits within the bounds of the DPT SOC limit without having to obtain a new SOC limit each time.

Since dynamic packet trunking does not have fixed trunk members, it is possible that a single trunk group in the office can use all the available DPT port capacity. To prevent starvation of DPT ports for calls on other trunk groups, the maximum number of simultaneous DPT calls allowed on a particular trunk group can be limited. This adjustment is made on a trunk group basis using the MAXCALLS field in table DPTRKMEM.

119.9.2Two New Session Server SOCs (CS2B0008 and CS2B0009)

The two new core usage based SOC options for the SIPT Gateway application are CS2B0008 “Call Server to Call Server SOC” and CS2B0009 “Call Server to Application Server SOC”. The combined total limits of these two SOCs should not exceed the limit of the base DPT SOC option, CS2B0005. The maximum number of simultaneous DPT calls allowed for the office is still governed by the DPT_MAX_PORTS parameter in table OFCVAR, although the maximum number of simultaneous Session Server Manager calls can be further restricted by these new SOC options.

Each Session Server Manager call is designated as either a “Call Server to Call Server” call or a “Call Server to Application Server” call. This designation is made in field CONNTYPE of table SIPLINK in the core. In table SIPLINK, each SIP

access communication link is marked according to whether that link is used to communicate to another call server or to an application server. If the link is used to connect to another CS 2000 or an MCS, then field CONNTYPE should be set to CS2CS, denoting a call server to call server connection. If the link is used to connect to some other type of SIP server, then field CONNTYPE should be set to CS2AS, denoting a call server to application server connection.

Current simultaneous usage for each Session Server Manager call type is tracked in the core and calls will be rejected if they cause the corresponding Session Server Manager SOC limit to be exceeded.

119.10 Hardware Requirements or Dependencies

The Session Server Manager is an integrated platform consisting of hardware and software. Please refer to section 119.4.1 for the hardware configuration. There are no additional hardware requirements or dependencies

119.11 Software Requirements or Dependencies

Software requirements include the following:

- Nortel Carrier Grade Linux. Provided by Activity A00004005.
- Session Server Manager NGSS07
- SN07 GWC, CM
- CS2M

In order to maintain the Session Server Manager a web client is needed. The requirement for a web client is as follows:

Supported web clients on a PC:

- Windows 2000, XP, or 2003 based operating system.
- Supported web browsers on those operating systems include:
  - — Internet Explorer 6.0 SP1and above
  - — Netscape 6.2.x, and Netscape 7.1 and above

Supported web clients on a Sparc:

- Solaris 8 or 9
- Supported web browsers on those operating systems include:
  - — Netscape 6.2.x, and Netscape 7.1 and above

The following browser are NOT supported:

- Any browser running on Linux
- Any browser running an OS under VMware
- Any browser running under Solaris on a PC
- Any browser running on MacIntosh hardware
- Mozilla

119.12 Limitations and restrictions

The following limitations and restrictions exist for the Session Server Manager platform and the SIP Gateway application.

1. See section "119.11 Software Requirements or Dependencies" on page 1421 for a comprehensive list of operating systems and web browsers that are supported.
2. Javascript must be enabled in the web browser used.
3. Popup blocking should **not** be enabled within the web browser. Verify that popup blocking is not enabled prior to using the web browser to access the Session Server Manager.
4. When adding or deleting mapping tables via the web client, the craftsperson should allow the add operation to complete before performing other web actions. Aborting a web action via a "Stop" or "Back" can cause incomplete data to be added to the database.

   Invalid mapping tables can always be deleted by the craftsperson via the "Delete Mapping" command in the respective mapping sub-folder.
5. When a new mapping is added to any of the mapping table folders, the folder menu at the left side of the web-browser does not automatically refresh. The user should close/open the folder to see the newly added mapping.
6. For Call scenarios, where an ISUP payload is to be generated, mandatory parameters are mapped from appropriate SIP Headers. As a result, some of the services depending on the trunk-type (IBNT2, IT, EANT) may not be available, if appropriate mapping is not defined.
7. For the List Mappings sub-folder in the "ISUP to SIP Map", "SIP to ISUP Map", "ISUP Variant Map", and "SIP Redirection" mappings:

   If the List Mappings sub-folder is open when a mapping table is added or deleted, the mapping names under the particular List Mappings sub-folder won't change *visually* until that sub-folder is closed and re-opened. The mapping tables will have been added or deleted per the user action. The user is **not** required to open or close the List Mappings sub-folder for the add or delete action to take effect.
8. If the optional trunk telephony profile header is not used in the SIP messages between the Session Server Manager and destination SIP servers, then only a single trunk group can be used to carry the traffic between the Session Server Manager and a single destination SIP server. If multiple trunk groups are required between the Session Server Manager and a single destination SIP server, trunk telephony profile headers are required in the SIP messages to identify which trunk to use for a particular incoming call to the Session Server Manager.

9. Multiple independent and redundant pairs of Session Servers are not supported.
10. No backup and restore functionality is available for the Session Server Manager node in SN07.
11. All currently active SIP Gateway calls will be taken down during a SIP Gateway cold SWACT.
12. The Session Server Manager Web interface utilizes and requires the use of HyperText Transport Protocol Secure (HTTPS).
13. Before HTTPS can be used on the Session Server Manager, a Secure Sockets Layer (SSL) certificate must be obtained and installed.
14. OM values pegged in an application such as the SIP Gateway application may not reach the OM subsystem for a full minute. This impact what is displayed when the omshow command is used since omshow pulls values from the OM subsystem.
15. OM group register data pegged on one unit of a Session Server is independent of register data on its mate unit. Register data is not transferred from one unit to another.
16. WARNING: To ensure data integrity, the command line interface should not be used to enter or change data in the database. Only the web interface should be used to enter or change the provisioned data.
17. Improper reboot or shutdown of the Session Server can result in data loss. Proper procedures should be followed when rebooting or shutting down a Session Server unit.
18. The Session Server 2000 GUI does not support being accessed over a NAT'd connection in SN07. Only direct (same-LAN) and SSPFS web proxied connections are supported.
19. The physical limit for table SIPLINK is 2048 tuples; however, due to the DDM limitation for table DPTRKMEM, table SIPLINK should not be datafilled to more than 400 tuples.
20. If the Session Server goes out of service due to a system failure or because of improper shutdown (thereby disrupting the ability to communicate the link status change to the gateway controllers), all in-service SIPT trunks associated with any access links on the Session Server will remain in-service.

119.13 Interactions

N/A.

119.14 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	___X___
Configuration	
Data Schema	___X___
User Interface	_____
Element Management	_____
Security	_____
Service Order	___X___
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)_	_____

119.15 Glossary

CI	Command Interpreter
CLUI	Command Line User Interface
CM	Computing Module (aka “Core”)
CS2M	Call Server 2000 Manager
CS 2000	Call Server 2000
CS 2000 OAMP	Call Server 2000 OAMP (aka CS2M aka PTM)
DMS	Digital Multiplex Switch
DNS	Domain Name Server
DPT	Dynamic Packet Trunking
GA	General Availability
GWC	Gateway Controller
HIOP	High performance Input Output Processor
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
IEMS	Integrated Element Management System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network User Par
JRE	Java Runtime Environment
MAPCI	Maintenance, Administration, and Provisioning Command Interpreter
MCS	Multi-Media Communication Server
MGC	Media Gateway Controller
NCGL	Nortel Carrier Grade Linux
NTP	Network Time Protocol
OAM&P	Operation, Administration, Maintenance, and Provisioning
OSS	Operations Support System
OSSGate	OSS Gateway
PAM	Pluggable Authentication Module
PI	Progress Indicator
PRI	Primary Rate Interface
PTM	Packet Telephony Manager
PVG	Packet Voice Gateway
RFC	Request For Comments
RPI	Remote Party Id
RTCP	Real-Time Control Protocol

RTP	Real-Time Protocol
RTS	Return To Service
SAM	SIP Application Maintenance
SCP	Secure Copy
SCS	Succession Communication Server/Call Server
SCTP	Stream Control Transmission Protocol
SG	SIP Gateway application
SDM	Supernode Data Manager
SDP	Session Description Protocol
SESM	Succession Element and Sub Element Manager (aka CS 2000 OAMP, aka PTM) Former name of CS2M.
SIP	Session Initiation Protocol
SIPT	Session Initiation Protocol (SPI) for Telephones
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SNM	Session Server Node Maintenance
Session Server	Platform for the SIP Gateway application
SPM	Spectrum Peripheral Module
SQL	Standard Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STORM	STORage Management
SWACT	Switch of Activity
TCP	Transmission Control Protocol
TPM	Telephony Profile Message
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VToIP	Voice Trunking over IP
VRDN	Virtual Router Distribution Node

119.16 References

1 RFC 3261: Session Initiation Protocol

2 RFC 2327: Session Description Protocol

3 RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol

4 RFC 3264: An Offer/Answer Model with the Session Description Protocol

5 RFC 3265: SIP Event Notification

6 RFC 3311: The SIP Update Method

7 RFC 3515: SIP Refer Method

8 A00003270: SIP Open Interop Call Processing

9 A00003271: Session Server Web Server Interface

10 A00003272: SIP on Session Server Provisioning Framework

11 A00003273: SIP on SIP Gateway Application Maintenance

12 A00003277: SIP on Session Server OM Subsystem

13 A00003278: SIP on Session Server OSS Interface

14 A00003279: SIP on Session Server Link Maintenance and Load Balancing

15 A00003280: SIP on Session Server Tracing/Debug Framework

16 A00003281: SIP on Session Server Call Audits

17 A00003282: SIP on Session Server Datasync

18 A00004005: NCGL support for SAM-XTS and SP2000

119.17 Appendix A: Miscellaneous Items

This section contains miscellaneous topics for this FN.

119.17.1 ISUP Variant to SIP Version Mapping information

This sub-section lists the legal permutations and combinations for tuples that may be added to an ISUP Variant to SIP Version mapping.

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q764			ANSI88	<user defined string>
UCS			ANSI88	<user defined string>
UCP			ANSI88	<user defined string>
CCITT	100_BLUE	V1	ITU-T88	<user defined string>
	100_WHITE	V2	ITU-T92-PLUS	<user defined string>
CCITT250				<user defined string>
Q767	100_BLUE	BASE	ETSI121	<user defined string>
		SPANISH		<user defined string>
		ITALY		<user defined string>
		FRANCE		<user defined string>
		NORWAY		<user defined string>
		NEW_ZEALAND		<user defined string>
		DENMARK		<user defined string>
		PORTUGAL		<user defined string>
		MEXICO		<user defined string>
		TURKEY		<user defined string>
		BRAZIL		<user defined string>
		CZECH		<user defined string>
		BANGLADESH		<user defined string>

Table 13 ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
		BASE		<user defined string>
		PNG		<user defined string>
		CHILE		<user defined string>
		COSTA_RICA		<user defined string>
		GERMANY		<user defined string>
		TURKEY		<user defined string>
		SAUDI		<user defined string>
		ETHIOPIA		<user defined string>
		GEORGIA		<user defined string>
		MYANAMAR		<user defined string>
		VIETNAM		<user defined string>
		ISDEFO		<user defined string>
		ACIF_AUSTRALIA		<user defined string>
		BELGIUM		<user defined string>
		SWEDEN		<user defined string>
		JPN_INTERCONN		<user defined string>
Q767	100_WHITE	EGYPT	ETSI356	<user defined string>
		AUSTRIA		<user defined string>
		POLAND		<user defined string>
		HUNGARY		<user defined string>
		PERU		<user defined string>
		CA30_AUSTRALIA		<user defined string>
		HONG_KONG		<user defined string>
		TAIWAN		<user defined string>
		SPAIN		<user defined string>
		CHINA		<user defined string>
		SINGAPORE		<user defined string>
		ARGENTINA		<user defined string>
		BANGLADESH		<user defined string>
		RUSSIA		<user defined string>
		GISUP		<user defined string>
		TISUP		<user defined string>
		ITALY		<user defined string>

Table 13 ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_EIV3	FRANCE	ETSI356	<user defined string>
		SPIROU		<user defined string>
		UK		<user defined string>
AISUP	AUST			<user defined string>
	INTRCONN			<user defined string>
	PTUP			<user defined string>
	MISUP			<user defined string>
JPNISUP			TTC93-PLUS	<user defined string>
NCCI	V1			<user defined string>
	V2			<user defined string>

Table 13 ISUP Variant to SIP Version mappings

Note blank areas indicate “Not Applicable” values. When adding tuples via the web form that have no applicable values for the respective columns, select “Not Applicable” to represent the blank areas listed in the table.

119.18 Appendix B: SIP on NGSS Tracing/Debug Framework

SIP on NGSS Debug and Tracing (Feature A00003280) is a stand alone tool. It controls the Radvision SIPT Toolkit log module and filters the internal NGSS traces which are written into the tracing files.

This section is primarily targeted to Customer Support groups like GNPS. While the tool will be available in the field, it should not be done on a regular basis or at high traffic levels due to the impact of running the tracing session on the capacity of the field office.

This tool can run in two modes:

1. Simple Mode - straightforward usage tracing SIP messages
2. Prompt Mode - more sophisticated usage, needs a deeper knowledge regarding what to trace and how to used this tool.

119.18.1 Simple Mode

The following is an overview of a typical Simple Mode tracing session.

1. user needs a telnet session to the NGSS
2. start a Simple Mode by a command **/opt/apps/bin/sp2ktrace start**
3. stop a Simple Mode by a command **/opt/apps/bin/sp2ktrace stop**
4. tracing file is located in NGSS directory **/opt/apps/logs** with the name as siptrace.YYYYMMDD.MSG.001 (example **siptrace.20040318.MSG.00001**)
5. the siptrace file contains the SIP messages provided by Radvision Transport layer:

```
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -
T  88b63c8 03/19/2004 14:09:13 DEBUG  - TRANSPORT    - TransportCallbackMsgToSendEv:
    Application did not register to call back, default bSendMsg = 1
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportUdpSendMessage -
    Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportSendMessage -
    About to send message with size = 335
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - --> OPTIONS sip:1.2.3.4 SIP/2.0
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     From:
    <sip:MGCA>;tag=40c0a8c0-13c4-405afefd-49811d5-18457876
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     To: <sip:CCAONE@1.2.3.4>
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -    Call-ID: 8909008-40c0a8c0-
    13c4-405afefd-49811d5-16ba7f11@MGCA
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     CSeq: 30 OPTIONS
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Via: SIP/2.0/UDP
    192.168.192.64:5060;branch=z9hG4bK-405afefd-49811d5-218c6e77
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Max-Forwards: 70
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Supported: 100rel
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -     Content-Length: 0
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    -
T  88b63c8 03/19/2004 14:09:13 DEBUG  - TRANSPORT    - TransportCallbackMsgToSendEv:
    Application did not register to call back, default bSendMsg = 1
T  88b63c8 03/19/2004 14:09:13 INFO   - TRANSPORT    - SipTransportUdpSendMessage -
    Sending message. local-address=192.168.192.64:5060. remote-
    address=192.168.192.59:5060
```

6. for continuous tracings you can type command on NGSS:

> tail -f /opt/apps/logs/siptrace.20040318.MSG.00001

to get traces onto the screen.

119.18.2Prompt Mode

The following is an overview of a Prompt Mode tracing session.

1. user needs a telnet session to the NGSS
2. enter a Prompt Mode (command line interface) by a command **/opt/apps/bin/sp2ktrace** as example:

```
root@unit0 root]# /opt/apps/bin/sp2ktrace
```

3. type **help** to see which commands are available

```
SIPTRACE> help
These commands are provided:
  Help
  set (layer<1-19>  filter<0-63>)
  status
  start
  stop
  Users
  display <all | Session Server Name> - for IP address status
  Quit
-------------------------------------------------------------
Additional info for SET command:
  Layers and their corresponding numbers are shown by
  STATUS command.
  1 - all layers (ex. SET 1 2 sets all layers filter=INFO=2).
  There are 6 Filters as:
  DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32.
  Filters can be logically combined - if you want to trace for ex.
  layer PARSER (7) with filters ERROR (8) and EXCEP (16)
  SET 7 24
  For cleanup use filter 0 (example SET 7 0 for above).
  Use SET 1 63 (to set tracing for everything)
  use SET 1 0  (to cleaunp everything).
  Please be aware SET command only sets tracing.
  You must use START command to start tracing
  and use STOP command to end it.
Tracing files are in the directory /opt/apps/logs/.

SIPTRACE>
```

4. type **status** command to see all available Layers and Filters:

```
SIPTRACE> status

Active Users: 1         Radvision    L  o   g   F   i   l   t   e   r   s
[pid:15734]  active=OFF ----------------------------------------------------
        RV Layers       DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
=============================================================================
 1      all             -       -       -       -       -       -
 2      core            -       -       -       -       -       -
 3      msg             -       -       -       -       -       -
 4      transport       -       -       -       -       -       -
-----------------------------------------------------------------------------
 5      transaction     -       -       -       -       -       -
 6      call            -       -       -       -       -       -
 7      parser          -       -       -       -       -       -
 8      stack           -       -       -       -       -       -
-----------------------------------------------------------------------------
```

```
 9      msgBuilder      -       -       -       -       -       -
10      authenticator   -       -       -       -       -       -
11      regClient       -       -       -       -       -       -
12      subscription    -       -       -       -       -       -
++++++++++++++++++++++++ S P 2 K     L  o  g    F   i   l   t   e   r   s
13      callpAppMTC     -       -       -       -       -       -
14      GCP             -       -       -       -       -       -
15      other           -       -       -       -       -       -
16      sipmsg          -       -       -       -       -       -
17      gcpmsg          -       -       -       -       -       -
18      gcpmtcmsg       -       -       -       -       -       -
19      linkmtc         -       -       -       -       -       -
================================================================================
SIPTRACE>
```

5. type **set** command to set Layers/Filters selection (in this example you chose to trace a **transport** layer (4) for **filters** DEBUG (1), INFO (2) and ERROR (8) and the another layer msgBuilder (9) for ERROR (8) only. Thus type two command: **set 4 11** (4-transport, 11= 1+2+8) and **set 9 8**

```
Active Users: 2         Radvision    L  o   g   F   i   l   t   e   r   s
[pid:22958]  active=OFF ------------------------------------------------------
        RV Layers       DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
================================================================================
 1      all             -       -       -       -       -       -
 2      core            -       -       -       -       -       -
 3      msg             -       -       -       -       -       -
 4      transport       x       x       -       x       -       -
--------------------------------------------------------------------------------
 5      transaction     -       -       -       -       -       -
 6      call            -       -       -       -       -       -
 7      parser          -       -       -       -       -       -
 8      stack           -       -       -       -       -       -
--------------------------------------------------------------------------------
 9      msgBuilder      -       -       -       x       -       -
10      authenticator   -       -       -       -       -       -
11      regClient       -       -       -       -       -       -
12      subscription    -       -       -       -       -       -
++++++++++++++++++++++++ S P 2 K     L  o  g    F   i   l   t   e   r   s
13      callpAppMTC     -       -       -       -       -       -
14      GCP             -       -       -       -       -       -
15      other           -       -       -       -       -       -
16      sipmsg          -       -       -       -       -       -
17      gcpmsg          -       -       -       -       -       -
18      gcpmtcmsg       -       -       -       -       -       -
19      linkmtc         -       -       -       -       -       -
================================================================================
SIPTRACE>
```

Note: Please note “x” at the transport and msgBuilder Layer.

6. start the tracing by a **start** command

```
SIPTRACE> users

                                    R   a   d   v   i   s   i   o   n    S  P  2  K
                          Layers:  1  2  3  4  5  6  7  8  9  10 11 12   13  14  15
    16     17     18        19
                                   al co ms tp tr ca pa st mB au rC su   MTC GCP
    oth SIPMSG GCPMSG GCPMTCMSG LINKMTC
User                pid     active
--------------------------------------------------------------------------------
    -----------------------------------
server              15704   1       0  0  0  31 0  0  0  0  0  0  0  0    0   0   0
    0      0      0         0
mtc                 16802   0       0  0  0  0  0  0  0  0  0  0  0  0    0   0   0
    0      0      0         0
MSG                 00001   1       0  0  0  31 0  0  0  0  0  0  0  0    0   0   0
    0      0      0         0
SIPTRACE>
SIPTRACE> stop
```

In the example above you can see three users. A server is a permanent thread with a pid (processID=15704), your session with a userID mtc and pid 16802 and one Simple Mode with userID MSG and hardcoded pid 00001. The “00001”s behind a pid column belong to the active column indicating that this session is active - it means it is collects data.

7. the siptrace file for the above tracing session (pid 22958) is located in NGSS directory /oipt/apps/logs/siptrace.20040319.mtc.22958 with few first lines as:

```
=== SESSION ENTERED: [pid:22958/mtc]  Fri Mar 19 14:17:19 2004
=== MONITOR UPDATED: [pid:22958/mtc]  Fri Mar 19 14:38:53 2004
  Filters: 0  0  0  11 0  0  0  0  0  0  0  0 ::0  0  0  0  0
=== MONITOR UPDATED: [pid:22958/mtc]  Fri Mar 19 14:38:59 2004
  Filters: 0  0  0  11 0  0  0  0  8  0  0  0 ::0  0  0  0  0
=== MONITOR STARTED: [pid:22958/mtc]  Fri Mar 19 14:42:27 2004
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
    TransportMultiThreadTimerEventHandler - Allocating timer expired event for timer
    0x88dafe4
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
    TransportProcessingQueueTailEvent - TIMER_EXPIRED_EVENT 0x8906a20
T  88b63c8 03/19/2004 14:42:28 DEBUG  - TRANSPORT    -
    TransportProcessingQueueDispatchEvents - TIMER_EXPIRED_EVENT 0x8906a20
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - SipTransportUdpSendMessage -
    Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - SipTransportSendMessage -
    About to send message with size = 335
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    - --> OPTIONS sip:1.2.3.4 SIP/2.0
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     From:
    <sip:MGCA>;tag=40c0a8c0-13c4-405b06b8-4b643e6-4fdb17be
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     To: <sip:CCAONE@1.2.3.4>
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -    Call-ID: 890bb28-40c0a8c0-
    13c4-405b06b8-4b643e6-69016e79@MGCA
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     CSeq: 30 OPTIONS
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Via: SIP/2.0/UDP
    192.168.192.64:5060;branch=z9hG4bK-405b06b8-4b643e6-5c79301f
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Max-Forwards: 70
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Supported: 100rel
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -     Content-Length: 0
T  88b63c8 03/19/2004 14:42:28 INFO   - TRANSPORT    -
```

8. stop the session by the **stop** command.
9. exit session by a **quit** command.

119.19 Hardware Requirements or Dependencies

Customer offices without the Session Server Manager will not have the functionality delivered by this feature.

119.20 Software Requirements or Dependencies

The Session Server Manager feature must be available. Also, certain other features developed for the Session Server Manager will be required (Call Processing support, etc.) as well.

119.21 Limitations and restrictions

This tool has the following limitations:

1. Tool is currently configured for 10 concurrent Trace Clients. The Simple Mode is counted as a Client.
2. The user of this tool needs access (a telnet session) to the NGSS machine.
3. Only one Client can run in the Simple Mode at a time.
4. Every Trace Client gets its own output trace file which is being used until the Trace Client session ends (by **quit** command in the Prompt Mode or ***sp2ktrace stop*** in the Simple Mode). For example, if a user starts a session on Monday and runs it over 3 days, there will be only one Trace Client file with a creation date i.e. Monday date.
5. The Trace Server trace file. In contrast of the Trace Client trace file, the Trace Server trace file is created on every day. (to give a chance to get rid of old/yesterday's files). The trace file creation is not done few seconds after midnight but by the first execution (after midnight) of the print routine (which can be few hours from the midnight) depending on monitoring activities/setup.
6. If the size of any output file (siptrace) created by this tool (in the directory /opt/apps/logs) exceeds limit of 10 MBytes then this file will be over written from the beginning. This event is recorded together with the overwritten counter.
7. All siptrace* files in the directory /opt/apps/logs/ older than 3 days will be deleted automatically by the tracing tool.
8. Other files in the directory /opt/apps/logs need to be deleted manually. ***Note:*** The file created by monitoring in the Simple Mode is appended every time tracing starts (by a command ***siptrace start***) on the same date.
9. **WARNING**: Do not delete active/current (today) server files. Prevent the deletion of active Trace Client's files. Deleted files will not be re-created.
10. This tool provides tracing for multiple threads, which may attempt to write to the same tracing file concurrently. Non-waiting semaphores are used to prevent concurrent access into the client file. This may result in a "lost" trace record rather than to block a thread waiting on the semaphore.
11. **Configuration:** The configuration file sp2ktraceConfig is created when tool runs for very first time in the directory /opt/apps/logs. This file has currently two (default) parameters:

- NUMBEROFINITLOGS 300
- CLIENTFILESIZEMB 10

The first parameter configures the number of logs to be printed into the server siptrace file during the initialization (when SIP Gateway is Unsuspended). The default value is 300 logs but can be increased up to the maximum of 25000.

The second parameter allows to increase the size of the client siptrace file from the default value 10 Mbytes up to the maximum of 500 Mbytes.

These parameter must be changed prior the SIP Gateway is Unsuspended to be used.

119.22 References

- A00003698 - SIP Msg trace

119.23 Appendix C: Database Backup and Recovery

This section explains how database backups are made and how to recover the database from a backup copy.

119.23.1 Database Backup

Database backups are made to secure the information stored in the database. If there is a system or database failure the database can be restored from the backup files. The Solid database is automatically backed up daily based on a timed command. The automatic backup is performed at 1:00 AM each day.

There is only one backup copy of the database. It contains the last or most recently backed up copy of the database. If additional security measures are desired the customer may periodically retrieve the files saved in the backup directory and store them on another machine. A customer could maintain a history of database changes in this manner.

119.23.2 Restoring database from a backup copy

The following procedure is used to restore the database from the backup copy. The database is restored to its state when the backup was made. In general this procedure should only be followed when database corruption has occurred on both units of the NGSS. The database must be restored on the active unit of the NGSS.

1. Jam the Active Unit.
2. Suspend Call Processing
3. Login in to the active unit as mtc and su to root.

   ssh -l mtc <ipaddress>

   su root
4. Run the restorebackup script as shown from the following directory:

   cd /opt/apps/database/solid_install/

   ./restorebackup.sh
5. Unsuspend Call Processing
6. UnJam the Active Unit

Jamming the active unit is necessary to prevent the database from switching activity while its being restored. The database must be restored on the active unit. Call processing should be suspended since the database will not be available.

119.24 Appendix D: CSV file information

This section details the CSV file formats, its location, and shows examples.

119.24.1 CSV File Location

SSH Login Access

If the user desires to login to a session server unit via an account such as MTC and look at the CSV files, the main directory path is /opt/apps/ngsspm. Two subdirectories are located here:

stdhist - This directory contains the 24 hour long term values.

trafhist - This directory contains the 30 minute short term values.

FTP Access

This future section will contain the access information when FTP is utilized using the NGSSPM account to pull CSV files from a session server unit.

119.24.2 CSV File Format

The CSV File Format is shown below:

```
PMFile=Begin
MeasurementCategory,FileCreationTime,EarliestStartTime,LatestCaptureTime,RegisterTypeDefault,ValueTypeDefault
<string="pm">,<string>,<string>,<string>,<string="counter">,<string="integer">
System=Begin
SystemId
<string="SessionServer">
Entity=Begin
Entity
<string= Unit IPAddress>
SubEntity=Begin
SubEntity
<string=["Unit0" | "Unit1"]>
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
<string="PeriodBased">,<string>,<string>,<integer>,<string="Valid">
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg9Name,Reg9Value,Reg10Name,Reg10Value,Reg11Name,Reg11Value,Reg12Name,Reg12Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg13Name,Reg13Value,Reg14Name,Reg14Value,Reg15Name,Reg15Value,Reg16Name,Reg16Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg17Name,Reg17Value,Reg18Name,Reg18Value,Reg19Name,Reg19Value,Reg20Name,Reg20Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg21Name,Reg21Value,Reg22Name,Reg22Value,Reg23Name,Reg23Value,Reg24Name,Reg24Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg25Name,Reg25Value,Reg26Name,Reg26Value,Reg27Name,Reg27Value,Reg28Name,Reg28Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg29Name,Reg29Value,Reg30Name,Reg30Value,Reg31Name,Reg31Value,Reg32Name,Reg32Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
<string="PeriodBased">,<string>,<string>,<integer>,<string="Valid">
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg5Name,Reg5Value,Reg6Name,Reg6Value
<string>,<integer>,<string>,<integer>
GroupVals=End
SubEntity=End
Entity=End
System=End
PMFile=End
```

Note the above example format consists of two groups. The first with 32 registers and the second with six registers.

119.24.3 Examples

An example CSV file is shown below:

```
# more NGSS.OMs.QoS.2004.5.5_10.15_EDT.csv
PMFile=Begin
MeasurementCategory,FileCreationTime,EarliestStartTime,LatestCaptureTime,RegisterTypeDefault,ValueTypeDefault
pm,NGSS.OMs.QoS.2004.5.5_10.15_EDT.csv,unknown,unknown,counter,integer
System=Begin
SystemId
SessionServer
Entity=Begin
Entity
47.142.123.46
SubEntity=Begin
SubEntity
Unit0
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_CALLP,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
IC_CALL_ATTEMPTS,0,OG_CALL_ATTEMPTS,0,CALLS_ABANDONED,0,CALLS_ANSWERED,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value
CALLS_REJECTED,0,CALLS_REDIRECTED,0
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_SERVICES,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
REFER_ATTEMPTS,0,REFER_SUCCESS,0,IC_DTMF_SUBSCRIBES,0,OG_DTMF_SUBSCRIBES,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
IC_DTMF_NOTIFYS,0,OG_DTMF_NOTIFYS,0,IC_FAX_SUBSCRIBES,0,OG_FAX_SUBSCRIBES,0
Reg9Name,Reg9Value,Reg10Name,Reg10Value
IC_FAX_NOTIFYS,0,OG_FAX_NOTIFYS,0
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_MISC,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
TCP_CALLS,0,UDP_CALLS,0,SIP_MSG_SEND_FAILURES,0,SIMULTANEOUS_CALLS,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
UDP_CALLS_HIGHWATERMARK,0,TCP_CALLS_HIGHWATERMARK,0,SIMULTANEOUS_CALLS_HIGHWATERMARK,0,INCOMING_SDP_IN
COMPATIBLE,0
Reg9Name,Reg9Value
OUTGOING_SDP_INCOMPATIBLE,0
GroupVals=End
SubEntity=End
Entity=End
System=End
PMFile=End
```

119.25 Appendix E: Session Server Manager MR Procedure

This procedure details how to perform a software upgrade for a Session Server Manager, Maintenance Release (MR). The MR will consist of release notes, NCGL Platform Manager software, Session Server Manager SIP application software and NCGL Platform Manager patches. The software will be delivered via DVD or via Electronic Software Delivery (ESD) which will be a compressed ISO image that will be delivered to a customer's electronic drop-box. This procedure also details how to back-out of a partially completed MR.

Note: It is important that the individuals performing the MR upgrade record their actions and the CLI sessions to log files.

119.25.1Prerequisites

- Check release notes to see if you can directly upgrade your system to this MR or if you need to first upgrade to a previously released MR. Release notes will be provided on the DVD or with the ESD MR image.
- Obtain physical DVD with MR software or have a copy of the ESD MR image.
- Upgrades NTP, NN10349-461
- A backup copy of the existing SIP application installed on your system needs to be either on DVD or the ISO image needs to be stored locally in the /opt/swd directory.

119.25.2Procedure

119.25.2.1 Perform System Backups

119.25.2.1.1 Backup database

Backup and archive the database before starting the MR and transfer the database file to a secure location of the customer's choosing.

Note: Since the SIP application upgrade procedure overwrites the database files stored in directory /opt/apps/database/solid/, the database backup will be required in the event that you need to downgrade the MR software to the previous load.

To backup the database from the active unit, use a secure file transfer program like scp. The database files that need to be retrieved from Session Sever Manager are in: /opt/apps/database/solid/dbfiles/. The files are solid.db, solid.ini and solmsg.out.

119.25.2.1.2 Backup Security Certificates

If the customer has purchased security certificates from a Certificate Authority then ensure that the customer has a backup of the security certificates files:

server.key, server.crt and certificate.keystore located in directory /opt/base/share/ssl. If not, then transfer a copy of the files to a secure location of the customer's choosing. For more information on Session Sever Manager security certificates see the Session Server and Administration NTP NN10346-611.

119.25.2.2 MR Software upgrade via DVD:

Before beginning the upgrade, check the release notes.

Check Release notes:

- Log into the command line interface on the inactive unit via ssh
- Set the user to **root**
- **su –l** <Enter>
- password <Enter>
- Insert the DVD into the inactive unit
- **mount /cdro**m <Enter>
- **cd /cdrom** <Enter>
- Find and review the release notes
- **ls**
- **Read release notes**
- **cd /** <Enter>
- **umount /cdrom** <Enter>

Step 1 Upgrading NCGL Platform Load

- Check the current version of NCGL software running on the inactive unit by looking at the Current Version indicated in the Platform System Information panel.
- Compare the current version of the “NCGL Platform Load” with the MR Release Notes to see if you need to upgrade the NCGL platform load.
- If the MR contains a newer version of the NCGL platform load then proceed with the NCGL platform upgrade. If not then jump to Step 2 **Applying NCGL Patches**.
- Insert the DVD with the MR software into the inactive Unit.
- Log into the Active Session Server Manager unit via WEB EM and “JAM” the Inactive unit.
  - — From the Session Server Manager launchpoint web page go to Succession Communication 2000 NCGL Platform Manager -> Node Maintenance. In the Maintenance panel click the JAM button on the active unit.

- Log into the NCGL Platform Manager for the Inactive Session Server Manager unit and go to the NCGL Administration page and upgrade the NCGL software.
  - From the Session Server Manager launchpoint web page go to Succession Communication 2000 NCGL Platform Manager -> Administration
  - On the Software Upgrade panel under Protocol select “Local CD ROM”
  - Under the Action heading select the Upgrade button.
  - Once the new NCGL load has been successfully copied to the unit the load name will be display in the Bootload Management panel.
  - Set the new NCGL load to be the default by clicking on the “Set Default” button for the new NCGL load in the Bootload Management panel
- Remove the DVD from the CDROM drive.
- Log into the Active Session Server Manager unit and go to the NCGL Administration web page and select the “RebootMate” button to reboot the Inactive Unit.
- After the reboot completes, log into the Inactive Unit and go to the System Information Web Panel. Verify that the Current Version indicated matches the expected new version of NCGL software.

Step 2 Applying NCGL Patches

- Review MR release notes and identify the required NCGL patches for the load.
- Jam Inactive unit if not already Jammed.
- Copy all required patches from the MR DVD into the /patching/patchholding directory.
  - Log into the command line interface on the inactive unit via ssh
  - Set the user to **root**
  - **su –l** <Enter>
  - password <Enter>
  - Insert the DVD into the inactive unit
  - **mount /cdrom** <Enter>
  - **cd /cdrom** <Enter>
  - Find and identify the patches
  - **ls**
  - Copy patches to /patching/patchholding
  - **cp patchfile /patching/patchholding** <Enter>
  - **cd /** <Enter>

— **umount /cdrom** <Enter>

- Apply and commit the required NCGL patches to the inactive unit. Consult the Upgrades NTP, NN10349-461, for details on NCGL patching procedures.

Step 3 Installing Session Server Manager Software

- Jam Inactive unit if not already Jammed.
- Log into the command line interface on the inactive unit via ssh
- Set the user to **root**
- **su –l** <Enter>
- password <Enter>
- Insert the DVD into the inactive unit
- **mount /cdrom** <Enter>
- **cd /cdrom** <Enter>
- **./InstallApps** <Enter>
- `The NGSS Application layer is currently installed.`
- `Do you wish to uninstall the previous application and install the newer version? (yes, no)`
- **yes** <Enter>

The system will now begin installing the actual Session Server Manager applications. You will see a lot of messages scrolling across the screen. Once they have completed scrolling the process is complete and you can remove the DVD from the CDROM.

To remove the DVD type the following:

- **cd /** <Enter>
- **umount /cdrom** <Enter>
- Remove the DVD from the CDROM drive.
- Login to the Active Session Server Manager unit and reboot the inactive unit by selecting the Rebootmate button from the Administration Web page.
- After the reboot has completed, login to the Session Server Manager for the Inactive unit. Select Version Info and verify that it is updated to correct values for the MR.

Step 4 Activate and soak New Load

- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units by performing a QueryInfo from the SIP Gateway Application.
- Unjam the inactive side.

- Places test calls and soak the new load on the inactive side for a period of time specified by the customer.
- Check logs and alarms on the inactive unit.
- Switch activity to make the upgraded Session Server Manager unit active by performing a SWACT.
- Jam newly inactive unit.
- Execute test calls on the new load.
- Check logs and alarms for the active Session Server Manager unit
  Note: There will be an alarm for the jam.
- Monitor system for appropriate period.
- On successful completion of test calls and live traffic soak proceed to step 5 **Complete Duplex Upgrade of Session Server Manager**. If unsuccessful proceed to step 6 **Abort Maintenance Release Upgrade**.

Step 5 Complete Duplex Upgrade of Session Server Manager

- Ensure unit with pre-MR load is JAMMED.
- Repeat Step 1 **Upgrading NCGL Platform Loa**d
- Repeat step 2 **Applying NCGL Patches**
- Repeat step 3 **Installing Session Server Manager Software**
- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units.
- Unjam the inactive side.
- Switch activity to make the upgraded Session Server Manager unit active by performing a SWACT.
- Execute test calls on the new load.
- Check logs and alarms for both Session Server Manager units.
- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units by performing a QueryInfo from the SIP Gateway Application.
- Monitor system for appropriate period.
- MR Upgrade Procedure is now complete.

Step 6 Abort Maintenance Release Upgrade

- Unjam Inactive unit.
- Switch activity of the Session Server Manager to the unit that has the pre-maintenance release load.

Note: There is a risk that some or all of the existing calls will be lost when the SWACT is performed.

- Jam inactive unit.
- Logon to inactive Session Server Manager unit and from the NCGL platform manager, Administration page, set the default NCGL bootfile to the pre-MR load and Reboot the inactive unit.

  Note: All committed NCGL patches are re-applied by the system when the unit is rebooted.
- Using the pre-MR SIP application DVD perform installation of the software as per Step 3 **Installing Session Server Manager Software.**
- Reboot inactive unit.
- Check to ensure the SIP application is synchronized between both units. If in sync, release the JAM on the inactive unit.
- Switch activity to make the downgraded unit active.
- Execute test calls on the newly active unit.
- Check logs and alarms for both Session Server Manager units.
- Monitor system for appropriate period.
- If the system is unstable, switch activity and Jam Inactive unit. Contact Session Server Manager GNPS for assistance.

119.25.2.3 MR Software upgrade via Electronic Software Delivery

To perform a MR upgrade using the ESD method, the MR package needs to be transferred onto both Session Server Manager units into the /opt/swd directory using a secure file transfer program like scp.

Note: The /opt/swd directory has a size of 1GB and can contain no more than two SIP Gateway loads at once. You may need to remove old ISO images before transferring the latest MR onto the unit. Make sure that you do not delete the ISO image that is currently running on the system, since you will need it in the event that you need to abort the MR upgrade.

Before starting the upgrade backup the database and security certificate.

119.25.2.4 Prepare the ISO Image and Check Release Notes

Prior to beginning this procedure, check the release notes:

- Log into the command line interface on the inactive unit via ssh
- Set the user to **root**
- **su –l** <Enter>

- password <Enter>
- **cd /opt/swd** <Enter>
- Unzip and untar the ISO image.
- **gunzip <ESD_ISO_Image.tar.gz>** <Enter>
  For example: gunzip NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar.gz
- **ls** <Enter>
- **tar –xvf <ESD_ISO_Image.tar>** <Enter>
  For example: tar –xvf NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar
- Verify that tar is successful (you should see a new directory called NGSS0070.70.P.NCL.NAP.VAULT.6.D and it should contain ISO.tape file)
- **rm <ESD_ISO_Image.tar>** <Enter>
  ie. rm NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar
- **cd <ESD_ISO_directory>** <Enter>
  For example: cd NGSS0070.70.P.NCL.NAP.VAULT.6.D
- **ls** <Enter>
- **Read release notes** which are provided with the load in the ESD_ISO_directory.

Step 1 Upgrading NCGL Platform Load

- Check the current version of NCGL software running on the inactive unit by looking at the Current Version indicated in the Platform System Information panel.
- Compare the current version of the “NCGL Platform Load” with the MR Release Notes to see if you need to upgrade the NCGL platform load.
- If the MR contains a newer version of the NCGL platform load then proceed with the NCGL platform upgrade. If not then jump to Step 2 **Applying NCGL Patches**.
- Log into the Active Session Server Manager unit via WEB EM and “JAM” the Inactive unit.
  - — From the Session Server Manager launchpoint web page go to Succession Communication 2000 NCGL Platform Manager -> Node Maintenance, in the Maintenance panel click the JAM button on the active unit.
- Log into the NCGL Platform Manager for the Inactive Session Server Manager unit and go to the NCGL Administration page and upgrade the NCGL software.
  - — From the Session Server Manager launchpoint web page go to the Succession Communication 2000 NCGL Platform Manager -> Administration

— On the Software Upgrade panel under Protocol select “Local File”

— Under the **File** panel enter the location of the bootload image file, (e.g **/opt/swd/<ESD_ISO_directory>/<ESD_ISO_Image>** /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO.tape).

— Under the Action heading select the Upgrade button.

— Once the new NCGL load has been successfully copied to the unit, the load name will be display in the Bootload Management panel.

— Set the new NCGL load to be the default by clicking on the “Set Default” button for the new NCGL load in the Bootload Management panel.

- Log into the Active Session Server Manager unit and go to the NCGL Administration web page and select the “RebootMate” button to reboot the Inactive Unit.
- After the reboot completes, log into the Inactive Unit and go to the System Information Web Panel. Verify that the Current Version indicated matches the expected new version of NCGL software.

Step 2 Applying NCGL Patches

- Review MR release notes and identify the required NCGL patches for the load.
- Jam Inactive unit if not already Jammed.
- Copy all required patches from directory**/opt/swd/<ESD_ISO_directory** >/ into the **/patching/patchholding** directory.
- Apply and commit the required NCGL patches to the inactive unit. Consult the Upgrades NTP, NN10349-461, for details on NCGL patching procedures.

Step 3 Installing Session Server Manager Software

- Jam Inactive unit if not already Jammed.
- Log into the command line interface on the inactive unit via ssh and switch to be root user.
- **su –l** <Enter>
- password <Enter>
- Verify that the /cdrom device is not currently mounted by typing: umount /cdrom
- Mount the ISO image that was transferred electronically to the /cdrom device: **mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_ISO_Image> /cdrom** <Enter>
  For example: mount –o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO.tape /cdrom
- **cd /cdrom** <Enter>
- **./InstallApps** <Enter>

- `The NGSS Application layer is currently installed.`
- `Do you wish to uninstall the previous application and install the newer version? (yes, no)`
- **yes** <Enter>

The system will now begin installing the actual Session Server Manager applications. You will see a lot of messages scrolling across the screen. Once they have completed scrolling then the process is complete and you will need to type the following:

- **cd /** <Enter>
- **umount –f /opt/swd/<ESD_ISO_directory>/<ESD_ISO_Image>** <Enter>
  For example: umount –f /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO.tape
- Login to the Active Session Server Manager unit and perform a Rebootmate from the Administration Web page.
- After the reboot has completed, login to the Session Server Manager for the Inactive unit. Select Version Info and verify that it is updated to correct values for the MR.

Step 4 Activate and soak New Load

- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units by performing a QueryInfo from the SIP Gateway Application.
- Unjam the inactive side.
- Place test calls and soak the new load on the inactive side for a period of time specified by the customer.
- Check logs and alarms on the inactive unit.
- Switch activity to make the upgraded Session Server Manager unit active by performing a SWACT.
- Jam newly inactive unit.
- Execute test calls on the new load.
- Check logs and alarms for the active Session Server Manager unit (Note there will be an alarm for the jam).
- Monitor system for appropriate period.
- On successful completion of test calls and live traffic soak proceed to step 5 **Complete Duplex Upgrade of Session Server Manager**. If unsuccessful proceed to step 6 **Abort Maintenance Release Upgrade.**

Step 5 Complete Duplex Upgrade of Session Server Manager

- Ensure unit with pre-MR load is JAMMED.
- Repeat Step 1 **Upgrading NCGL Platform Load**
- Repeat step 2 **Applying NCGL Patches**
- Repeat step 3 **Installing Session Server Manager Software**
- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units.
- Unjam the inactive side.
- Switch activity to make the upgraded Session Server Manager unit active by performing a SWACT.
- Execute test calls on the new load.
- Check logs and alarms for both Session Server Manager unit.
- Verify that the Session Server Manager application has achieved synchronization between both Session Server Manager units by performing a QueryInfo from the SIP Gateway Application.
- Monitor system for appropriate period.
- MR Upgrade Procedure is now complete.

Step 6 Abort Maintenance Release Upgrade

- Unjam Inactive unit.
- Switch activity of the Session Server Manager to the unit that has the pre-maintenance release load.

  Note: There is a risk that some of the existing call will be lost when the SWACT is performed.

- Jam inactive unit.
- Logon to inactive Session Server Manager unit and from the NCGL platform manager, Administration page, set the default NCGL bootfile to the pre-MR load and reboot the inactive unit

  Note: All committed NCGL patches are re-applied by the system when the unit is rebooted.

- Using the pre-MR SIP application ISO image **<ESD_ISO_Image>,** perform installation of the software as per Step 3 **Installing Session Server Manager Software.**
- Reboot inactive unit
- After reboot, check to ensure the SIP application is synchronized between both units. If in sync, release the JAM on the inactive unit.
- Switch active to make the downgraded unit active.

- Execute test calls on the newly active unit.
- Check logs and alarms for both Session Server Manager units
- Monitor system for appropriate period.
- If the system is unstable, switch activity and Jam Inactive unit. Contact Session Server Manager GNPS for assistance.

120: Functional Description (FN): A00003947

120.1 Feature name

Trimodal LOGs and Operational Measurements (OM)

120.2 Description

Beginning in the SN07 release, work is being started to implement a Trimodal Call Server, which will allow TDM agents and multiple packet fabric agents to interwork. In SN07, the packet fabrics that interwork will be limited to IP and ATM (AAL1, AAL2 and AAL5), and the TDM fabric is limited to ENET.

This activity addresses the OMs, Logs, Traver and Translations components of the trimodal call server. This actvity address the following

- New office parameter MULTINET_DISPLAY_ACTIVE
- OM Enhancements
  - New OM group IWBMNODE
  - New OM group TRK2NET1
  - New OM group TRK2NET2
  - New OM group OFZ2NET1
  - New OM group OFZ2NET2
  - New OM group DPTOFCP
  - Enhance DPTNODE
- Log Enhancements
  - IWBM 800 series log enhancements to display the bridge pool
  - new XNET600 series logs for external patcket bearer network connectivity problems
- Translations Enhancements
  - Conditional PKT selector renamed to “FABRIC” and enhanced to support ATM and IP fabrics.

— New BEARNET conditional selector to support criteria checking based on network name.

- Traver enhancements
  - — New Traver option BEARNET to input the network name of the incoming trunk agent to support FABRIC and BEARNET conditional selector routing
  - — Traver TRKMEM option is enhanced to derive the originating trunk bearer network/fabric. The bearer network/fabric is used to support FABRIC and BEARNET conditional selector routing

120.2.1 Office Parameter MULTINET_DISPLAY_ACTIVE

New office parameter MULTINET_DISPLAY_ACTIVE is introduced in CM with an default value of “NO”. The MULTINET_DISPLAY_ACTIVE paramter provides the following functionality

- Control the creation of new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2, DPTOFCP
- Control the display of OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2, DPTOFCP and DPTNODE
- Control the display of bridge pool information in IWBM 800 series logs

The datafilling procedure in TABLE OFCVAR is explained below:

- In response to PARMNAME prompt, type “MULTINET_DISPLAY_ACTIVE”
- In response to PARMVAL prompt, type either YES or NO to indicate the MULTINET display preference.

Please refer to “Table 1 Sample Datafill in table OFCVAR” on page 1454. for sample datafill of MULTINET_DISPLAY_ACTIVE parameter.

Table 1 Sample Datafill in table OFCVAR

PARMNAME	PARMVALUE
MULTINET_DISPLAY_ACTIVE	YES
MULTINET_DISPLAY_ACTIVE	NO

120.2.1.1 Behavior when the parameter is set to ‘YES’

- First time change from ‘NO’ to ‘YES’ using table control or using Table transfer.
  - — The new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are created.
  - — The tuples in the new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are displayed.

- — Pegging of the OM group registers in IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
- — The signaling type for the DPT node tuple in the DPTNODE OM group is displayed.
- — The display of bridge pool in IWBM 800 series of LOGS is enabled.

• Second time change from ‘NO’ to ‘YES’ using table control

- — The tuples in the new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are displayed.
- — Pegging of the OM group registers in IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
- — The signaling type for the DPT node tuple in the DPTNODE OM group would be displayed.
- — The display of bridge pool in IWBM 800 series of LOGS is enabled.

120.2.1.2 Behavior when the parameter is set to ‘NO’

• Change from ‘YES’ to ‘NO’ using table control

- — A warning message would be displayed “All OM and LOGs data pertaining to Trimodal call server will be lost.”.
- — The tuples in the new OM groups would not be displayed.
- — The signaling type for the DPT node tuple in the DPTNODE OM group would not be displayed.
- — All the counters for the registers of the new OM groups would be set to zero.
- — The counters of the registers of the new OM groups would not be pegged.
- — The display of bridge pool in IWBM 800 series of LOGS would be disabled.
- — The OMSHOW command would display the OM groupsIWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

120.2.2 OM Enhancements

120.2.2.1 New OM group IWBMNODE

120.2.2.2 New OM group TRK2NET1

120.2.2.3 New OM group TRK2NET2

120.2.2.4 New OM group OFZ2NET1

120.2.2.5 New OM group OFZ2NET2

120.2.2.6 New OM group DPTOFCP

120.2.2.7 Enhance OM group DPTNODE

120.2.3 Log Enhancements

120.2.3.1 IWBM 800 Series Enhancements

The IWBM 800 series logs provide information about usage/thresholds for the IW bridge pool. Prior to SN07, there was only 1 pool of bridges available. Trimodal Call Server would introduce support for multiple bridge pools, so these logs need to be generated for each pool allocated in the office (based upon Table NETBRDGE). IWBM 800, 801, 802, 803 logs is enhanced to show the information about the bridge pool.

The bridge pool info is displayed only when the OFCVAR patameter MULTINET_DISPLAY_ACTIVE is set to YES.

Figure 1 Enhanced IWBM 800 Log with MULTINET_DISPLAY_ACTIVE = YES

```
RTP7  **  IWBM800 SEP17  12:16:55  6600  1st Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 70 percent of all bridges in the pool.
           Total number of IW bridges:  2016
           Number of available IW bridges:   25
           Bridge Pool:  ENET_to_ATM
```

120.2.3.2 XNET 600 Series logs

The XNET 600 series logs provide information on external packet network bearer connection problems. Three new logs are created:

- XNET605 - Bearer Networks Cannot Connect

  This log indicates that the bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET.

The telco should determine whether the identified bearer networks are permitted to interconnect. If so, the appropriate datafill should be added to tables NET2NET, and if necessary NETPATH and NETBRDGE. If the bearer networks are not permitted to connect, the telco can:

a. if possible, change DN translations so that the originator can no longer dial the terminator, but will receive a treatment of some type,

b. use the EXTLOGCI command to disable the XNET605 log (see section 120.2.3.3)

c. use LOGUTIL to SUPPRESS the XNET 605 log

d. do nothing, the log will continue to print when two parties on the specified bearer networks attempt to dial one another.

Figure 2 XNET605 Log Example

```
RTP7   XNET605  MAY17  12:16:55  9600 INFO Bearer Networks Cannot Connect
       From Agent              : VOIP 42 2 04 00      DN 6137204200
       From Bearer Network:  IP_PRIMARY
       To     Bearer Network: AAL1_SECONDARY
       Bearer Network Translations resulted in no interconnect
       Check Table NET2NET, NETPATH and NETBRDGE
```

The ‘From Agent’ line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,
- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined
- or an “Unavailable” indication when the conection source was an ENET hosted party, but that party can no longer be determined.

The ‘From Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the source party . The ‘To Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

- XNET606 - PKT Pathend Has NIL Bearer Net ID

This log indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt.

The telco should report this log to appropriate Nortel Product Support.

The telco can:

- use the EXTLOGCI command to disable the XNET606 log (see section 120.2.3.3)
- use LOGUTIL to SUPPRESS the XNET 605 log
- do nothing, the log will continue to print when the suspect party attempts to place calls

Figure 3 XNET 606 Log Example

```
RTP7   XNET606  MAY17  12:16:55  9600 INFO PKT Pathend Has NIL Bearer Net ID
       Path   - Node: LGRP   07   Tid:  124
       Agent - VOIP 42 2 04 00     DN 6137204200
       Contact Product Support
```

The ‘Path’ line indicates the node at the network connection point, this can be in two forms:

- a PM name and number, and a channel or TID id,
- a node number, and a channel or TID id, when the PM name and number cannot be determined from the node number

The ‘Agent’ line identifies the suspect party, this can be in several forms:

- a LEN and DN,
- a Trunk Group name and member number
- or a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined

- XNET607 - IW Bridge Not Available

  This log indicates that an IW SPM interworking bridge was not available for the connection request, either because

  - of a bridge exhaust condition on one of the bridge pools involved in the connection request,
  - bridges are not inservice, or provisioned for one of the bridge pools involved with the connection request

  The telco can:

  - check for IWBM602 logs indicating a bridge exhaust condition,
  - verify that the bridge pool identified in the log is provisioned on an SPM in table MNNODE,
  - verify that the bridges in the bridge pool identified in the log are in-service.
  - use the EXTLOGCI command to disable the XNET607 log (see section 120.2.3.3)
  - use LOGUTIL to SUPPRESS the XNET 607 log

Figure 4 XNET 607 Log Example

```
RTP7    XNET607  MAY17  12:16:55  9600 INFO IW Bridge Not Available
        Bridge Pool       : ENET_TO_IP
        From Agent        : VOIP 42 2 04 00      DN 6137204200
        From Bearer Network:  IP_PRIMARY
        To      Bearer Network: AAL1_SECONDARY
```

The ‘Bridge Pool’ line indicates the name of the bridge pool, as specified in table NETBRDGE, that has the ‘trouble’ condition. The ‘From Agent’ line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,
- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined
- or an “Unavailable” indication when the conection source was an ENET hosted party, but that party can no longer be determined.

The ‘From Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the source party. The ‘To Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

120.2.3.3 EXTLOGCI Tool

The EXTLOGCI tool is an existing CI command that controls the XNET series of logs. By using the ENABLE and DISABLE commands, the user can control the production of XNET logs. The XNET 605, 606 and 607 logs are automatically enabled on all restarts.

120.2.4 Translations Enhancements

120.2.4.1 Conditional PKT Selector Enhancements

The CND selector CND_PKTSEL_TYPE was created in SN06 to support Trunk selection based on the incoming Agent Bearer Fabric type ENET or Otherwise

The existing CND “PKT” selector is renamed to “FABRIC” to reflect a more accurate functionality of the selection criteria. Also the Trimodal call server supports multiple packet fabrics like IP, AAL1 and AAL2 on the same switch. To support this the FABRIC selector criteria is expanded to ENET, IP and AAL1 and AAL2 fabrics.

Refer to Figure 5, "CND FABRIC Selector Criteria ENET, IP and ATM" for an overview of the renamed “FABRIC” selector criteria based routing.

Figure 5 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901) ===> If fabric = ENET then take OFRT Route 901
   (CND FABRIC IP ST 902) ===> If fabric = IP then take OFRT Route 902
   (CND FABRIC AAL1 ST 903) ===> If fabric = AAL1 then take OFRT Route 903
   (CND FABRIC AAL2 ST 904) ===> If fabric = AAL2 then take OFRT Route 904
```

Please refer to “Table 2 CND FABRIC selector enhancements” on page 1461. for an overview of CND FABRIC selector enhancements.

Table 2 CND FABRIC selector enhancements

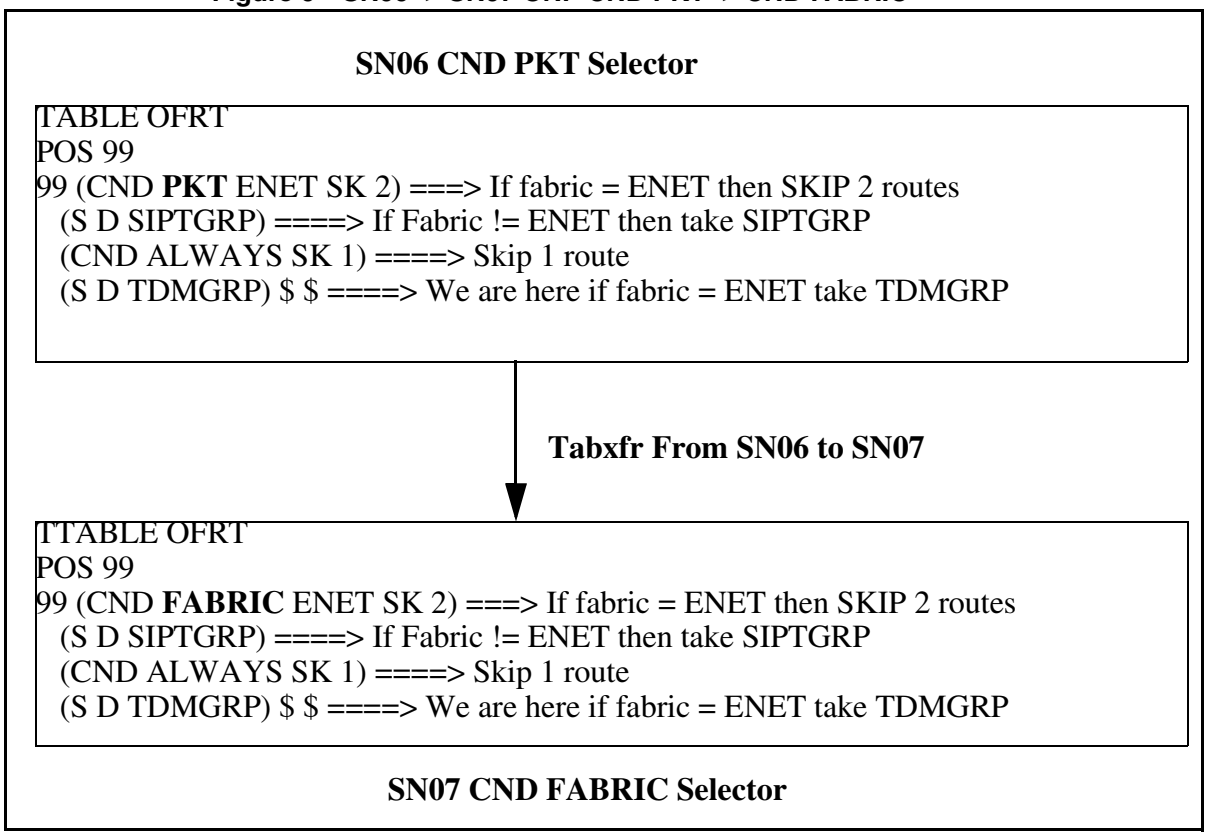
Fileds			Description	Values
RTE			Unchanged	
RTESEL			Unchanged	
	CNDSEL = FABRIC		Changed. New selector FABRIC Replaces PKT	ALWAYS,RND,SNPA,EA,TOD,MIGRATE,NARS,COSMAP,NRR,SITE,CALLCHR,INTERLATA,PKT,TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC**,BEARNET
		PKTSEL	Changed. New Fabric Types added	UNDEF[a], ENET, AAL1, AAL2, IP
		RTETYPE	Unchanged	ST, T, SK

a. No trunk and line agent can belong to an network with fabric as “UNDEF”. Hence “UNDEF” fabric selector is blocked form being datafilled.

120.2.4.1.1 ONP Impact

The SN06 “PKT” selector will be renamed to “FABRIC” in SN07 and later releases. Refer to Figure 6, "SN06 -> SN07 ONP CND PKT -> CND FABRIC" for SN06 to SN07 ONP tabxfr behavior.

Figure 6 SN06 -> SN07 ONP CND PKT -> CND FABRIC



120.2.4.2 New Conditional Selector BEARNET

A new table BEARNET is introduced to support multiple networks for a Trimodal Callserver. The bearer network names are provisioned in table BEARNET. The new BEARNET selection criteria is created based on network names. The BEARNET conditional selector provides routing based on the bearer network name.

Refer to Figure 7, "CND BEARNET Selector Criteria Based on Network Name" for an overview of the BEARNET selector criteria based routing.

Figure 7 CND BEARNET Selector Criteria Based on Network Name

TABLE OFRT
POS 99
100 (CND BEARNET **DFLTTDM** ST 901) ===> BEARNET = DFLTTDM then take OFRT Route 901
(CND BEARNET **DFLTIP** ST 902) ===> BEARNET = DFLTIP then take OFRT Route 902
(CND BEARNET **DFLTATM** ST 903) ===>BEARNET = DFLTATM then take OFRT Route 903

Please refer to “Table 3 CND BEARNET selector” on page 1463. for an overview of CND BEARNET selector..

Table 3 CND BEARNET selector

Fileds			Description	Values
RTE			Unchanged	
RTESEL			Unchanged	
	CNDSEL = BEARNET		New selector FABRIC Replaces PKT	ALWAYS,RND,SNPA,EA,TOD,MIGRATE,NARS,COSMAP,NRR,SITE,CALLCHR,INTERLATA,PKT,TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC**,BEARNET
		NETSEL	NEW.	NTWKNAME values provisioned in Table BEARNETS
		RTETYPE	Unchanged	ST, T, SK

120.2.5 Traver Enhancements

120.2.5.1 Traver option BEARNET based on bearer network name

The new traver option BEARNET is created to input the incoming trunk agent bearer network name. The bearer network name is used to support CND FABRIC and BEARNET selector routing in traver. Refer to Figure 8, "Traver example: with BEARNET Option"for an overview of BEARNET option.

When the BEARNET option is not present in the traver command,

- The Traver tries to determine if the agent is on the TDM network (first tuple in table BEARNET).
- If the agent is not on TDM the office default BEARER NETWORK is used for CND FABRIC and BEARNET selector routing.

For functionality of traver without BEARNET option refer to Figure 9, "Traver example: without BEARNET Option"

Note: The network names defined in table BEARNET will not be displayed in traver command help or prompting.

Figure 8 Traver example: with BEARNET Option

```
traver tr isupicitt 7211001 BEARNET MyAAL1NW b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
.  .  . SAME TABLE
 .  .  . 1002 S D ISUPITOG
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 9 Traver example: without BEARNET Option

```
traver tr isupicitt 7211001 b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .  . SAME TABLE
 .  .  . 1002 S D ISUPOGITT
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYAAL1NW ST 1003
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPOGITT             7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

120.2.5.2 Traver option TRKMEM enhancemens

The existing traver TRKMEM option is enhanced to obtain the originating trunk bearer network name. The bearer network name is used to support CND FABRIC and BEARNET selector routing in traver. Please refer to “Figure 10 Traver example: with TRKMEM Option” on page 1466. for an overview of TRKMEM option.

When the TRKMEM option is not present in the traver command, the traver assumes the default TDM network (first tuple in table BEARNET). The

default TDM network is used for CND BEARNET and FABRIC selector routing. Please refer to “Figure 11 Traver example: without TRKMEM Option” on page 1467. for an overview of traver functionality without TRKMEM option.

Note: When both TRKMEM and BEARNET options are present in the Traver command the “BEARNET” option will be ignored.

Figure 10 Traver example: with TRKMEM Option

```
traver tr isupicitt 7211001 TRKMEM 1001 b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
 .  .  . SAME TABLE
 .  .  . 1003 S D ATMTRK1
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Note: When the TRKMEM is present in the Traver command and the Trunk member is invalid the TRKMEM option is ignored. i.e the Traver will proceed as if there was no TRKMEM option.

Figure 11 Traver example: without TRKMEM Option

```
traver tr isupicitt 7211001 b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .  . SAME TABLE
 .  .  . 1002 S D ISUPOGITT
 .  .  . EXIT SAME TABLE
 .  .     CND BEARNET MYAAL1NW ST 1003
 .  .     CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPOGITT            7211001                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

120.3 Hardware Requirements or Dependencies

None

120.4 Software Requirements or Dependencies

None

120.5 Limitations and restrictions

MULTINET_DISPLAY_ACTIVE parameter is changed from ‘YES’ to ‘NO’ using table control

- The OMSHOW command would display the OM groupsIWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

120.6 Interactions

None

120.7 Applicable customer facing sections

Fault Management

Logs	X_____
Alarms	N/A___

Configuration

Data Schema	X_____
User Interface	X_____
Element Management	N/A___
Security	N/A___
Service Order	N/A___
Office Parameters	X_____

Accounting (includes AMA billing)	N/A___
Performance (includes operational measurements)	X_____

120.8 Glossary

Term	Description
CND	Conditional
OM	Operational Measurements

121: Functional Description (FN): A00003948

121.1 Feature name

There are some diagrams in this document that were imported from powerpoint slides and do not transfer well to unix. They can be viewed using the PC version of Framemaker.

Tri-modal provisioning - A00003487 in FMDOC library.

Note that this Functional Description covers all the SN07 Trimodal Call Server Features:

- a00003488: TriModal Call Signaling and Connectivity
- a00003662: TriModal Call Server Bridge Maintenance
- a00003509: TriModal Support for Lawful Intercept
- a00003947: TriModal Logs and OMs
- a00003948: TriModal GWC EM

121.2 Approval/Agreement List

Table 1 Agreement List

Name	Role/Title	ArchID, DRU, Module, or Functional Area	Mandatory Reviewer (Y/N)	Agreed To
BLM				
Sam Jones	BLM Prime	OAM BLM	Y	
Ron Lau	BLM	BLM	Y	
John Haney	BLM	BLM	Y	
Design/Architecture				
Craig Telke	Project Manager	Succession	Y	
Jane Simms	Architect	Succession Trimodal	Y	
David Rogers	Architect	Succession Provisioning	Y	
Keith Raker	Design prime	PNM, PTM_EM_GWC	Y	
Helen Yokeley	Design Prime	Prime for Provisioning and OAMP	Y	
Mike Hayes	Design Prime	Line Call Processing Prime	Y	
Don Backshall	Design Prime	Trunk Call Processing Prime	Y	
Alfredo Sisiruca	Design Prime	SPM/Bridge Prime	Y	
Scott Emenheiser	Design Prime	ECAN Prime	Y	
Larry Horton	Design Prime	ECAN	Y	
Chris Kittlitz	Design Prime	LI Prime	Y	
Documentation/Upgrades/Software Configuration				
Dave Graves	Documentation Prime	Documentation	N	
Dave Collier	Manager	Documentation	N	
Kyle Mawst	Engineer	Upgrades	N	
Don Howell	Engineer	Upgrades	N	
Carol Feddeman	Engineer	S/W Configuration Suport and Rules	N	
Carl Akai	Engineer	S/W Configuration Suport and Rules	N	

Table 1 Agreement List

Name	Role/Title	ArchID, DRU, Module, or Functional Area	Mandatory Reviewer (Y/N)	Agreed To
Mark Kujanpaa	Engineer	GIST - Global Installation Services Technology	Y	
PV Test Primes				
Chris Markovich	PV	UA-IP focus	Y	
George Bradley	PV	Main, UA-ATM focus	Y	
Harry Ogan	PV	Large lab	Y	

121.3 Description

121.3.1 Existing Functionality

Prior to SN07, the CS2000 call server had very limited knowledge about the packet bearer network. Only a single packet bearer network was supported along with the legacy ENET bearer network. Individual agents were associated with a bearer network based upon the connectivity of the node that hosted the agent. For example, a trunk member that was assigned to a DTC would be associated with the legacy ENET bearer network. A trunk member that was assigned to either a GWC or an MG4K would be associated with the packet bearer network. Since both the GWC and the MG4K tag their hosted agents as ‘packet bearer network’, the core connectivity cannot distinguish between the various types of packet bearer networks are are available (i.e., IP, AAL1, AAL2). This is the basis for the CS2000 call server restriction that it can only support a single packet bearer network prior to SN07.

121.3.2 Feature Functionality

In the SN07 release, work is being started in the CS2000 Call Server to support multiple bearer networks. These bearer networks include both the legacy ENET bearer network and up to seven additional packet bearer networks.

In the SN07 release, a bearer network framework is implemented but full integration of all possible supported configurations will not be supported in this release. In SN07, the focus will be on supporting three bearer networks[1]:

- ENET
- AAL1 packet network
- IP packet network

[1]AAL2 packet networks are not going to be tested in a multi-bearer network configuration, but there is nothing to block this type of bearer network from being configured.

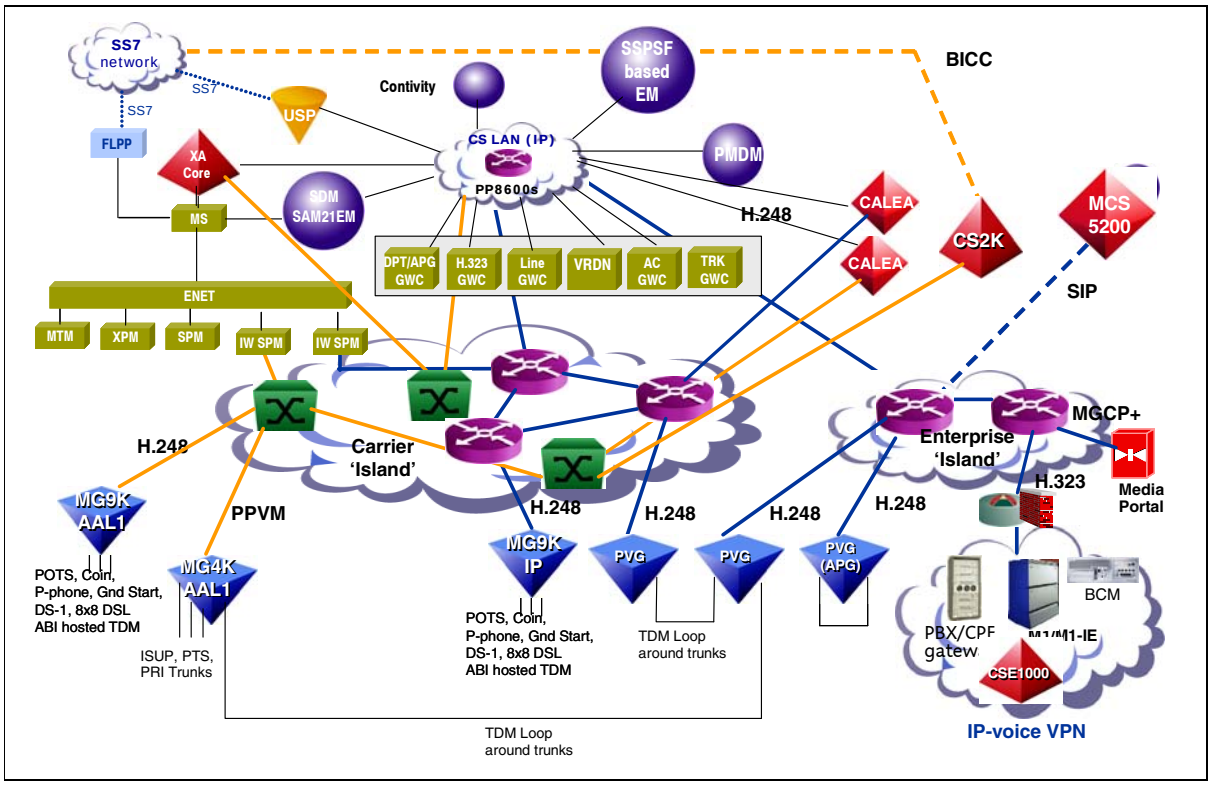
The main focus in SN07 is to support a Universal Access (UA)- AAL1 and a Universal Access (UA) - IP configuration with a single CS2000 Call Server. In addition, there are requirements to support some limited Carrier Hosted Services (CHS) functionality as well (i.e., H.323 and Media Call Server 5200 (MCS5200).

Interworking between the UA-AAL1 and UA-IP configurations in a multi-bearer network configuration is supported in SN07. However, interworking with the CHS agents is limited in SN07. In SN07, there is no support for interworking between the H.323 gateway (using a Media Portal) and the IP IW SPM. For this reason, a loop around trunk, hosted by a PVG on the CHS bearer network and hosted by a PVG in the UA IP bearer network or an MG4K in the UA AAL1 bearer network or an SPM/DTC in the ENET network, must be used to provide connectivity between the H.323 GW and all other agents on the CS2000 Call Server. The following list provides a view of the limitations associated with H.323 calls in this configuration:

- Multiple billing records generated - A call from am H.323 agent to an MG9000 AAL1 native line would be represented as two calls in the CS2000 call server, each generating its own billing record.
- H.323 agent access to announcements - Since there is no announcements accessible to the CHS IP network (i.e., no IP IW bridge supported), announcements cannot be played to the H.323 agent. Any CS2000 Call Server services will not be able to use announcements and any treatments will have to be configured to ‘release with cause’ and the announcement would be provided by the enterprise bearer network.
- H.323 agent access to conferencing - Since there is no conference circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), conferencing services cannot be supported to the H.323 agent.
- H.323 agent access to test trunk facilities - Since there is no test trunk circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), trunk tests cannot be supported to the H.323 gateway.

A diagram of the network topology is shown in the following figure.

Figure 1 SN07 supported multi-bearer network topology



In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Table 1 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	all Succession supported legacy peripherals	supported SN07 legacy peripherals which includes both lines and trunk

Table 1 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC[a]	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
IP (CHS)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	GWC[b]	SIP-T DPT trunks
	H.323 GWs (Cisco, Westel, BCM, M1)	PRI trunks

a. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk support.
b. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk support.

Connectivity between the supported bearer networks is accomplished by using IW SPM bridges. The CS2000 Call Server is modified to allow support of both the ATM AAL1 based IW SPM and the IP based IW SPM at the same time. Prior to SN07, the CS2000 Call Server could only support one type of IW

SPM. A single IW bridge pool was supported. In SN07, support for multiple bridge pools is introduced.

Control is given to the Succession customer to configure how the supported bearer networks in the CS2000 Call Server connect to each other. This is controlled by provisioning the types of interworking bridges needed to connect one bearer network to another. The interworking bridges available in SN07 are the following:

- IW SPM AAL1 - connects an AAL1 bearer network to the ENET
- IW SPM IP - connects an IP bearer network to the ENET

Prior to SN07, Succession configurations used the IW SPM AAL1 to connect an AAL1 bearer network to the ENET and used the IW SPM IP to connect an IP bearer network to the ENET. This is still supported in SN07 with multi-bearer network support. In this multi-bearer network configuration, a connection between an AAL1 bearer network and an IP bearer network will use two IW bridges (i.e., 1 IW SPM AAL1 and 1 IW SPM IP using the ENET to connect the two packet bearer networks). The following figure illustrates this connection topology.

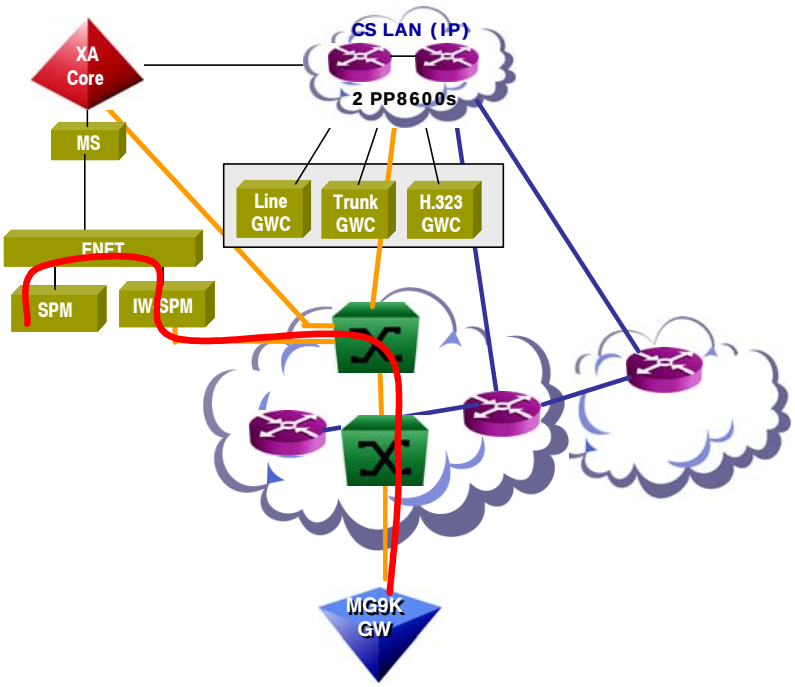


Figure 2 ATM AAL1 (UA) to ENET connection topology

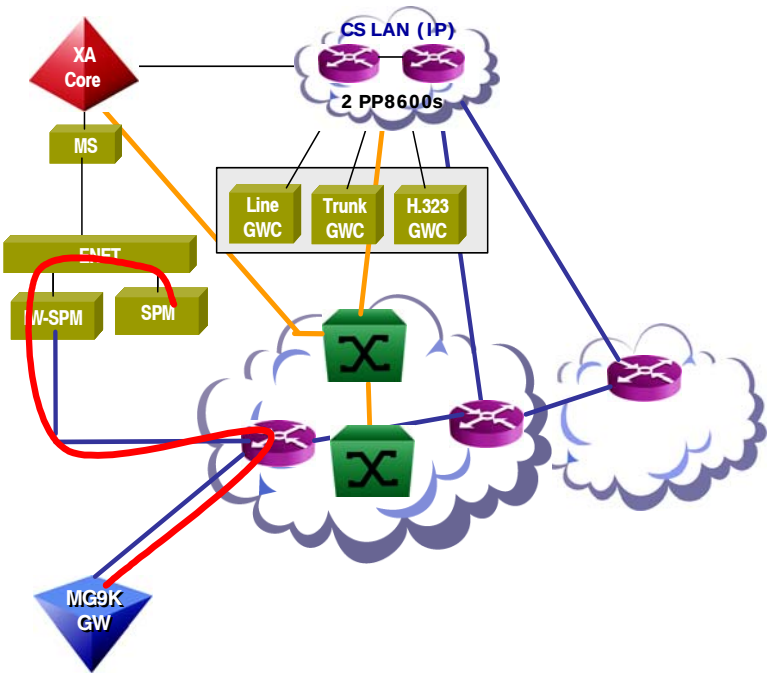


Figure 3 IP (UA) to ENET connection topology

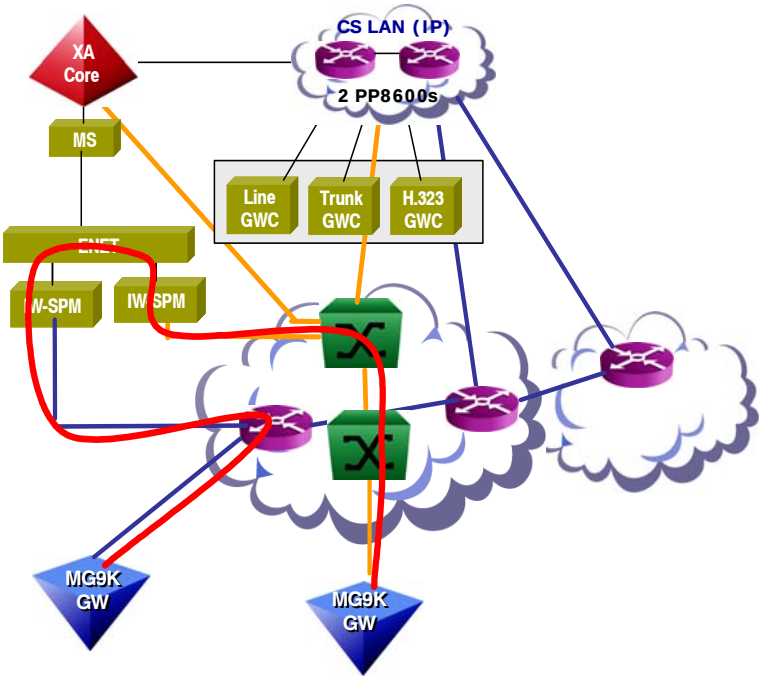


Figure 4 ATM AAL1 (UA) to IP (UA) connection topology

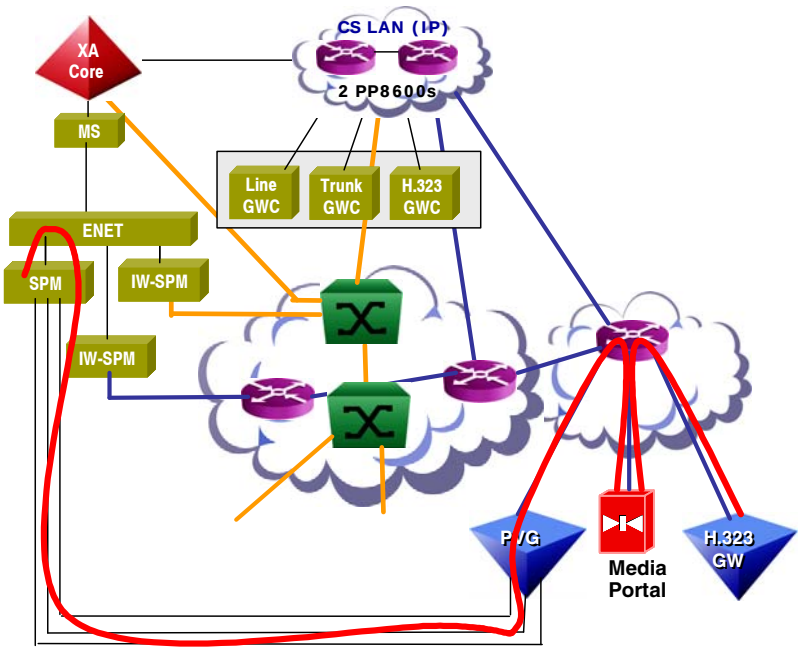


Figure 5 IP (CHS) to ENET connection topology

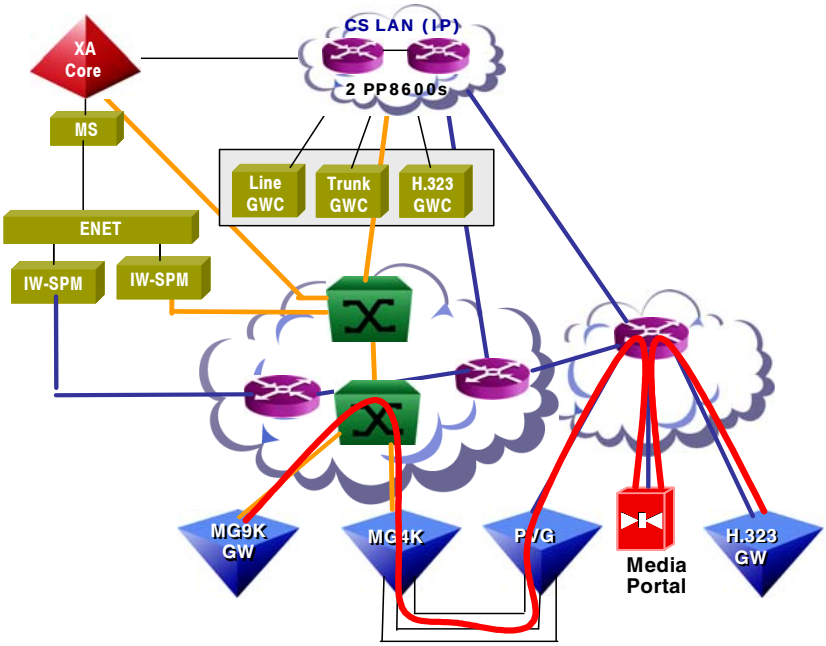


Figure 6 IP (CHS) to ATM AAL1 (UA) connection topology

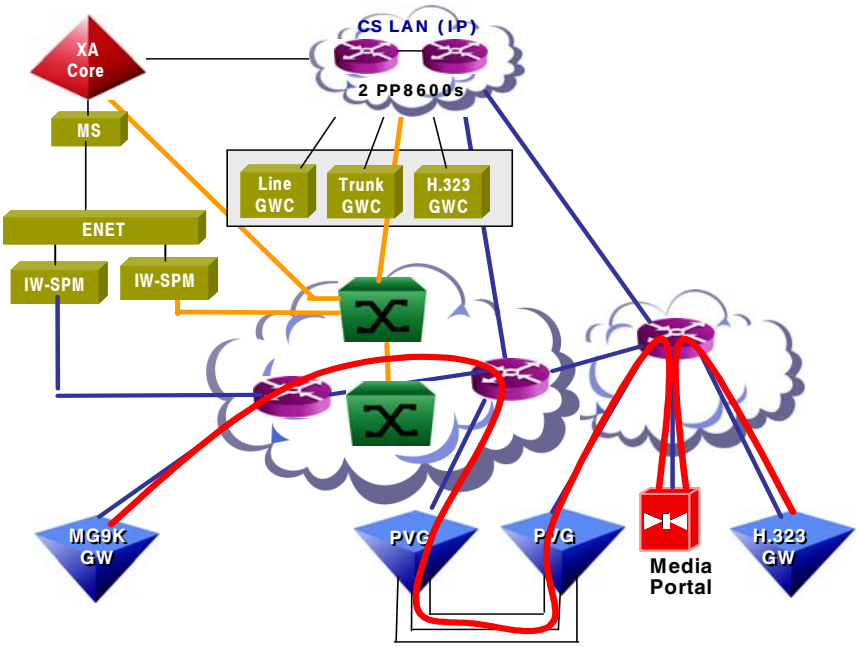


Figure 7 IP (CHS) to IP (UA) connection topology

The following areas will be addressed in more detail in the following sections:

- Bearer network and connectivity provisioning
- Multiple bearer network support in the GWC EM
- Core connectivity connection management
- IW Bridge management
- OAMP changes on the CS2000 Call Server
- Lawful Intercept
- Trunk selection (like network selection)
- DPT (BICC and SIP-T) interworking including audible ringing support
- Translations and Routing changes
- USP messaging
- ECAN across multiple bearer networks
- Voice quality
- ONP

121.3.2.1 Bearer network and connectivity provisioning

The purpose of the provisioning changes are to allow bearer networks to be defined and associated to individual agents. Once this is accomplished, there are rules created that define which bearer networks can connect to each other and how that connection is accomplished.

When the CS2000 Call Server is requested to make a connection between two endpoints, it needs to know the bearer network associated with each endpoint. If this model were followed for provisioning, then each line and trunk member datafill would have to include an indication of the bearer network. This level of provisioning is cumbersome and very repetitive in most cases. For this reason, a hierarchical model is used in SN07. An assumption is made that a node (either an SPM node or a line/trunk GWC) supports one and only one bearer network. This allows the bearer network to be associated with the node and then this information is applicable to all the endpoints associated with that node. In other words, the bearer network for the endpoint is derived from the bearer network of the node that hosts the endpoint[1].

There is one exception to the above behavior and it is in the area of DPT trunk support. Given the dynamic endpoint association that is made between the hosting node and the DPT trunk member, GWCs configured as DPT GWCs will not have an associated bearer network at the node level. The bearer network is associated with the DPT trunk group. The DPT endpoint obtains its associated bearer network from the DPT trunk group that is associated to it on a call-by-call basis.

The following provisioning changes are made by this activity:

- Bearer network definition
- Bearer network node association
- Bearer network DPT trunk group association
- IW bridge pool definition
- IW bridge pool assignment
- Bearer network connectivity

121.3.2.1.1 Bearer network definition A new table is introduced (Table BEARNETS) that defines the bearer network and the bearer fabric associated with this bearer network. The key to the table is a bearer network index. This index is needed to make it easy to change the bearer network name (i.e., without having to delete and re-add the entry). Index 0 is always reserved for the ENET tuple, if it exists.

[1]Note that endpoints that are hosted on legacy peripherals which are then hosted on MG9000 ABI, will derive their bearer network from the GWC that hosts the MG9000 ABI.

The OPTIONS field in this table identifies an optional bearer network characteristics. In SN07, the following options are supported:

- Default packet network - specifies the default packet bearer network in the office. This is used during the ONP process as well as an endpoint bearer network designation if a node-based bearer network cannot be determined.
- ECAN strategy - specifies that the ECAN region strategy should override the bearer network default ECAN edge strategy. This option obsoletes the office parameter ECAN_EDGE_STRATEGY.

Table BEARNETS supports up to eight bearer networks in the CS2000 Call Server. Refer to the Configuration section for more details on Table BEARNETS.

Figure 8 Table BEARNETS example datafill

```
TABLE: BEARNETS
NETIDX BNETNAME     DISPLAY FABRIC OPTIONS
----------------------------------------
NET 0  TDM_ENET     ENET    ENET   $
NET 1  NET_AAL1     ATM     AAL1   (PACKET_NETWORK_DEFAULT)$
NET 2  NET_IP       IP      IP     $
NET 3  NET_AAL2     AAL2    AAL2   $
```

121.3.2.1.2 Bearer network node association Association of the bearer network is done at the node level in the CS2000 Call Server. In order to minimize table changes and to provide minimal impact to DMS legacy offices, legacy peripheral nodes do not require an explicit association to the ‘ENET’ bearer network. This will be assumed in within the CS2000 Call Server.

However, any node that hosts packet bearer network endpoints requires that the bearer network be associated with the node. This is applicable to the following nodes:

- GWC (Table SERVRINV) - GWCs host many types of endpoints: lines and trunks)
- MG4K (Table MNNODE)
- DPT SPM (Table MNNODE)

Table SERVRINV is modified to include a new field BEARNETS. This field lists all the supported bearer networks associated with the GWC. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. This information is populated by the GWC Element Manager when a GWC is defined in SN07. Refer to the Configuration section for more details on Table SERVRINV.

Figure 9 Table SERVRINV example datafill

```
TABLE: SERVRINV
SERVRNAME SERVRADDR SERVREXEC SERVRTONE BEARNETS SERVROPTS
-----------------------------------------------------------
GWC 0     IP  47 192 48 24 (POTS POTSEX)  (KEYSET  KSETEX)  $
NORTHAA (NET_AAL1 Y) $ $
```

Table MNNODE is modified for ‘SMG4’ class of SPM’s (i.e., MG4Ks) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the MG4K. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Figure 10 Table MNNODE example datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM  1             SPM_1          SMG4   0   SYNC   LINE   50
(COT 60)  (DTMF 60)  (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT)  (MANB MJ RPT)  (ISTB MN RPT)  (SYSBNA CR RPT)(MANBNA MJ
RPT)  (COTLOW MN RPT)  (DTMFLOW MN RPT)(ECANLOW MN RPT)  (MFLOW
MN RPT)  (CMRLOW MN RPT)(TONESLOW MN RPT)  (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT)(ATMBCN CR RPT)  (STE3HLD MJ RPT)  (STE3HLD24
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  (SPMSRMNTD MN RPT)
(LOCUR MJ RPT)  (TMCFAIL CR RPT)  $ $  N  0  $  N  N  (NET_AAL1 Y) $
```

Table MNNODE is modified for ‘IW’ class of SPM’s whose DPT_INFO indicates a DPT SPM (i.e., DPT SPMs) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the DPT SPM. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Figure 11 Table MNNODE example datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM 1   SPM_1   IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $ (SYSB CR RPT)  (MANB MJ RPT)  (ISTB MN RPT)
(SYSBNA CR RPT)(MANBNA MJ RPT)  (DTMFLOW MN RPT)  (ECANLOW MN RPT)
(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN CR RPT)(SMCHLD MF
RPT)  (SMCHLD24 CR RPT)  $DPT_ONLY  (NET_AAL1 Y) $
(SPMECIDX 0)$
```

121.3.2.1.3 Bearer network DPT trunk group association DPT trunk groups require an association to the bearer network. Changes are made

to Table TRKOPTS where the DPT trunk groups are defined. As part of this change, it was decided to change the option used to indicate a DPT trunk group. The DPT application is removed from the DYNAMIC option. A new DPT option is created to define a DPT trunk group. This new option contains a field to designate the associated bearer network. Other application users for the DYNAMIC option remain unchanged. Refer to the Configuration section for more details on Table TRKOPTS.

Figure 12 Table TRKOPTS example datafill

```
TABLE: TRKOPTS
OPTKEY          OPTINFO
----------------------------------------
DPTTRK DPT      DPT BICC NET_AAL1 1
SIPTRK DPT      DPT SIPT NET_IP MGC2 PROF MGCTWO Y
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC
```

121.3.2.1.4 IW bridge pool definition A framework is needed to allow multiple bridge pools to be defined in the CS2000 Call Server. This framework is intended to support any type of bridge that may be used to connect two bearer networks together.

In SN07, there is only one bridge type supported, the core-managed IW SPM bridge. In defining a bridge pool of this type, the two bearer networks that this bridge can connect together are specified. Other types of bridges may require additional information to be defined.

The bridge pool name is first defined in Table CLLI. Note that the number of members in the CLLI is not applicable to the bridge pool. New table NETBRDGE is created to define the bridge pool and its type. Refer to the Configuration section for more details on Table NETBRDGE.

Figure 13 Table CLLI and Table NETBRDGE example datafill

```
TABLE CLLI
CLLI          ADNUM   TRKGSIZ                    ADMININF
-----------------------------------------------------
ENET_TO_AAL1  321     0       ENET_TO_AAL1_BRIDGE_POOL
ENET_TO_IP    322     0       ENET_TO_IP_BRIDGE_POOL

TABLE: NETBRDGE
BRDGCLLI      TYPE        DISPLAY BEARNETS
-------------------------------------
ENET_TO_AAL1  CORE_BRDG   E-A1    (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG   E-IP    (TDM_ENET NET_IP)   $
```

121.3.2.1.5 IW bridge pool assignment Once a bridge pool has been defined, the individual IW SPM bridge nodes needs to be associated with a bridge pool. Table MNNODE is modified for ‘IW’ class of SPM’s whose

DPT_INFO indicates an IW SPM (i.e., not a DPT SPM) to include a new field BRDGGRPS. This field lists all the supported bridge pools associated with the IW SPM. In SN07, only one entry for this field is supported. Refer to the Configuration section for more details on Table MNNODE.

Figure 14 Table MNNODE example datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-------------------------------------------------
SPM  1 SPM_1  IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $(SYSB CR RPT)  (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT)(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

121.3.2.1.6 Bearer network connectivity Now that the bearer networks have been defined and the bridge pools have been defined, the next step is to define the connectivity rules between the bearer networks. An assumption is made that a connection between two endpoints on the same bearer network will always be allowed to proceed. The rules being discussed here apply only to a connection request made between two endpoints that are associated with different bearer networks. These rules answer the following questions:

- Can a bearer network connect to another bearer network?
- What bridge pool or bridge pools are used to support a connection between two bearer networks?

Two new tables are created to allow the customer to provide answers to these questions. Table NETPATH provides a set of bridge pool combinations. These can be thought of as ‘connectivity routes’ and assist in answering the second question posed above. Note that it is possible to create a NETPATH entry that contains more that one bridge pool. Table NET2NET allows the customer define which bearer networks connect to other bearer networks and what ‘connectivity route’ should be used (i.e., points to an entry in Table NETPATH). If there are no connecting networks specified in Table NET2NET, then a connection request from that bearer network to any other bearer network will be denied. Refer to the Configuration section for more information on Tables NETPATH and NET2NET.

Figure 15 Table NETPATH example datafill

```
TABLE: NETPATH
PATHIDX       NETBRDGE
----------------------------------------
  0           (ENET_TO_AAL1)  $
  1           (ENET_TO_IP)    $
  2           (ENET_TO_AAL1), (ENET_TO_IP)$
  3           (AAL1_TO_IP)    $
```

Figure 16 Table NET2NET example datafill

```
TABLE: NET2NET
BNETNAME             CONNETS
-------------------------------------------------
  TDM_ENET         (NET_AAL1 0),   (NET_IP 1)    $
  NET_AAL1         (TDM_ENET 0),   (NET_IP  2)   $
  NET_IP           (TDM_ENET 1),   (NET_AAL1 2)  $
```

121.3.2.2 Multiple bearer network support in the GWC EM

As described in the previous section, the bearer network needs to be associated with the GWC. New GWCs are added using the GWC Element Manager (EM). Information input using the GWC EM GUIs is then automatically updated in CS2000 Call Server tables (such as Table SERVRINV).

Prior to SN07, the GWC EM supported only one packet network. Characteristics about that packet bearer network were defined and associated with all the GWCs in the office.

In SN07, changes are made to the GWC EM to support multiple bearer networks. These changes involve the following:

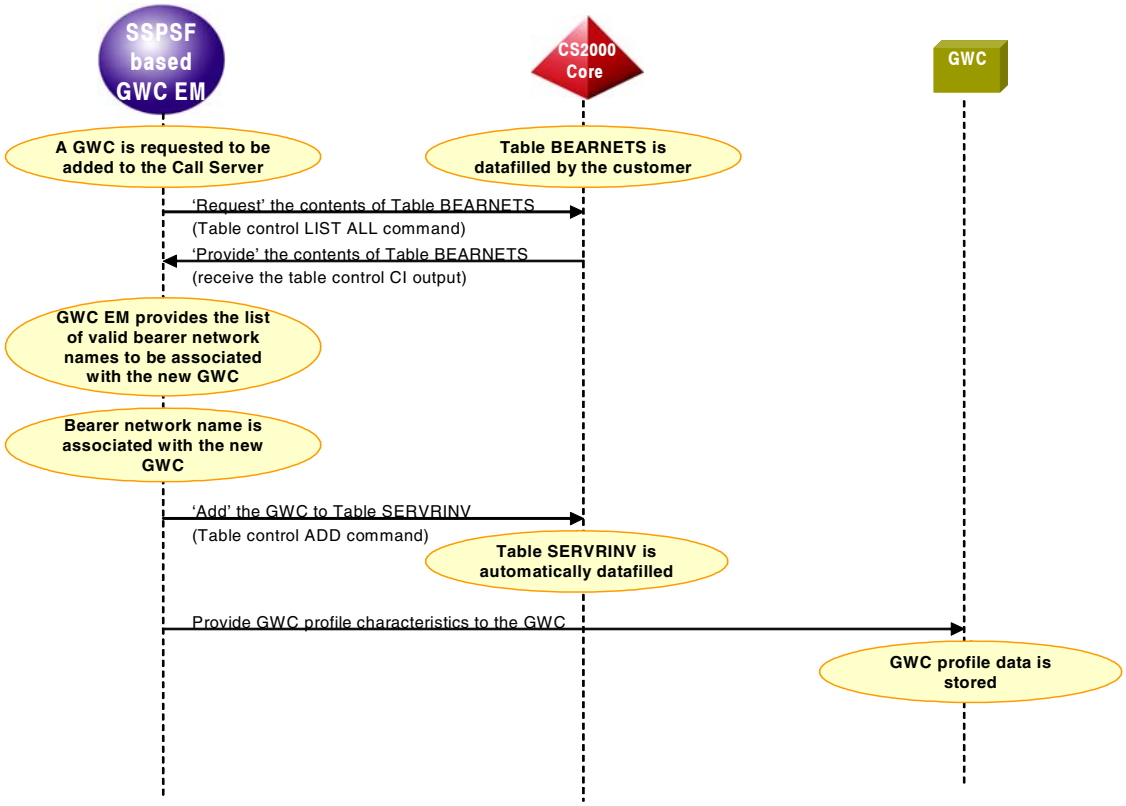
- Support the provisioning of multiple bearer network codec profiles.
  - — Display bearer network codec profile on GWC-EM GUI.
  - — Add bearer network codec profile from GWC-EM GUI.
  - — Delete bearer network codec profile from GWC-EM GUI.
  - — Change bearer network codec profile from GWC-EM GUI.
- Support the specification of a bearer network and a bearer network codec profile for each GWC.
  - — Display the bearer network and network codec profile of each GWC on GWC-EM GUI.
  - — Associate the bearer network and network codec profile with one GWC when adding GWC node from GWC-EM GUI.

— Change the associated bearer network codec profile of one GWC node from GWC-EM GUI.

- Support population of the selected bearer network in the CS2000 Call Server table SERVRINV

The following figure illustrates the steps involved in flowing the data from the GWC EM to the CS2000 Call Server. Refer to the Configuration section for more information on the GWC EM GUI screens that are available in SN07.

Figure 17 GWC EM flow through provisioning for bearer network



121.3.2.3 Core connectivity connection management

Core connectivity is a function in the CS2000 Call Server that handles connection requests that are made from the CallP and Services applications. Prior to SN07, core connectivity processed requests to make a connection between endpoints. Endpoints were designated as being 'internal' (i.e., connected to the ENET) or 'external' (i.e., connected to the packet bearer network). Core connectivity knew that if a request was made to connect and 'internal' endpoint to an 'external' endpoint, then an IW bridge was needed. It would request a bridge from the office-wide IW bridge pool.

In SN07, core connectivity is changed to support multiple bearer networks and multiple bridge pools. Rather than making assumptions that a bridge from a bridge pool is needed to make a connection, core connectivity references tables NET2NET and NETPATH when a connection between two unlike bearer networks is requested. If these tables indicate that a connection should not be made, then core connectivity denies the connection request to the CallP application. The CallP application would then route the call to a Network Blocking (NBLH) treatment causing the call to not be completed.

The following figures provide examples on how core connectivity uses the datafill to process a connection request from the CallP application.

Figure 18 ATM AAL1 (UA) to ENET connection request

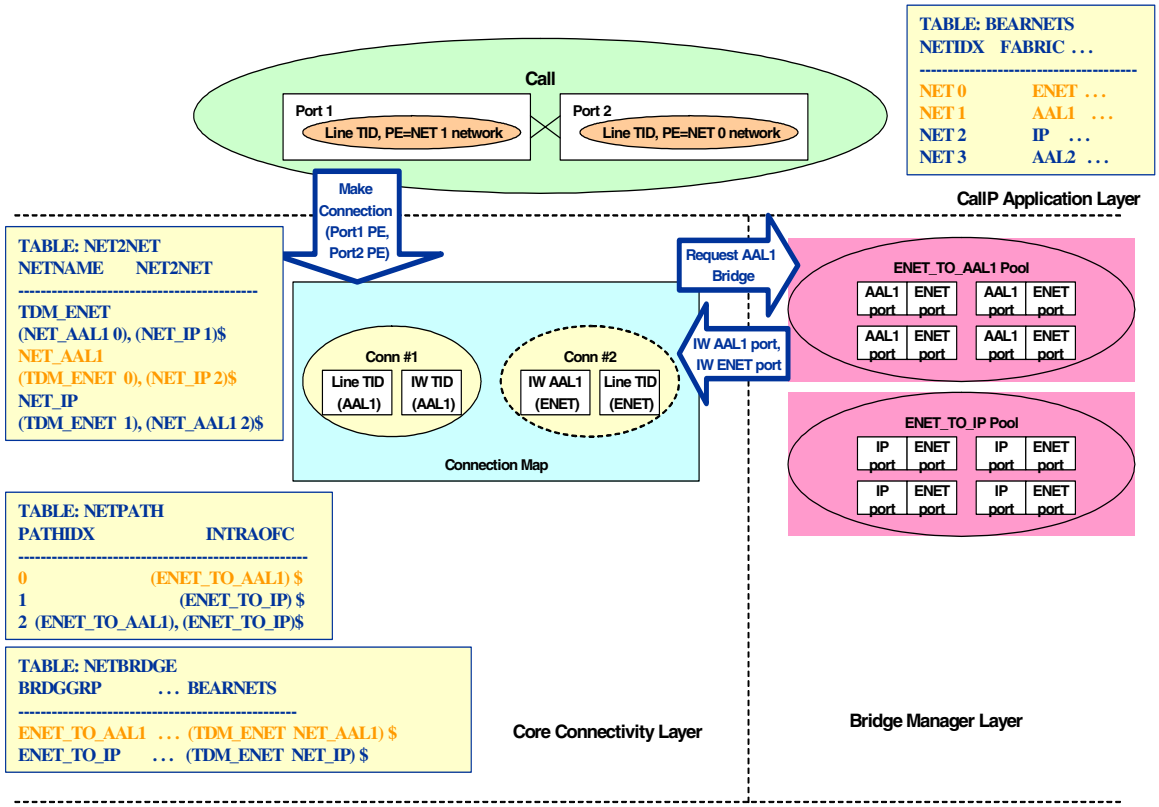


Figure 19 IP (UA) to ENET connection request

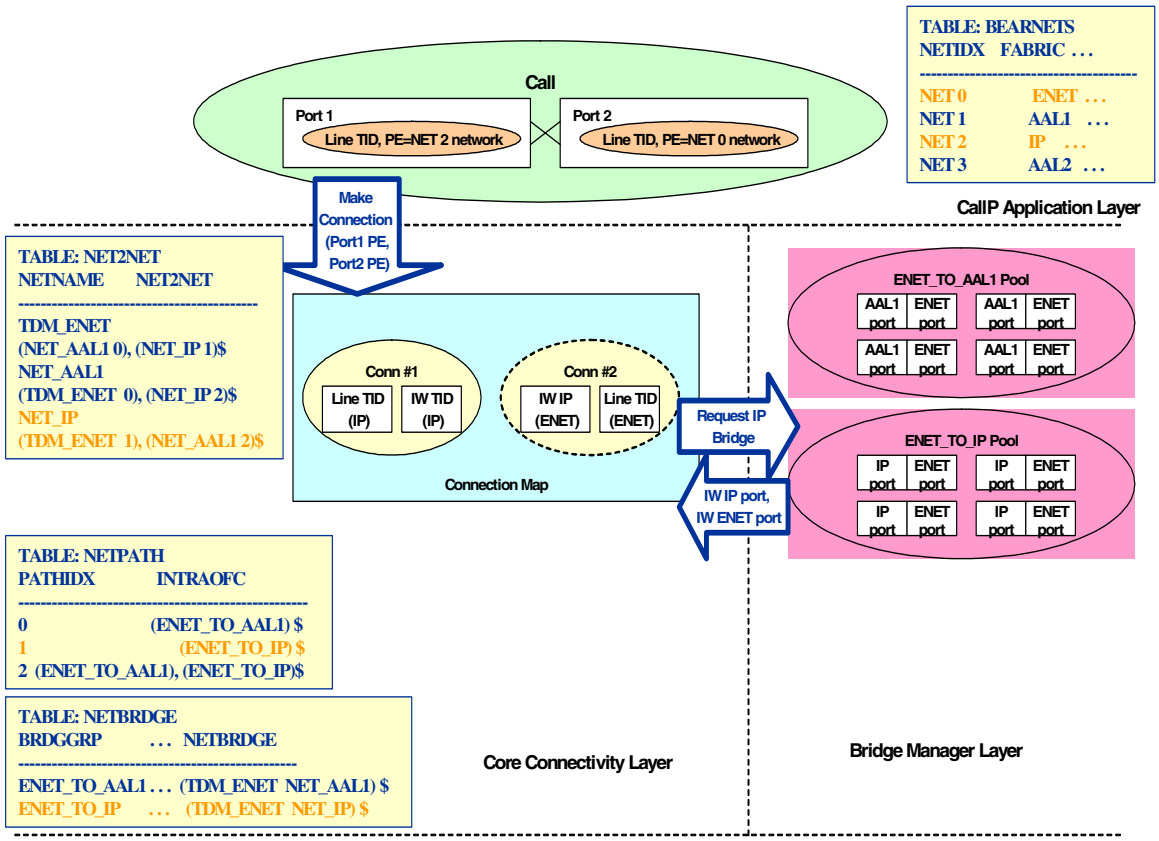


Figure 20 ATM AAL1 (UA) to IP (UA) connection request

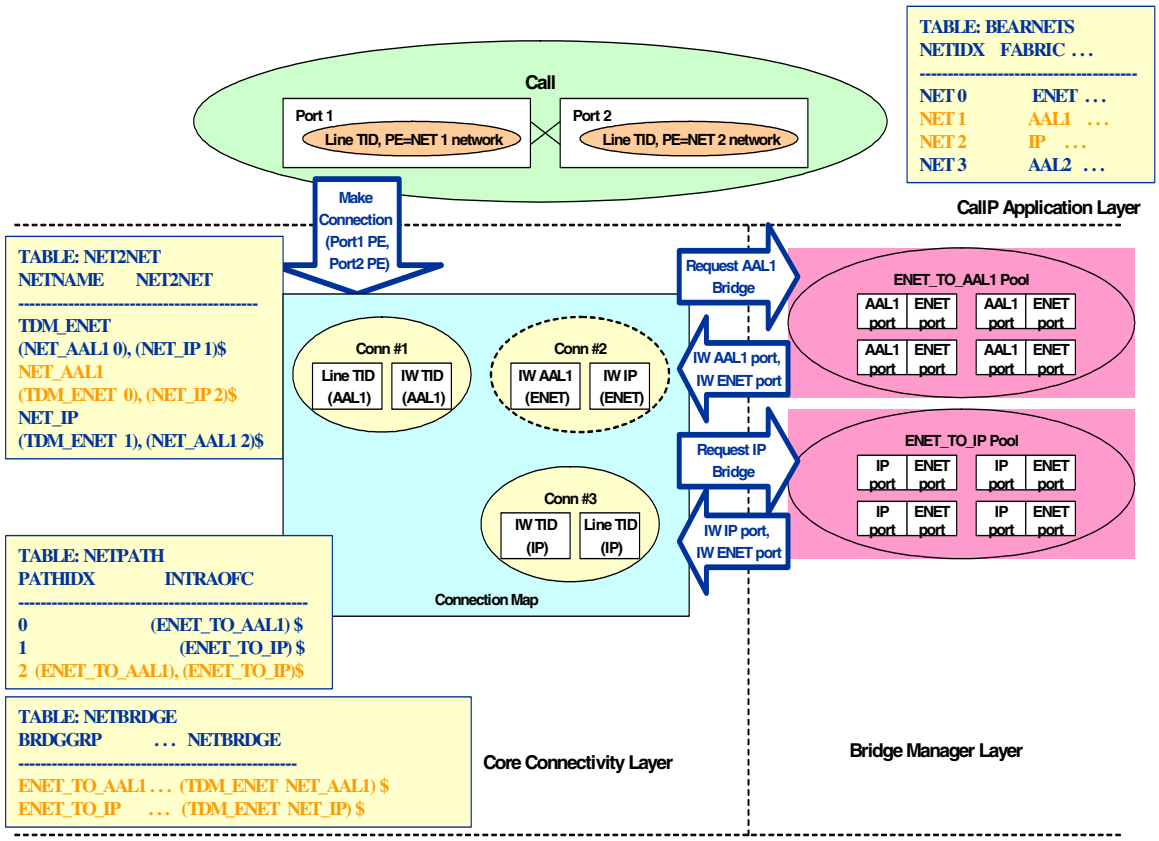
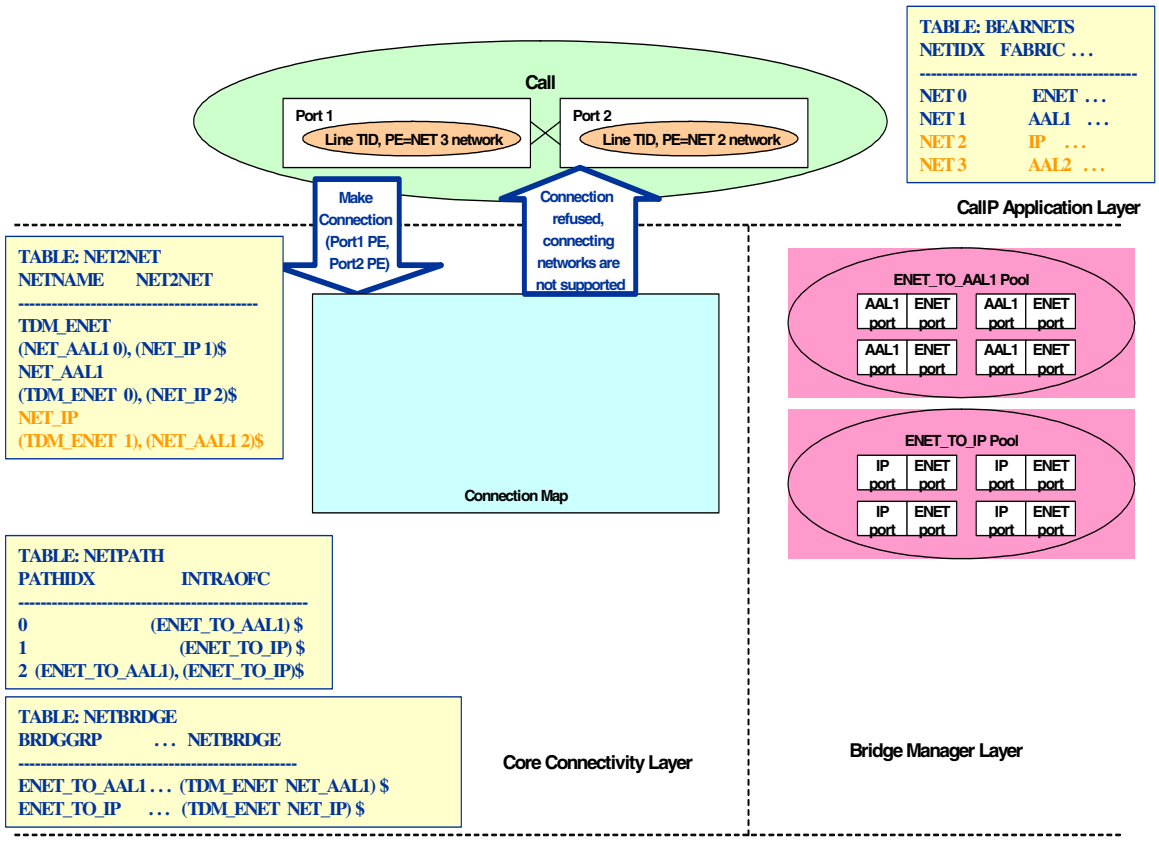


Figure 21 ATM AAL2 to IP (UA) connection request



Core connectivity supports a set of connection operations. All of the possible connection requests that the CallP application may request in support of the services supported on the CS2000 Call Server map to one of these connection operations. It is important to understand what these operations mean for connection maps that contain more that one IW bridge. The following table documents this behavior.

Table 2 Core connectivity connection operations

Connection Operation	Description	Actions taken
Make connection	There are 2 external connections involved being created. The packet connections are created first, followed by the ENET connection.	Connection 1 - FCM Makes sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Makes sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (make) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
Break connection	Free the ENET connection, and then to break both packet connections. It should be noted that although the ENET connection is freed from the connection maps, the actual ENET path is not physically freed.	Connection 1 - FCM Breaks sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Breaks sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (free) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
Hold connection	Hold both packet connections and to free the ENET connection. It should be noted that although the ENET connection is freed from the connection maps, the actual ENET path is not physically freed	Connection 1 - FCM Holds sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Holds sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (free) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)

Table 2 Core connectivity connection operations

Connection Operation	Description	Actions taken
Restore connection	Restore both the packet connection and then to make a new ENET connection.	Connection 1 - FCM Restores sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Restores sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (make) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
Hold as pending move	Free the HOLDING side connection (endpoint that is leaving the call) and freeing the bridge on the holding side. Then hold the HELD side (endpoint that is staying in the call). It should be noted that although the internal connection is freed from the connection maps, the actual ENET path is not physically freed	Connection 1 - FCM Breaks sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Holds sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (free) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
Move connection (1 existing IW bridge requiring adding a new IW bridge)	Reuse the bridge connected with the FROM agent, and acquire a bridge for the new TO agent.	Connection 1 - FCM Restores sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - FCM Makes sent • TO endpoint (NET_IP) • Bridge # 2 endpoint (NET_IP) Connection 3 - ENET control (Make) sent • Bridge #1 endpoint (ENET) • Bridge #2 endpoint (ENET)
Move connection (1 existing bridge requiring removing the existing bridge)	Remove the bridge connected with the FROM agent, and connect the two packet agents directly. Note that the connection map collapses from three connections to just one.	Connection 1 - FCM Moves sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) • TO endpoint (NET_AAL1)

Table 2 Core connectivity connection operations

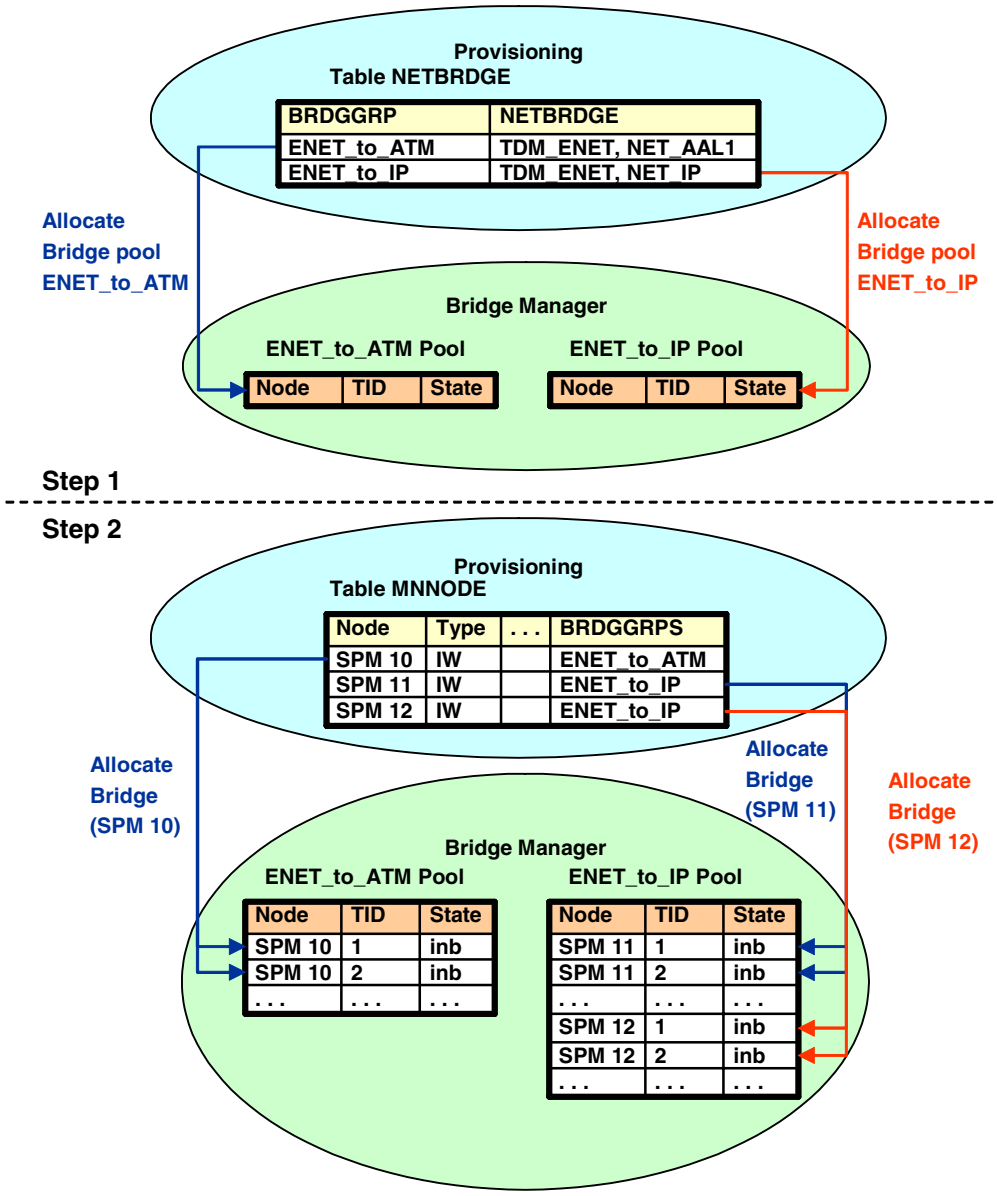
Connection Operation	Description	Actions taken
Move connection (1 existing bridge requiring maintaining existing bridge)	Keep the bridge connected with the FROM agent, and make a connection through the ENET to the TO agent. Note that the connection map collapses from three connections to two connections.	Connection 1 - FCM Restores sent • FROM endpoint (NET_AAL1) • Bridge #1 endpoint (NET_AAL1) Connection 2 - ENET control (Make) sent • Bridge #1 endpoint (ENET) • TO endpoint (ENET)

121.3.2.4 IW Bridge management

IW bridge management is a function in the CS2000 Call Server that manages the pool of IW SPM bridges. Prior to SN07, a single, office-wide pool of available IW bridges was managed by this utility. Each IW bridge node is composed of four groups of 512 bridge endpoints each. When an IW bridge node was provisioned in Table MNNODE, a set of four groups of 512 endpoints were added to the bridge pool. As the group of 512 endpoints was brought into service, these endpoints became available for Core Connectivity to use. The bridge manager function interfaced with maintenance and Core Connectivity to manage the set of available IW bridge endpoints in the office.

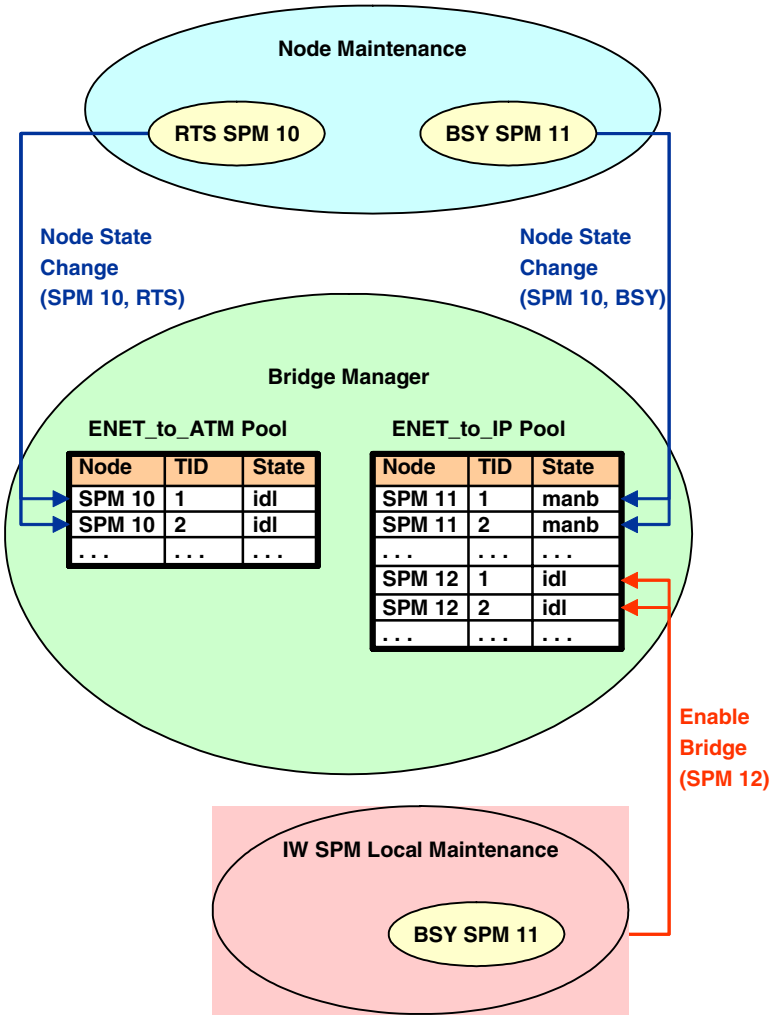
In SN07, the office-wide, single bridge pool is changed to support multiple bridge pools in a single CS2000 Call Server. A bridge pool is created when it is datafilled in Table NETBRDGE. Individual IW bridge nodes are added (still in the 4 groups of 512 endpoints each) as they are provisioned in Table MNNODE against the newly created bridge pool.

Figure 22 IW bridge pool creation



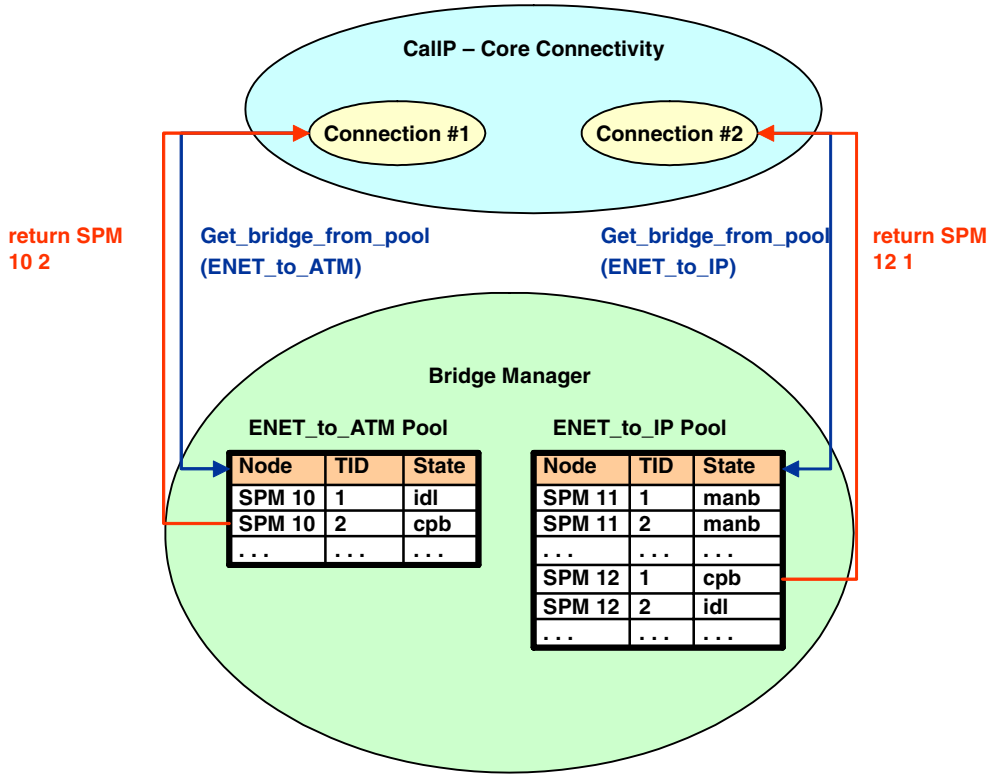
Once the bridge pools are created through provisioning, the individual IW bridge nodes are brought into service. This causes the nodes in the associated bridge pool to become available for use.

Figure 23 IW bridge maintenance



With idle IW bridge endpoints available in their associated bridge pools, the Bridge Manager can respond to requests from Core Connectivity to get a bridge. If more that one bridge is needed for a connection request, the Core Connectivity makes a request for each bridge needed.

Figure 24 IW bridge request



121.3.2.5 OAM changes on the CS2000 Call Server

OAM changes associated with the support of multiple bearer networks are limited in SN07. It is recognized that many additional requirements should be implemented and will be addressed in a future release.

In SN07, this feature does address the following areas:

- Multiple IW bridge pool OAM
- Trunk group OAM
- DPT OAM
- Office-wide usage OAM

Since many of these changes have impacts to customer OSSMINE interfaces, the activation of these changes is controlled by a new office parameter, MULTINET_DISPLAY_ACTIVE. Setting this parameter to ‘Y’ allows these changes to be visible. Setting this parameter to ‘N’ hides these changes. Note that this parameter does not impact the ability to support call connections between multiple bearer networks.

121.3.2.5.1 Multiple IW bridge pool OAM In SN07 with the support of multiple bridge pools, changes are made to the IWBM 800 series logs. These

logs are generated to monitor the usage thresholding of the bridge pools in the office. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then a new information line is output indicating the associated bridge pool that is causing the generation of the log. Refer to the Fault Management section of the document for more information.

Figure 25 IWBM 800 log example

```
RTP7  **  IWBM800 SEP17  12:16:55  6600  1st Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 70 percent of all bridges in the pool.
           Total number of IW bridges:  2016
           Number of available IW bridges: <NN>
           Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

In addition to the modified IWBM 800 logs, a new OM group (IWBMNODE) is created. IWBMNODE provides a set of registers for each IW bridge node provisioned in the CS2000 Call Server. It contains registers to monitor the following usage information:

- Number of attempts to get a bridge
- Number of failures to get a bridge
- Number of get bridge aborts
- Number of attempts to free a bridge
- Number of failures to free a bridge
- Number of free bridge aborts
- Number of times a bridge was used to connect to a test facility
- Number of times a bridge was used to connect to an announcement or conference facility
- Number of times a bridge was used to connect to a line
- Number of times a bridge was used to connect to a trunk

In order to get a view of the usage for the entire bridge pool, the individual bridge node information will have to be summed. Note that the associated bridge pool name is included in the OM group for each node. Refer to the Performance Management section of the document for more details.

Note that the value of MULTINET_DISPLAY_ACTIVE office parameter does not impact the availability of this OM group. It is always available in SN07.

Figure 26 IWBMNODE OM group example

```
>omshow iwbmnode active

IWBMNODE

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (IWBMNODE_SPM_INFO)
            IWGBATT      IWGBATT2      IWGBFAIL      IWGBABRT
            IWFBATT      IWFBATT2      IWFBFAIL      IWFBABRT
            IWBTLTST     IWBCNFAN      IWBCALLN      IWBCLTRK

0
   SPM  1    IW     ENET_TO_ATM
               0              0              0              0
               0              0              0              0
               0              0              0              0

1
   SPM 10   IW     ENET_TO_IP
               0              0              0              0
               0              0              0              0
               0              0              0              0
```

121.3.2.5.2 Trunk group OAM With support for multiple bearer networks, a trunk group can be configured to have members is multiple bearer networks. The existing TRK and TRNK2 OM groups only provide data on a per trunk group basis. When office parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’, then new OM groups (TRK2NET1 and TRK2NET2) are created to provide a per trunk group and per bearer network view of the trunk group usage.

OM group TRK2NET1 contains the same set of registers that existing OM group TRK contains. It contains registers to monitor the following usage information:

- Automatic congestion control
- Invalid or no automatic number identification (ANI)
- Answered call usage
- Number of calls answered
- Automatic number identification (ANI) office failure

- Number of successful connections
- Network management reroutes
- Directional reservation
- Glare
- Answer messages sent and received on incoming trunks
- Answer messages sent and received usage on incoming trunks
- Total incoming attempts
- Incoming failures
- Maintenance busy usage
- Total outgoing attempts
- No answer on trunk (timed out)
- Number of overflows, all trunks busy
- Answer messages sent and received on outgoing trunks
- Outgoing failures
- Outgoing matching failures
- Pre-route abandons
- Protective reservation usage
- System busy usage
- Number of tandem calls
- Total usage
- Traffic busy usage

Figure 27 TRK2NET1 OM group example

```
>omshow trk2net1 active
TRK2NET1
CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;
   KEY (COMMON_LANUAGE_NAME_BEARNETS)
   INFO (OM2TRKINFO)
            INCATOT      PRERTEAB     INFAIL       NATTMPT
            NOVFLATB     GLARE        OUTFAIL      DEFLDCA
            DREU         PREU         TRU          SBU
            MBU          OUTMTCHF     CONNECT      TANDEM
            AOF          ANF          TOTU         ANSWER
            ACCCONG      NOANSWER     INANSWER     OUTANSU
            INANSU
100   TRK_TO_A NET 0 TDM_ENET
  2W    0     0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0
100   TRK_TO_A NET 1 NET_AAL1
  2W    0     0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0
100   TRK_TO_A NET 2 NET_IP
  2W    0     0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0              0              0              0
            0
```

OM group TRK2NET2 contains the same set of registers that existing OM group TRNK2 contains. It contains registers to monitor the following usage information:

- Number of calls answered (extension from TRK2NET1)
- Number of successful connections (extension from TRK2NET1)
- Network management reroutes (extension from TRK2NET1)
- Directional reservation (extension from TRK2NET1)
- Total incoming attempts (extension from TRK2NET1)
- Total outgoing attempts (extension from TRK2NET1)
- System busy usage (extension from TRK2NET1)
- Number of tandem calls (extension from TRK2NET1)
- Total usage (extension from TRK2NET1)
- Traffic busy usage (extension from TRK2NET1)

Figure 28 TRK2NET2 OM Group Display

```
>omshow trk2net2 active

TRK2NET2

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   KEY (TRK2NET_KEY)
   INFO (OM2TRKINFO)
            INCATOT2      NATTMPT2     DEFLDCA2      TRU2
            SBU2          CONNECT2     TANDEM2       TOTU2
            ANSWER2

100   TRK_TO_A      NET 0 TDM_ENET
  2W    0     0
            0             0             0             0
            0             0             0             0
            0

100   TRK_TO_A      NET 1 NET_AAL1
  2W    0     0
            0             0             0             0
            0             0             0             0
            0

100   TRK_TO_A      NET 2 NET_IP
  2W    0     0
            0             0             0             0
            0             0             0             0
            0
```

121.3.2.5.3 DPT OAM In providing support for multiple bearer networks, a requirement to support both BICC and SIP-T DPT protocols in the same office was also requested. Prior to SN07, the DPT OM groups did not indicate the associated DPT protocol.

In SN07, when office parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’, then the following changes are made:

- Provide an office-wide, per-protocol DPT performance summary
- Provide a per-DPT node, per-protocol DPT performance summary

A new OM group (DPTOFCP) is created to provide an office-wide, per-DPT protocol performance summary. This group is modeled after the DPTOFC OM group and contains the same set of registers. Two DPT protocols are supported: BICC and SIP-T. The following registers are included per protocol:

- Get DPT terminal attempts
- Get DPT terminal failures
- Get DPT optimized terminal failures
- DPT terminal usage
- DPT terminal usage high water mark
- DPT port depletion

Figure 29 DPTOFCP OM group example

```
>omshow dptofcp active

DPTOFCP

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PROTOCOL_INFO)
            DPGTAT      DPGTAT2     DPGTFL      DPGTFL2
            DPUSAG      DPUSAG2     DPGTFLO     DPGTFLO2
            DPHWT       DPHWT2      DPDPL       DPDPL2

0
   BICC
            0           0           0           0
            0           0           0           0
            0           0           0           0

1
   SIPT
            0           0           0           0
            0           0           0           0
            0           0           0           0
```

Changes are made to the existing DPTNODE OM group. This OM group provides a per-DPT node performance summary. In SN07, each DPT node can only support one DPT protocol. For example, a DPT capable MG4K node can only support BICC. DPT GWC nodes can support either BICC or SIP-T but not at the same time. When MULTINET_DISPLAY_ACTIVE is set to ‘Y’,

additional information is added to the DPTNODE OM group to display the following additional information:

- DPT protocol
- For SPM-type nodes, the associated bearer network and SPM node type are also displayed[1]

Figure 30 DPTNODE OM group example

```
>omshow dptnode active

DPTNODE

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PM_INFO)
            DPTGTAT       DPTGTAT2      DPTGTFL       DPTGTFLO
            DPTUSAG       DPTUSAG2      DPTHWT

0
   GWC  3    93 BICC
               0              0              0              0
               0              0              0

1
   GWC   4   94 SIPT
               0              0              0              0
               0              0              0

2
   SPM    1   70 NET 2 NET_AAL1 BICC SMG4
               0              0              0              0
               0              0              0
3
   SPM    2   71 NET 0 ENET_TO_AAL1_DPT   BICC     DPT
              0              0              0              0
               0              0              0
```

121.3.2.5.4 Office-wide usage OAM With support for multiple bearer networks, it is a requirement to be able to monitor the performance of the traffic over each bearer network. The existing OFZ and OFZ2 OM groups only

[1]DPT GWCs are considered bearer independent, so the associated bearer network is not included for DPT GWCs.

provide an office-wide view. When office parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’, then new OM groups (OFZ2NET1 and OFZ2NET2) are created to provide a per bearer network view of office traffic.

OM group OFZ2NET1 contains the same set of registers that existing OM group OFZ contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- Incoming trunk subscriber abandoned calls
- Incoming trunk switch abandoned calls
- Incoming trunk calls routed to an announcement
- Incoming trunk calls routed to a tone
- Incoming trunk calls to lock-out
- Incoming trunk calls to outgoing trunk calls
- Incoming trunk calls to terminating line calls
- Lines manual busy
- Number of incoming trunk calls
- Number of originating line calls
- Originating line switch abandoned calls
- Originating line calls routed to an announcement
- Originating line calls to lock-out
- Originating line calls to outgoing trunk calls
- Originating line calls routed to a tone
- Originating line calls to terminating line calls
- Outgoing trunk match failures
- Outgoing trunk network attempts
- Outgoing trunk original seize failures
- Outgoing trunk retrial match failures
- Outgoing trunk retrial seize failures
- Terminating line blocked
- Terminating line match failures
- Terminating line network attempts

Figure 31 OFZ2NET1 OM group example

```
>omshow ofz2net1 active
OFZ2NET1
CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;
   INFO (BEARNETS_INFO)
          INANN          INLKT          INOUT          INOUT2
          INTONE         NIN            NIN2           OUTNWAT
          OUTNWAT2       OUTMFL         OUTRMFL        OUTOSF
          OUTROSF        INABNM         INABNC         ORIGANN
          ORIGLKT        ORIGOUT        ORIGOUT2       ORIGTRM
          ORIGTRM2       ORIGTONE       NORIG          NORIG2
          INTRM          INTRM2         TRMNWAT        TRMNWAT2
          TRMMFL         TRMBLK         LNMBPC         ORIGABDN
0
     NET 0 TDM_ENET
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
1
     NET 1 NET_AAL1
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
2
     NET 2 NET_IP
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
```

OM group OFZ2NET2 contains the same set of registers that existing OM group OFZ2 contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- No circuits available on business network trunks
- No circuits available on inward dial trunks
- No circuits available on intermachine trunks
- No circuits available on intertoll trunks
- No circuits available on local tandem trunks
- No circuits available on offnet trunks
- No circuits available on connect trunks
- No circuits available on toll completing trunks
- No circuits available on circuit trunks
- No circuits available on all other trunks
- Calls routed to GNCT treatment
- Switch originated partial dial calls
- Switch originated calls to permanent signal treatment

Figure 32 OFZ2NET2 OM group example

```
>omshow ofz2net2 active
OFZ2NET2

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (BEARNETS_INFO)
            OFZNCIT       OFZNCTC       OFZNCLT       OFZNCBN
            OFZNCID       OFZNOSC       OFZNCOT       OFZNCRT
            OFZNCIM       OFZNCON       OFZNCOF       PSGM
            PDLM           DPTR          DPTR2

0
NET 0 TDM_ENET
            0             0             0             0
            0             0             0             0
            0             0             0             0
            0             0             0
1
NET 1 NET_AAL1
            0             0             0             0
            0             0             0             0
            0             0             0             0
            0             0             0
2
NET 2 NET_IP
            0             0             0             0
            0             0             0             0
            0             0             0             0
            0             0             0
```

121.3.2.6 Lawful Intercept

Lawful Interception is the ability to perform call monitoring on selected agents. Call monitoring includes;

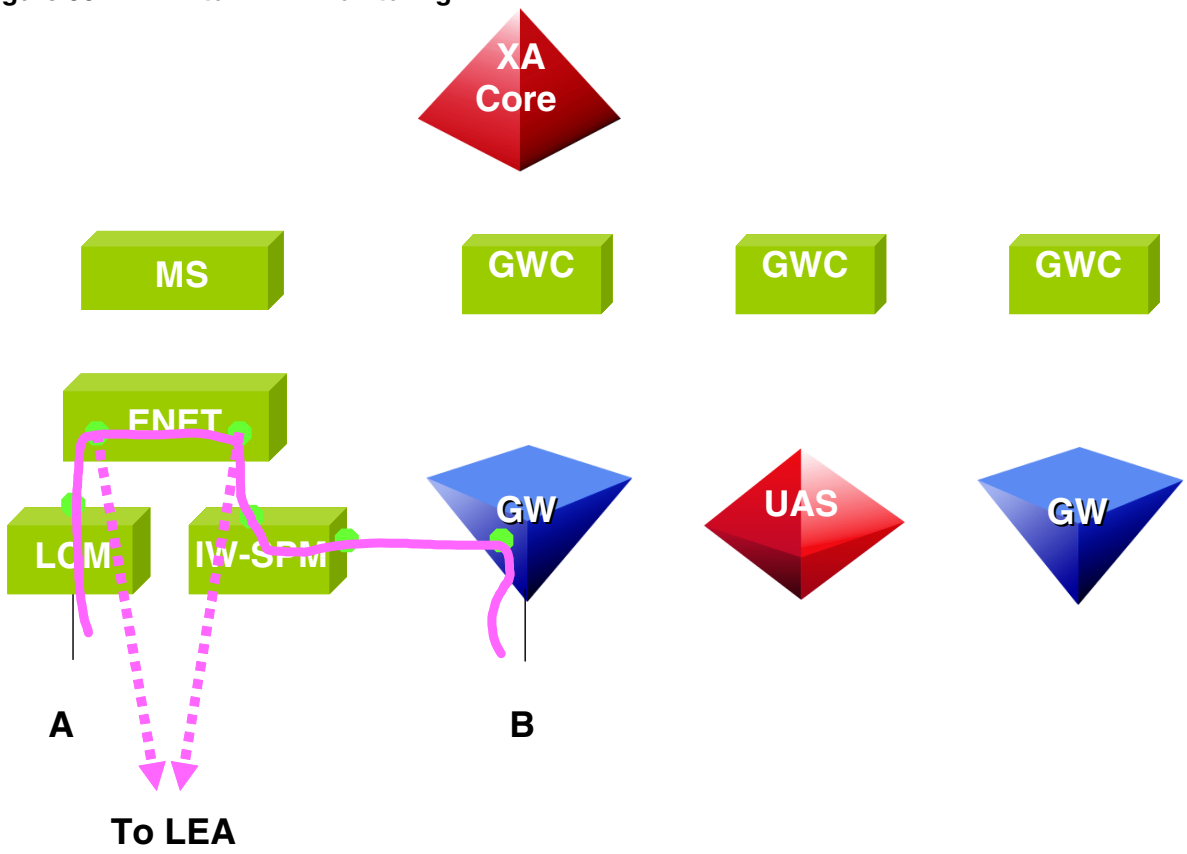
- Call Data monitoring - reporting details about monitored calls (e.g. time of the call, dialled digits, parties involved, etc.)
- Call Content monitoring - delivery of both sides of a monitored conversation to law enforcement

With support for multiple bearer network in a single CS2000 Call Server, lawful intercept must provide the ability to do Call Content monitoring on all

required call types and all supported bearer connections. Previous to SN07, Call content monitoring was supported for the following call types:

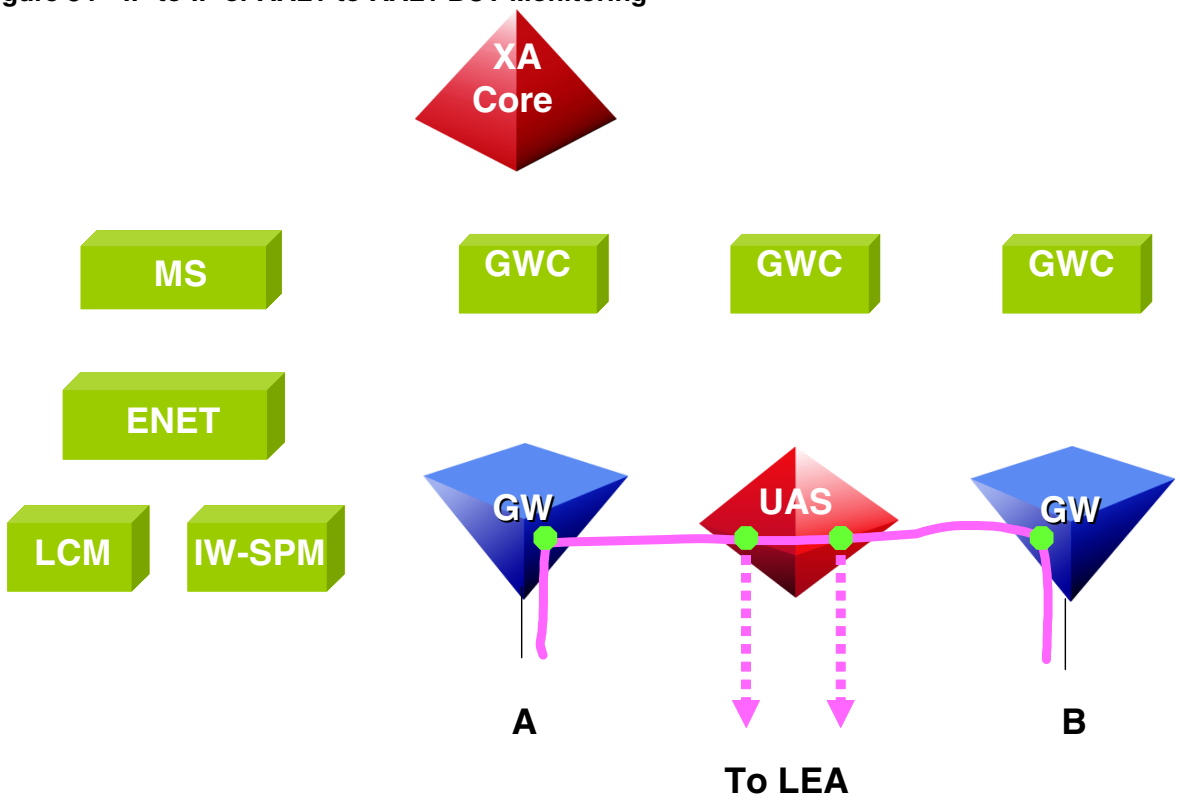
- ENET-to-ENET: replicas are attached to the primary ENET pathends which broadcast the transmit of each endpoint (legacy monitoring)

Figure 33 ENET-to-ENET Monitoring



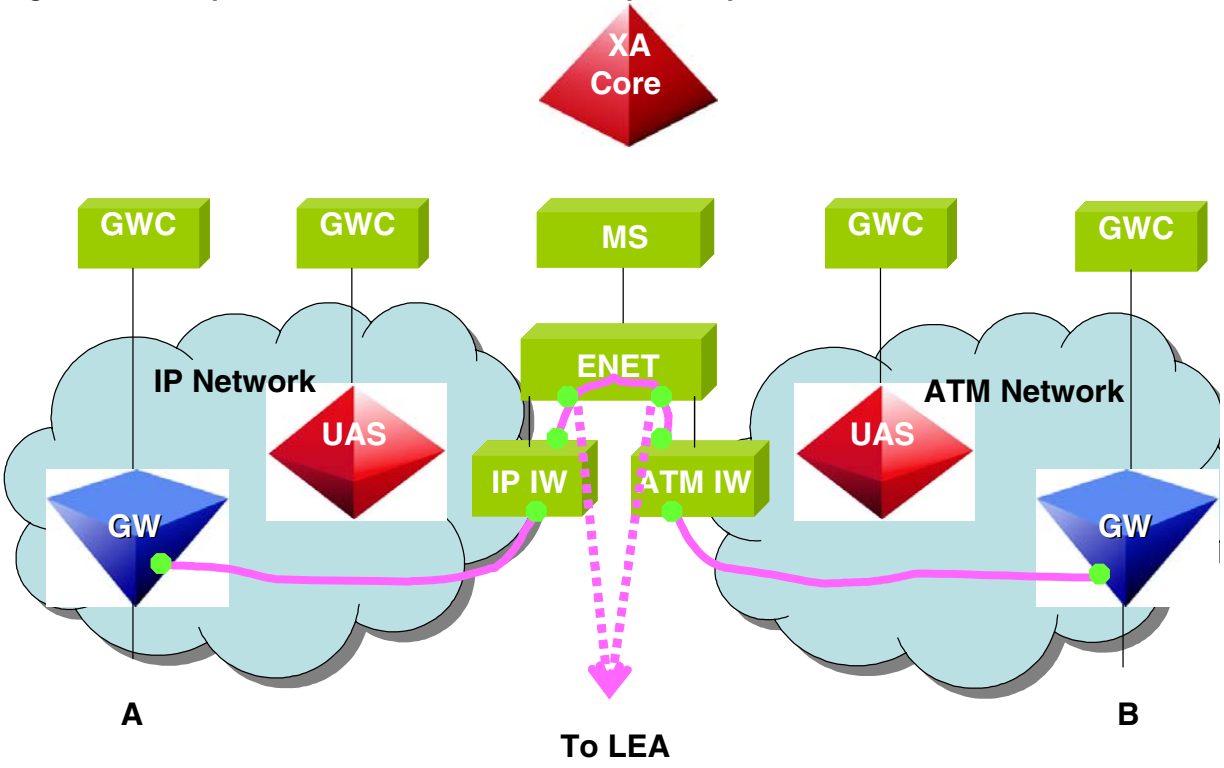
- IP-to-IP: primary call is tandemed through a Centralized Replicator (CR) to which replicas are attached. This functionality is known as Bearer Channel Tandeming (BCT).
- AAL1-to-AAL1: when BCT is active, the same strategy is used as in IP-to-IP calls. If not, then broadcast connections are attempted. This works for Packet Trunking - AAL1 solutions where the only AAL1-to-AAL1 calls involve MG4Ks which support broadcast connections.

Figure 34 IP-to-IP or AAL1-to-AAL1 BCT Monitoring



In SN07, there are no impacts to the replication models that are used to lawful intercept. Since the connection model for supporting a packet bearer network 1 to packet bearer network 2 connection involves using 2 IW SPM bridges, lawful intercept will used the ENET-to-ENET model to perform replication. Refer to the following figure for an example connection with lawful intercept.

Figure 35 Multiple bearer network lawful intercept example



In summary, this means that in a CS2000 Call Server that supports three bearer networks (ENET, AAL1 and IP), that the following replication points will be used:

- ENET
  - — for ENET-to-ENET calls
  - — for AAL1-to-IP calls
  - — for ENET-to-AAL1 calls
  - — for ENET-to-IP calls
- UAS IP
  - — for IP-to-IP calls
- UAS AAL1
  - — for AAL1-to-AAL1 calls[1]

121.3.2.7 Trunk selection (like network selection)

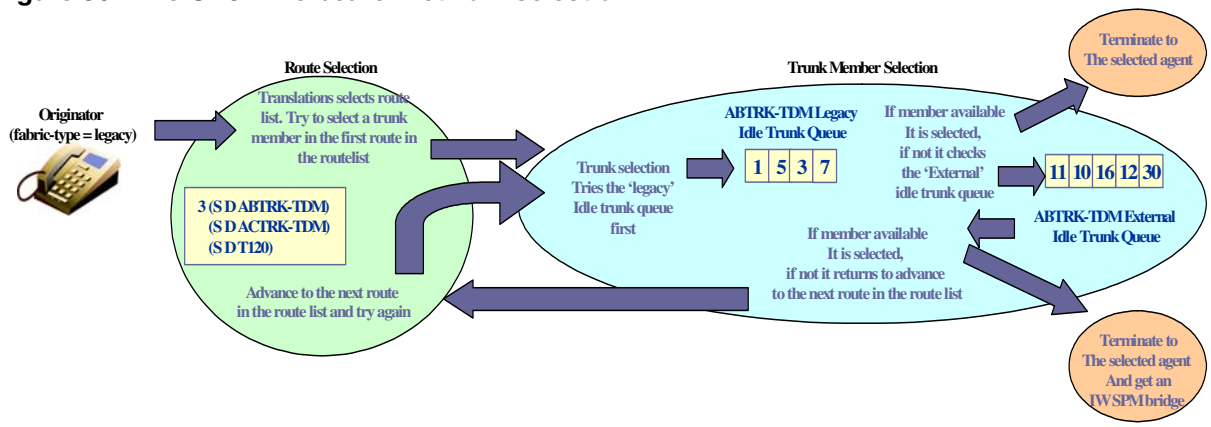
Prior to SN07, the CS2000 Call Server tried to optimize bearer network connections by trying to select a trunk member whose bearer network matched the bearer network of the originating agent. Since there were only two bearer

[1]If the call involves only 2 MG4Ks, then the UAS is not needed (MG4Ks can broadcast the bearer path). But if an MG9K is involved, then the UAS is required.

networks supported (‘internal’ and ‘external’), the trunk selection utility internally maintained an idle trunk queue for each of the two bearer networks. When a request was made to select a trunk member, the trunk selection utility would determine the bearer network of the originating agent and then traverse the ‘matching’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

If it did not find a member, it would search the ‘other’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If both queues are checked and no available member can be found, then the request is returned with an indication that the call should advance to the next route in the route list.

Figure 36 Pre-SN07 like bearer network selection

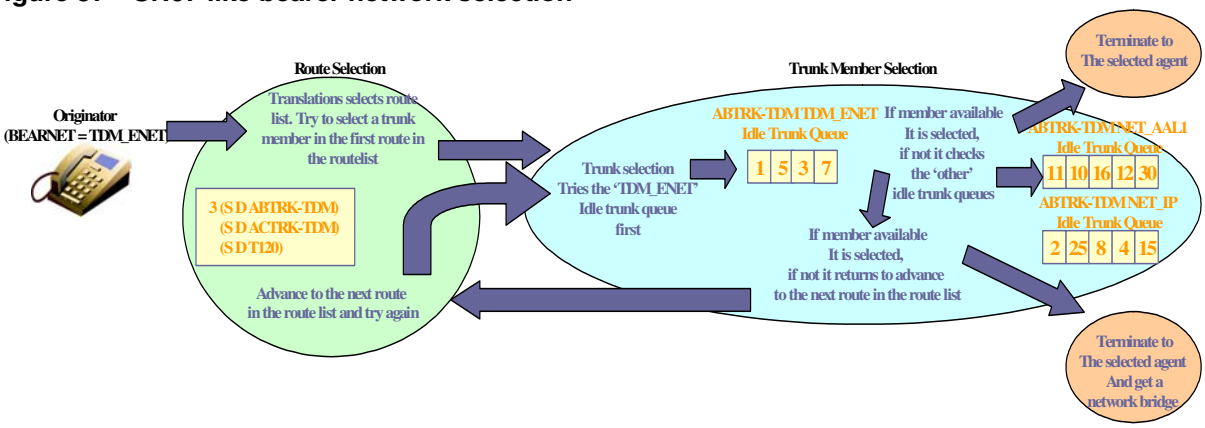


In SN07, the trunk selection utility is changed to support multiple bearer networks (i.e., more that two). When a request was made to select a trunk member, the trunk selection utility determines the bearer network of the originating agent and then traverses the ‘matching’ bearer network’s idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

If it did not find a member, it would search the ‘next’ bearer network’s idle trunk queue looking for an available trunk member. The ‘next’ bearer network is determined by the order that the bearer networks are datafilled in Table BEARNETS. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If it did not find a member, it would continue searching it’s idle trunk queues in the

Table BEARNETS bearer network order until it either found an available member or exhausted all of its queues. If all queues are exhausted, then the request is returned with an indication that the call should advance to the next route in the route list.

Figure 37 SN07 like bearer network selection



The following is an example trunk selection request.

- Originating agent's bearer network = NET_AAL1
- Table BEARNETS datafill
  - — NET 0 TDM_ENET . . .
  - — NET 1 NET_AAL1 . . .
  - — NET 2 NET_IP
- Terminating trunk group has members in all three bearer networks

The following is the order that the trunk selection utility will try to find an available trunk member:

1. Trunk group members in the NET_AAL1 bearer network
   - — This is first because this is the originator's bearer network.
2. Trunk group members in the TDM_ENET bearer network
   - — This is second because it is the first entry in Table BEARNETS.
3. Trunk group members in the NET_IP bearer network
   - — This is third because this is the third entry in Table BEARNETS. Note that the second entry in Table BEARNETS had already been attempted.

121.3.2.8 DPT (BICC and SIP-T) interworking including audible ringing support

Providing support for both BICC and SIP-T DPT protocols in the same CS2000 Call Server impacts the following areas:

- DPT terminal selection
- DPT audible ringing support

121.3.2.8.1 DPT terminal selection The algorithm for determining which node to host a DPT trunk call differs for BICC and SIP-T. Now that both are supported in the same CS2000 Call Server, this feature must ensure that both function properly.

Changes are needed for the BICC DPT terminal selection algorithms to make sure the bearer network of the hosting DPT capable node matches the bearer network of the DPT trunk group that was selected in translations.

The following table defines the algorithms for each protocol.

Table 3

DPT Protocol	Direction	Algorithm
SIP-T	outgoing	CS2000 Call Server selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRINV and SERVSINV). Note that the bearer network of the DPT trunk group does not factor into the selection process.
SIP-T	incoming	The VRDN GWC selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRINV and SERVSINV). The VRDN GWC builds it list of available SIP-T GWCs because the SIP-T GWCs register with it. BICC GWCs do not register with the VRDN GWC.

Table 3

DPT Protocol	Direction	Algorithm
BICC	outgoing	CS2000 Call Server tries to put the DPT trunk on the most optimized BICC DPT capable node. BICC DPT capable nodes include the following: • BICC GWCs (bearer network independent) • MG4Ks (with an associated bearer network) • DPT SPMs (with an associated bearer network) If the originating agent is on the MG9K, then a BICC GWC is selected. Note that the bearer network of the DPT trunk group does not factor into the selection process because BICC GWCs can support any bearer network. If the originating agent is on the MG4K, then that same MG4K is selected provided the bearer network of the DPT trunk group matches the bearer network of the MG4K. If the bearer network of the DPT trunk group does not match the bearer network of that same MG4K, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get another MG4K that does support the DPT trunk group's bearer network. If the originating agent is on a legacy peripheral, then the DPT SPM is selected (if present) provided the bearer network of the DPT trunk group matches the bearer network of the DPT SPM. If the bearer network of the DPT trunk group does not match the bearer network of any DPT SPM in the office, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get any MG4K that does support the DPT trunk group's bearer network.

Table 3

DPT Protocol	Direction	Algorithm
BICC	incoming	Prior to SN07, the CS2000 Call Server attempts to initially put the DPT terminal on an MG4K for message normalization and then will move it to the most optimized location based upon what agent the call terminates to. The reason for doing this was to provide a hosting node that had the ability to play tones and collect digits in the case where a service was invoked prior to digit translations and line/trunk termination. In SN07, the CS2000 Call Server continues to place the DPT terminal on an MG4K or DPT SPM for normalization. However, this MG4K/DPT SPM's associated bearer network must now match the bearer network of the incoming BICC DPT trunk group. If no match can be found, then the call is sent to a BICC GWC to be normalized. Note that this leaves no place to support tones and digit collection for those services that may be invoked prior to agent termination. Once the DPT call is normalized, the CS2000 Call Server attempts to optimize the location of the DPT context based on the terminating agent in the call. If the terminating agent is on an MG9K, then the DPT context is moved to a BICC GWC. Note that the bearer network of the BICC DPT trunk group does not factor into the optimization process because BICC GWCs can support any bearer network. If the terminating agent is on an MG4K, then the DPT context will be moved to that MG4K provided the bearer network of the terminating agent's MG4K matches the bearer network of the BICC DPT trunk group. If it does not match, then the DPT context remains where it is (i.e., where it was normalized). If the terminating agent is on a legacy peripheral, then the DPT context will be moved to a DPT SPM (if present) provided the bearer network of the DPT SPM matches the bearer network of the BICC DPT trunk group. If a DPT SPM cannot be found, then the DPT context is moved to a BICC GWC and an IW SPM bridge from the associated bridge pool is used to connect the bearer network of the DPT trunk group and the legacy peripheral. If a BICC GWC is not present, then the call remains where it is (i.e., where is was normalized) and an IW SPM bridge from the associated bridge pool is used.

121.3.2.8.2 DPT audible ringing support The means for providing audible ringing on egress DPT trunk calls differs based upon the DPT protocol being used. Now that both protocols are support in the same CS2000 Call Server, care is taken to ensure that audible ringing functions properly is all scenarios, including bearer network interworking scenarios.

On an incoming DPT SIP-T trunk call where the DPT SIP-T trunk is asked to apply audible ringing, the DPT SIP-T trunk uses Remote Bearer Control (RBC) to ask the originating call server to apply the audible ringing tone on its behalf. On an incoming DPT BICC trunk, the DPT BICC trunk uses Bearer Channel Proxy - No-Anchor (BCP-NA) to ask the terminating gateway to apply audible ringing back towards the originating call server. The following table illustrates the scenarios and how audible is applied.

Table 4 DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
Line (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Line GW towards the line agent
Trunk (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Trunk GW towards the trunk agent
DPT BICC (NET_AAL1)	Line (TDM_ENET)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	Line (NET_AAL1)	BCP-NA used to ask the MG9K to apply audible ringing towards the AAL1 network

Table 4 DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
DPT BICC (NET_AAL1)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	Line (NET_IP)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (TDM_ENET)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_AAL1)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_IP)	BCP-NA used to ask the line gateway to apply audible ringing towards the IP network. If it cannot accomodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.
DPT BICC (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
DPT SIP-T (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible riging is applied in the next call server.

121.3.2.9 Translations and Routing changes

With support for multiple bearer networks, there is an assumption that calls should remains on the same bearer network as much as possible. Given this assumption, the following changes are made in SN07:

- Routing based upon the bearer network
- TRAVER modifications to support multiple bearer networks

121.3.2.9.1 Routing based upon the bearer network Prior to SN07, the PKT conditional route selector allowed the customer to force routing between the ENET and the packet bearer network. In SN07, this selector is replaced by two new conditional route selectors:

- FABRIC
- BEARNET

The FABRIC conditional route selector replaces the PKT conditional route selector. During translations and routing, the fabric of the originating agent's bearer network is examnied and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network fabric. During the ONP to SN07, the FABRIC selector replaces any PKT selectors found.

The BEARNET conditional route selector is new in SN07. During translations and routing, the originating agent's bearer network is examnied and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network.

Refer to the Configuration section of the document for additional information.

Figure 38 Conditional routing example datafill

```
TABLE: OFRT
-------------------------------------------------------
100 (CND FABRIC ENET ST 200) (CND FABRIC AAL1 ST 201)
    (CND FABRIC IP ST 202) $
101 (CND BEARNET TDM_ENET ST 200) (CND BEARNET NET_AAL1 ST 201)
    (CND BEARNET NET_IP ST 202) $
```

121.3.2.9.2 TRAVER modifications to support multiple bearer networks In order to support the new conditional route selectors described above, changes are needed in TRAVER to provide the correct route selection. In SN07, TRAVER needs to determine either the fabric or the bearer network of the originating agent.

If the originating agent is a line, then TRAVER will identify the fabric or bearer network and apply that knowledge to any FABRIC or BEARNET conditional route selectors that it finds.

If the originating agent is a trunk group, then TRAVER identify the fabric or the bearer network. However, a trunk group does not have a fabric or bearer network designation. That designation is done at the trunk member level. Therefore, changes are made to TRAVER to allow either a trunk member to be specified explicitly or to specify the bearer network to use for the originating trunk group. The existing TRAVER option TRKMEM is modified to include the determination of the associated bearer network. A new option, BEARNET, as added to support the bearer network designation for a trunk group[1].

Refer to the Configuration section of the document for additional information.

[1]TRAVER determines the fabric based upon the associated bearer network.

121.3.2.10 USP messaging

In SN07, the USP is an optional component. When it is present, it provides the connection from the CS2000 Call Server to the SS7 network. ISUP signaling messages and TCAP transaction messages traverse through the USP interface.

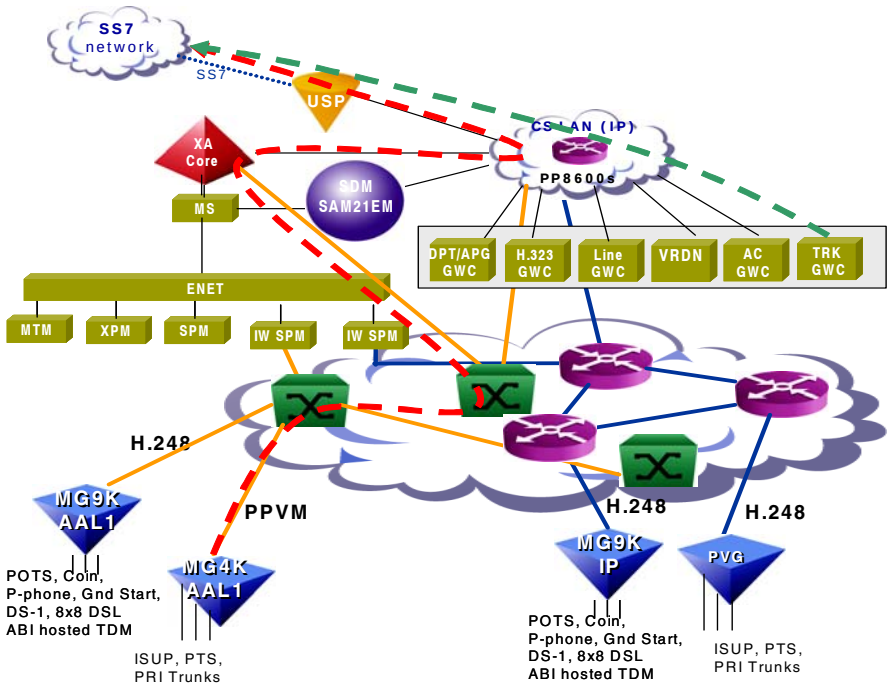
TCAP transaction messages are always generated by the CS2000 Call Server. However, ISUP signaling messages are generated from the ISUP trunk peripherals. The path that the ISUP message takes to get to the USP varies based upon the type of trunk peripheral.

Table 5 USP messaging path for ISUP signaling messages

ISUP trunk peripheral	USP messaging path
GWC	GWC -> CS LAN -> USP
MG4K (AAL1)	MG4K -> AAL1 bearer network -> CS2000 -> CS LAN -> USP
DPT SPM (AAL1)	DPT SPM -> CS2000 -> CS LAN -> USP
legacy peripheral	Legacy peripheral -> CS2000 -> CS LAN -> USP

The USP supports multiple messaging paths and defines them on a per node basis.

Figure 39 USP messaging paths



121.3.2.11 ECAN across multiple bearer networks

Echo cancellation (ECAN) can be applied differently in each bearer network. In an IP bearer network, the packet latency is generally large enough to require 100% ECAN. ECAN is only turned off if an individual call requires that it be turned off (i.e., FAX call).

In an AAL1 bearer network, the packet latency may not be large enough to require ECAN. ECAN in the AAL1 network is generally expensive hardware to purchase and would like to be avoided, if possible.

Prior to SN07, the CS2000 Call Server implemented an office parameter, ECAN_EDGE_STRATEGY to control the ECAN behavior for the office. In SN07, this office parameter is replaced by a new option in Table BEARNETS that allows the ECAN strategy to be defined per bearer network.

Refer to feature A00004046: Echo Cancellation Support for TriModal Call Server 2000 for more information on ECAN.

121.3.2.12 Voice quality

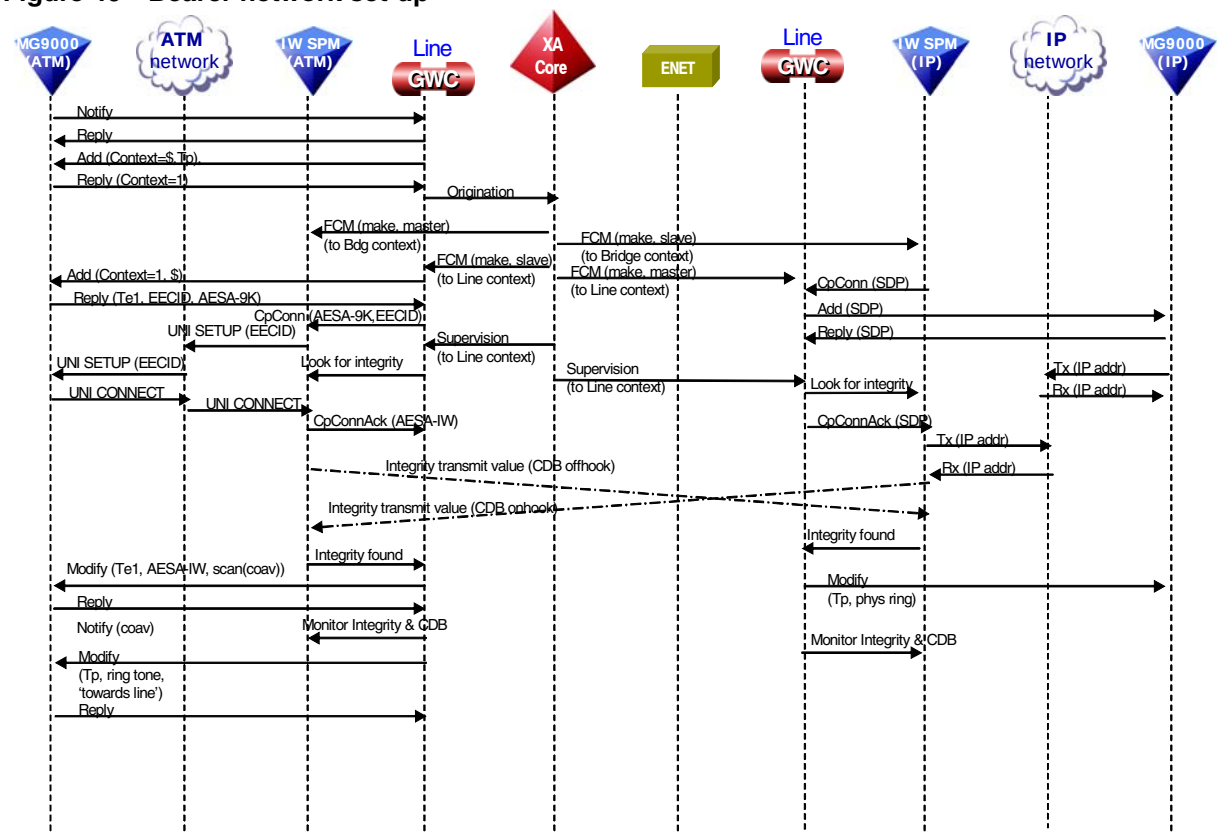
In supporting the connections between packet bearer networks using multiple IW bridges, the voice quality may experience some degradation. The following areas are of concern:

- Possible speech clipping
- Latency and delay

121.3.2.12.1 Possible speech clipping By providing support for multiple bearer networks, the connection set-up times may be very different for each bearer network. It may be possible to set up a bearer connection is one network, ring the line and have the subscriber answer and begin talking prior to the connection being set-up in the other bearer network.

To prevent this from happening, changes are made to the IW SPM to delay sending integrity through the ENET until the packet bearer connection is set-up. This causes the ‘other’ IW SPM to not find integrity and report integrity found to it’s connection peer until the packet bearer network connection has been established. The line GWC will not start physical ringing until it’s connection peer returns that integrity has been found.

Figure 40 Bearer network set-up



121.3.2.12.2 Latency and delay Latency and delay are concerned with how long it takes for a packet of voice to transit the bearer network(s) from end to end. Generally, there is a budget of 150 ms given to a packet. If the delay increases past 150 ms, then the possibility of the end subscribers talking over top of each other increases. The following factors effect the latency and delay that a packet experiences:

- packetization rate and jitter buffer
- transcoding delay
- ECAN
- IP routers
- overall distance travelled

The following tables provides a few examples of latency.

Table 6 MG9K IP to MG9K AAL1 call analysis

MG9K IP to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
MG9K IP packetization	10	20

Table 6 MG9K IP to MG9K AAL1 call analysis

MG9K IP to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
Leg 3 router hops, assume 3 routers	3	3
IP IW SPM jitter buffer	30	60
ENET	1	1
AAL1 IW packetization	6	6
MG9K AAL1 jitter buffer	2	2
Total latency	52	92

Table 7 H.323 to MG9K call analysis

H.323 to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
H.323 packetization	10	20
Leg 1 router hops (1 ms per router) assume worst case, 5 routers	5	5
Media Portal (1 ms assumed)	1	1
Leg 2 router hops, assume 1 router	1	1
PVG jitter buffer (3 x packetization rate)	30	60
PVG transcoding (G.729 to TDM)	5	5
PVG packetization	10	20
Leg 3 router hops, assume 3 routers	3	3
IP IW SPM jitter buffer	30	60
ENET	1	1
AAL1 IW packetization	6	6
MG9K AAL1 jitter buffer	2	2
Total latency	104	184

121.3.2.13 ONP

Given the changes made to the connectivity function in the CS2000 Call Server, they are applicable to all Succession configurations in SN07, regardless of how many bearer networks are supported. In order to preserve call processing over the ONP, the provisioning of Tables BEARNETS, NETBRDGE, NETPATH and NET2NET must be accomplished during the table transfer.

Refer to the Configuration section for more details on the ONP procedures.

121.4 Hardware Requirements or Dependencies

In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Table 8 Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	all Succession supported legacy peripherals	supported SN07 legacy peripherals which includes both lines and trunk
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC[a]	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
IP (CHS)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	GWC[b]	SIP-T DPT trunks
	H.323 GWs (Cisco, Westel, BCM, M1)	PRI trunks

a. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk support.
b. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk support.

121.5 Software Requirements or Dependencies

This feature requires SN07 North America XA-CORE load or later.

121.6 Limitations and restrictions

- In SN07, only one bearer network entry will be supported in table SERVRINV and it will be restricted to the default network because SESM will only support a single bearer network per GWC.
- In SN07, an IW bridge will be restricted to a single bridge pool.
- In SN07, only one bearer network entry will be associated for DPT SPM and it will be restricted to the default network.
- In SN07, only one bearer network entry will be associated for MG4K and it will be restricted to the default network.
- In SN07, the table TRKOPTS will be restricted to a single network and this network will be the default network.
- The datafill procedure proposed in table CLLI is only for documentation purpose in SN07.
- The maximum size of the table BEARNETS will be 8 tuples.
- The maximum size of the table NETBRDGE shall be 64 tuples.

The following list provides a view of the limitations associated with H.323 calls in this configuration:

- Multiple billing records generated - A call from am H.323 agent to an MG9000 AAL1 native line would be represented as two calls in the CS2000 call server, each generating its own billing record.
- H.323 agent access to announcements - Since there is no announcements accessible to the CHS IP network (i.e., no IP IW bridge supported), announcements cannot be played to the H.323 agent. Any CS2000 Call Server services will not be able to use announcements and any treatments will have to be configured to ‘release with cause’ and the announcement would be provided by the enterprise bearer network.
- H.323 agent access to conferencing - Since there is no conference circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), conferencing services cannot be supported to the H.323 agent.
- H.323 agent access to test trunk facilities - Since there is no test trunk circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), trunk tests cannot be supported to the H.323 gateway.

121.7 Interactions

N/A

121.8 Applicable customer facing sections

Fault Management

- Logs ___X__
- Alarms _____

Configuration

- Data Schema ___X___
- User Interface ___X___
- Element Management ___X__
- Security _____
- Service Order __n/a_
- Office Parameters ___X__

Accounting (includes AMA billing) __n/a_

Performance (includes operational measurements) ___X___

121.9 Glossary

Term	Explanation
AAL1	ATM Adaptation Layer 1
AAL2	ATM Adaptation Layer 2
ABI	Access Bridging Interface
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
CODEC	Coder DECoder
CS2K	Call Server 2000
CS2K - MT	Communication Server 20000 Management Tool

DPT	Dynamic Packet Trunk
DPT-SPM	Interworking SPM (ENET interface on the c-side, packet network on the p-side)
ECAN	Echo Cancellation
ENET	Enhanced Network
GUI	Graphic User Interface
GW	GateWay
GWC	GateWay Controller
GWC-EM	Gateway Controller Element Manager
H.323	ITU-T “umbrella” standard for multimedia communications.
IDL	Interface Definition Language
IP	Internet Protocol
IW	Interworking
IW-SPM	Interworking SPM (ENET interface on c-side, packet network on p-side)
JNET	Junctored Network
LGRP	Logical Group
MG4K	Media Gateway 4000 - SPM capable of supporting TDM trunks and DPTs. External network only, no ENET.
MSH	Multi-Service Hub Layer
NA	North America
NV	Network View
OSSDI	Operations Support System DAta Interface
SESM	Succession Element Sub-element Manager
SHR	SHaRed Layer
SIP-T	Session Initiated Protocol - Trunking
SMG4	SPM Media Gateway 4000
SNMP	Simple Network Management Protocol

SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
TL	Telecom Layer
TRKOPTS	TRunK OPTionS

122: Functional Description (FN): A00003951

This Functional Description (FN) covers the work required to support the i2001 Internet Telephone. The FN also covers the work required to support a common User Interface for the i2001, i2002and i2004.

The intended audience: CICM Design community, CICM Test community and Product Line Management.

Intended release: Series 7.0.

122.1 Description

The i2001 is a reduced functionality sibling of the i2002 to reduce cost of manufacture it has a smaller screen, fewer buttons and a cheaper build

The i2001 is also a Phase II Unistim Terminal. Currently the CICM supports Phase I Terminals, as part of the scope of this feature, existing support for the i2002 and i2004 Phase I Terminals will be updated to support the new range of Phase II i2002 and i2004's.

Phase 1 terminals will be MD when the Phase II terminals become available so support for the whole range of Phase II terminals (i2001, i2002 and i2004) on the CICM will be required

Table 1 Table 1 i200x Configuration/menu matrix

			Terminal type		
	Function	Sub-options	I2001	I2002	I2004
	Login/Logoff	N/A	✓	✓	✓
	Firmware upgrades	N/A	✓	✓	✓
Options	Audio	Profile	✓	✓	✓
	Display Contrast	N/A	✓	✓	✓
	Feature Keys	Assign	✓	✓	✓
		Label	✓	✓	✓
		Reset	✓	✓	✓
	Language	N/A	✓	✓	✓
	Time	Time Format	✓	✓	✓
		Date Format	✓	✓	✓
		Hours from GMT	✓	✓	✓
		Daylight Saving	✓	✓	✓
	User	Username	✓	✓	✓
		Login Type	✓	✓	✓
		Auto Login	✓	✓	✓
Services	Inbox	Display	✓	✓	✓
		Store	✓	✓	✓
		Clear	✓	✓	✓
		Dial	✓	✓	✓
	Outbox	Display	✓	✓	✓
		Store	✓	✓	✓
		Clear	✓	✓	✓
		Dial	✓	✓	✓
	Directory	Add	✓	✓	✓
		Edit	✓	✓	✓
		Delete	✓	✓	✓
		Dial	✓	✓	✓

122.1.1 Display

The following details apply to the i2001.

- i2001 will have a *32x143* pixel, fully bit-mapped, monochrome, non-grayscale display. This will display 2 lines of 24 5x9 characters.
- The number of Soft labelled feature keys on the i2001 is zero
- Dedicated icon area in the main display area has been removed.
- Dedicated Clock / Calendar area present.
- Dedicated number and context label are present.
- Dedicated down arrow removed.

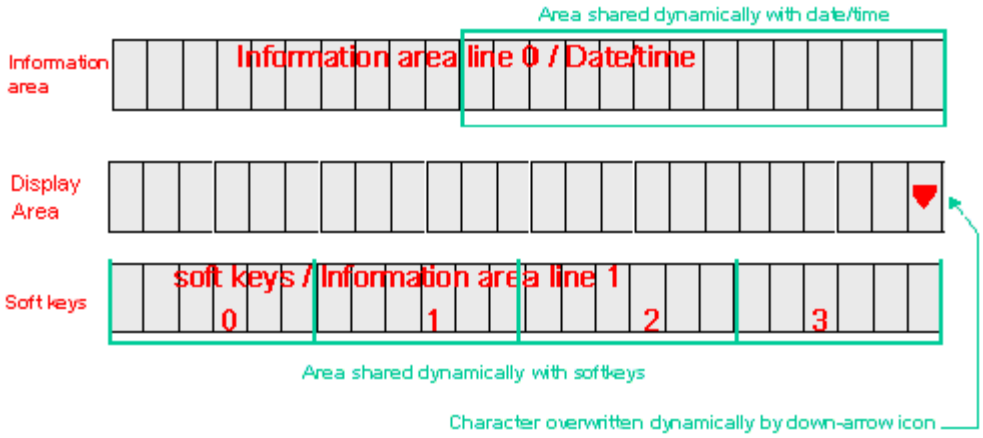


Figure 1 Display layout of i2001

122.1.2 Generic Display Rules

The following rules have been devised for the i200x terminals. These rules have been introduced to allow one common interface across both terminal types and to help avoid issues with Language Translations on soft key strings.

- All strings for menu options should be created with the following rules in mind

  a. Recommended length 12 characters – strings meeting this condition will always be shown in full (both on the information lines and in the context field)

  b. Maximum length 20 character – strings above 12 characters in length and equal to or below 20 characters will be fully displayable in the information line but not in the context field. Long strings in the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.

  c. Strings above 20 characters to be shown:

  — In the information lines will be cropped off to 19 characters and terminated with an ellipsis to indicate they have been cropped.

  — In the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.

- The Login Screen echoes entered digits to information line 0 rather than line 1 (please see Figure 2). The username and passwords entered may be up to a maximum of 15 digits. If the username/password entered is longer than the field space left on the screen (i.e. if the “Username” string is 14

characters and 12 username digits are to be entered), the digits will be scrolled to the left and an ellipsis will be inserted to the left of the username to indicate this (please see example below).

U	S	E	R	N	A	M	E		T	E	S	T	:	.	.	3	4	5	6	7	8	9	0	

- Bottom Soft key labels are set to a maximum of 5 characters with the exception of the last soft key on the screen which may use up to a maximum of 6 characters (please see Figure 2). This is due to a limitation of screen space on the i2001.

Figure 2 i2001 - Login Display

- Soft key labels are limited to a small generic subsection of the previously used soft keys (“Ok”, “Cancel”, “Clear”, “Bkspc”, “Menu”, “Help”, “Yes” and “No”).
- Menu options are selected via a scrollable list (instead of being assigned to a soft key). Scrolling may be carried out using the up and down navigation. This allows menu options to be displayed in strings which may be up to a maximum of 20 displayable characters (see rule 1). This is advantageous for the following reasons:
  - — A greater area makes language translations easier.
  - — A more informative string may be displayed.
- The position within a scrollable list is displayed to the far right hand side of the display. 1 character space is reserved to show scroll position.
- All Menu Options in the scrollable list are numerically indexed with the shortcut key number assigned to that option. The numerical indexes will

go from 1 – 9. Options above 9 will have no shortcut assigned/displayed next to the menu option

- A menu option may be selected by either highlighting the option (i2004) or viewing the option (i2002, i2001) and selecting “Ok”. Alternatively the appropriate shortcut key assigned to an option may be selected using the key pad. This will cause the user to jump straight into the menu option required without scrolling.
- All Menu Options are set to a recommended length of 12 characters (so they may be displayed in the context field on the i2004). Please see rule number 1) for further details.
- The Logout option is presented as the first option in the Menu Options List. This will avoid language translation issues on when using a soft key for the same operation.
- All user prompts will be presented on Information line 0 on the display. The maximum length of a prompt is 23 characters. Prompts beyond 23 characters will be cropped down to 22 characters and an ellipsis will be presented as the 23rd character to indicate cropping has taken place. Further text to describe the prompt is viewable on a help screen which is accessed by selecting a “Help” soft key (Please see Figure 3). The help screen presents text to the user by using scrolling pages (Please see Figure 4). The help screen has a maximum number of 255 characters (due to the scrolling functionality). The recommended word size is 24 characters (words exceeding this limit will be word wrapped onto the next line of the display).

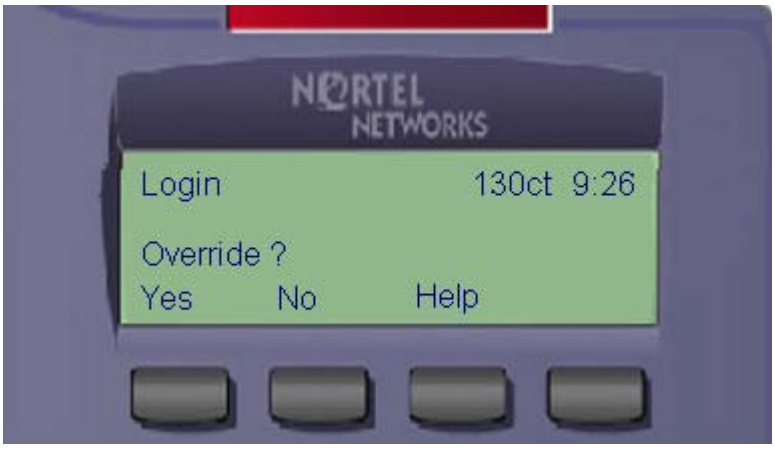


Figure 3 i2001- Override prompt

- User permissions disable

Figure 4 i2001 - Override Help screen

- The Menu system is accessible by either selecting the “Menu” softkey or by selecting the “service” physical key (please see at any time (idle or non-idle).

Figure 5 i2001 - Service key position (used to launch Menu system)

122.1.3 i2001 Display Rules

To show the information required to the user on such a restricted display, the following list of rules have been devised specifically for the i2001. The context-sensitive display that these rules entail are not as intuitive to use as that of the i2004, however there is no choice but to change the position and visibility of information on the display depending upon context if that information is to be displayed at all.

- The Menu options are selected via a scrollable list.
- The relative position within the list is show to the far right of information line 0 via up and down arrows.

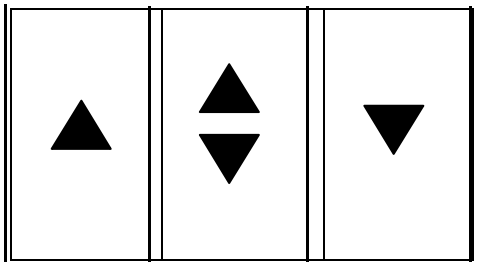


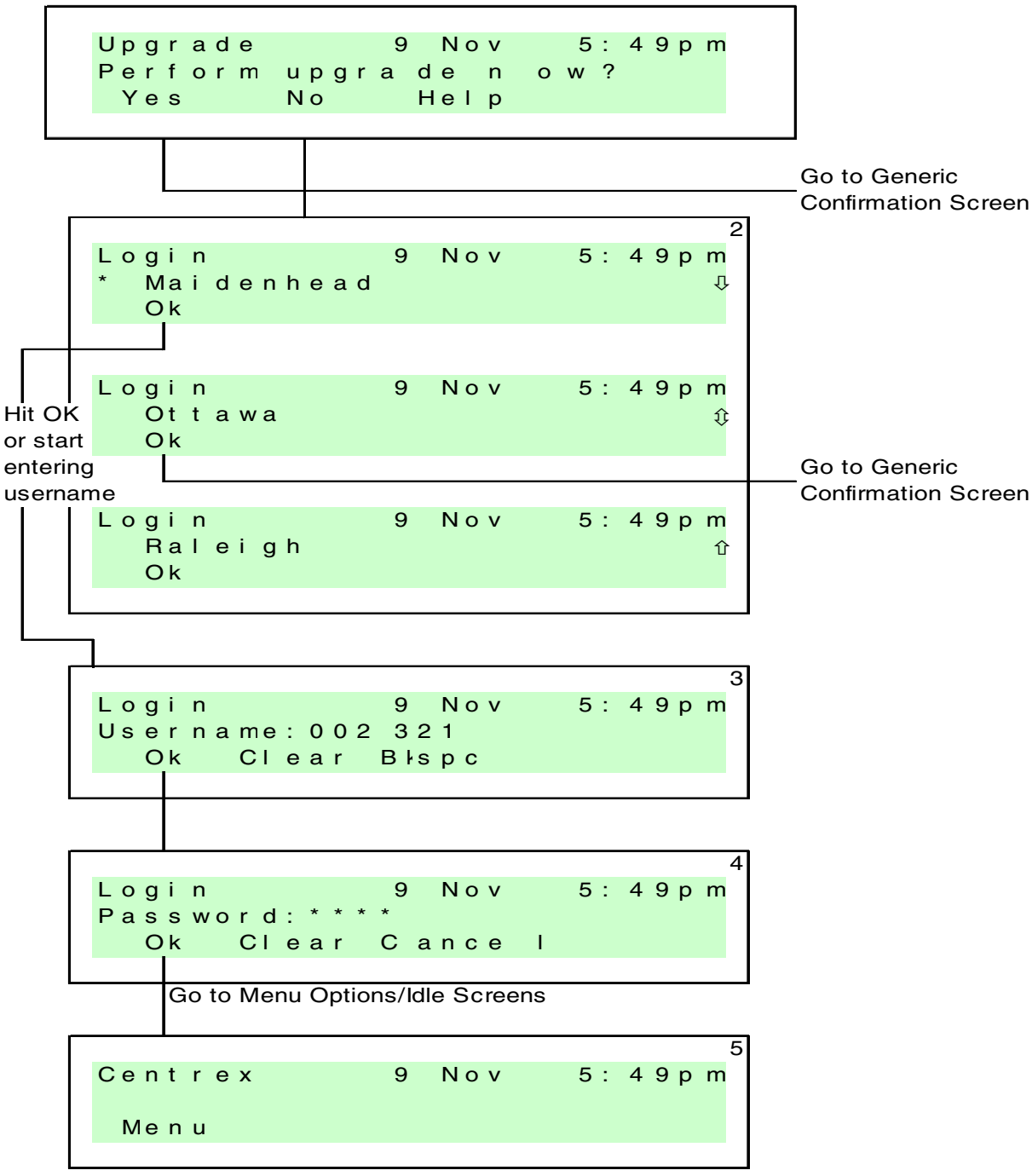
Figure 6 Example of navigation arrows

- Information line 1 is dedicated for the Soft keys.
- Time / Date displayed on context line.

122.1.4 i2001 Menu Map

The following screen representations show what will be presented to the user when logging on to a gateway, and navigating the menu options of the i2001.

122.1.4.1 Login Screens



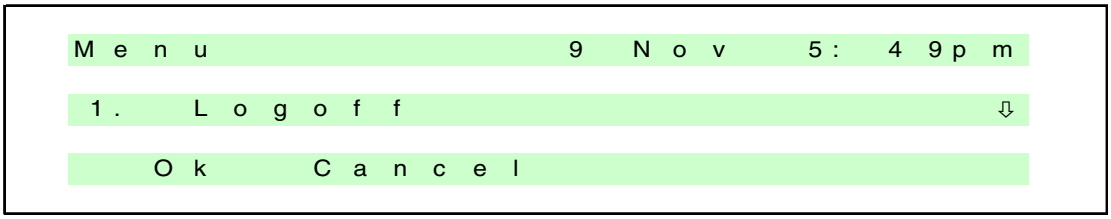
Screen 1 – Only shown if an upgrade is available / required.

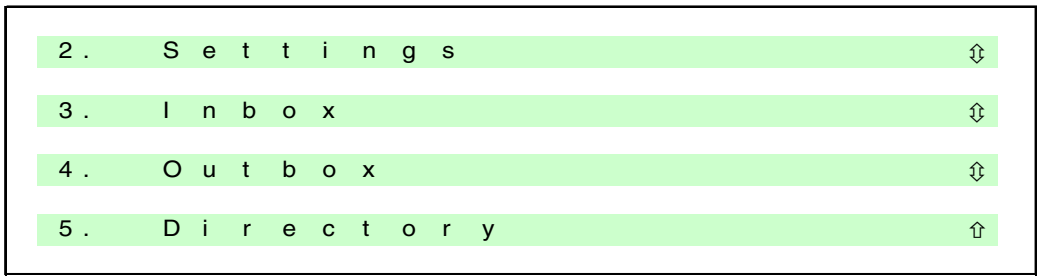
Screen 2 –Selective Gateway Login feature

Screen 2 – A user can either hit “Ok” to accept a gateway to login to, they will then be presented with Screen 3 to login. Alternatively the user may start entering their username digits and this will also accept the currently selected gateway, go to Screen 3 and insert the digit(s) already entered.

Screen 3 – If the username is too long for the display the digits entered will scroll to the left and an ellipsis will be shown to the left of the username to indicate this to the user.

122.1.4.2 Menu Option/Idle Screens



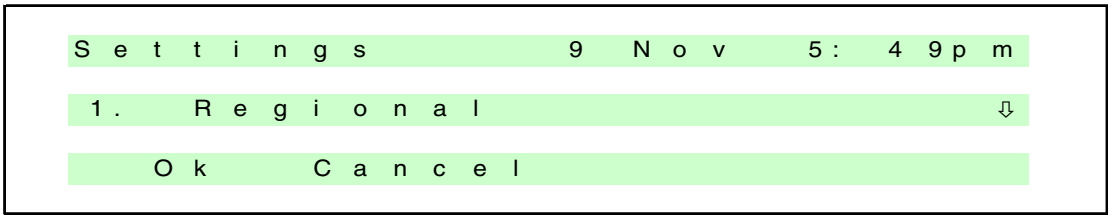


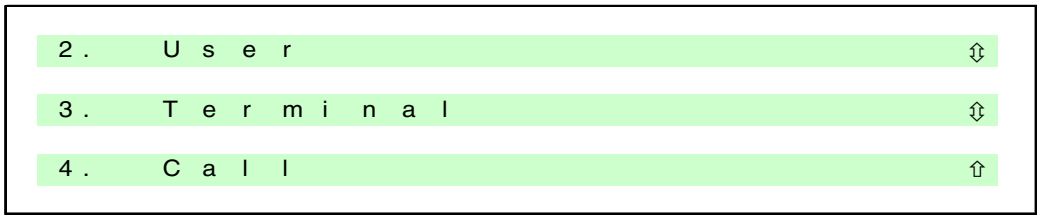
- Menu Option 1: Logoff – a Generic confirmation screen is displayed.
- Menu Option 2: Settings – launches the new i2001 settings menu.
- Menu Option 3: Inbox – Launches the inbox, Inbox is also available via dedicated Inbox key on terminal (i200x). The i2002 will be able to launch the inbox via both the menu and the dedicated key, the i2004 will only be able to access via its existing implementation of the dedicated key.
- Menu Option 4: Outbox – Launches the Outbox, the i2001 does not have a dedicated Outbox key and will only be able to access the Outbox via this

menu system, the i2002 and i2004 terminals will be able to launch the Outbox via the dedicated key. The i2002 will be able to access the Outbox via both the menu and the dedicated key. The i2004 will only access the outbox via the dedicated key.

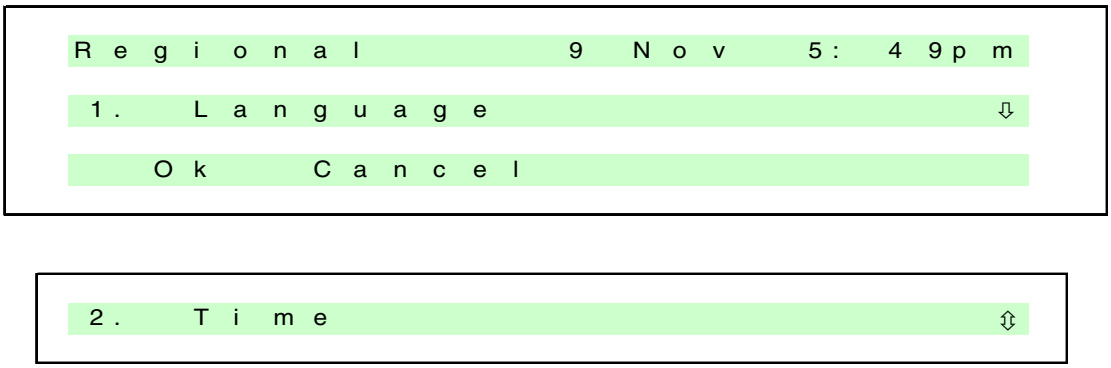
- Menu Option 5:Directory – Launches the directory contact list, the i2001 does not have a dedicated Directory key and will only be able to launch the directory via this menu system, the i2002 and i2004 have dedicated Directory keys to launch the directory

122.1.4.3 Menu Option: Settings

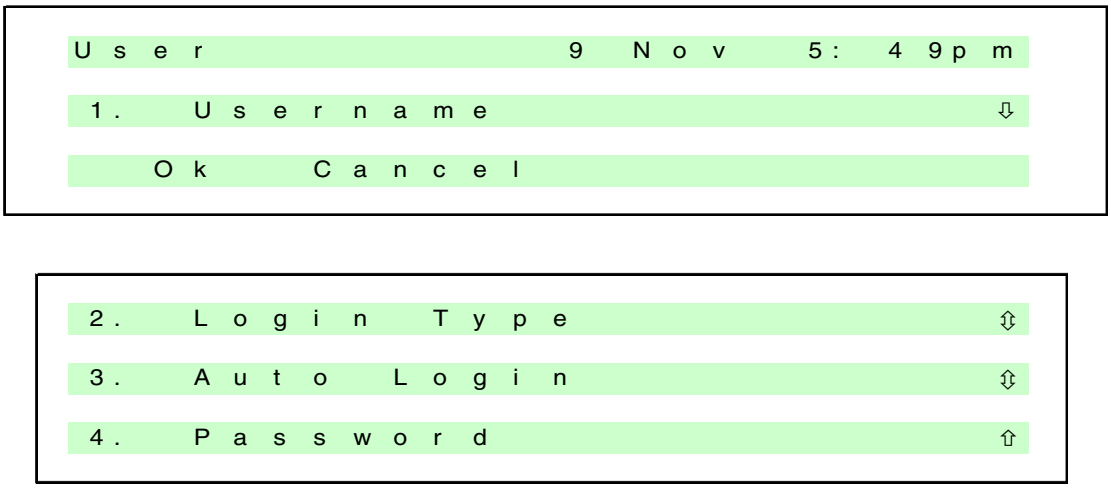




122.1.4.4 Menu Option: Regional Settings

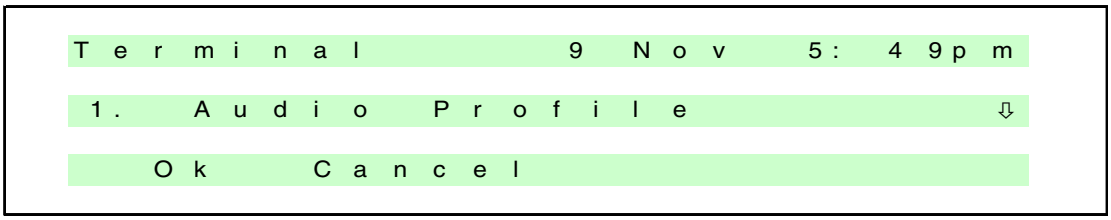


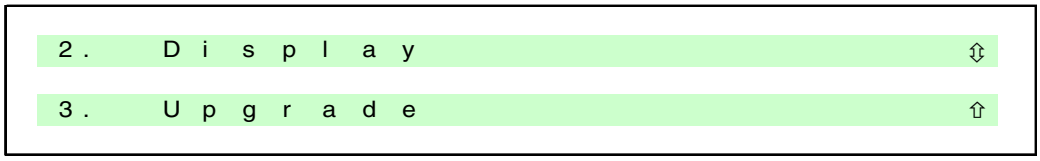
122.1.4.5 Menu Option: User Settings



See section 1.1.4.9 for details of user information screens.

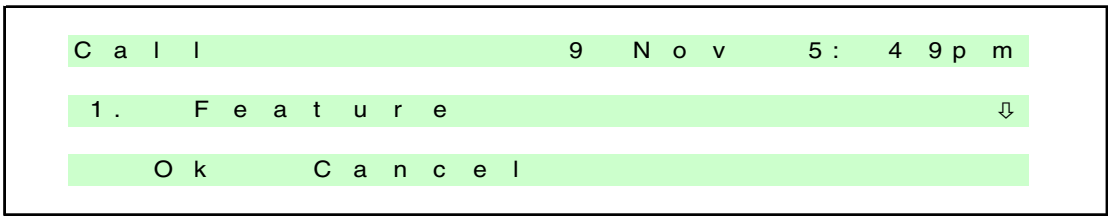
122.1.4.6 Menu Option: Terminal Settings

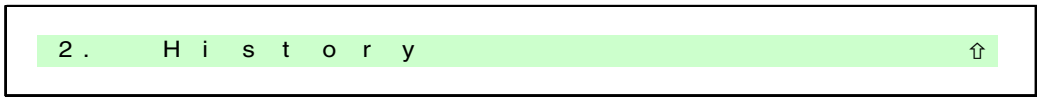




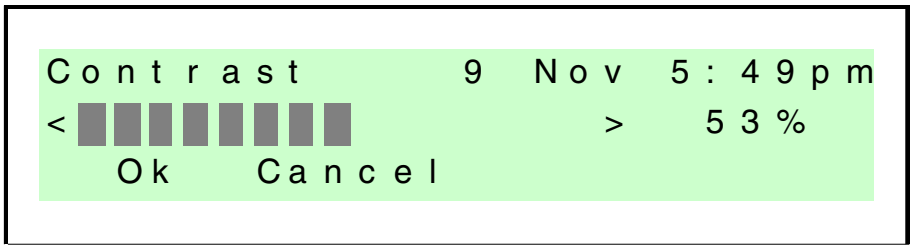
- Terminal Settings Option 1: Launches the Audio Profile menu.
- Terminal Settings Option 2: Launches the display Contrast screen. (2.1.4.8)
- Terminal Settings Option 3: Launches the Upgrade confirmation menu, depending on if an upgrade is available or necessary.

122.1.4.7 Menu Option: Call Settings

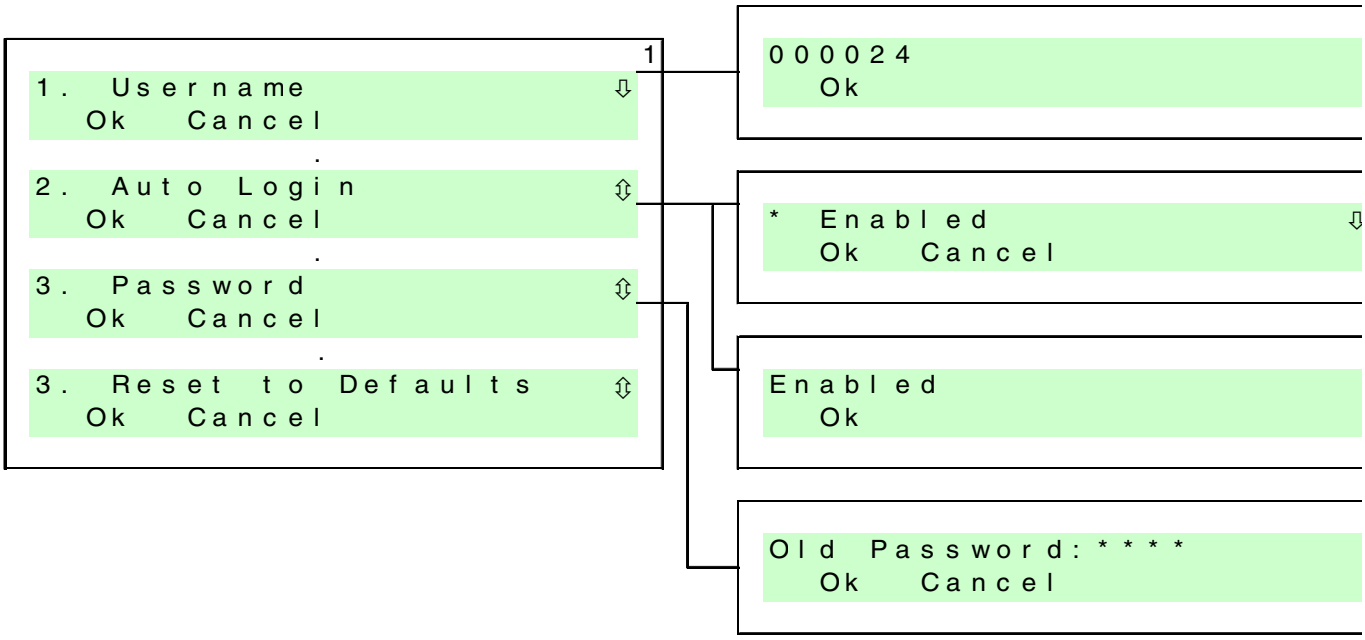




122.1.4.8 Display Contrast Screen



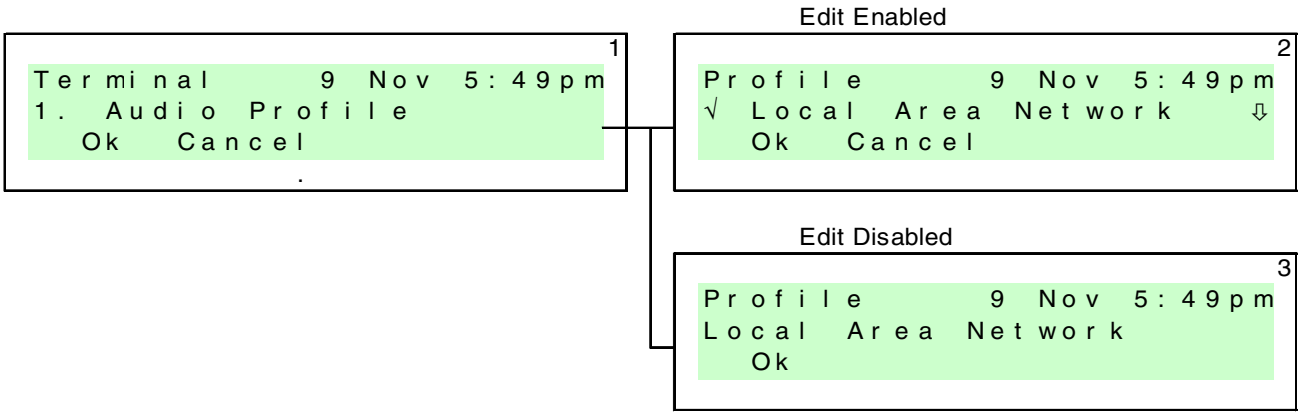
122.1.4.9 User Information Screens



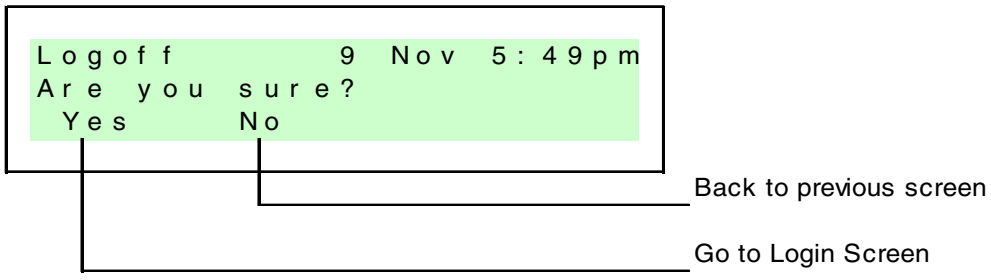
- Screen 3 – The user has permission to edit their Auto Login functionality. The user may enable/disable the feature from this screen.
- Screen 4 – The user has view permission to the Auto Login functionality. The user may only view what their current setting is.

Note: NOTE: The permissions are configurable via the element manager in the user/user profile settings.

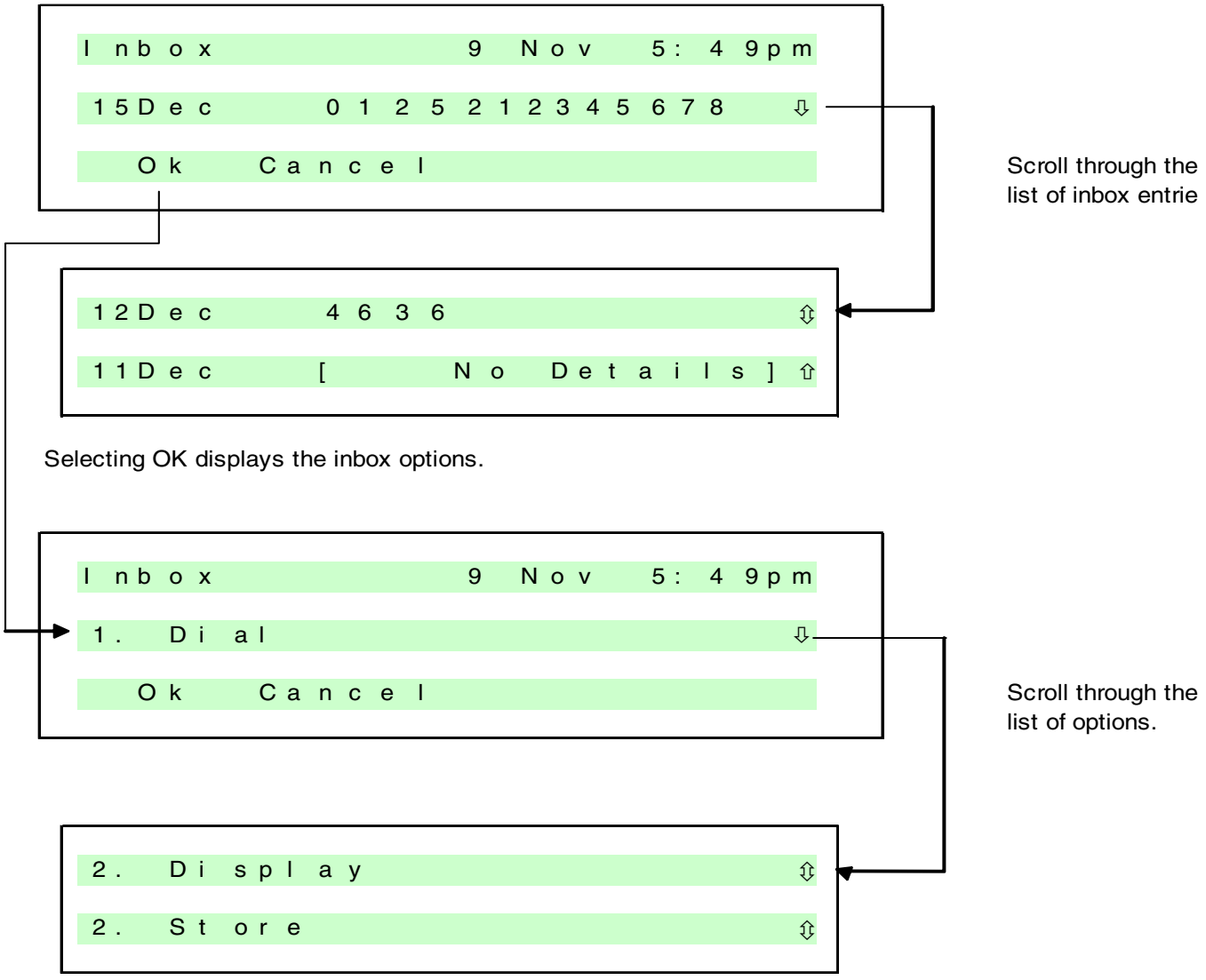
122.1.4.10 Audio Screens



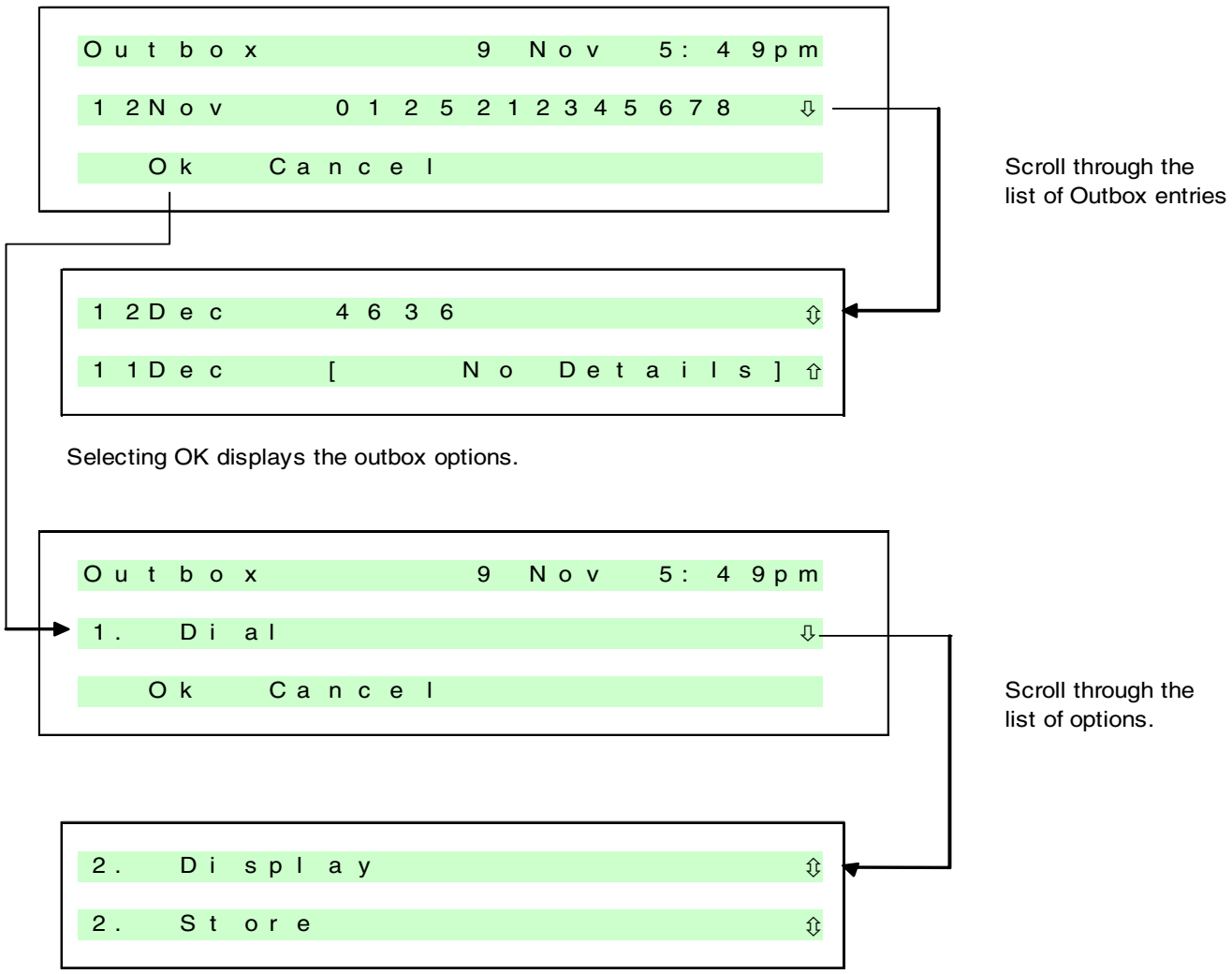
122.1.4.11 Generic Confirmation Screen



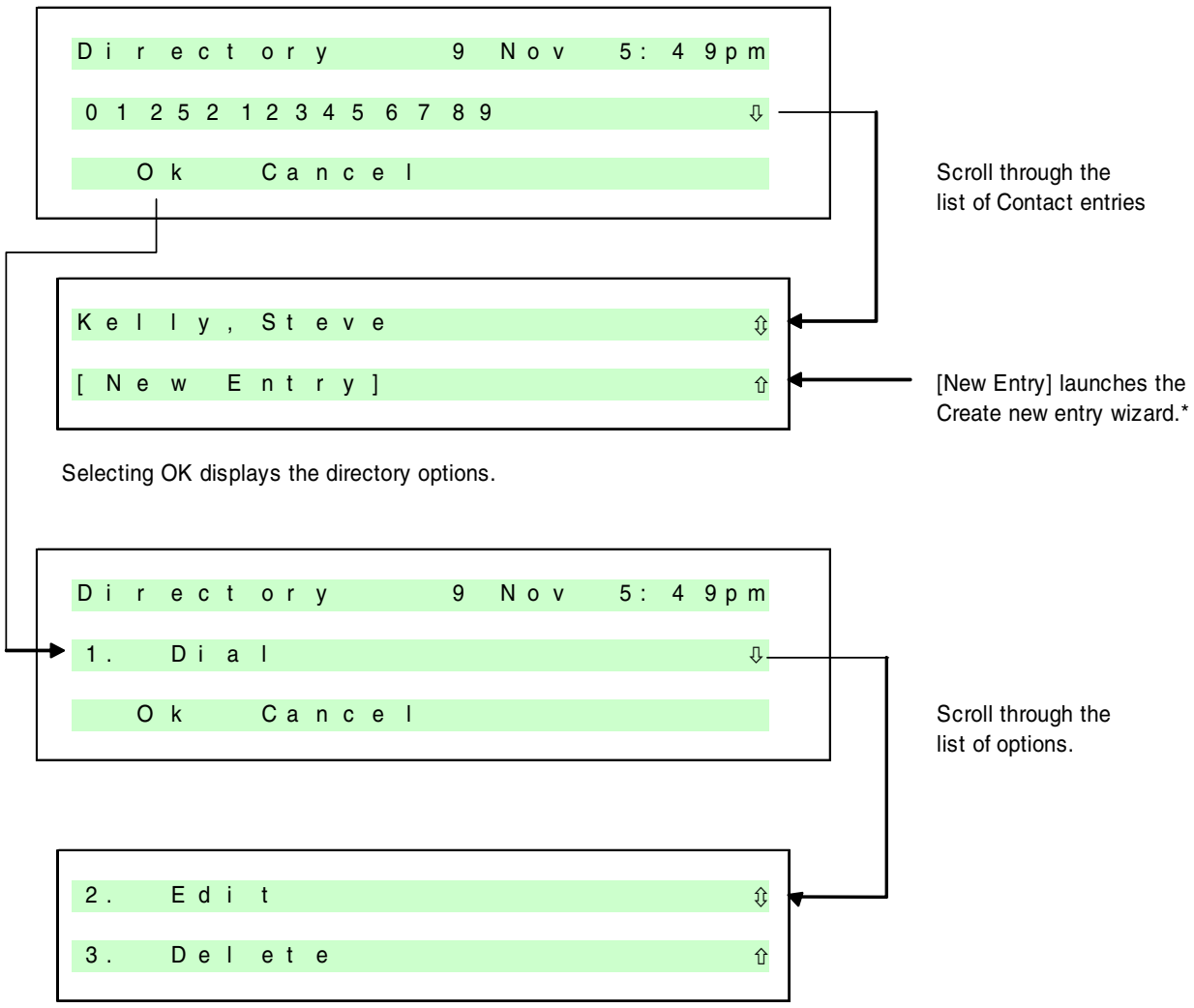
122.1.4.12 Inbox and submenu screens



122.1.4.13 Outbox and submenu screens

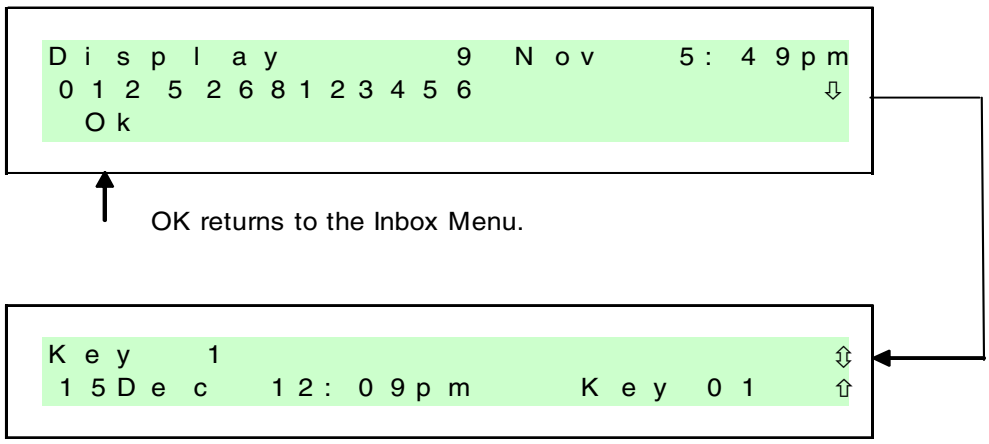


122.1.4.14 Directory display screens

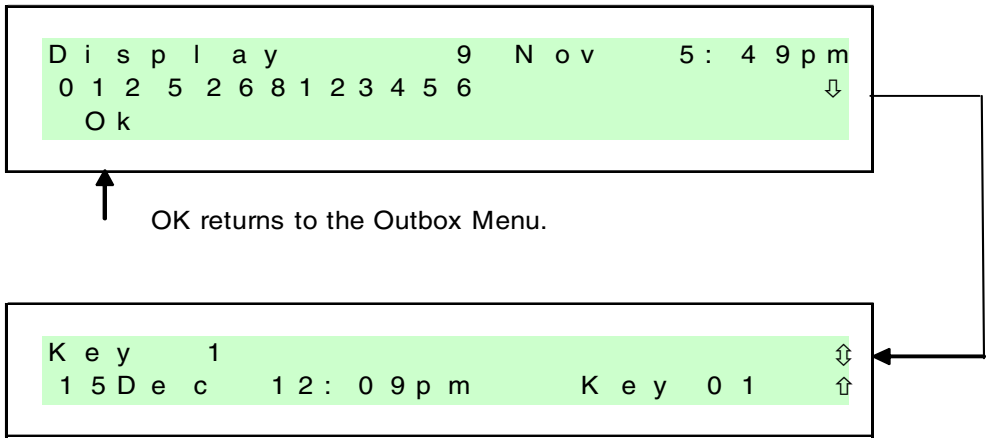


* The [New Entry] option may be ordered to feature at the top of the directory list, so upon entering the directory you will be presented with the first actual entry and press up to select [New Entry]

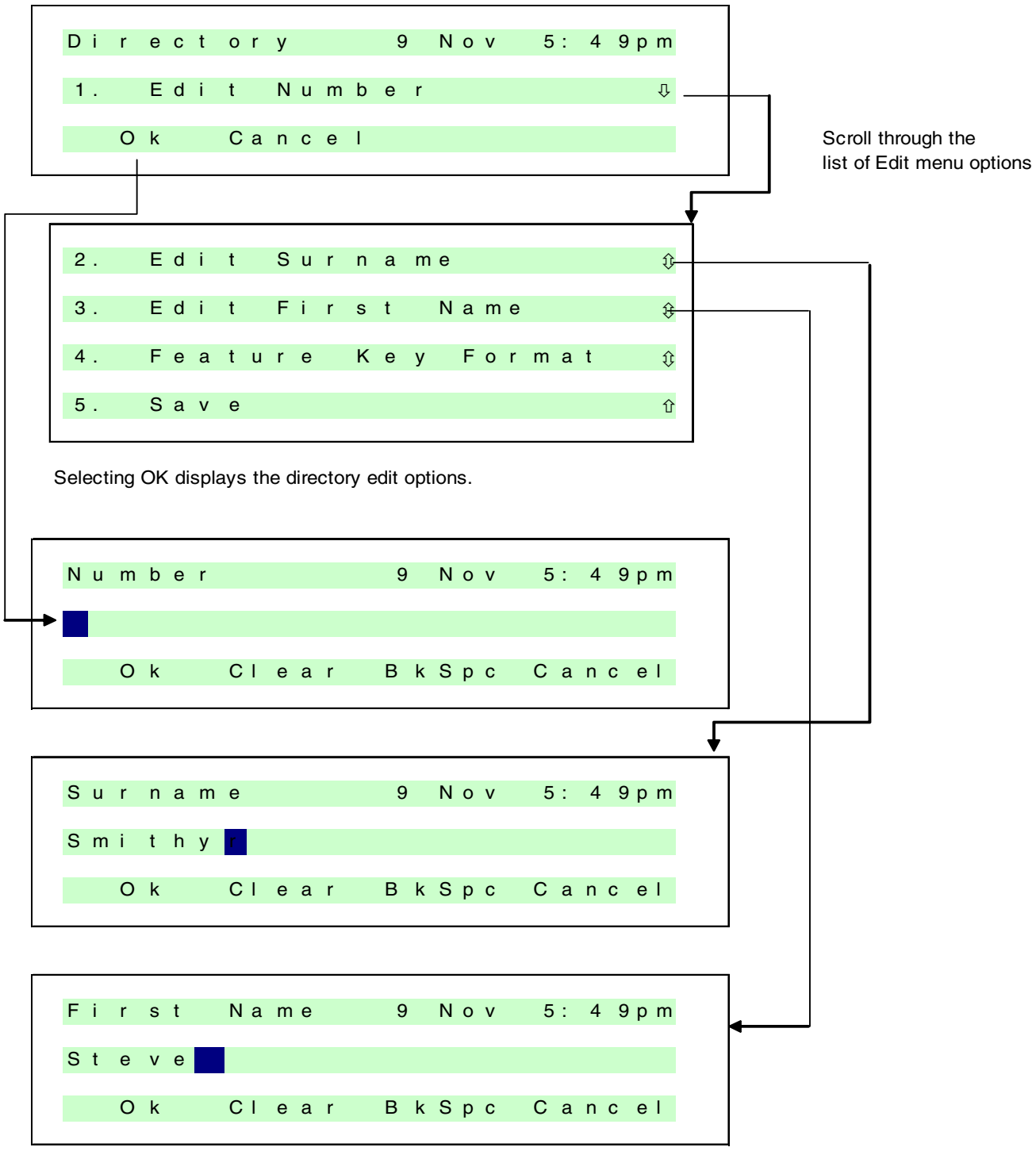
122.1.4.15 Inbox Display Screen



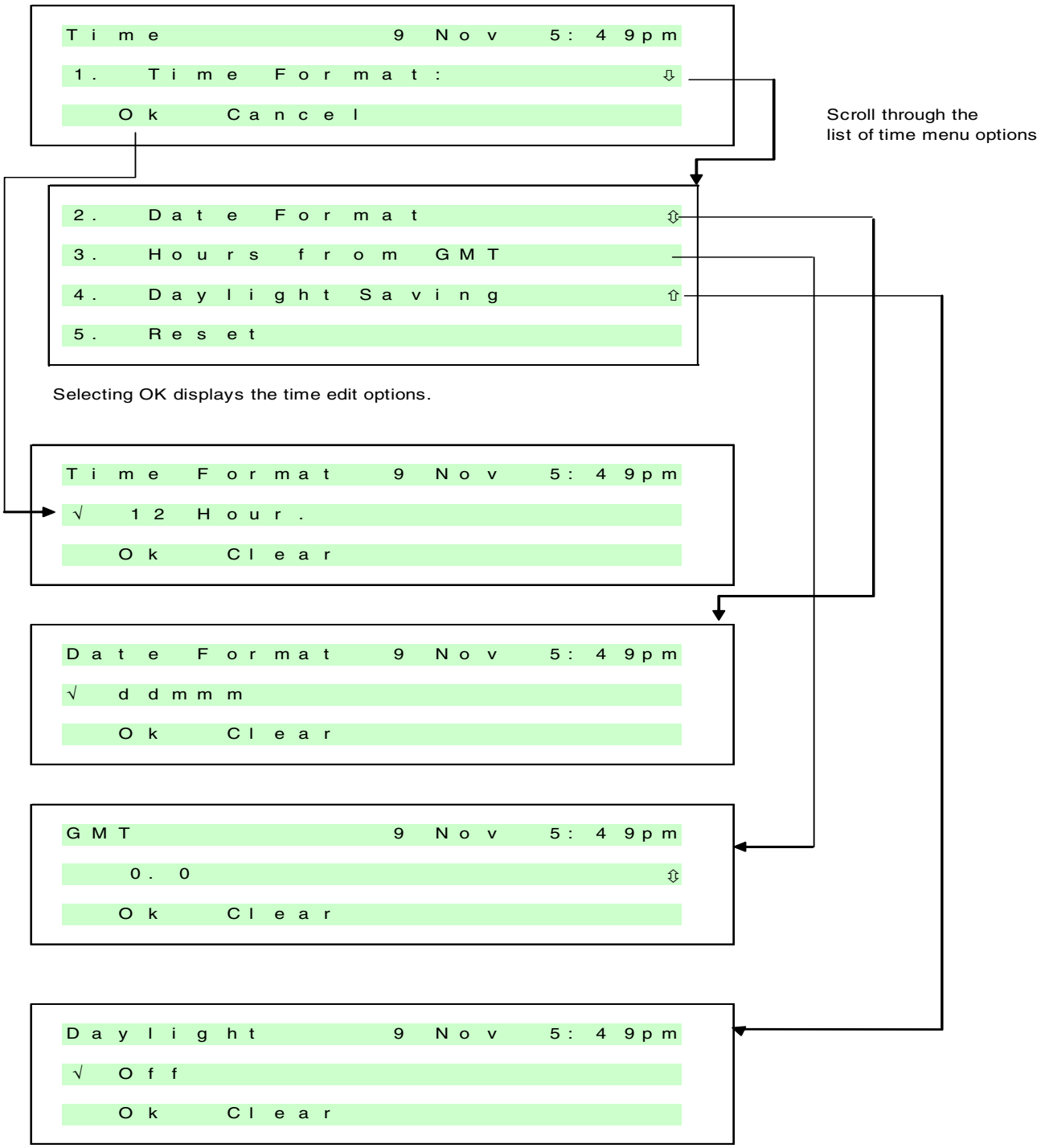
122.1.4.16 Outbox Display Screen



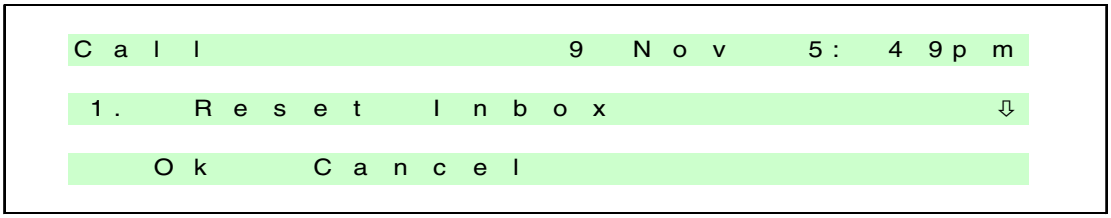
122.1.4.17 Directory Edit screens

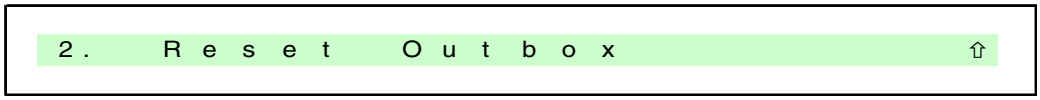

Directory 9 Nov 5:49pm
1. Edit Number
Ok Cancel
Scroll through the list of Edit menu options
2. Edit Surname
3. Edit First Name
4. Feature Key Format
5. Save
Selecting OK displays the directory edit options.
Number 9 Nov 5:49pm
Ok Clear BkSpc Cancel
Surname 9 Nov 5:49pm
Smithyr
Ok Clear BkSpc Cancel
First Name 9 Nov 5:49pm
Steve
Ok Clear BkSpc Cancel

122.1.4.18 Time display screens



122.1.4.19 Call History screens





122.1.5 Administration - Element Manager

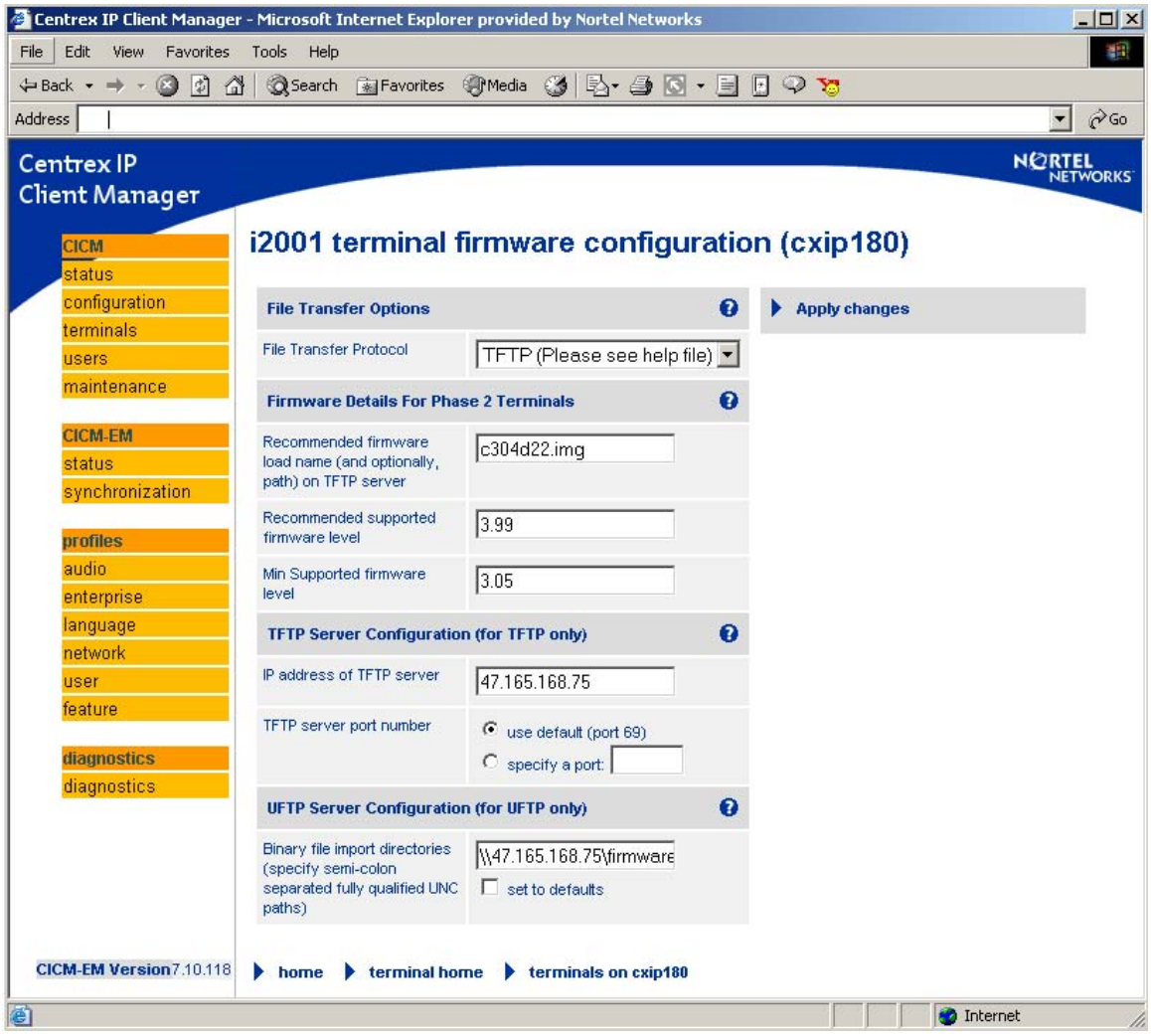


Figure 7 Screen capture of terminal firmware upgrade page

The administration and configuration of the i2001 terminals will use the same pages which are already provided for the i2004 and i2002 terminals (See Figure 7).

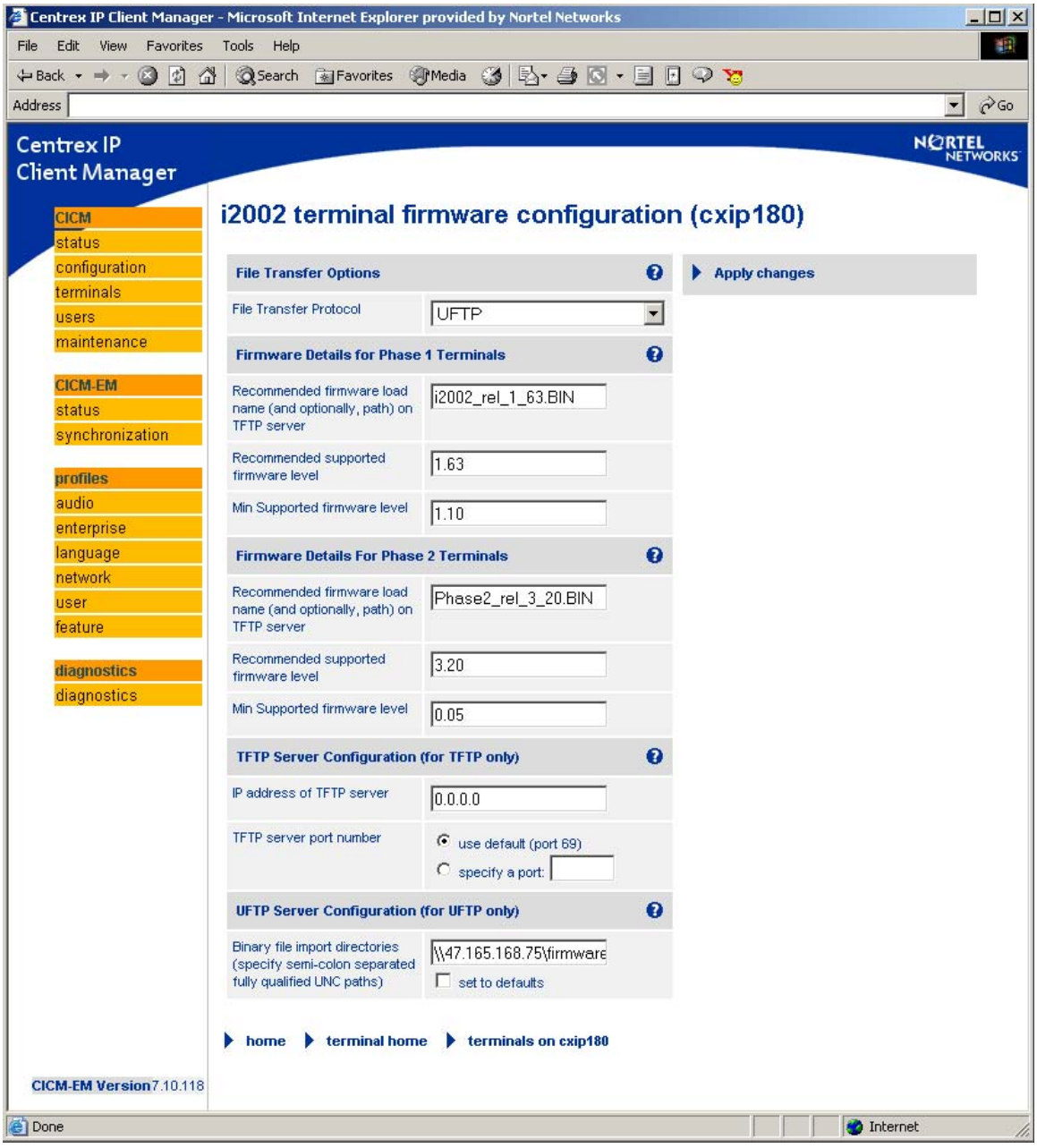


Figure 8 Screen capture of phase 2 terminal firmware upgrade page

User permissions will be editable via the user/user profile pages.

122.2 Interactions

122.2.1 Joint Sessions

The i2001 will only be able to have a joint session with the m6350 Softclient. In this scenario it will always adopt the master position in their master/slave

relationship. In this case, the i2001 will function in the same manner as the i2004.

There will be no support for the i2001 to have a joint session with another i200x.

122.3 Software Requirements or Dependencies

Firmware load *.bin will be used for the development of this feature on the i2001.

122.4 Interactions

This feature will change the existing menu system employed by the i2004 and i2002. Menu options previously displayed on the soft keys will be displayed in the main screen as a scrollable list (using the up and down navigation keys). The Soft keys will only be used for a small sub section of set functions.

The change is beneficial on the i2004 for the support of different languages as longer strings may be used for menu options. Problems had previously been encountered upon translating soft key options which were limited to only 7 characters i.e. a 7 character soft key in English may translate into a 9 character soft key in French which is not easily abbreviated.

122.5 References

123: Functional description (FN): A00003952

123.1 Feature name

Centrex IP Client Manager 3069 termination capacity

123.2 Description

The activity provides both increased capacity, improved RTS performance for the CICM platform as well as the GWC changes required for the CICM line and nodal flow through provisioning work in SN07.The capacity of the CICM is being increased to support around 3000 terminations.

This activity is an enabler for the flow through provisioning actvities ‘A00001935: SESM Provisioning support for Centrex IP Nodes and Lines’ and ‘A00003717: CICM OSMINE READINESS - FLOWTHROUGH PROVISIONING’. All customer visible chaneges are documented under A00001935 and A00003717.

123.3 Hardware Requirements or Dependencies

SN07 baseline hardware required.

123.4 Software Requirements or Dependencies

SN07

123.5 Limitations and restrictions

This activity does not increase the BHHCA.

123.6 Interactions

None

123.7 Applicable customer facing sections

Fault Management

Logs _N/A__

Alarms _N/A__

Configuration

Data Schema _N/A__

User Interface _N/A__

Element Management _N/A__

Security _N/A__

Service Order _N/A__

Office Parameters _N/A__

Accounting (includes AMA billing) _N/A__

Performance (includes operational measurements) _N/A__

123.8 Glossary

Term	Description
CICM	Centrex IP Client Manager
RTS	Return To Service
BHHCA	Busy Hour Half Call Attempts
GWC	GateWay Controller

124: Functional Description (FN): A00003971

124.1 Feature name

A00003971 - SPM Log Robustness

124.2 Description

SPM Log robustness initiative is intended to enhance the logs generated for SPMs.

During an analysis of the CSR responsiveness, it was found that SPM logs did not provide sufficient data for analysis. To provide a faster resolution of SPM issues, a need was felt to enhance the logs generated for SPMs. In conjunction, MAP responses for various commands have been enhanced to provide greater details about the failure/refusal of MAP commands.

124.3 Hardware Requirements or Dependencies

None

124.4 Software Requirements or Dependencies

124.4.1 MAP response modification

When a manual or force swact is issued on the CEM protection level MAP, if the command fails, a reason is displayed along with the existing response. When a RTS is issued on a RM, if the command fails because of the RM not having a valid load in flash, a message appears. This message has been corrected to include a ‘have a’ in the existing message ‘RM does not valid load in Flash’.

More details can be found in the Chapter 13 Configuration of this book.

124.4.2 LOGS

The following existing logs are impacted by this activity

Activity status of the unit/device will be displayed along with the other fields for the following logs

- SPM300 - Device Fault report log
- SPM500 - Device state change log
- SPM650 - Boot loader pass log
- SPM651 - Boot loader fail log
- SPM684 - Erase Flash log
- SPM301 - Patch failed log
- NODE302 - Software Alarm log
- NODE303 - Wrong Application Data
- NODE326 - Hardware Fault
- NODE600 - System Recovery Action
- NODE601 - System Status Notification

TaskName will be displayed along with the taskID for the following logs.

- SPM311 - SW Exception Report
- SPM312 - Trap

New field ‘Reason’ will be added to the following log to provide a reason for protection switch failure.

- SPM331 - Failed Device Protection Switch

The following new logs have been introduced

- SPM 682 - indicates CEM manual reset.
- SPM 683 - indicates reason for CEM swact.
- NODE 602 - indicates reason for CEM state transition

For more details about the enhancement to the above logs, please refer to the Fault Management chapter of this book.

124.5 Limitations and restrictions

None

124.6 Interactions

None

124.7 Applicable customer facing sections

Fault Management

Logs __X____

Alarms _____

Configuration

Data Schema _____

User Interface __X____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

124.8 Glossary

Term	Description
CEM	Common Equipment Module
CSR	Customer Service Request
MAP	Maintenance and Administration Position
SPM	Spectrum Peripheral Module
SWACT	Switch Activity

125: Functional Description (FN): A00003995

125.1 Feature name

SN07 H.323 Gateway Change Capability - Actid A00003995

125.2 Description

This document details the Succession CS2K H.323 provisioning functionality being delivered in SN07. It describes the changes being made to the CS2K Management Tools (CMT) GUI (manual) and XML (machine-driven) provisioning components of the CS2K Configuration Management System.

This feature is introduced as on ongoing effort for provisioning H.323 Gateways (GW) and Endpoint Groups (EPG) within the Succession software suite. Software that was included in the 6.1 and 6.2 releases gave users the ability to provision H.323 gateways of fixed capacity and attributes. A desirable amendment to existing functionality is the ability to change the initial provisioning without affecting already provisioned GWs and EPGs.

This feature provides the following new or amended functionality:

- Change the capacity of a H.323 GW after initial provisioning
- Change the IP address of a H.323 GW after initial provisioning
- Change the Port of a H.323 GW after initial provisioning
- Allow users to specify the TID location of EPGs
- Provide modified GUI display capabilities for H.323 EPGs

An important change to point out as a consequence of this feature is that EPGs are no longer automatically added when a H.323 GW is added. This change was implemented so that greater flexibility could be realized when adding EPGs. It gives the users the ability to specify the location of the EPs in the system so that Terminal Space can be controlled, and therefore fragmentation can be better managed.

This document will describe in detail how the new functionality is used and modifications to existing H.323 provisioning features. For a comprehensive discussion concerning H.323 provisioning, please refer to FN SN06.1 CS2K H.323 Provisioning Application - Actid A00001913.

125.3 Hardware Requirements or Dependencies

N/A

125.4 Software Requirements or Dependencies

N/A

125.5 Limitations and restrictions

N/A

125.6 Interactions

N/A

125.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Upgrade ___X__
- Data Schema _____
- Service Order _____
- Element Management ___X__
- User Interface ___X__

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

125.8 Glossary

Acronym	Definition
ASPEN	Nortel proprietary GW control protocol (not an acronym).
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools
CORBA	Common Object Request Broker Architecture

CPE	Customer Premises Equipment
CS	Call Server
CS2K	Call Server 2000
DDMS	DMS Data Management System
DMS	Digital Multiplex System
DTC	Digital Trunk Controller
DTCI	ISDN Digital Trunk Controller
DTD	Document Type Definition
EP	Endpoint
EPG	Endpoint Group
EPID	End Point Identifier
ETSI	European Telecommunications Standards Institute
GPS	Global Product Support
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
HLD	High Level Design
HTML	HyperText Markup Language
IDL	Interface Definition Language
IP	Internet Protocol
ITA	Internet Transparency Agent
JAR	Java Archive
JDBC	Java Database Connectivity
JNLP	Java Network Launching Protocol
JWS	Java Web Start

LAN	Local Area Network
LTC	Line/Trunk Controller
MEGACO	H.248. Industry protocol for MG/MGC <->MG/MGC communication.
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Block
MI2	Manatee Iteration II
MOP	Method of Procedure
MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
NV	Network View
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PLM	Product Line Management
PSTN	Public Switched Telephone Network
PTM	Packet Telephony Manager
RMGC	Redirecting Media Gateway Controller
SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol

SQL	Structured Query Language (for DBs)
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number

126: Functional Description (FN): A00004005

126.1 Feature name

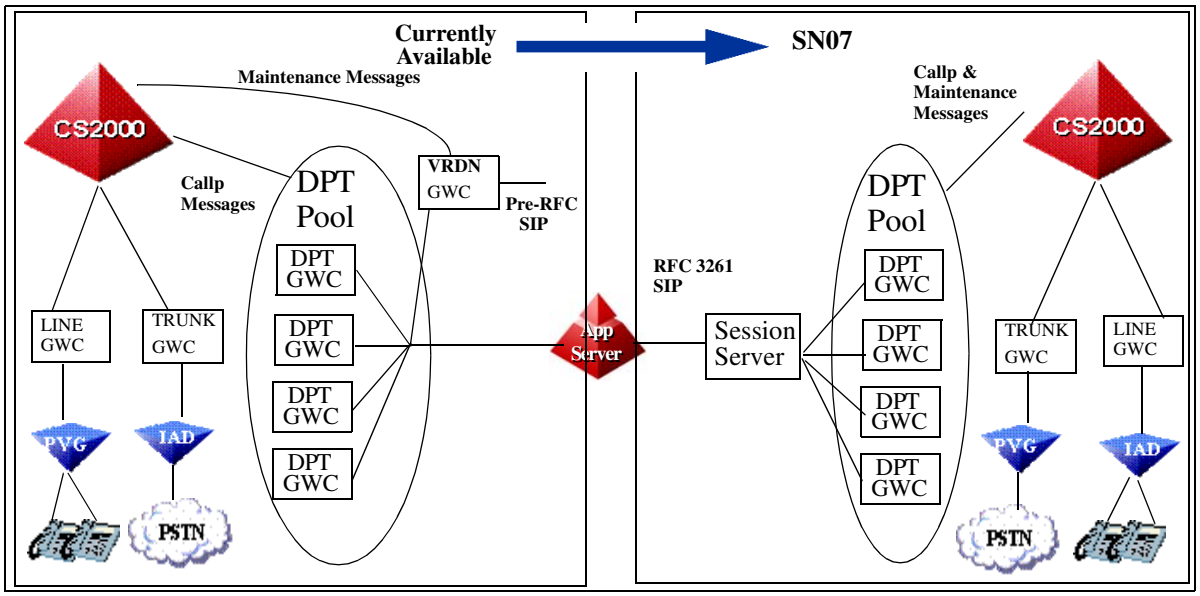
This feature is called Nortel Carrier Grade Linux (NCGL) platform “Session Server” and is being developed under ACTID A00004005.

126.2 Description

126.2.1 Overview

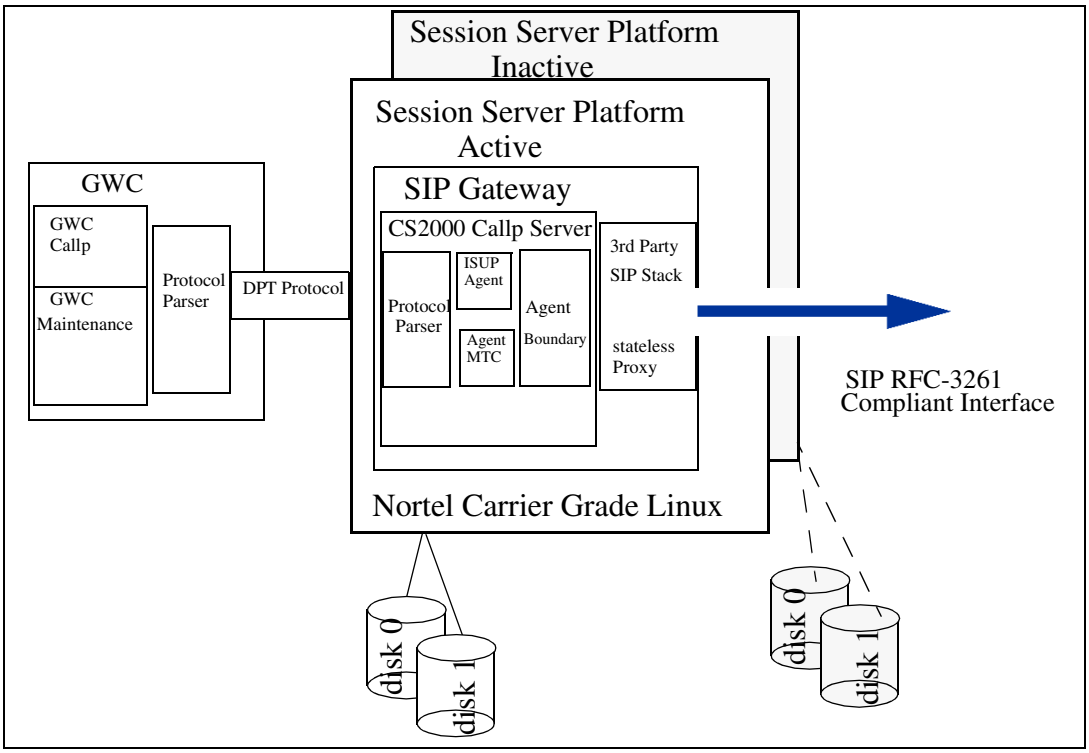
The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services.

Figure 1 Design Intent of Session Server Platform



In the SN07 release, the architecture for the Session Server will consist of a mated pair of Services Application Module- eXtreme Thin Server (SAM-XTS) with a configuration similar to that of gateway controller. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server that is interconnected via a gigabit ethernet LAN as shown in Figure 2, "Mated Pair Session Server". Each server provides processor capacity, local disk storage, and high-bandwidth network connectivity.

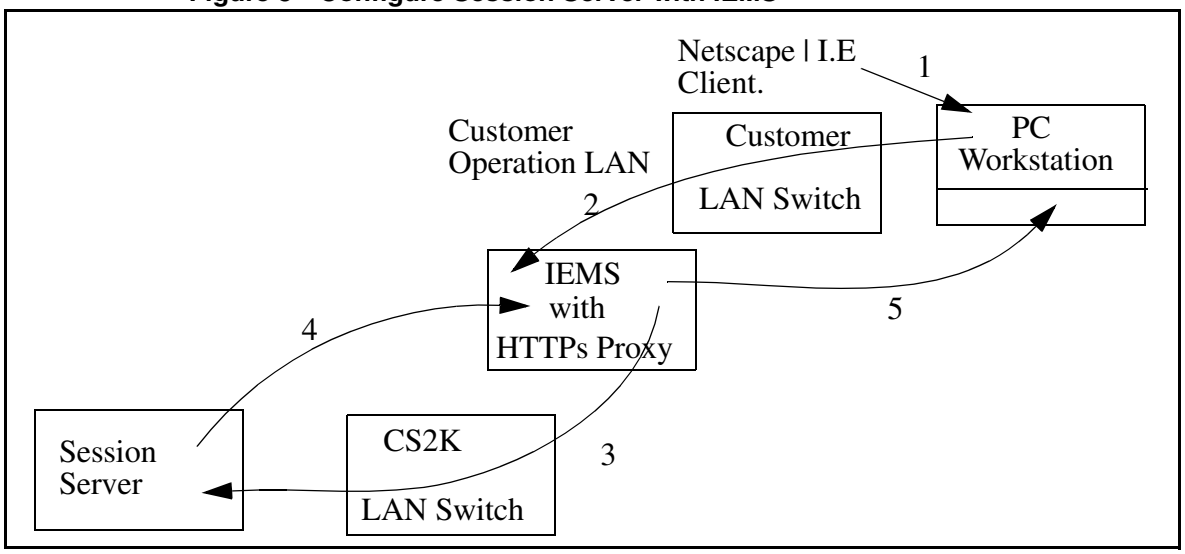
Figure 2 Mated Pair Session Server



The Session Server can be configured to use the Integrated Element Manager System (IEMS) between the customer operation LAN and the Call Server 2000(CS2K) LAN or it can be configured without the IEMS.

Figure 3 shows a proposed configuration with IEMS, where an Hypertext Transfer Protocol (HTTP) proxy is configured on the IEMS to redirect the Netscape/Internet Explorer browser to the Session Server.

Figure 3 Configure Session Server with IEMS



The configuration steps include:

1. user point the browser to web link on the IEMS
2. IEMS invoke the HTTPs proxy
3. the HTTPs proxy on the IEMS will redirect the link to the Session Server
4. Session Server will reply back to IEMS
5. IEMS will in turn respond to user request

The SIP Gateway application is the initial application for the Session Server platform, with the intention to provide a reusable infrastructure that can support additional applications. For complete details on the SIP Gateway Application, please refer to the latest version of the functional description section for feature A00003933.

126.3 Hardware Requirements or Dependencies

The Session Server technology is based on the SAM-XTS a second generation 2U NEBS compliant server from Intel. It is the same chassis as the currently shipping SAM-XTS for STORM, but adds additional CPUs and more RAM.

Each server will be equipped with:

- Dual Intel 2.4 GHz P4 Xeon Processors
- 4 GB RAM is the Standard - could have up to 12 GB RAM
- Memory Speed - 266 MHz DDR
- Local Disk - Dual hot swap 73GB
- Multiple GigE copper interfaces(2 on board + 2 Port NIC)

— NEBS Level 3 compliant

— 2U Form Factor

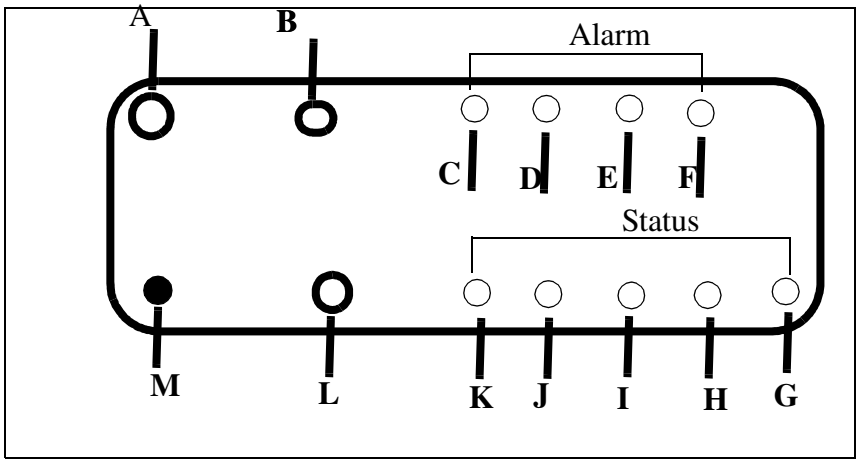
The field replaceable components on the Session Server are:

- Hard disk
- Power supply
- CD drive

126.3.1 Front/Back Panel Features and LEDs

The Session Server front panel features and LEDs are shown in Figure 4, on page 1566.

Figure 4 Front Panel LEDs on The Session Server



Something worth noting here is only the most critical alarm LED is illuminated. For example, if a minor alarm is present and a major alarm occurs, the minor alarm data will be retained; only the major alarm LED will be illuminated. If the condition that set the minor alarm previously still exists when the major alarm is cleared, the minor alarm will once again become illuminated.

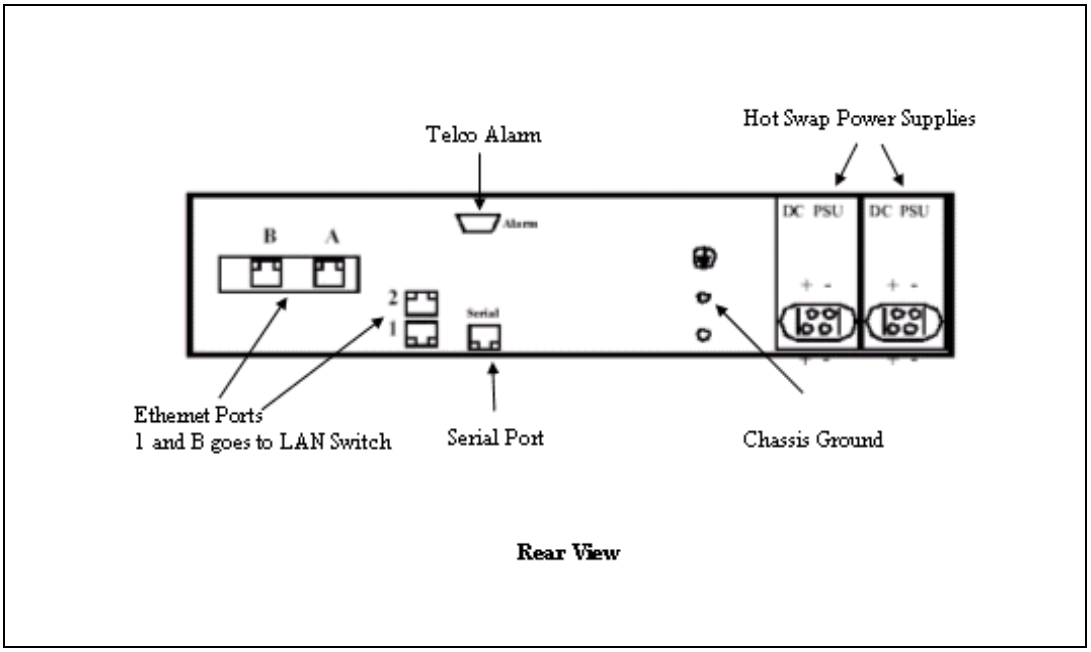
Table 1 Front Panel Features

Item	Feature	Description
		Front Panel Switches
A	Power switch	Toggle the server power
B	Reset switch	Reset the server
L	ID switch	Toggles server ID LED
		Front Panel Alarm LEDs and

Item	Feature	Description
C	Critical CRT (red)	When continuously lit, indicates the presence of a critical system fault.
D	Major MJR (red)	When continuously lit, indicates the presence of a major system fault.
E	Minor MNR (red)	When continuously lit, indicates the presence of a minor system fault.
F	Power (amber)	When continuously lit, indicates the presence of a power system fault. The front panel power alarm relay will be engaged.
		Front Panel Status LEDs
G	Disk 0 Activity/Fault LED (green or red)	Indicates disk 0 SCSI hard drive activity when green, or a disk 0 SCSI hard drive fault when red. When flashing green/red indicates that disk 0 is rebuilding disk array.
H	Disk 1 Activity/Fault LED (green or red)	Indicates disk 1 SCSI hard drive activity when green, or a disk 1 SCSI hard drive fault when red. When flashing green/red indicates that disk 1 is rebuilding disk array.
I	Main power LED (green)	When continuously lit, indicates the presence of DC power in the server. The LED goes out when the power is turned off or the power source is disrupted.
J	NIC0/NIC1 activity LED (green)	Indicates activity on either NIC0 or NIC1.
K	System ID LED (green)	Reserved for indicating any system SCSI hard drive activity. This Functionality is not implemented in SN07.

The connection ports on the rear view of the Session Server is shown in Figure 5, on page 1568.

Figure 5 Connection Ports



126.4 Software Requirements or Dependencies

The Session Server software has a layered architecture, which consists of the following:

- The base NCGL layer, running on Linux version 2.4 kernel.
- An application layer that includes a maintenance process for each application, which manages the associated processes.

The software running on this server has the following features:

- Linux operating system
- Maintenance applications for node maintenance, fault detection, and failover
- Apache Web server for provisioning and maintenance

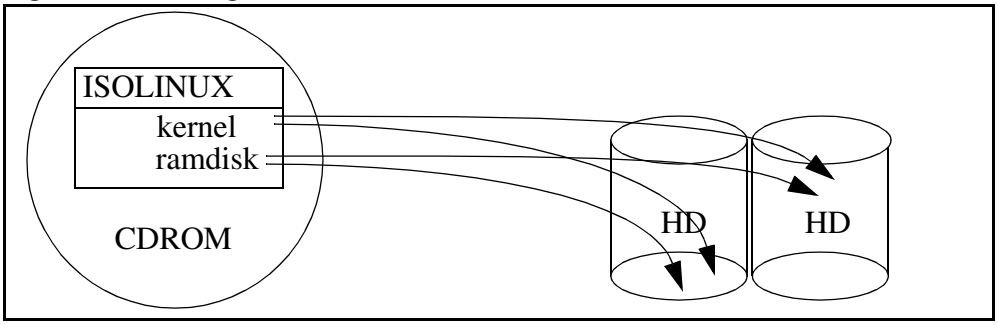
The Session Server has its own requirements in terms of software delivery and upgrade.

126.4.1 Software Delivery

The Session Server software load packages the kernel and ramdisk images using CDROM as the software delivery mechanism. The CDROM will be bootable, so that software installation and upgrades are as simple as inserting

the CD into the drive and rebooting. The software installation procedure is done separately on a per Session Server unit.

Figure 6 CD Image Installation to Hard Disks



126.4.2 Software Upgrade

This section addresses the upgrade of a simplex Session Server. The Session Server web interface contains a section under the admin panel to allow for upgrade to new load, as shown in Figure 19, on page 1596. The customer can select a default boot load as well as remove any older loads, which may no longer be needed. Space will be reserved on the hard drive to maintain approximately 3 or 4 Session Server loads in case fallback to a previous load is required. Further, it will allow for an upgrade of the Session Server load from either a CD inserted in the CDROM drive, from an ISO image located on the network, or from a Session Server CD mounted elsewhere in the network (via FTP). In summary the supported upgrade methods are:

- local cdrom
- local file (iso image, or load.tgz from CDROM)
- remote file via ftp (iso image, or load.tgz from CDROM)
- remote file via http (iso image, or load.tgz from CDROM)
- remote file via https (iso image, or load.tgz from CDROM)

126.5 Network Connectivity

Each Session Server (SS) is configured with two GigE interfaces directed to the LAN switch, as represented by link 0 and link 1 in Figure 7, on page 1570. In addition, two interfaces connect unit 0 to unit 1, as shown as the Point To Point (PTP) link.

Figure 7 Link Configuration of the Session Server

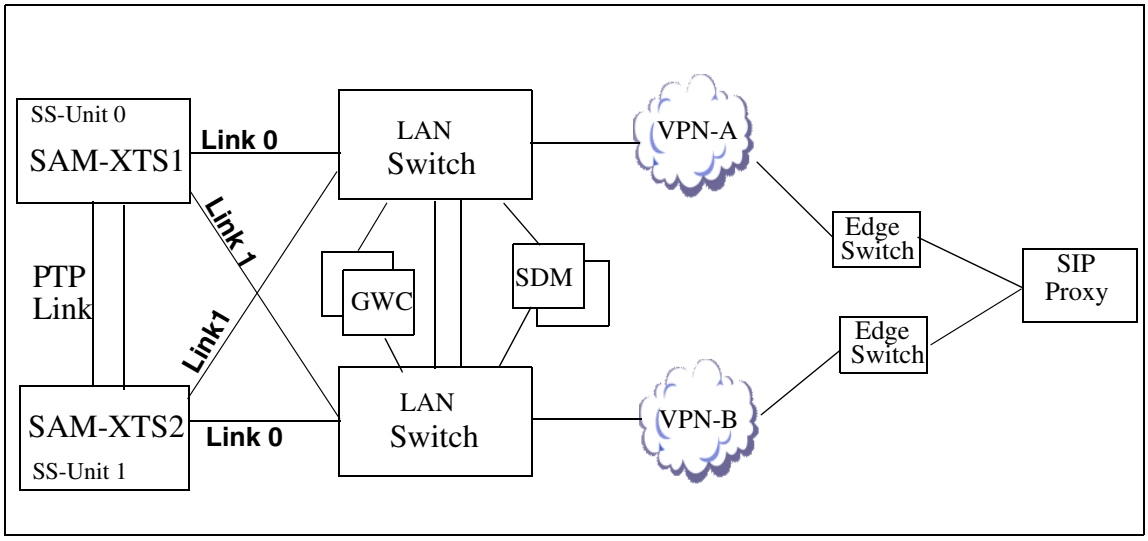
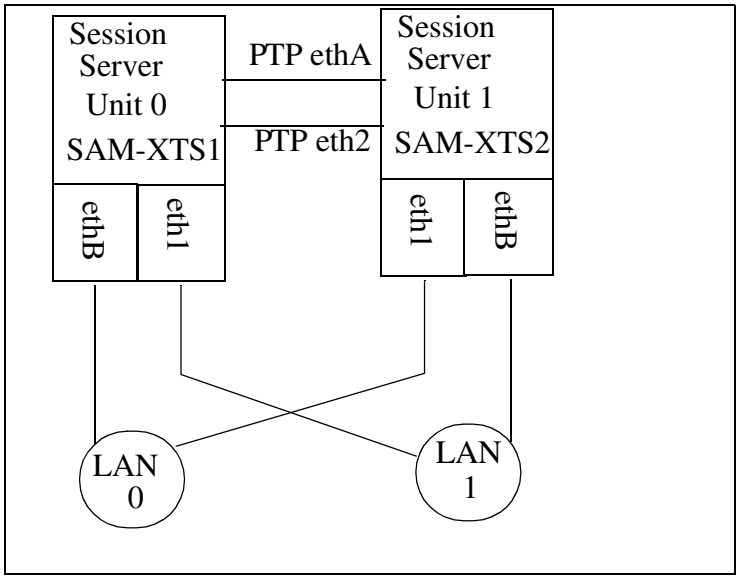


Figure 8, on page 1570 shows an example of the link configuration on the Session Server where “ethB” of each server is connected directly to the LAN switch, and “eth1” is connected to the alterative LAN switch.

Figure 8 Link Configuration for Session Server



126.5.1 Network Monitor IP Address

Network Monitor IP address is the address of one of the reliable node within the network that co-exist with SAM-XTS node. The Network Monitor IP address is used by SAM-XTS as a primary node reference unit to make sure its network connectivity is good and unit is connected with in the network. In case of failure to get proper network connection with the Network Monitor IP

address, SAM-XTS uses NTP server IP address as secondary backup reference to verify its connectivity in the network.

126.5.2 Session Server IP addresses

The Session Server requires a block of eight consecutive IP addresses that have to be on the same subnet as the Call Server (CS) LAN. The customer determines the IP addresses. The last octet of the IP address must be divisible by 8. Please refer to “Table 2 Example of Session Server Configuration” on page 1571. It is worth indicating that the PTP IP addresses are internally set by the system to 192.168.1.1 and 192.168.1.2.

Table 2 Example of Session Server Configuration

Session Server IP addresses	Example Unit 0	Example Unit 1	Datafilled By user	Description
Active Node[a]	172.16.16.72	172.16.16.72	no	Logical application
Inactive Node	172.16.16.71	172.16.16.71	no	Logical application
Local unit	172.16.16.67	172.16.16.70	yes	Logical unit link
Local unit, Link 0	172.16.16.65	172.16.16.68	no	Physical unit link
Local unit, Link 1	172.16.16.66	172.16.16.69	no	Physical unit link
Mate unit	172.16.16.70	172.16.16.67	yes	Logical unit link
Mate unit, Link 0	172.16.16.68	172.16.16.65	no	Physical unit link
Mate unit, Link 1	172.16.16.69	172.16.16.66	no	Physical unit link
Local PTP link 0	**192.168.1.1**	**192.168.1.2**	no	Local point to point link[b]
Mate PTP link 1	**192.168.1.2**	**192.168.1.1**	no	Mate point to point link

a. Active node last set of digits must be divisible by 8

b. The IP addresses **192.168.1.1/192.168.1.2** are assigned to the local/mate Point to Point (PTP) links. To avoid conflict, make sure **not** to assign the same IP addresses for the Session Server.

126.6 Session Server OA&M

This section discusses Operations, Administration, and Maintenance (OA&M) topics for the new Session Server platform.

As mentioned earlier, the architecture for the Session Server will consist of a dual unit configuration similar to that of gateway controllers. The units consists of an active and inactive unit. Both units have the ability to raise alarms and generate logs. The alarms raised on the active and inactive units can be viewed from either unit. However, the logs can be viewed on the same unit that generated the log.

126.6.1 Web Based OAM

The Session Server runs its own Element Manager (EM). This means that the web server runs locally on the Session Server. Which in turn means that maintenance type activities for the Session Server also take place on the Session Server.

The crafts person uses a web-based interface to perform the maintenance activities. This interface consists of a web server running on the Session Server that provides maintenance and monitoring related web pages.

The web agent is the browsing application which will be used to display the Session Server EM. The supported browsers are:

- Internet Explorer 6
- Netscape Navigator 6.2 & 7.1

Netscape is supported on both PC (Windows) and Solaris clients, but not on Linux clients.

All Session Server web pages are divided into three areas:

- **Header**

  The area with the Nortel logo and the “Platform”, “Application”, and “Help” tags. All functions will be performed under the “Platform Tag”.

- **Menu Frame**

  The user uses the menu bar on the left to locate the proper function in the web page hierarchy.

- **Interaction Frame**

  This area is where a user fills in forms, performs maintenance actions, and obtains relevant information.

An example of the home page of the Session Server is shown in Figure 17, on page 1594.

Figure 9 Session Server home page

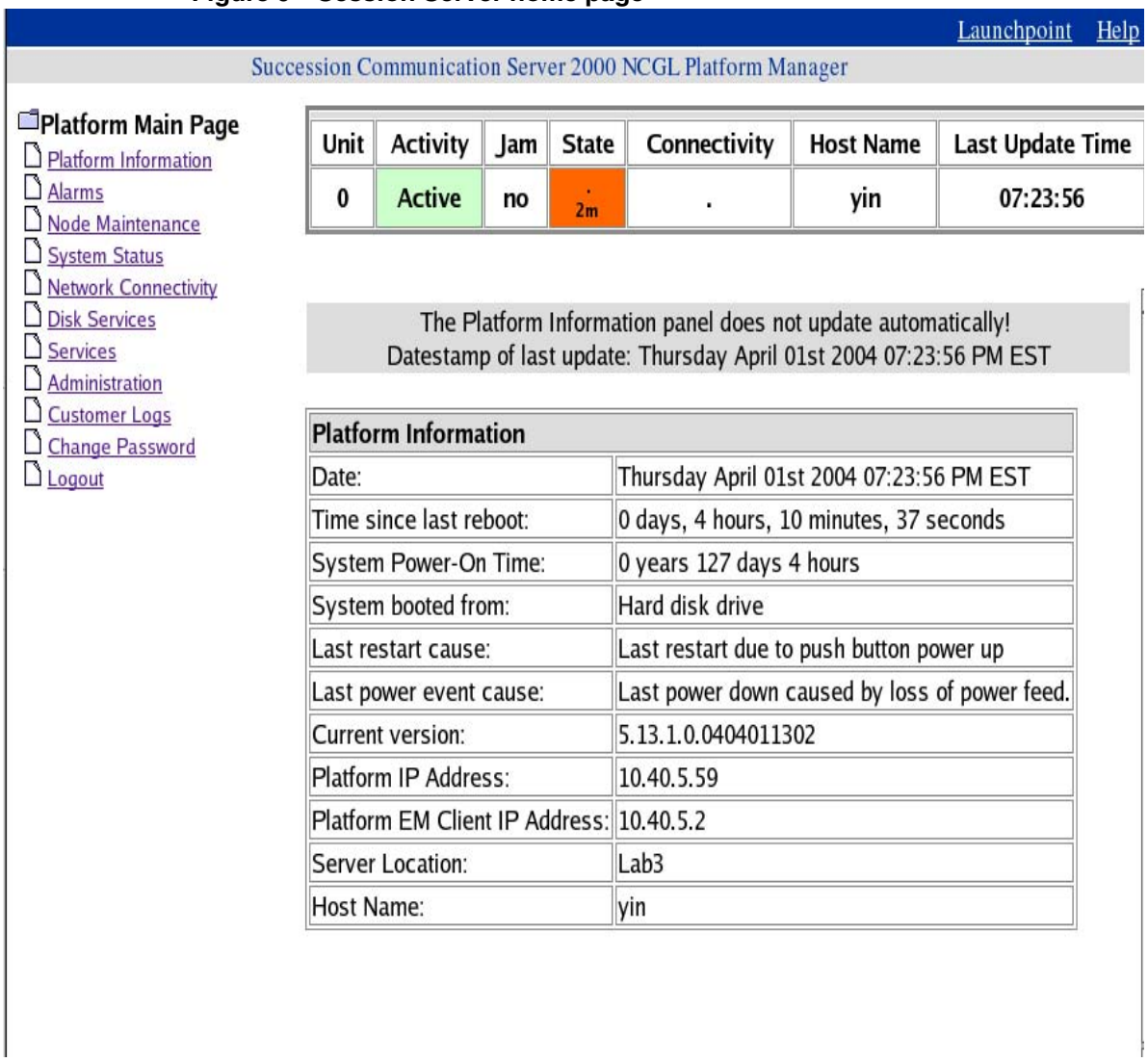


Table 3 Platform Main Page Links Description

Function	Description
System Information	Displays basic system information in an introductory screen.
Alarms	Provides the ability to view alarm information which consists of type, id, timestamp, severity, and description.
Node Maintenance	Provides the ability to perform the node maintenance actions like Swact/ Swact Force, Jam/Jam Force & UnJam.
System Status	Provides the ability to view chassis data, CPU Load, CPU Utilization, Process Information, and Memory Information.
Network Connectivity	Provides the connectivity status of local ethernet ports and network connectivity to the mate server and the ability to perform link maintenance actions such as lock/ unlock and swlnk.
Disk Services	Allows a view of file system data including partition specific data such as total space, used and available space. Also provides the ability to do Disk and Filesystem maintenance action.
Services	Provides the ability to view network active remote sessions and NTP information.
Administration	Allows the user to perform administrative tasks related to the system such as bootload management to setup the default load, software upgrade, reboot, reboot mate, halt and halt mate.
Customer Logs	Provides the ability to view customer logs.
Change Password	Provide the ability to change logged in user pass word
Logout	Provide the ability to log out of the session

126.6.2 System Status

The intention is to have the ability to view the status of both SS units at the same time when the user logs in. The status will be displayed as a frame on top of the interaction frame. Within the status frame the following information will be shown:

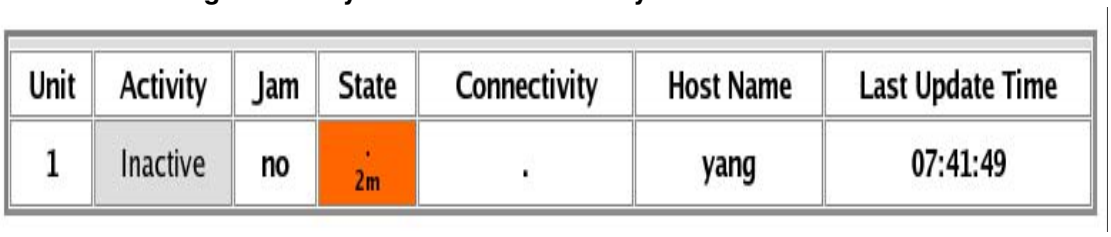
- unit number
- unit activity status (Active/Inactive) -- Active has green back ground -- Inactive has gray back ground
- unit jam status (yes/no)
- Overall system State - with number of alarms on both units
- session server host name
- last update time

In order to display the system status, a PHP script will be used to pool the required information to display within the frame. The status frame is refreshed approximately every 20 seconds. The valid link states mapping is captured in Table 4, “Mapping of link States,” on page 1575.

Table 4 Mapping of link States

Link State	Description
.	INSV - In SerVice
M	MANB - MAN Busy
S	SYSB - SYStem Busy
-	UNEQUIP -UNEQUipPed IP
NA	UNKNOWN

Figure 10 System Status Frame Layout



126.6.3 System Information

The home panel will display platform information for both Session Server units, which includes the following:

- Current date
- Time since last reboot
- System Power-On Time:
- System booted from
- Last restart cause
- Last power event cause
- Current version
- Platform IP Address
- Platform EM Client IP Address
- Server Location
- Host Name

126.6.4 Alarms

The Session Server has the capability to generate Alarms to report faults due to:

- network connectivity

- maintenance action failure
- mate communication
- disk usage
- memory usage
- disk mirroring failures

The alarms that are raised at this panel are the ones that are currently active on the system. The alarm panel is refreshed approximately every 54 seconds.

In addition, an application on the Session Server, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OM). The alarms that are raised on the Session Server are reported to the SNMP Trap destination server, if one is provisioned.

Alarms are formatted and displayed as defined in ITU-T Recommendation X.733(Systems management: Alarm reporting function), as follows:
`<Type> <ID> <Timestamp> <Host> <Serverity> <Description>`

126.6.4.1 Type

The alarm type specifies the alarm category for the given alarm. Valid alarm types are:

Table 5 Alarm Type (CCITT X.733)

1	Communications alarm
2	Quality of service alarm
3	Processing error alarm
4	Equipment alarm
5	Environmental alarm

126.6.4.2 ID

The alarm ID specifies, in general terms, why the given alarm was raised.

Examples of alarm IDs seen on Session Server are:

- Threshold Crossed
- Communications subsystem failure
- Loss of Signal

Please refer to section “126.19 Appendix B - Alarms” on page 1597 for a complete list of alarm IDs.

126.6.4.3 Timestamp

The alarm timestamp specifies when the alarm was raised. The date and time given were current on the Session Server system when the given alarm was raised.

126.6.4.4 Host

The session server host name from where alarm was raised.

126.6.4.5 Severity

The alarm severity specifies the seriousness of the given alarm.

Alarm severity can be one of the following:

— Warning

Indicates the detection of a potential or impending service affecting fault.

— Minor

Indicates the detection of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

— Major

Indicates that a service affecting condition has developed and an urgent corrective action is required.

— Critical

Indicates that a service affecting condition has developed and immediate corrective action is required.

Note: 'cleared' is also a valid alarm severity, but will not be seen on the Alarms Panel, since the Alarms Panel only shows alarms that are currently raised.

126.6.4.6 Description

The alarm description provides specific details about the given alarm.

126.6.4.7 Alarms Panel Limitations

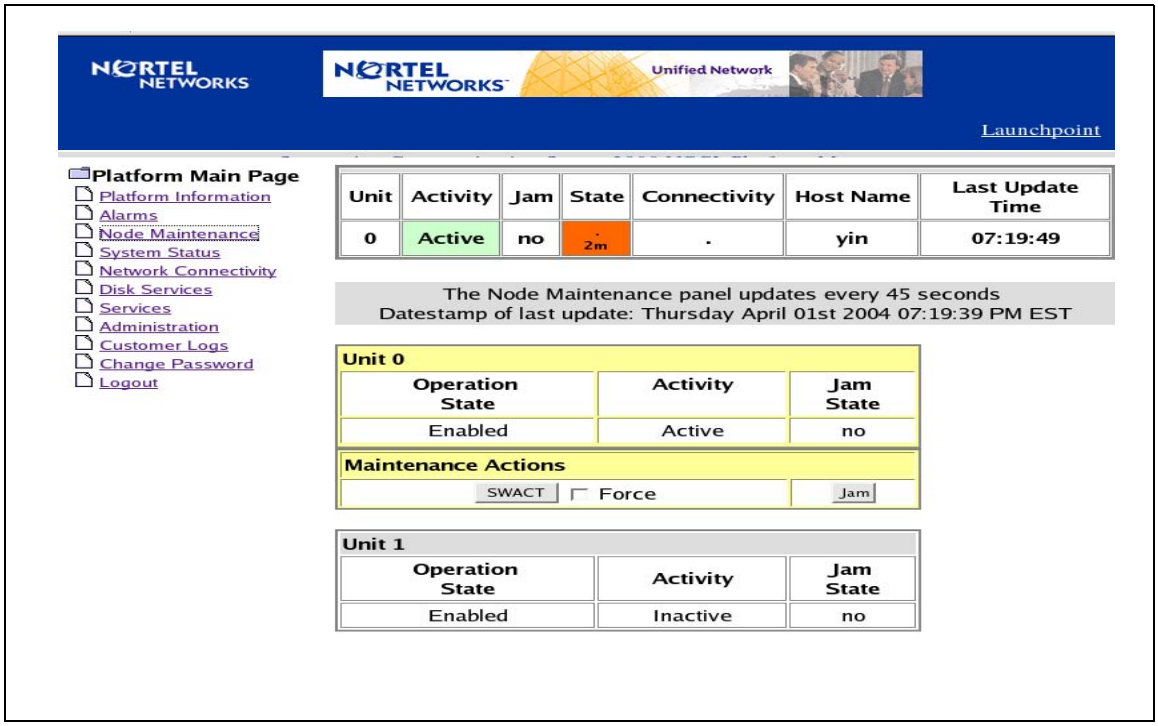
- The Alarms Panel sort order cannot be modified (it defaults to sorting by severity then by time), nor does the Alarms Panel support filtering of alarms.
- The Alarms Panel header will scroll out of sight if the browser client is not large enough to view all alarms and the user scrolls to the bottom of the window.
- If the SS system date/time are changed after an alarm is raised, the Alarms Panel does not update its timestamps. The timestamps shown at the Alarms Panel were those current at the time that the alarms were raised.

- The Alarms Panel refreshes automatically every 45 seconds. The refresh period is set by the system and is not configured
- If the system threshold values are changed after an alarm is raised, the Alarms Panel does not update its values in the *description* field. The threshold values shown at the Alarms Panel are still the values that were current at the time that the alarms were raised. In general, any of the text in an alarm is valid from the time the alarm was raised and is never updated.
- A critical alarm will not necessarily cause the system to SWACT. For a complete list of conditions that could cause the system to reset please refer to section 126.10 “Fault Handling” on page 1585.

126.6.5 Node Maintenance Actions

From the Session Server EM the user can perform node maintenance actions such as SWACT and JAM/UNJAM. This panel is refreshed approximately every 54 seconds. Figure 11, "Node MTC Frame Layout" shows the proposed layout for the node maintenance frame.

Figure 11 Node MTC Frame Layout



This frame is accessible from the menu list, namely “Node MTC”. The unit that the user is logged into will be highlighted. If that unit reboots, then the connectivity to that session will be lost. On the other hand, if the connection to the mate unit is lost, then all the fields for that unit will show unavailable status until the unit recovers.

126.6.6 System Status

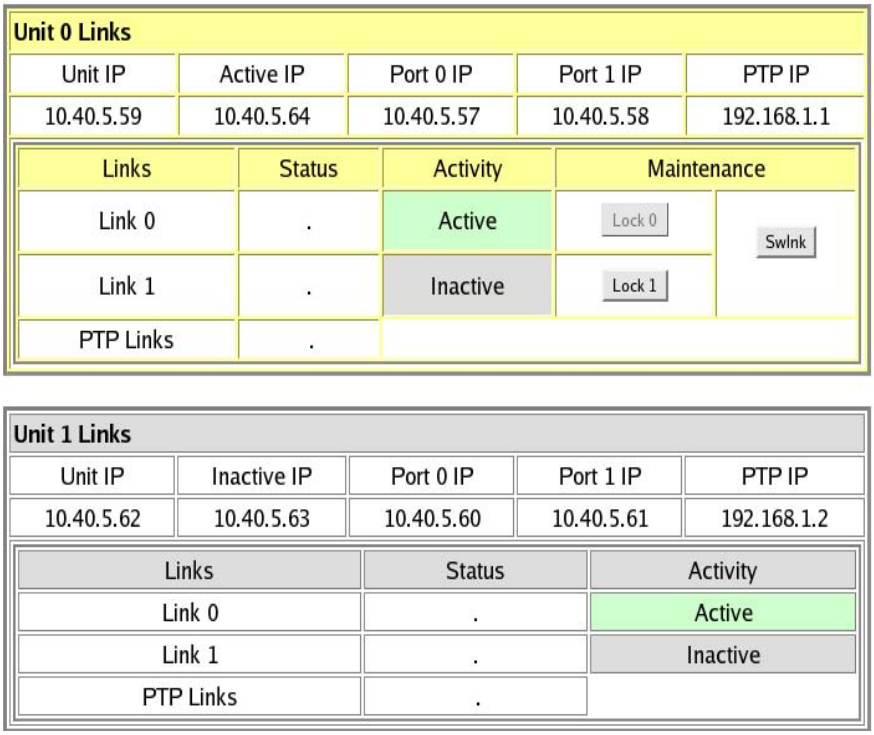
The system panel is used to view system parameters for Session Server unit. From the system panel the following parameters are available:

- view Chassis Information (system self test, chassis subsystem).
- view CPU usage (shows 1 min, 5 mins, and 15 mins load average/ threshold).
- view CPU Utilization (shows 5, 20 & 30 minsUtilization average and respective alarm thresholds)
- view the number of zombie processes on (shows minor, major, and critical alarm thresholds).
- view memory usage (shows minor, major, and critical alarm thresholds).

126.6.7 Network Connectivity / Link Maintenance

This section discusses the connectivity panel where link maintenance can be performed. When selecting this tab, the user can view both unit’s Ethernet connectivity status as well as perform link maintenance actions to lock/unlock and switch link activity. The Network Connectivity panel is refreshed approximately every 54 seconds. Figure 12, "Link MTC Frame Layout" shows the connectivity frame layout. The list of IP addresses will be shown when selecting the QueryIP button. For a complete list of valid link status please refer to Table 4, “Mapping of link States,” on page 1575.

Figure 12 Link MTC Frame Layout



Unit 0 Links

Unit IP	Active IP	Port 0 IP	Port 1 IP	PTP IP
10.40.5.59	10.40.5.64	10.40.5.57	10.40.5.58	192.168.1.1

Links	Status	Activity	Maintenance	
Link 0	.	Active	Lock 0	SwInk
Link 1	.	Inactive	Lock 1	
PTP Links	.			

Unit 1 Links

Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
10.40.5.62	10.40.5.63	10.40.5.60	10.40.5.61	192.168.1.2

Links	Status	Activity
Link 0	.	Active
Link 1	.	Inactive
PTP Links	.	

Note: In SN07 actions on mate links is not supported.
Hence the gray color for lock/unlock/SwLnk.

126.6.8 Disk Services

The Session Server EM has a storage panel which provides the following disk management functionality:

- view RAID array status
- disk maintenance
  - — remove disk
  - — insert disk
- view volume group information
- view filesystem information
- create a new filesystem
- remove a filesystem
- modify a filesystem

This panel displays information that is relevant to the local unit to which the browser is pointing.

126.6.9 Services

This panel is used to display the network active remote session status connected to the server and to view the NTP servers status.

This panel will display information specific to the Session Server unit the user is logged into. If the server local time is significantly out of sync with the NTP server, then the only way to resync the time is to reboot the inactive server, perform a swact, and reboot the newly inactive unit.

126.6.10 Admin

The admin panel is used to perform administrative tasks related to the Session Server unit. The actions supported from this panel are:

- Bootload Management (to set default bootload, or remove bootload)
- Software Upgrade, the user has the following options to upgrade the bootload:
  - — Anonymous FTP
  - — FTP
  - — HTTP
  - — HTTPS
  - — Local File
  - — Local CDROM
- Server Maintenance (reboot or halt)

126.6.11 Customer Logs

The Session Server provides the capability for the system or the application running to generate logs. The logs can be viewed on the Session Server's log view web page. Information shown about a particular log include fields shown in Table 6, "Example of Customer Logs Format," on page 1582. The Session Server generates different types of logs. This section, however, addresses the customer logs.

```
<time stamp> <hostname> <process name> <Name> <Number> <Severity> <Event Type>
<Label> <Description>

* Nov 12 15:54:56 loopback alarmd: NXTS802 MINOR INIT Array: '/dev/md0'
* |               |        |       |    |    |     |    |      |
* |               |        |       |    |    |     |    |      +--- description
* |               |        |       |    |    |     |    +---------- label
* |               |        |       |    |    |     +--------------- event type
* |               |        |       |    |    +--------------------- Severity
* |               |        |       |    +-------------------------- log number
* |               |        |       +------------------------------- log name
* |               |        +--------------------------------------- process name
* |               +------------------------------------------------ hostname
* +-------------------------------------------------------------- time stamp
```

```
Nov 11 16:20:43 loopback alarmd: XTS301 MINOR INIT Array: '/dev/md0' (/boot)
Status: The array is currently being rebuilt.
```

Table 6 Example of Customer Logs Format

Name	Number	Severity	Event Type	Label	Description
NXTS	301	CLEARED, MINOR, MAJOR, CRITICAL	Fault (FLT)	Array	Hard disk related alarm
NXTS	802	CLEARED, MINOR, MAJOR, CRITICAL, NONE	Fault (FLT) Trouble (TBL)	Error Status Threshold exceeded	Filesystem-related alarms

For screen shots of each panel on the platform main page, please refer to “126.18 Appendix A - Platform Main Web Page Interface” on page 1590.

126.7 Conditions for SWACT

There are three types of swact supported on the platform: manual, system initiated and application requested. Those types of Swacts will be performed on the node depending on the state of the system and failure conditions according to the following set of rules (except under extraordinary circumstances causing the swact to fail; the rules are listed in order of precedence):

1. A Session Server running cannot swact when running in a simplex configuration (!) or when the inactive side is completely isolated and unreachable (!!) or in “jammed” state.
2. Manual “forced” request always causes the system to swact
3. Critical failure conditions on the inactive side will prevent a swact to that inactive side.
4. Applications can reject swact requests
5. Critical failure conditions on the active side will cause a system-initiated swact.

These rules can also be summerized by the following table:

Unit status		Applications accept the SWACT		Application rejects SWACT	Manual "Force" SWACT
Active	**Inactive**	**Manual / Application requested SWACT**	**System Initiated SWACT**		
Not critical	Not critical	SWACT	(not applicable)	(no action)	SWACT
Not critical	critical	(no action)	(not applicable)	(no action)	SWACT
critical	Not critical	(not applicable)	SWACT	(no action)	SWACT
critical	critical	(no action)	(no action)	(no action)	SWACT

In the above set of rules, "critical failure conditions"are symmetrical in that the same conditions that would cause a swact from the active side would also prevent a swact to a failed inactive side. These correspond to the following cases:

- Unit not available: power loss, in the process of rebooting
- Sanity watchdog timeout, kernel panic or critical hardware failure.
- Critical netmon alarms, such as becoming isolated or otherwise no longer responding to its mate.
- Loss of one or both disks.

  Note: Manual Swact is allowed to a system which has single disk missing/fail alarm.

"Critical failure conditions" does NOT include the following, even though some alarms for those may be categorized as "critical":

- "major" or "minor" alarms for connectivity and most h/w faults
- Most H/W failures: power supply fault detection, voltage, temperature, fan, CPU, memory and other h/w failures (this is candidate content for sn08).
- OS status faults: cpu usage, memory usage, # zombie processes
- Disk usage

  Note: The OS status critical alarm is not symmetrical, It will prevent swact but does not cause system initiated swact.

126.8 Commissioning

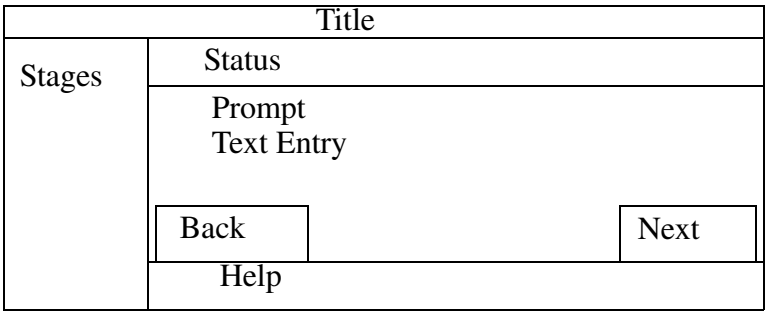
The Session Server is a standalone system. It is equipped with a commissioning tool called "commish" to allow the customer to configure the system as part of the initial setup of the server. This tool can be used at the

vt100 console port of the Session Server. The following values can be configured using the commish:

- hostname
- IP address
- Subnet Mask
- Gateway (default CS LAN router)
- Timezone
- One or more NTP servers
- Log server IP address
- NetNodes IP (Network Monitor, HTTPs proxy, and Core IP addresses)
- Server Location
- SNMP Trap destination

The user interface of the commish tool is broken up into the following sections as depicted in Figure 13, on page 1584 .

Figure 13 Commish user Interface Areas



The general philosophy is that for each screen:

- The title remains constant and indicates that this is the system setup
- The Stage bar along the left will highlight the stage on which the user is currently
- The Status will indicate in a longer form with what stage the user is interacting
- The help along the bottom indicates some useful piece of advice about what the user is being asked
- The prompt requests a piece of information from the user
- The text entry area is where the user types the requested information
- The back and next buttons are used to navigate between the screens

- The interface is navigated by using the ‘tab’ key to cycle between the text entry area and the ‘next’ and ‘back’ buttons. The ‘enter’ key is used to make a selection.

For some screenshots and details about the interface, please See “Appendix C - Commish Human Machine Interface” on page 1599.

126.9 SNMP Support

The Session Server supports SNMP V3 with “No Privacy” and “No Authentication” options. The user can use the commish tool, described in “126.8 Commissioning”, to configure two TRAP destinations and SNMPv3 user name. As part of SNMP support, the Session Server can raise the following traps to report alarms severity:

- nortelNMIalarmClearNotification
- nortelNMIwarningAlarmNotification
- nortelNMIminorAlarmNotification
- nortelNMImajorAlarmNotification
- nortelNMIcriticalAlarmNotification

126.10 Fault Handling

This section provides a summary of the fault handling behavior of the SAM-XTS node maintenance in reaction to various faults. The fault handling behaviour is based upon the compact Call Agent behavior for all but the disk cases.

Table 7 SAM-XTS Fault Handling

Fault Event	Simplex/ Duplex, Affected Unit	Action
Total Loss of LAN Connectivity	Duplex, Active	Failover to the inactive. Reset former active if condition persists for 20 seconds. After LAN connectivity is restored and reset completes, inactive unit comes back into sync.
Total Loss of LAN Connectivity	Simplex, Active	Wait about two minutes and reset active unit if persistent. (The wait handles SDM and router upgrade outage.)
Total Loss of LAN Connectivity	Duplex, Both	Wait about two minutes and reset if persistent; wait 60 seconds and reset inactive if persistent.
Single Ethernet Outage	Any, Any	Switch active ethernet if necessary. Monitor for ETH recovery.
Loss of Point to Point Connectivity	Duplex, Both	Alarm and log. Continue mate communication via LAN.
Sanity Time Out or Power Cycle	Duplex, Active	Inactive immediately takes over; former active resets.

Table 7 SAM-XTS Fault Handling

Fault Event	Simplex/ Duplex, Affected Unit	Action
Sanity Time Out or Power Cycle	Duplex, Inactive	Inactive resets
Sanity Time Out or Power Cycle	Simplex, Active	Active resets and determines mastership.
Total Disk Outage.	Duplex, Active	Failover to inactive.
Total Disk Outage	Simplex, Active	Alarm and log but wait for manual action.
Total Disk Outage	Duplex, Inactive	Alarm and log but wait for manual action.

126.11 Logs and Alarms

For a complete list of logs and alarms please refer to the FM section of ActId a00004005 book in PLS FMDOC.

126.12 Users Categories

The following is a list of groups that will be used on SAM-XTS platform. This list comes from Succession Element and Sub Element Manager (SESM), and is consistent with the existing Succession users.

Table 8 Authorization Groups

Group Name	Group Number	Description
mgcadm	1011	Can do anything. This is equivalent to being the root user
mgcmtc	1014	Can do any non-service impacting platform maintenance activities. Cannot change provisioning data.
mgcsprov	1013	Application provisioning user. Can modify provisioning data, but cannot take any platform maintenance actions
mgcrw/mgcro	1012/1015	Can view base or provisioning information but cannot initiate any changes.
succssn	104	required for login access to the Session Server

Note: The user group access permissions are not enforced on NCGL platform for SN07.

The following table describes the list of default users on the system, and their associated groups. At commissioning time, the customer will be able to remove any unneeded users, and will be forced to change the passwords on any of those which remain.

Table 9 Default Users

User Name	Groups	Removable	Description
root	mgcadm root system	no	System root user. Direct login will not be allowed - must login as another user, and can then su to the root user.
mtc	succssn users mtc mgcadm mgcrw mgcro mgcsprov mgcmtc	yes	NCGL-XTS maintenance user.

126.13 Limitations and restrictions

The Session Server does not support software alarming of the following failure situations:

- Over temperature
- CPU failure
- RAM failure
- Fan Failure
- Power supply failure (the power LED and relay contact will be raised)

There is no support for backup and restore in SN07 release.

In this release, to halt the Session Server from the admin panel is equivalent to the administrative state to lock the server.

The Session Server software does not support/include the STORM (STOrage Management) functionality.

The following process are not monitored. If any of these process die, a manual interact is required to start them.

- ssh
- syslogd

126.14 Interactions

The following external interfaces are supported on the Session Server to provide access to the server:

- SFTP or SCP (for secure file transfer)
- SSH (for secure login), which supports the following encryption algorithms:
  - 3DES 168 bits
  - Blowfish 128 bits
  - Twofish 128 bits
  - AES 128 bits

  The SSL encryption algorithms supported are:
  - RC4 - 128-bit keys
  - RC2 - 40 bit key
  - DES - 40 bit key
  - DES - 56 bit key
  - 3DES - 168 bit key
- HTTP (Session Server Web Interface)
- HTTPS (Secure HTTP)

All of the existing interfaces will be maintained, and since they are all standards based protocols, no compatibility issues are expected.

Note: The user will not be able to access the Session Server using the "telnet" command because it is not supported due to security issues.

126.15 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	___X___
Configuration	
Data Schema	___N/A___
User Interface	___X___
Element Management	___X___
Security	___N/A___
Service Order	____N/A__
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A___

Performance (includes operational measurements) ___N/A___

126.16 Glossary

Term	Description
CI	Command Interpreter
CM	Computing Module (aka “Core”)
CS2K	Call Server 2000
CS2K OAMP	Call Server 2000 OAMP (aka SESM aka PTM)
DMS	Digital Multiplex Switch
GWC	Gateway Controller
HTTP	HyperText Transport Protocol
IEMS	Integrated Element Management System
IMS	Interactive Multimedia Services
IP	Internet Protocol
MAPCI	Maintenance, Administration, and Provisioning Command Interpreter
MGC	Media Gateway Controller
NCGL	Nortel Carrier Grade Linux
NEBS	Network Equipment-Building System
NTP	Network Time Protocol
OAM&P	Operation, Administration, Maintenance, and Provisioning
OSS	Operations Support System
OSSGate	OSS Gateway
PAM	Pluggable Authentication Module
PTM	Packet Telephony Manager
PVG	Packet Voice Gateway
RFC	Request For Comments
RTS	Return To Service
SAM-XTS	Services Application Module- eXtreme Thin Server
SG	SIP Gateway application

Term	Description
SDM	Supernode Data Manager
SDP	Session Description Protocol
SESM	Succession Element and Sub Element Manager (aka CS2K OAMP, aka PTM)
SIP	Session Initiation Protocol
SIPT	Session Initiation Protocol (SPI) for Telephones
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SNM	Session Server Node Maintenance
Session Server	Platform for the SIP Gateway application
SPM	Spectrum Peripheral Module
STORM	STORage Management
SWACT	Switch of Activity
TCP	Transmission Control Protocol
VRDN	Virtual Router Distribution Node

126.17 References

1 A00003933: Session Server SIP Gateway Application

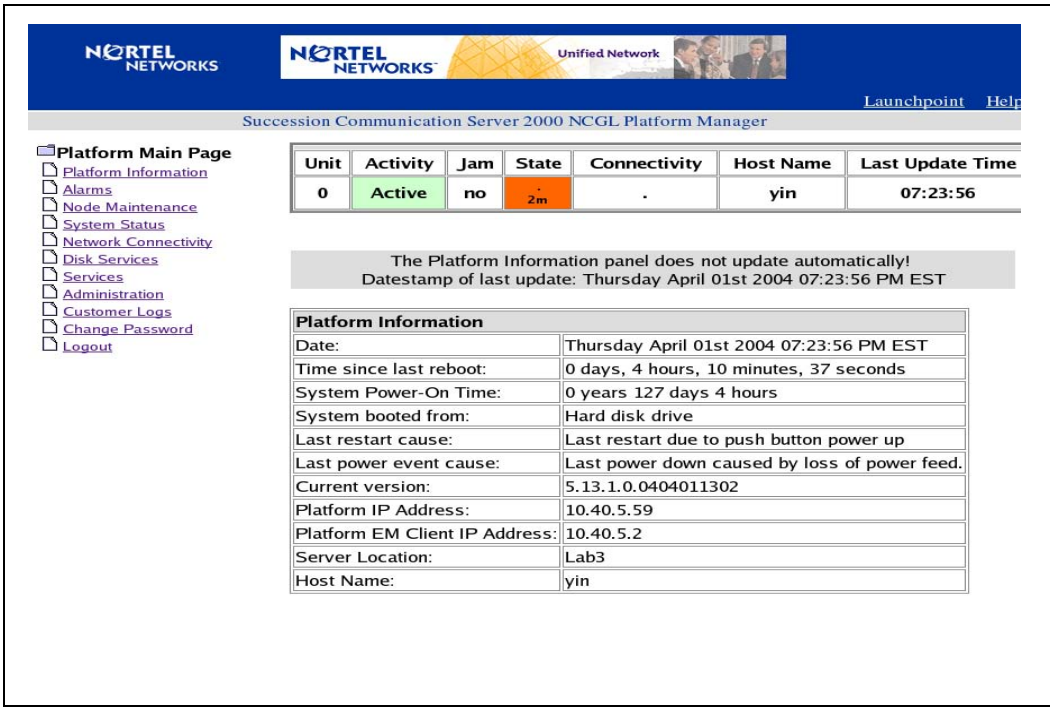
126.18 Appendix A - Platform Main Web Page Interface

This appendix contains the web page screenshots. Please note that screenshots captured here are for the Drop 1 deliverable, where the session server only supports simplex mode. This section will be updated when SN07session server full duplex functionality is completed.

126.18.0.1 Platform Home Panel

This panel will contain data for both Session Server units.

Figure 14 Home

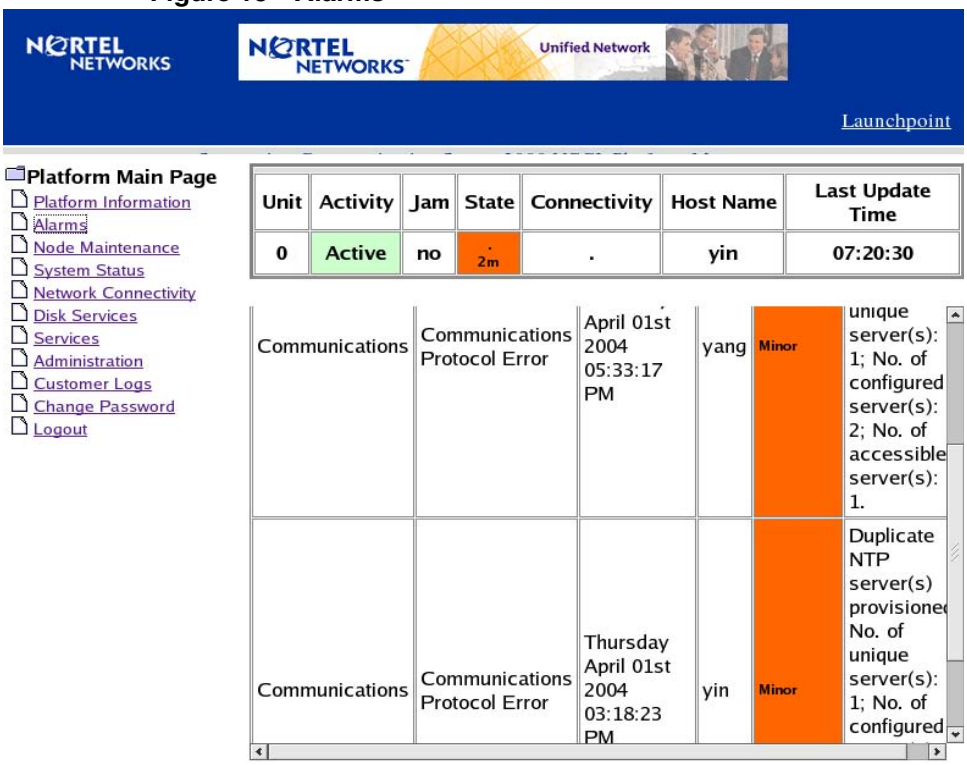


126.18.1 Alarms Panel

Like other Session Server EM panels, the Alarms panel will display the alarms on both the active and inactive units. The alarms are refreshed every 45 seconds.

Note: This screen shot is Drop1 functionality.

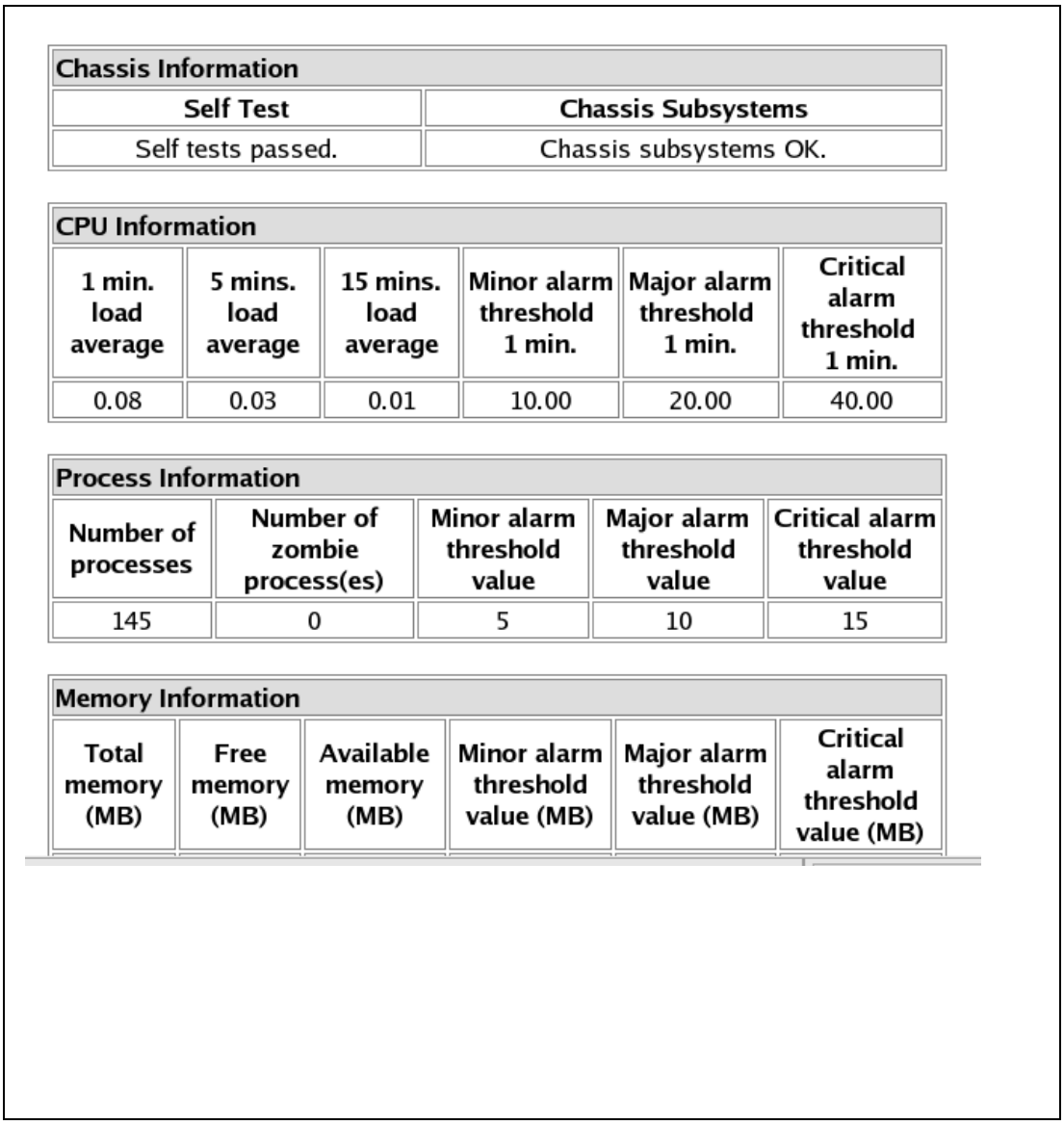
Figure 15 Alarms



126.18.2 System Panel

This panel contains data for the user's Session Server unit.

Figure 16 System Information



Chassis Information	
Self Test	Chassis Subsystems
Self tests passed.	Chassis subsystems OK.

CPU Information					
1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.08	0.03	0.01	10.00	20.00	40.00

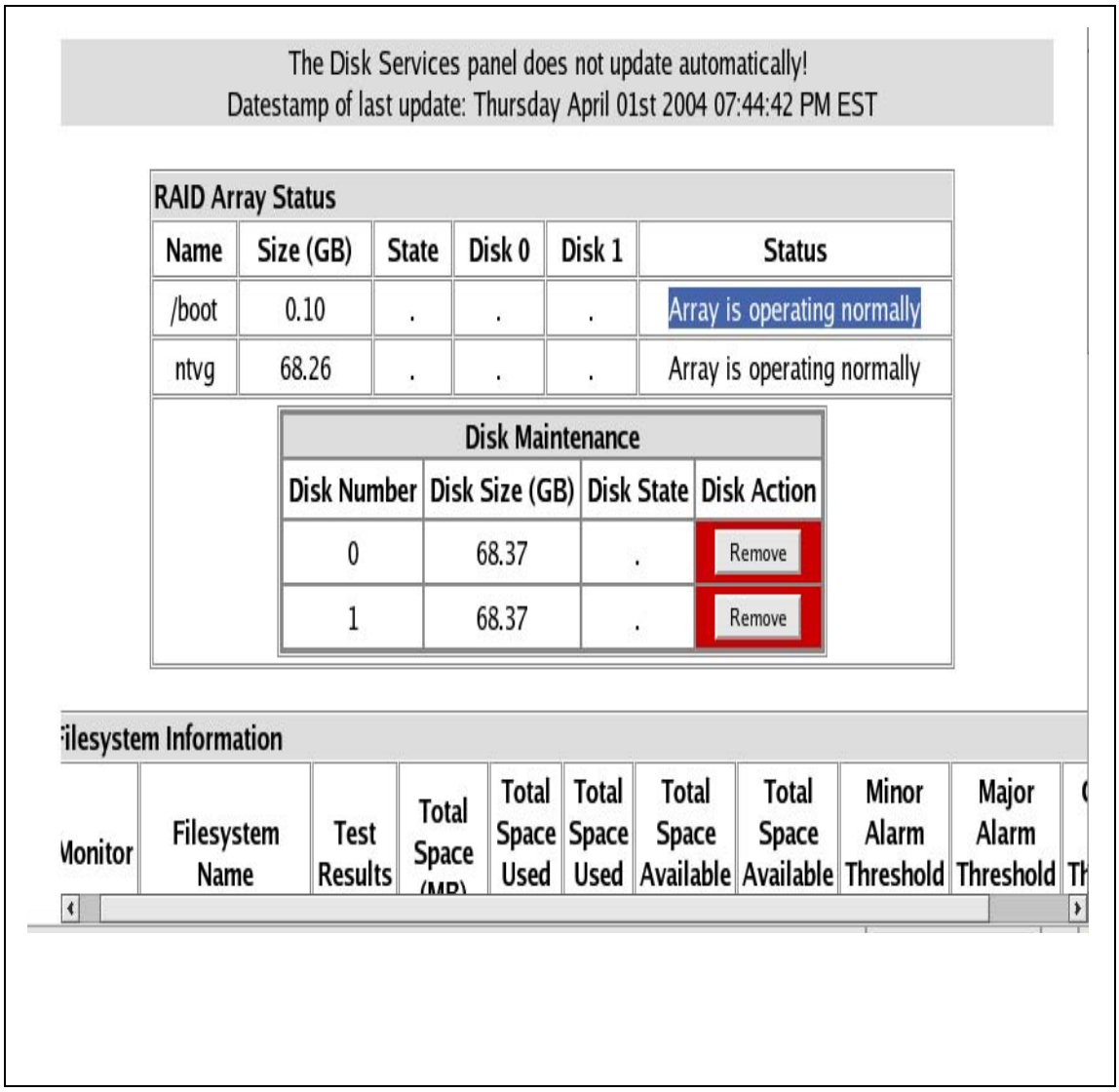
Process Information				
Number of processes	Number of zombie process(es)	Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
145	0	5	10	15

Memory Information					
Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)

126.18.3 Disk Storage Panel

This panel contains data for the user's Session Server unit.

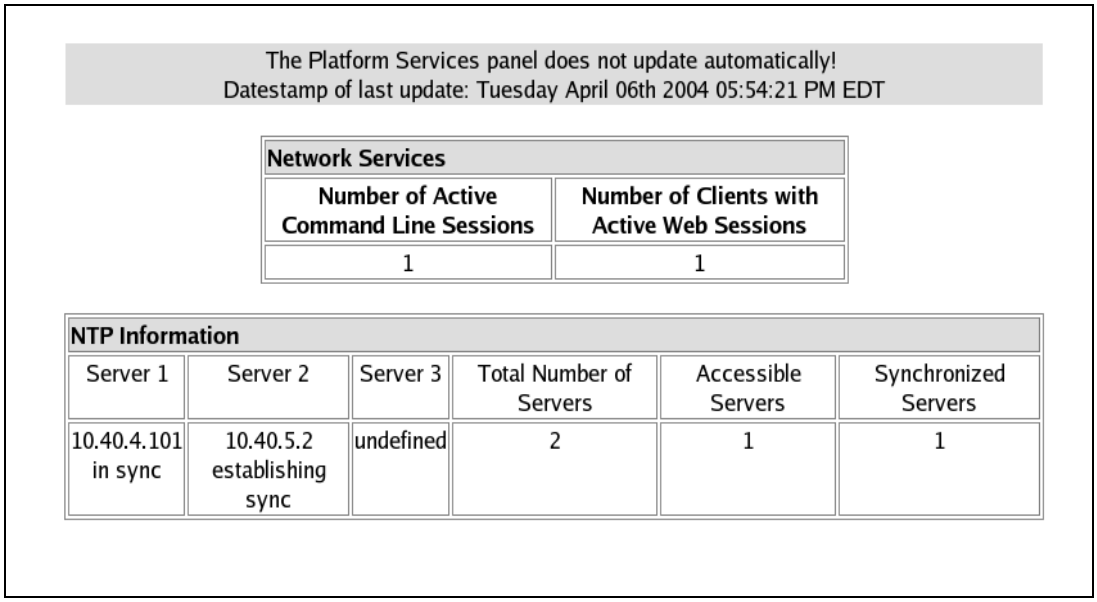
Figure 17 Storage Panel



126.18.4 Services Panel

This panel is used to display the active remote session status connected to the server, and to view the NTP servers status. This panel contains data for the user's Session Server unit.

Figure 18 Services



The Platform Services panel does not update automatically!
Datestamp of last update: Tuesday April 06th 2004 05:54:21 PM EDT

Network Services	
Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
1	1

NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
10.40.4.101 in sync	10.40.5.2 establishing sync	undefined	2	1	1

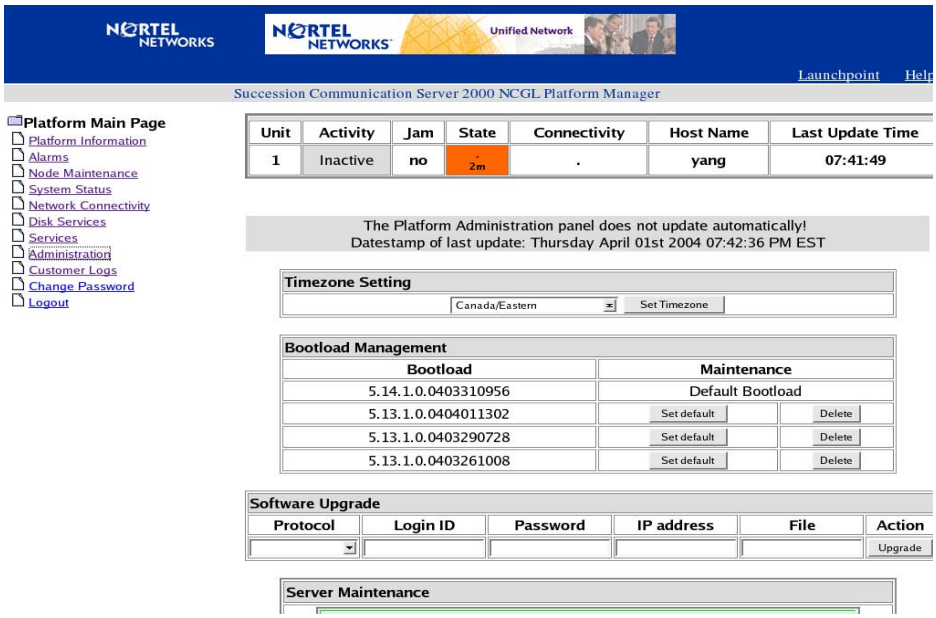
126.18.5 Admin Panel

The admin panel is used to perform administrative tasks related to the Session Server unit. The actions supported from this panel are:

- Bootload Management (to set default bootload, or remove bootload)
- S/W upgrade
- Server Maintenance (reboot or halt)

This panel contains data for the user's Session Server unit.

Figure 19 Admin

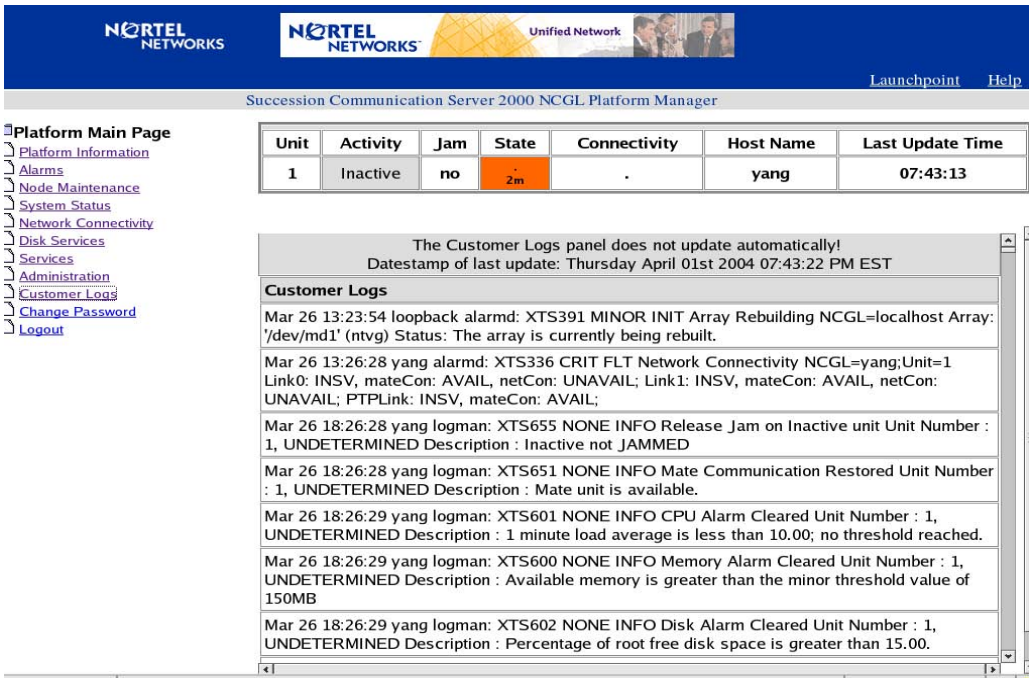


126.18.6 Customer Logs Panel

The customer logs panel displays a historical view of customer logs that have been generated on the Session Server unit. The most recent logs are displayed at the bottom of the log file.

Limitation of this panel is that the user can only view the logs that pertain to the user's specific unit.

Figure 20 Customer Logs



126.19 Appendix B - Alarms

Note that this appendix does not yet contain alarms relating to the hardware specific issues (e.g.: power supply failures, temperature, etc.).

Table 10 Alarm Id (ITU-T X.733)

ID	Type	ID	Type
1	Adapter error	30	Material supply exhausted
2	Application subsystem failure	31	Multiplexer problem
3	Bandwidth reduced	32	Out of memory
4	Call establishment error	33	Output device error
5	Communications protocol error	34	Performance degraded
6	Communications subsystem failure	35	Power problem
7	Configuration or customization error	36	Pressure unacceptable

ID	Type	ID	Type
8	Congestion	37	Processor problem
9	Corrupt data	38	Pump failure
10	CPU cycles limit exceeded	39	Queue size exceeded
11	Dataset or modem error	40	Receive failure
12	Degraded signal degradedSignal	41	Receiver failure
13	DTE-DCE interface error	42	Remote node transmission error
14	Enclosure door open	43	Resource at or nearing capacity
15	Equipment malfunction	44	Response time excessive
16	Excessive vibration	45	Retransmission rate excessive
17	File error	46	Software error
18	Fire detected	47	Software program abnormally terminated
19	Flood detected	48	Software program error
20	Framing error	49	Storage capacity problem
21	Heating/ventilation/cooling	50	Temperature unacceptable
22	Humidity unacceptable	51	Threshold crossed
23	I/O device error	52	Timing problem
24	Input device error	53	Toxic leak detected
25	LAN error	54	Transmit Failure
26	Leak detected	55	Transmitter Failure
27	Local node transmission error	56	Underlying resource unavailable
28	Loss of frame	57	Version mismatch
29	Loss of signal	101	Authentication Failure[a]
102	Breach of Confidentiality	103	Cable Tamper
104	Delayed Information	105	Denial of Service
106	Duplicate Information	107	Information Missing
108	Information Modification Detected	109	Information Out of Sequence

ID	Type	ID	Type
110	Intrusion Detection	111	Key Expired
112	Non Repudiation Failure	113	Out of Hours Activity
114	Out of Service	115	Procedural Error
116	Unauthorized Access Attempt	117	Unexpected Information
118	Unspecified Reason		

a. ITU-T X.733 alarm ids from 58 to 100 are reserved - not assigned yet

126.20 Appendix C - Commish Human Machine Interface

This appendix captures screenshots of the commish tool.

Figure 21 This is the introductory stage

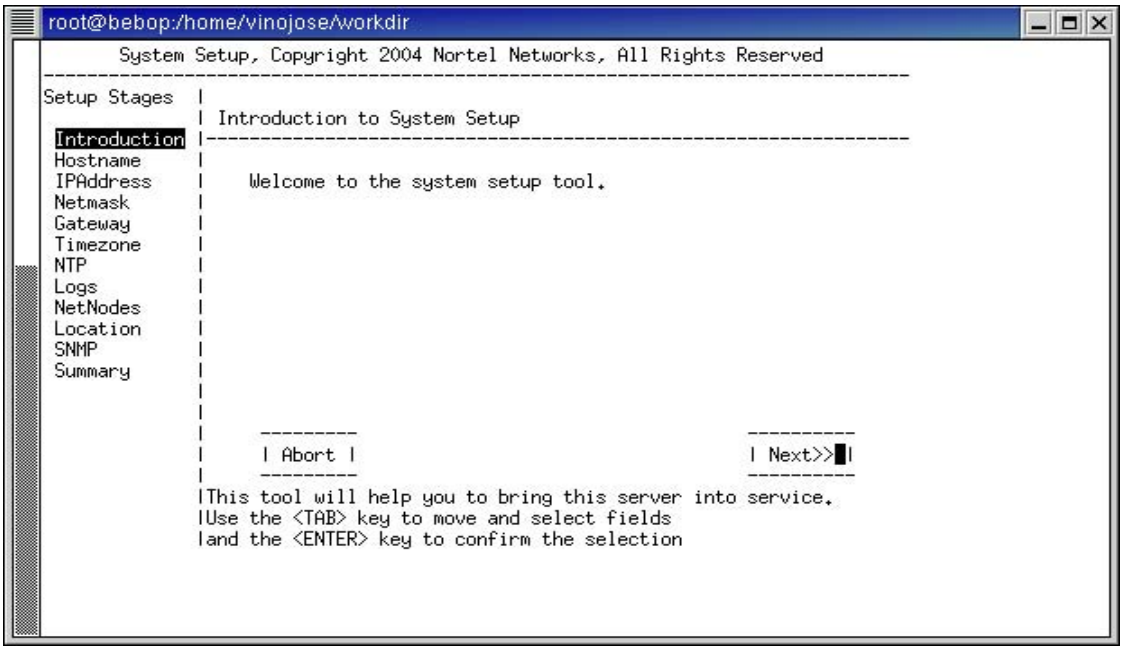


Figure 22 This stage allows the user to enter a hostname

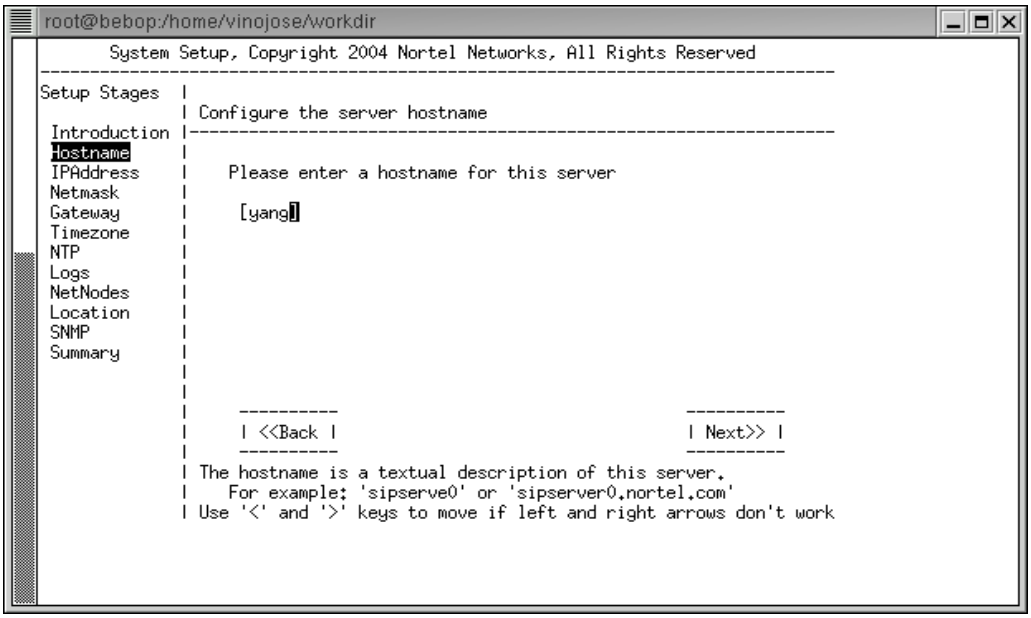


Figure 23 This stage allows the user to enter an IP address

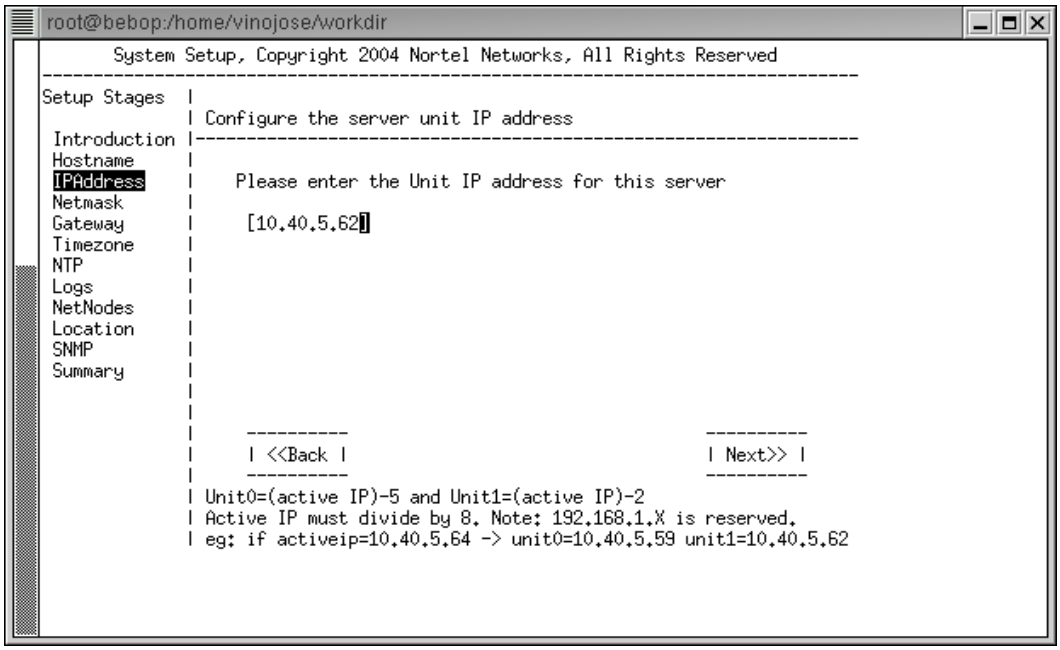


Figure 24 This stage allows the user to enter a network mask IP address

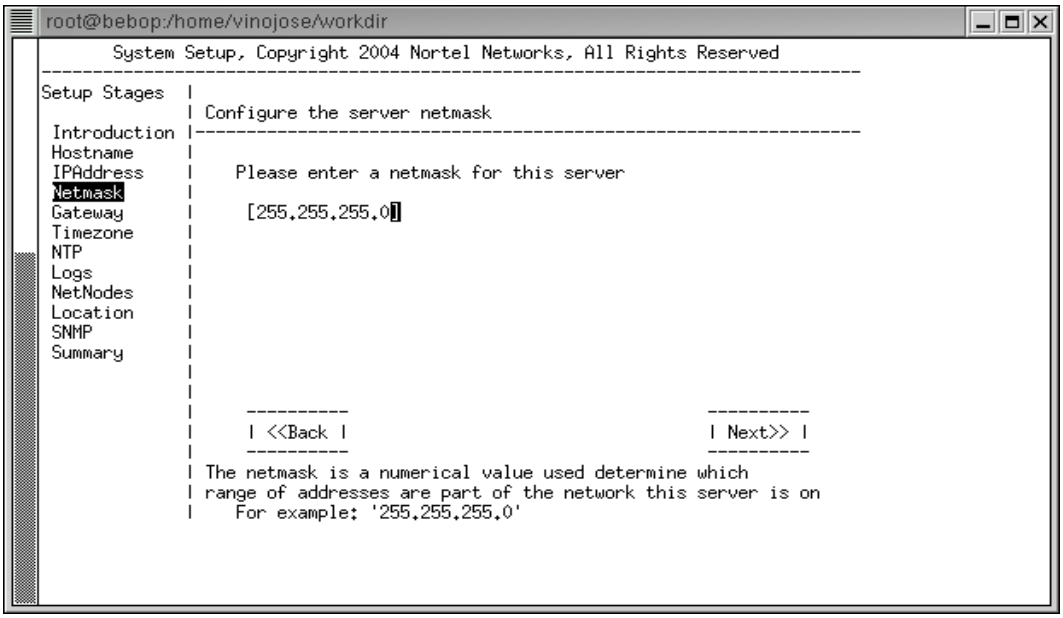


Figure 25 This stage allows the user to enter a gatway IP address

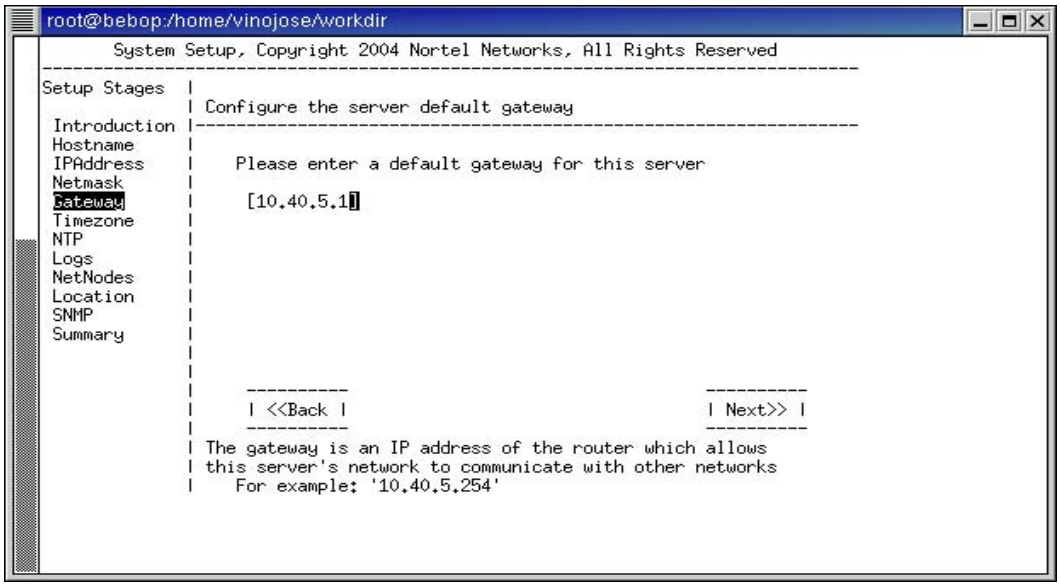


Figure 26 This stage allows the user to select time zone

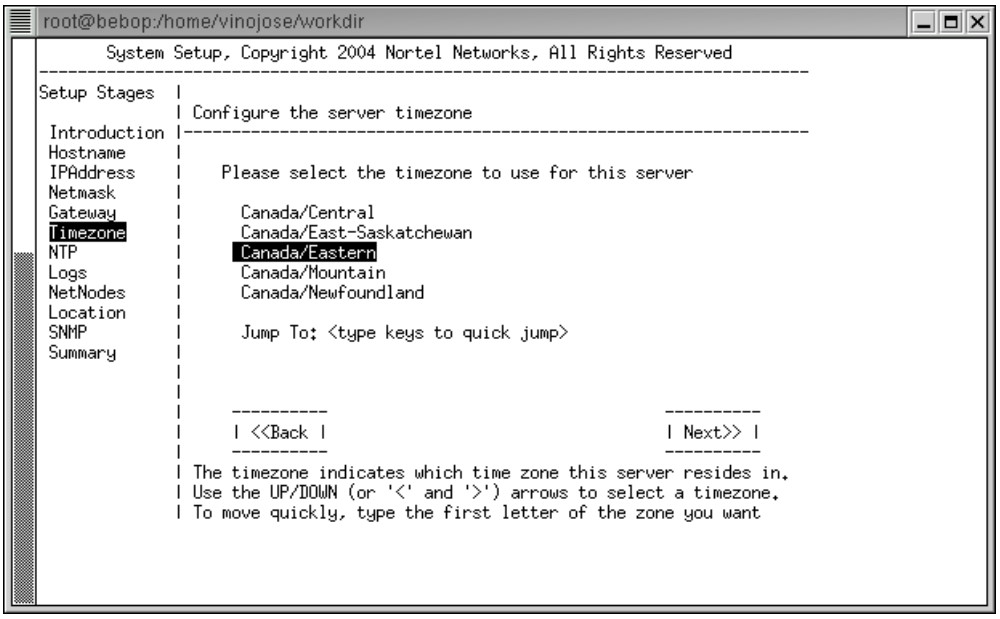


Figure 27 This stage allows the user to enter a NTP server IP address

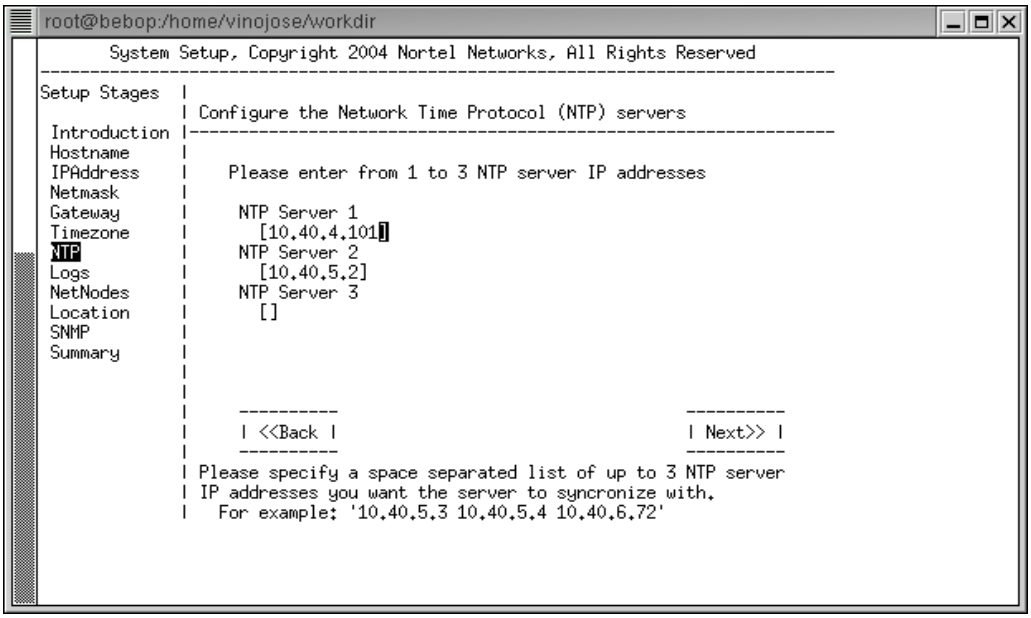


Figure 28 This stage allows the user to enter an IP address for log server

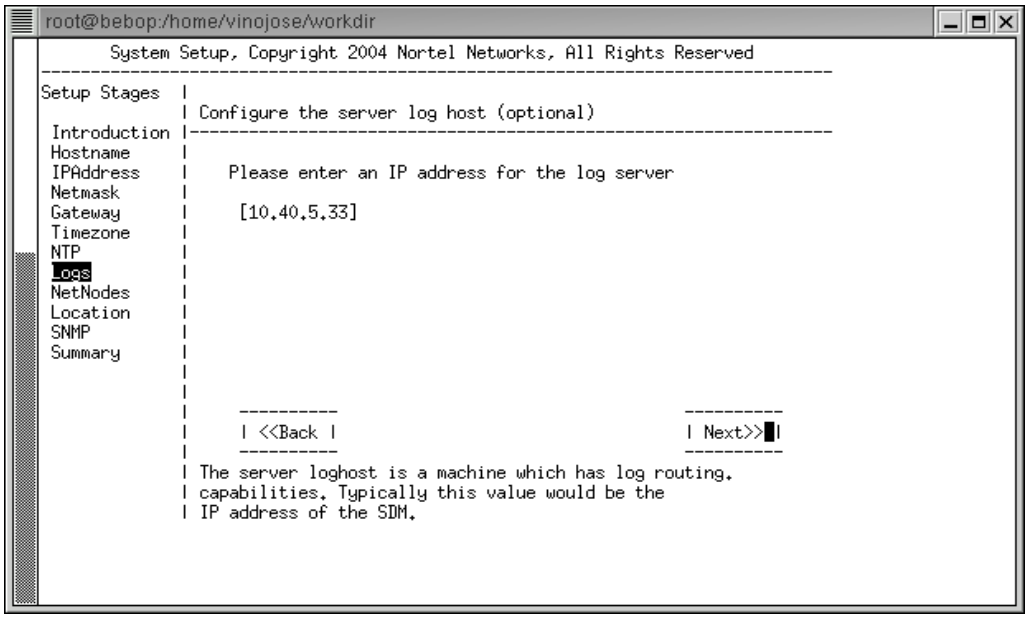


Figure 29 This stage allows the user to enter Network Monitor, Core and Proxy IP addresses

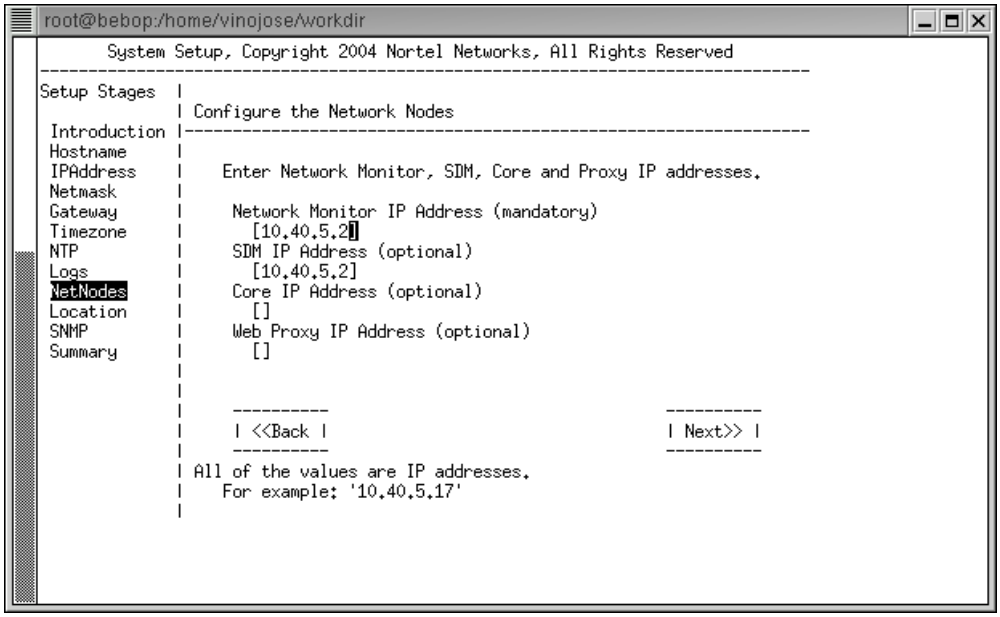


Figure 30 This stage allows the user to enter session server location

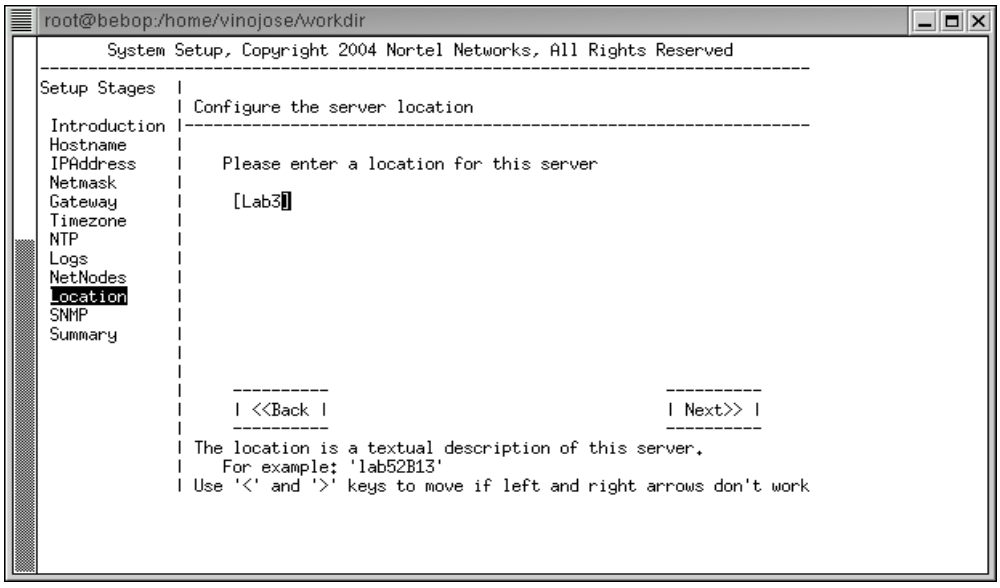


Figure 31 This stage allows the user to select SNMP trap destination

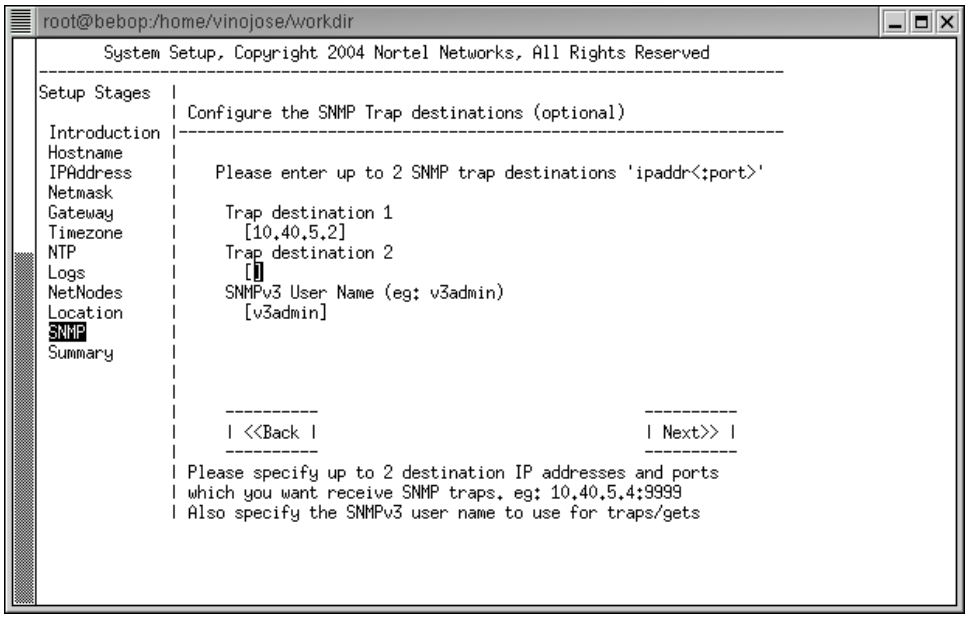
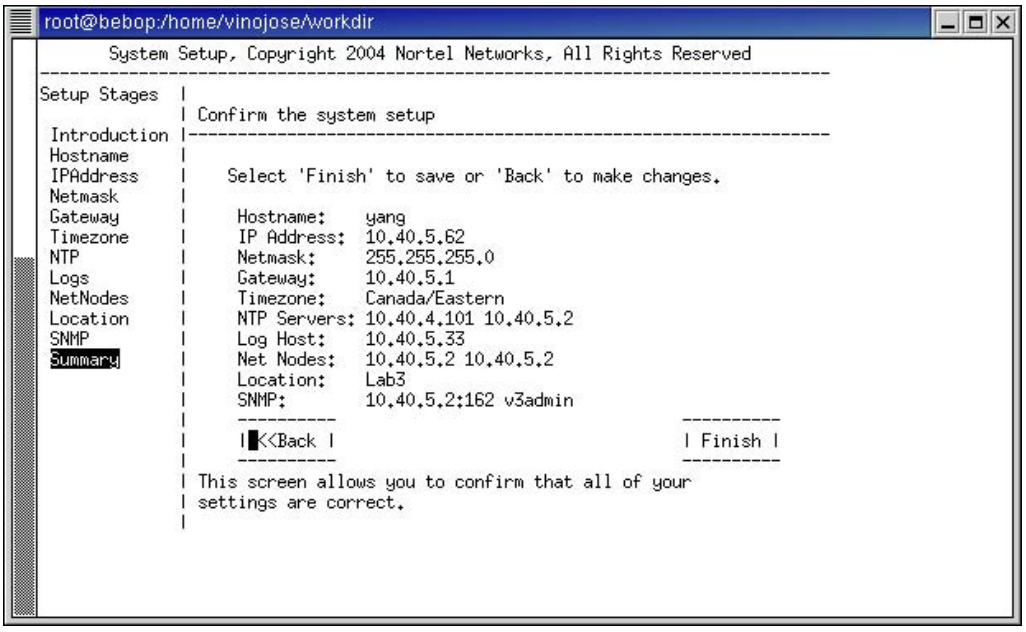


Figure 32 This is the summary screen



127: Functional Description (FN): A00004020, USP Java GUI Introduction to Succession

127.1 Reference Architecture

The following figure may be used as a reference architecture throughout this feature description

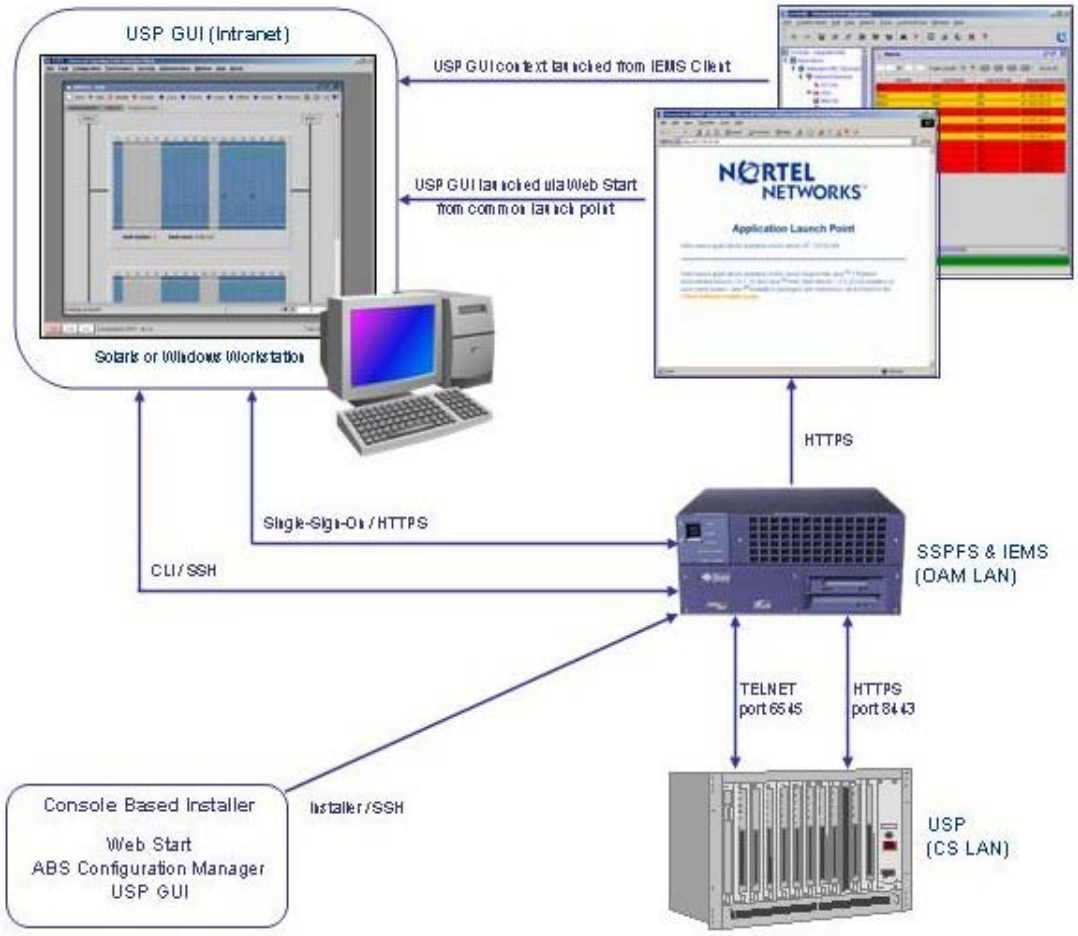


Figure 1 SN07 USP GUI Reference Architecture

127.2 Feature Descripion: GUI Enhancements

127.2.1 TELNET and SSH Proxy Support

Due to LAN security requirements, the USP GUI is not allowed to connect directly to the USP. In previous releases this was addressed by the use of a central PC running Citrix Metaframe. Users would connect to the PC via a Citrix client and then launch the USP GUI from the PC to connect to the USP. This function was referred to as “Reach Through.”

As of SN07 the GUI will be replaced with a thin Java compiled client GUI which will include the ability to connect to the USP via a TELNET or SSH proxy. For Succession solutions a SSH proxy function will be used on the SSPFS that will eliminate the need for the “Reach Through” PC in the solution.

The proxy function will actually be provided as a two-stage connection process between the GUI, the SSPFS and the USP (the complexity of this connection process will be hidden from the user by the GUI):

1. USP GUI establishes a SSH connection to SSPFS

2. USP GUI then establishes a TELNET from SSPFS to the USP

The configuration of the authentication and proxy function is captured in figures 2 and 3.

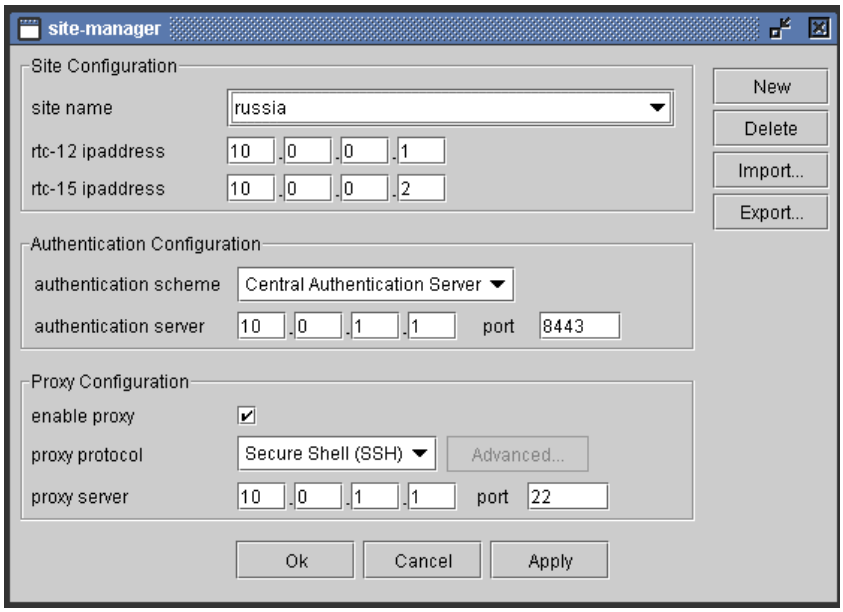


Figure 2 Site Manager Proxy Configuration - Basic

127.2.1.1 Site Configuration Export/Import

USP8.1 adds the ability to save a list of configured sites to a text file via the “Export” function. This file may then be distributed to all users and loaded via the “Import” function. This ability has been added due to the fact that we now have more data to configure for each site (authentication and proxy options). This will save the customer time and avoid configuration errors.

127.2.1.2 Authentication Scheme

User’s have the option of selecting “Standard Authentication” or “Central Authentication Server” authentication schemes. The standard authentication will use the supplied user name and password to perform authentication at the USP and proxy (if enabled). To perform advanced authentication the user may wish to use a central authentication server to perform a PAM + Proxy authentication using HTTPS. The standard authentication mechanism is the default authentication scheme for direct connections (no proxy) and the central authentication server mechanism is the default authentication scheme for proxy connections (proxy enabled). Refer to IEMS Single Sign-on Support for further details on using the PAM + Proxy authentication function.

127.2.1.3 Authentication IP Address and Port

If the authentication scheme is “Central Authentication Server” then an IP address and port must be supplied of the authentication server. The default port value is the HTTPS authentication port of 8443.

127.2.1.4 Proxy Protocol

User’s will have the option of selecting TELNET or SSH as the protocol to be used to connect to the proxy. For Succession solutions, SSH will be the required protocol (other customers and solutions may choose to use the TELNET option). If the proxy is enabled, SSH will be the default protocol.

127.2.1.5 Proxy IP Address and Port

If the proxy function is enabled, then an IP address and port must be supplied for the proxy server. The default port value is the well known Telnet or SSH port (dependent on the proxy protocol chosen).

127.2.1.6 Advanced Tokens

The advanced proxy token configuration allows the user to adapt the behavior of the proxy token matching when connecting through the proxy server. The default token values should be sufficient, but is provided for the ability to adjust the values to work with different Telnet proxy servers. Special keywords are available for the send value to eliminate the need to supply user name, password and/or IP addresses as part of the proxy token matching.

The following special send token values are available:

%u – resolves to the current user name

%p – resolves to the current password supplied (or special security token if using “central authentication server” authentication scheme)

%a – resolves to the IP address of the target end connection point (RTC)

%h – resolves to the fully qualified domain name of the target end connection point (RTC)

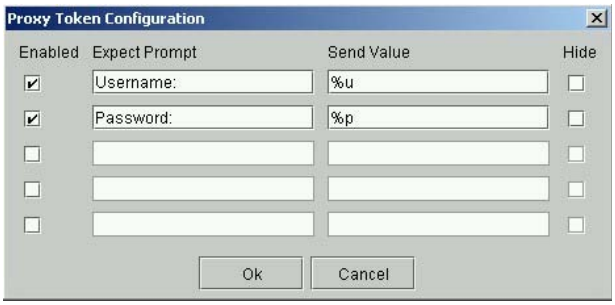


Figure 3 Site Manger Proxy Configuration - Advanced

127.2.2 Prompt for Password

During the log process or when the GUI is re-establishing a connection to the USP it is possible that the user's password may no longer be valid. For example, consider the case of a secure-id or another "time-to-live" security token. If the user has been logged in and an RTC is reboot the connection will need to be re-established and the user may need to re-authenticate (effort is being made to reduce the likelihood of this occurring). In this case we do not want the user to have to terminate the current simplex connection in order to re-establish the duplex connection. We will simply present the user with the session-login screen and prompt them to re-enter their password.

127.2.3 IEMS Single Sign-on Support & Context Launch

The IEMS provides a PAM + Proxy authentication mechanism for the central authentication server scheme. When "Central Authentication Server" authentication scheme is chosen, the GUI will use the supplied IP address and port to establish an HTTPS connection to the IEMS server. Using the supplied user name plus password or supplied security token (if context launched) to request a single time-to-live (TTL) security token from the IEMS. The TTL token will then be used to obtain single-use (SU) security tokens when establishing connections to any other end-points. This will ensure a secure authentication mechanism regardless of connection protocol.

The GUI can be context launched using either the user-name and password or a user-name and single-use security token. The user-name is supplied using the –u command line option and is used in conjunction with the –p (password) or –t (security token) options to perform the initial authentication with the IEMS server.

See figure 4 for a single sign-on walkthrough using the IEMS for central authentication.

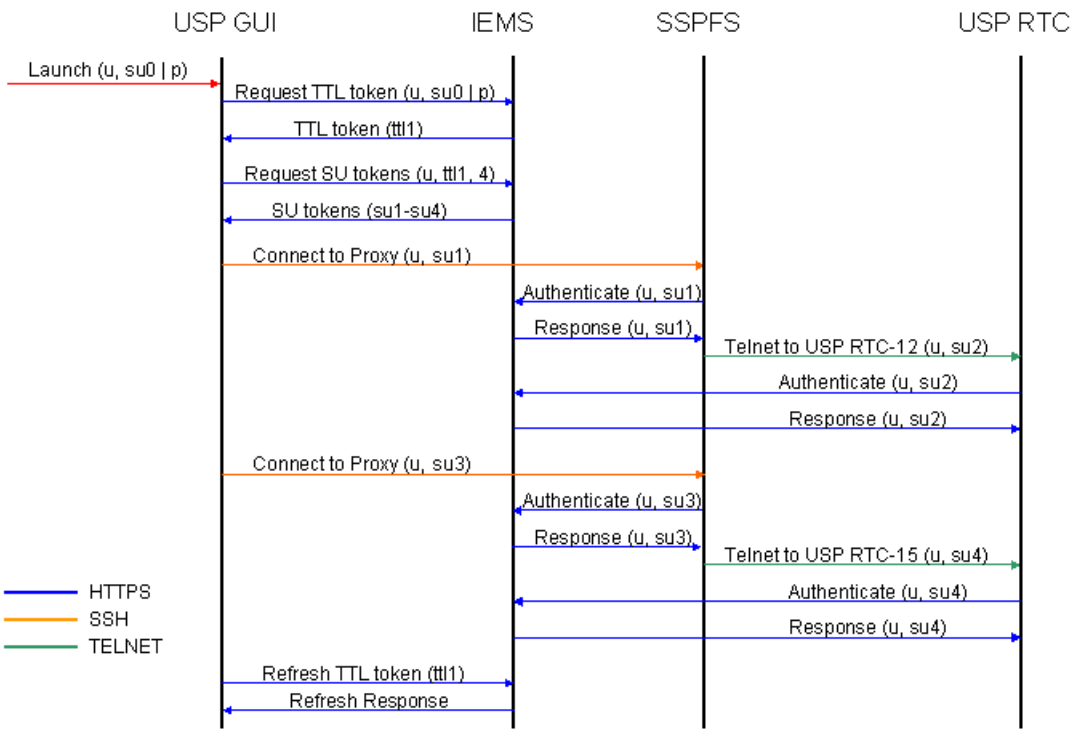


Figure 4 - single-sign-on Walk Through

127.3 Feature Descripion: Installer Enhancements

127.3.1 Web Start Support

In the past customers have always installed the GUI either on their local desktop or on the reach-through PC running Citrix Metaframe. As of USP9.0, users will still be able to install the GUI locally but will have the additional option of installing the GUI on a central web server and launching via Java Web Start. This is the option that will be used for Succession in SN07. The Web Server is provided by the SSPFS platform. Refer to Figure 1 as a reference.

127.3.2 Console Based Installer

The USP uses Install Anywhere™ to manage software installation. For a UNIX based installation (as used by Succession SN07) a console based install option is available. This eliminates the need to use the graphical version via remote display (i.e. Exceed). The installer provides the same functionality as the graphical version.

A user would simply insert the CD-ROM into the SSPFS platform (or FTP a copy of the CD image onto the SSPFS from a remote location), SSH (or TELNET) into the SSPFS and execute the installer with the `-i console` option.

A simulated trace of a console based install process is provided below:

```
$ ./install.bin -i console

Preparing CONSOLE Mode Installation...

===============================================================================
Universal Signaling Point v9.0.0      (created with InstallAnywhere by
Zero G)
-------------------------------------------------------------------------------


===============================================================================
Introduction
------------

InstallAnywhere will now guide you through the installation of the
Universal Signaling Point software components.

It is strongly recommended that you quit all programs before continuing
with this installation.

Respond to each prompt to proceed to the next step in the installation.
If you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

Press <ENTER> to continue:

===============================================================================
Component Selection
-------------------

Enter a comma separated list of numbers representing the software
components that you would like to install. To view a detailed
description of each software component enter '?<COMPONENT-NUMBER>'

    1- [X] USP Software Loads and ABS Manager
    2- [X] USP Graphical Interface Client
    3- [X] USP User Manuals and Documentation Suite
    4- [ ] USP GR-310 Mediation Application

Enter software component numbers and press <ENTER> to continue:
```

```
=============================================================Inst
allation Directory
----------------------

Default installation directory: /data/usp

Enter an absolute path, or press <ENTER> to accept the default:

=============================================================

Installation...started. This may take a few minutes to complete.

Installation...completed.

The selected Universal Signaling Point software components have been
successfully installed.

Press <ENTER> to exit
```

127.4 Log & OM Information

No change to existing logs and operational measurements.

127.5 Feature Impact

127.5.1 Memory, Real-Time or Disk Space etc

no impact

127.5.2 Hardware

test labs will need access to a SSPFS platform and SN07 load running the IEMS software.

127.5.3 Documentation

127.5.3.1 User Manuals

> The user manuals will need to be updated with respect to the changed site-manager GUI screens.

> The use of a proxy for connection will need to be added to the security overview section

> upgrade procedure will need to be changed to reflect GUI install on SSPFS

127.5.3.2 Readme.txt & Release Notes

> A reference should be added to the release notes regarding new proxy and web-start functions as well as the console based installer option.

> upgrade procedure will need to be changed to reflect GUI install on SSPFS

127.5.3.3 OAM Interface Specifications

no impact

127.5.3.4 Installation Methods

> initial install procedure will need to be changed to reflect GUI install on SSPFS

> migration mop for moving the GUI to the SSPFS and removing the PC from the solution will need to be written.

127.5.4 Compliancy Impact

no impact

127.6 Restrictions & Limitations

none

128: Functional Description (FN): A00004036

118.1 Feature name

Off-Board Service Control

118.2 Description

This activity addresses the development associated with enabling in the DMS the update and/or query capabilities for the service listed in the Chapter 5 Section 5.7 of GR-1298 “Information Revision Messages”, which outlines specific groups as well as the services and/or functions relevant to each group.

Given that the appropriate network architecture is available, with the addition of this set of capabilities in the DMS, subscriber’s will have the ability to both query the status and/or programmed information (if applicable) as well as activate/deactivate and update their corresponding service.

While the first iterations will rely heavily on Advanced Intelligent Network (AIN) (the initial protocol support is Abstract Syntax Notation 1 (ASN.1) via Signaling System No. 7 (SS7)), it should be understood that the intention is for the individual update and/or query service event handlers ***not*** be protocol dependent nor coupled to AIN directly.

There is much to benefit, however, in abiding by GR-1298; primarily compliance but it also provides an initial set of requirements and capabilities that are already generally available. The following sections outline GR-1298’s Service Data Function (*SDF)* groups as well as their corresponding capabilities and relevant services.

This development allows end user to activate/deactivate the service as if he/she have done from their own phone. Based on the service provider’s interface for the end-user it take out the complexity to activate, deactivate, add, change, delete or edit service specific data faced by end-user using a phone. The query/ update messages that are sent between the SSP and the SCP are logged into AINT700 logs using AINTRACE tool.

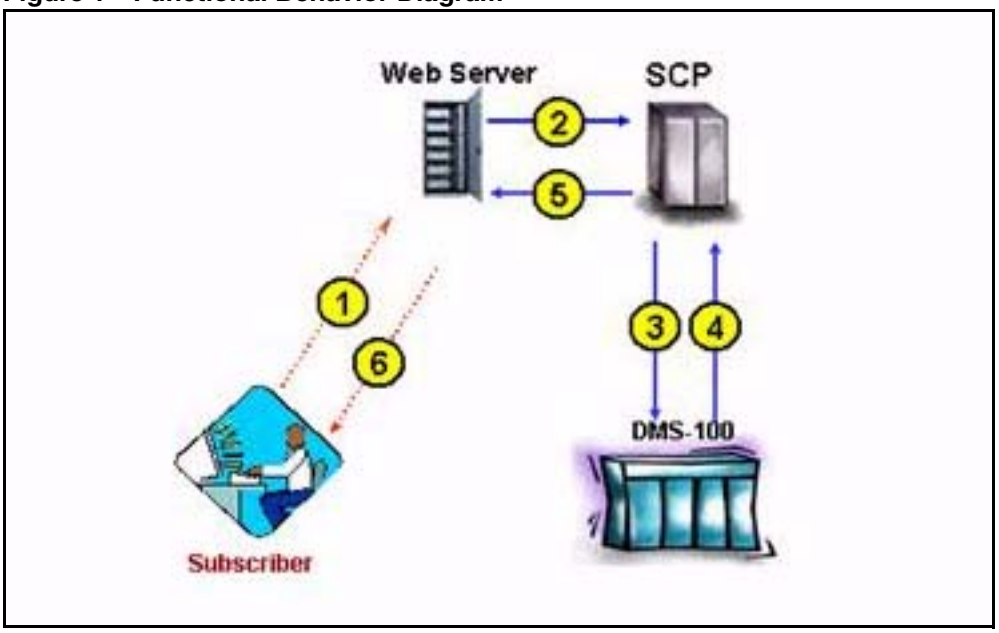
This development also allows the service providers to access the incoming / outgoing call memory of a particular DN.

118.2.1 Functional Behavior

Recognizing that the scope of this activity does not go beyond development in the Core, Figure 1, "Functional Behavior Diagram" below illustrates the basic control capabilities this activities intends to enable Off-board service control (given an AIN network solution). The following steps outline the basic tasks:

1. The subscriber logs into the Provider's network and, via Web or PC Client based application, gains access to his or her subscriber service control level. From here, the subscriber can generate a request for information about subscribed to services and/or an update to change, for example, the status of a service.
2. The subscriber's update/query request is delivered to the Provider's Network Server where a properly encoded message is created and dispatched to the SCP enabled in the Provider's network.
3. The update/query request is delivered to the SCP where a properly encoded message is created and dispatched via (SS7 or TCAP/IP) to the End-Office serving the subscriber.
4. The End-Office handles the request and replies with the appropriate response. A query response, for example, contains the information requested (e.g. status of a service).
5. The response is delivered to the Provider's Network Server where it is put into a format understood by the application serving the subscriber and, finally,
6. The formatted response makes gets delivered to the subscriber's application where the information is displayed.

Figure 1 Functional Behavior Diagram

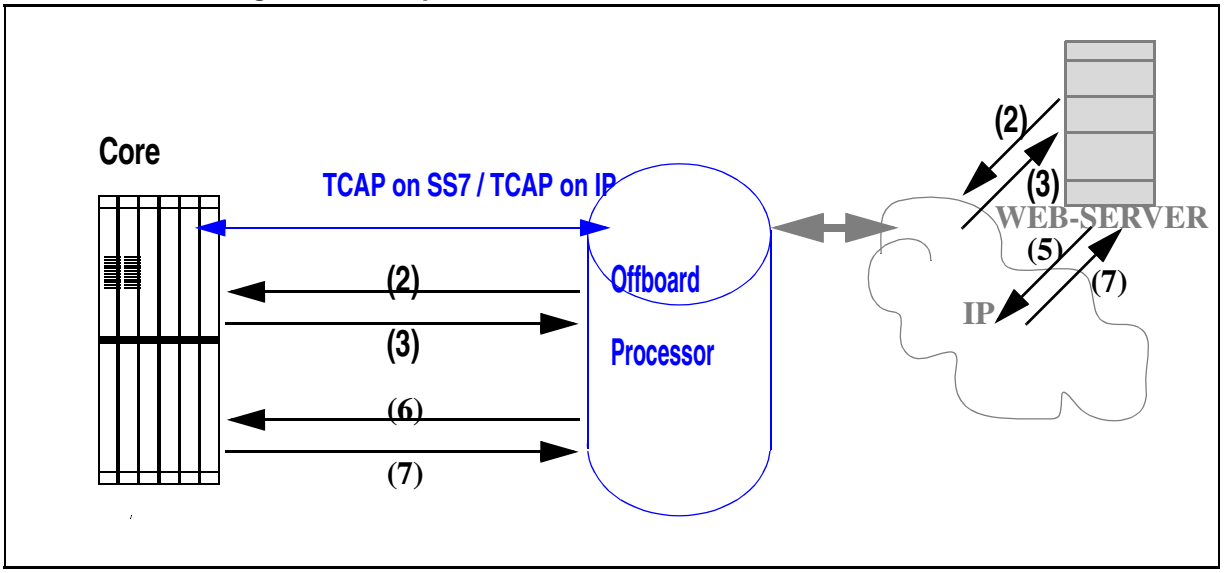


Note: It should be understood that the behavioral diagram outlined above represents only one of several possible network solutions and, while it represents the most plausible configuration in the short term, should not be considered the only alternative.

118.2.2 Sample Data Flow

The Figure 2, "Sample Data Flow" for the service management feature has been described below:

Figure 2 Sample Data Flow



1. The end-user browses the web-site, logs into the his / her account. E.g.: Myaccount@MyServiceProvider.com.
2. The Web client triggers a Query to the Off-board Processor, the Off-board Processor in turn generates a TCAP Query Request (NCR) to the Core.
3. The Core responds with the TCAP Query Response (NCR) message which return the users current profile, i.e. the current features assigned to the subscriber, their activation status and relevant attributes.
4. The end-user may decide to change certain services, for e.g.: SLE lists, call forward DN, or turn the call forward busy on the line. The user submits these changes.
5. This triggers the Offboard processor, which could be either of the SCP, IMS or an independent box.
6. The off-board processor in turn Builds TCAP Non Call Related Messages (e.g.: Update Message) and sends to the Core /Switch.
7. The Core / Switch will process the request and respond with the outcome of the request.
8. The Web-server could further use other Query Requests and Update Message to retrieve updated information for a user profile and change the feature attributes.

118.2.3 Query request for Incoming/ Outgoing call memory.

In order to obtain the incoming/ outgoing call memory of a DN, a query request is sent by the SCP. 'Provide Info' parameter of the query request contains parameter 'RequestMemorySlot' which contains subparameters 'incoming'and 'outgoing'. Once these parameters are received in the query request, the SSP sends back the following information in the 'MemorySlot' subparameter of the 'InfoProvided' parameter of the Response:

118.2.3.1 Incoming

The 'incoming' parameter contained within the 'MemorySlot' parameter contains the following subparameters.

- Calling Party number: This parameter displays the last number which had called the concerned DN.
  - — When the IncomingCall memory has OriginatingDN Presentation Indicator set to Suppressed, the Address Digits shall not be sent to the SCP in Query Response. The Presentation Indicator shall be set to Presentation Restricted.
  - — When the IncomingCall memory has Calling Party ID UNAVAILABLE, the SSP shall include the Empty parameter in the Query_Response Return Result with a value indicating the incoming memory slot is empty.

- Timestamp: This parameter defines the time at which the event has occured. It uses local time and gives the difference between the local time and GMT (Greenwich mean time). In this case it gives the time at which the calling party had made the call to the concerned DN.
- Empty: If the SSP, in processing the request finds the incoming or outgoing memory slot empty, or the list requested empty, the SSP shall include the Empty parameter in the Query_Response Return Result with a value indicating which requested data slots were found to be empty.

118.2.3.2 Outgoing

The ‘outgoing’ parameter contained within the ‘MemorySlot’ parameter contains the following subparameter.

- Called Party number: This parameter displays the last number called by the concerned DN.
- Empty: If the SSP, in processing the request finds the incoming or outgoing memory slot empty, or the list requested empty,, the SSP shall include the Empty parameter in the Query_Response Return Result with a value indicating which requested data slots were found to be empty.

118.2.4 DN Validation

The DN Validation requires TCAP query for certain services. GR-1298 is not clear on how to allow the DN validation for Non-CallP services. However, we are able to provide DN Validation using TCAP query. The following is the details for the DN Validation behavior for Non-CallP query and update request from the SCP:

118.2.5 SDF Group 1

Group1 services are those generally provided with the ability to

- activate and/or deactivate
- retrieve the status

The following is a list of services GR-1298-Core classifies as Group1.

- Message Waiting Indicator (MWT, CMWI, AINMWT etc.)
- Visual Message Waiting Indicator (MWL, CMWI, AINMWT etc.)
- Anonymous Call Rejection (ACRJ)
- Automatic Callback (deactivation or *cancellation* only) (ACB)
- Automatic Recall (deactivation or *cancellation* only) (AR)
- Call Screening (CSMI)
- Outside Calling Area Alerting (LDSA)

- Calling Identity Delivery and Suppression (activation -> *set the pps to public* and deactivation -> *set the pps to private*) (SUPPRESS)
- Call Waiting (CWTACT)

The following service is not classified by GR-1298-Core but supported by CM under Group 1:

- Make Set Busy (MSB)

Note: The Section 118.7.1 describes the encoding/decoding of MSB.

118.2.6 SDF Group 2

Group2 services are those generally provided with the ability to

- activate and/or deactivate
- update a corresponding delay interval value.
- retrieve the status and/or delay interval value.

The following is a list of services GR-1298-Core classifies as Group2.

- Audio Message Waiting Indicator (PRN)

118.2.7 SDF Group 3

Group3 services are those generally provided with the ability to

- activate and/or deactivate
- add/delete list entries corresponding to a specified Directory Number (DN), Speed Call Code or Incoming Memory Slot
- delete all list entries
- delete all private entries
- retrieve the status, list entries and/or list size

The following is a list of services GR-1298-Core classifies as Group3.

- Distinctive Ringing/Call Waiting
- Selective Call Rejection

The following service is not classified by GR-1298-Core but supported by CM under group 3:

- Simultaneous Ringing (SIMRING)

Note: The Section 118.7.2 describes the encoding/decoding of Simring.

118.2.8 SDF Group 4

Group4 services are those generally provided with the ability to

- activate and/or deactivate
- set or clear forwarding (remote) DN
- retrieve the status and/or forwarding DN

The following is a list of services GR-1298-Core classifies as Group4.

- Call Forwarding Variable
- Call Forwarding Don't Answer
- Call Forwarding Busy Line

Note: Please refer to section 118.7.3 for support of AINDigits Parm. This parm is not supported for Group4 in GR-1298 and GR-1299.

118.2.9 SDF Group 5

Group5 services are those generally provided with the ability to

- activate and/or deactivate
- add/delete list entries corresponding to a specified DN, Speed Call Code or Incoming Memory Slot
- delete all list entries
- delete all private entries
- set or clear forwarding (remote) DN
- retrieve the status, list entries, list size and/or forwarding DN

The following is a list of services GR-1298-Core classifies as Group5.

- Selective Call Forwarding
- Selective Call Acceptance

Note: Please refer to section 118.7.3 for support of AINDigits Parm. This parm is not supported for Group5 in GR-1298 and GR-1299.

118.2.10 SDF Group 6

Group6 services are those generally provided with the ability to

- update the relevant delay interval for number of rings prior to forwarding
- retrieve the delay interval value

The following is a list of services GR-1298-Core classifies as Group6.

- Ring Control

118.2.11 SDF Group 7

Group7 services are those generally provided with the ability to

- invoke the DMS-based CNDB or CNAB features

The following is a list of services GR-1298-Core classifies as Group7.

- Calling Number Delivery Blocking
- Calling Name Delivery Blocking

118.2.12 SDF Group 8

Group8 services are those generally provided with the ability to

- invoke a service

The following is a list of services GR-1298-Core classifies as Group8.

- Customer Originated Trace
- Cancel Call Waiting

118.2.13 SDF Group 9

Group9 services are those generally provided with the ability to

- change speed calling list entry to specified DN

The following is a list of services GR-1298-Core classifies as Group9.

- Speed Calling

For more information, please refer to GR-1298-Core, section 6.4.

Nortel has developed different variants of the GR's Speed Calling feature. For instance, Nortel's Speed Calling Short (SCS) allows an end user to store a maximum of ten (i.e., 0 to 9) often dialed DNs; therefore, SCS supports a single Speed Calling cell digit access. Nortel's Speed Calling Long (SCL) allows an end user to store up to seventy (i.e., 00 to 69) often dialed DNs; therefore, SCL supports two digits for Speed Calling Cell access.

> ***Note:*** for SCL (i.e., L30, L50 or L70), the end user must dial both digits of the two digit Speed Calling code, even if the first digit is zero.

This design intent makes the assumption that from the Speed Calling Cell digits provided (from the end user), a single Speed Calling (SC) digit indicates SCS, and two SC digits indicate SCL or Speed Calling User (SCU)[1].

GR-1298-Core allows for Group9 Update request(s); however, it does not provide for a Group9 Query message in order to retrieve/query the user's Speed Call data. However, Nortel will utilize the Extension Parm to retrieve/query a Block of 20 DNs (per Group9 Query Message). Each Query Block (of DNs) are labeled 0 to 5. For instance:

Nortel's Group9 Query Action $Block_X$: where x = 0 through 5:

- Query Action $Block_0$ contains DNs associated with Speed Call Codes 0 to 19
- Query Action $Block_1$ contains DNs associated with Speed Call Codes 00 to 19
- Query Action $Block_2$ contains DNs associated with Speed Call Codes 20 to 39
- Query Action $Block_3$ contains DNs associated with Speed Call Codes 40 to 59
- Query Action $Block_4$ contains DNs associated with Speed Call Codes 60 to 79
- Query Action $Block_5$ contains DNs associated with Speed Call Codes 80 to 99

Nortel's Group9 Query Action $Block_0$ is utilized for Speed Call Short only. Since Nortel's Speed Call Short list could contain up to a maximum of 10 DNs associated with a Speed Call Code, only the first 10 indexes (0 to 9) of Block0 will be utilized for a Speed Call query. The remaining indexes (10 to 19) will contain NIL DNs.

Nortel's Group9 Query Action Blocks 1-5 (i.e., Blocks1 through Blocks5) are utilized for Speed Call Long only.

Speed Calling directory number validation will be performed if the Speed Calling Validation (SCVAL) option is provisioned in Table CUSTSTN.

Please reference the appendix (Section 118.7.4 and Section 118.7.5) for Nortel's Group9 Query implementation, which utilizes the Extension Parm. Also, please refer to section 118.7.3 for support of AINDigits Parm. This parm is not supported for Group9 in GR-1298 and GR-1299.

[1]SCU - Speed Calling User: this user is allowed (if provisioned with the SCU Servord line option) to have access to a Speed Calling Long list. However, for this feature deployment, the SCU user is not allowed to add, change or query the Speed Calling list - only the SCL controller is allowed to modify or to query their SCL list.

118.3 AINTRACE support for UpdateRequest and QueryRequest

In order to obtain the logs for Update/Query Request and their responses, AINTRACE should be used to select these messages. These messages are sent by the SCP.

118.3.0.1 QueryRequest:

QueryRequest messages are subparameters of message 'Provide Info' .Each Query Request message contains the following subparameters: 'Service' and 'Request'. They are decoded and displayed on AINT700 logs using AINTRACE.

The 'Service' subparameter contained within the 'Requestgroup' parameter displays the name of the service for which the request is being made:

The 'Request ' subparameter contained within the 'Requestgroup' parameter contains the following subparameters:

- ActivationStatusCode: This parameter displays whether the service is presently active or not.
- DelayInterval: This parameter displays the delay that has been set to the service.
- EntireList: This parameter displays the enire list of DNs that were selected in the servord.
- ListSize: This parameter displays the size of the 'EntireList' parameter.
- ForwardingDn: This parameter displays the DN to which the call has been forwarded to.

118.3.0.2 UpdateRequest

Update messages are subparameters of SSP User Resource. Each update message contain the following subparameters: Service and Action.They are decoded and displayed on AINT700 logs using AINTRACE.

The 'Service' subparameter contained within the 'Updategroup' parameter displays the name of the service on which the 'Action' is to be performed.

The 'Action' subparameter contained within the 'Updategroup' parameter contains the following subparameters:

- ActivationStatusCode: This parameter displays whether the service is to be activated or not.
- DelayInterval: This parameter displays the new value to be set for the delay interval of the concerned service.
- EditSpecificEntry: This parameter contains further subparameters viz. (1)Entry: Displays DN,SpeedCalling Code and Memory Slot

(2)EditListType: Displays if the ‘Entry’ parameter has to be added or deleted.

- EditAllEntries: This parameter contains the following subparameters: (1)DeleteAllEntries (2)DeletePrivateEntries
- ForwardingDn: This parameter contains the following subparameters: (1)Set: This parameter displays the Dn and the SpeedCallingCode (2)Clear: This parameter is used to remove the service from the specified Dn.
- Toggle: Contains the parameter ‘PresentationStatusValue’
- Invoke: Contains the parameter ‘on’

118.4 Hardware Requirements or Dependencies

In order to enable this capability for affected subscribers, the following must be present in the provider’s network

- EO Switch providing the affected services must be enabled to handle the corresponding update and/or queries request via SS7.

118.5 Software Requirements or Dependencies

There are number of services are controlled via software optionality control (SOC). In order to use these services, appropriate SOC must be activated in the switch. Therefore, this development is depends on following SOC:

- AIN00002 - Essentials
- AIN00006 - Call Management
- AIN00210 - Service Enablers
- RES00008 - Long Distance Indicator
- RES00059 - LDA Enhancement
- RES00047 - Call Screening
- RES00053 - Enhanced CSMI
- RES00060 - Usage Sensitive Call Forwarding
- RES00073 - SLE/ACBAR NO TCAP
- RES00081 - Simultaneous Ring
- RES00085 - SimRing Virtual DN
- RES00102 - Enh Do Not Disturb

118.6 Limitations and restrictions

118.6.1 Limitations and restrictions for Incoming/ Outgoing Call memory.

Since the call memory is not captured for POTS lines, it will not be returned in the SSP 'Info Provided' message. When a query request for incoming/ outgoing parameter is made by SCP, the SSP sends back an 'EMPTY' bit string in the 'MemorySlot' parameter indicating that incoming/ outgoing information is not available.

118.6.2 Limitations and restrictions for each service

As discussed previously, the initial release of this capability is couple to AIN, specifically for signaling support and primary message (ASN.1) encoding/ decoding functions.

Because each group/service pair has its own unique set of limitations/ restrictions, a table is being provided to capture what, if any, limitations are present for each application.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Message Waiting Indicator	To support MWI, MSRID is required to be sent by off-board processor and it has to be data filled in Table MSRTAB in the DMS. In the response of the query for MWI status, the ON/OFF status is sent back to the off-board system. The requestor DN which is stored against the agent will not be sent because GR-1298-Core does not support any additional data. The DMS supports following type of Message Waiting Indicator and Services: • Message Waiting Lamp - for Integrated Business Network (IBN) and Key Set (KSET) lines in business • Stutter Dial Tone (STD) - for Residential (RES) lines in residential and IBN lines in business environment. • Class Message Waiting Indicator (CMWI) for RES lines in form of STD. All existing Message Waiting (MWT) limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MWT. Also, please refer to AIN Service Implementation Guide (SIG) for more details. This service does not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Visual Message Waiting Indicator	To support MWI, MSRID is required to be sent by off-board processor and it has to be data filled in Table MSRTAB in the DMS. In the response of the query for MWI status, the ON/OFF status is sent back to the off-board system. The requestor DN which is stored against the agent will not be sent because GR-1298-Core does not support any additional data. The DMS supports following type of Message Waiting Indicator and Services: • Message Waiting Lamp - for IBN and KSET lines in business • STD - for RES lines in residential and IBN lines in business environment. • CMWI for RES lines in form of STD. The DISPLAY TEXT is not supported. All existing MWT limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MWT. Also, please refer to AIN SIG for more details. This service does not generate an AMA record.
1	Anonymous Caller Rejection	All existing Anonymous Caller Rejection (ACRJ) limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for ACRJ. If there's a call billing requirement, a AMASlpId is present and it's operating in a CEPT compliant market and only if the line was originally provisioned by the Telco. Then an item will be appended to the end of the AMA record. Otherwise, no AMA record will be generated.
1	Automatic Callback	The only portion is supported to deactivate the Automatic Callback (ACB) as per GR-1298-Core. The activation request for ACB is rejected. All existing Automatic Callback (ACB) limitations and restrictions for deactivation are the same and applicable to query and update messages for ACB. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Automatic Recall	The only portion is supported to deactivate the Automatic Recall (AR) as per GR-1298-Core. The activation request for AR is rejected. All existing Automatic Recall (AR) limitations and restrictions for deactivation are the same and applicable to query and update messages for AR. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.
1	Call Screening	The Call Screening, Monitoring and Intercept (CSMI) is supported for both residential and business lines. All existing CSMI limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for CSMI. This service does not generate an AMA record.
1	Outside Calling Area Alerting	The Outside Calling Area Alerting is known as long distance alerting (LDA) in DMS. The LDA service along with LDA Enhancement (LDAE) supports LDSV, LDSO, LDSA, LDSR and LDST options in DMS switch. Out of these options, the only option allows end user to activate/deactivate is LDSA using access code. The query and update messages are only applicable to LDSA state and activation/deactivation. If LDS_AUTO_PROV_ENABLED office parameter is set to "Y", the LDSA is automatically provisioned to line if the LDSV option is data filled in Table LINEATTR. User action to deactivate is ignored by the LDSA service. The update message for LDSA is ignored. All existing LDSA limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for LDSA. This service does not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Calling Identity Delivery and Suppression	The Calling Identity Delivery and Suppression (SUPPRESS) is only supported for the PUBLIC network. The query returns the current status of the line as public or private. The update request to activate change the status pps to public. The update request to deactivate change the status pps to private. If current status is public and deactivate request is received, no change made to the status. If current status is private and activate request is received, no change made to the status. All existing SUPPRESS limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for SUPPRESS. This service does not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Call Waiting	The call waiting (CWT) service is always active on all the lines when assigned in the switch. It is only deactivated when Cancel Call Waiting (CCW) access code is dialed. In the response to the query request following is sent for CWT: • If only CWT option is assigned to the line than the status of CWT is active. • If CWTACT is also assigned to the line than the status of CWTACT. In the response to the update request following activation/ deactivation are done: • If only CWT option is assigned to the line than activate/deactivate request are rejected because we can not change the status of CWT on the line. • If CWTACT is also assigned to the line than the activate request change the status to active and deactivate request change the status to inactive. Prior to this release CWTACT was only supported for the business lines. This feature also makes CWTACT available to RES lines as well. All existing CWT and CWTACT limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for CWT and CWTACT. This service does not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Make Set Busy	The Make Set Busy (MSB) is not required nor supported by GR-1298-Core and GR-1299-Core. This is a group 1 service supported by this activity as additional supported service. The activate request turns MSB “ON” and deactivate request turns MSB “OFF”. All existing MSB limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MSB. For encoding/decoding of MSB, please refer to Section 118.7.1. If there’s a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.
2	Audio Message Waiting Indicator	The GR-1298 defined Audio Message Waiting Indicator (AMWI) allows control of both MWT indication for the line in terms of ping ring at a programmable interval. This is the main difference between MWT in group1 and AMWI in grouyp2. The DMS service PRN falls under AMWI category while all other flavor of MWT in DMS are Group1 services. The delay interval is not supported. The CM feature Periodic Ringing Notification (PRN) can only be activated or deactivated because PRN does not allow to control the ring interval or delay interval. This service does not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Distinctive Ringing/Call Waiting	• GR-219-Core provides the following guidance with respect to Distinctive Ringing/Call Waiting (DRCW) Traffic Measurements: *Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCRJ screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*61 or *81)* The end-office will peg any DRCW editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of DRCW OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. • DRCW editing will be denied if DOR option present. In such instances, a result cause of *denied unsuccessful update (27)* will be provided in the update response. • DRCW editing will be denied if DENY DRCW option present. In such instances, a result cause of *denied unsuccessful update (27)* will be provided in the update response. • Attempts to add Extension DNs to an IBN subscriber's DRCW list is not supported.[a] • TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. • The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. • A response of *confAllAnonymousEntriesRemoved* will be returned for *Delete All Anonymous Entries* update requests in which no private DNs are present in the subscriber's list. • When editing DRCW via Universal Access, the initial edit/query attempt will automatically add DRCW to the subscriber's line and take on the characteristics of DRCW as defined in table RESOFC. • Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. • A response of *deniedUnsuccessfulUpdate* will be returned for ADD attempts in which DN validation fails. • For entire list queries in which the number of DNs in the list exceeds 32,only the first 32 entries will be reported in the query response and a SLE106 log will be generated. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Selective Call Rejection	• GR-218-Core provides the following guidance with respect to Selective Call Rejection (SCRJ) Traffic Measurements: *Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCRJ screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*60 or *80)* The end-office will peg any SCRJ editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCRJ OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. • SCRJ editing will be denied if DOR option present. In such instances, a result cause of *denied unsuccessful update (27)* will be provided in the update response. • SCRJ editing will be denied if DENY SCRJ option present. In such instances, a result cause of *denied unsuccessful update (27)* will be provided in the update response. • Attempts to add Extension DNs to an IBN subscriber's SCRJ list is not supported. • TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. • The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. • A response of *confAllAnonymousEntriesRemoved* will be returned for *Delete All Anonymous Entries* update requests in which no private DNs are present in the subscriber's list. • When editing SCRJ via Universal Access, the initial edit/query attempt will automatically add SCRJ to the subscriber's line and take on the characteristics of SCRJ as defined in table RESOFC. • Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. • A response of *deniedUnsuccessfulUpdate* will be returned for ADD attempts in which DN validation fails. • For entire list queries in which the number of DNs in the list exceeds 32,only the first 32 entries will be reported in the query response and a SLE106 log will be generated. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Simultaneous Ringing	• The *EditSpecificEntry field* values of “add” or “delete” will be interpreted to add or delete only the NON-Pilot Member DN of a SIMRING group. • *EditAllEntries field* with a value of “deleteAllEntries “is interpreted as deleting only the Non-Pilot Member DNs in the SIMRING group. • *EditSpecificEntry field* with value of “delete” will result in SIMRING getting deactivated on the PILOT DN if no entries remain on the list. • *EditAllEntries field* with a value of “deleteAllEntries “will result in SIMRING getting deactivated on the PILOT DN. • *EditAllEntries field* with a value of “deleteAllPrivateEntries” is NOT valid for SIMRING. The update message with this action field will result in UnavailableResources result Cause being sent back as return error component. • The UPDATE message cannot edit the Non Pilot Member DN list during a SIMRING call (i.e. while all the member DNs are ringing). • Attempts to add NON-Pilot Member DNs via the ICM or given SpeedCall cell entry are not supported for SIMRING. • Edit attempts with SOCOption AIN00327 IDLE will result in a SLE106 log being generated. • A response of *deniedUnsuccessfulUpdate* will be returned for ADD attempts in which DN validation fails. This service does not generate an AMA record.
4	Call Forwarding Variable	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. ISDN agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFU Per Key is not supported. If there’s a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
4	Call Forwarding Don't Answer	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. Integrated Services Digital Network (ISDN) agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFB Per Key is not supported. This service does not generate an AMA record.
4	Call Forwarding Busy Line	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. ISDN agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFD Per Key is not supported. This service does not generate a AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
5	Selective Call Forward	• GR-217-Core provides the following guidance with respect to Selective Call Forwarding (SCF) Traffic Measurements (section 3.5.4): *Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCF screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*63 or *83)* The end-office will peg any SCF editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCF OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. • SCF editing will be denied if DOR option present. • SCF editing will be denied if DENY SCF option present. • If there are no entries in the list *and* no forwarding DN present, attempts to enable SCF will fail with a result cause of *denied invalid Forward DN*(17). • Attempts to add Extension DNs to an IBN subscriber's SCF list is not supported. • TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. • The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. • A response of *confAllAnonymousEntriesRemoved* will be returned for *Delete All Anonymous Entries* update requests in which no private DNs are present in the subscriber's list. • When editing SCF via Universal Access, the initial edit/query attempt will automatically add SCF to the subscriber's line and take on the characteristics of SCF as defined in table RESOFC. • Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. • A response of *deniedUnsuccessfulUpdate* will be returned for ADD attempts in which DN validation fails. • For entire list queries in which the number of DNs in the list exceeds 32,only the first 32 entries will be reported in the query response and a SLE106 log will be generated. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
5	Selective Call Acceptance	• GR-1298-Core provides for Selective Call Acceptance (SCA) to define the *no call acceptance treatment* as being a forwarding DN. Nortel Network's version of SCA does not allow for this capability. • The end-office will peg any SCA editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCA OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. • SCA editing will be denied if DOR option present. • SCA editing will be denied if DENY SCA option present. • Attempts to add Extension DNs to an IBN subscriber's SCA list is not supported. • TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. • The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. • A response of *confAllAnonymousEntriesRemoved* will be returned for *Delete All Anonymous Entries* update requests in which no private DNs are present in the subscriber's list. • When editing SCA via Universal Access, the initial edit/query attempt will automatically add SCA to the subscriber's line and take on the characteristics of SCA as defined in table RESOFC. • Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. • A response of *deniedUnsuccessfulUpdate* will be returned for ADD attempts in which DN validation fails. • For entire list queries in which the number of DNs in the list exceeds 32,only the first 32 entries will be reported in the query response and a SLE106 log will be generated. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.
6	Ring Control	Only supported for a ring control type of PRGRING. One ring will last 8s for lines off of non-RDT peripherals and 6s for lines off of Remote Digital Terminal (RDT) peripherals. The number of rings can range between what the OFCENG parm RINGCTRL_MIN_VALUE is set to and 10. This service will not generate an AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
7	Calling Number Delivery Blocking	A DN's Permanent Presentation Status (PPS) is stored in table DNATTRS under the SUPPRESS option. The CNDB feature allows the caller to override the Number portion of the PPS on a per-call basis. The line must be subscribed to the CNDB line or customer group option or the CNDB Universal option. The agent must be off-hook and in the dialing state for the CNDB service to be invoked. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.
7	Calling Name Delivery Blocking	A DN's Permanent Presentation Status (PPS) is stored in table DNATTRS under the SUPPRESS option. The CNAB feature allows the caller to override the Name portion of the PPS on a per-call basis. The line must be subscribed to the CNAB line or customer group option or the CNAB Universal option. The agent must be off-hook and in the dialing state for the CNAB service to be invoked. This service does not generate a AMA record.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
8	Customer Originated Trace	• As per GR-216-Core and the CM implementation of the Customer Originated Trace (COT) feature, two activation levels (ACTLEVEL) are available for conventional users accessing the feature via an access code on telephone. The UPDATE message will allow invoking of the COT feature only for ACTLEVEL of ONELEVEL, which does NOT have any confirmation prompt announcements for the user accessing the feature. • The UPDATE message will not be supporting any announcements or any language related enhancements for the COT feature invocation. • If the COT has already been activated by the user via the access code from a telephone for the last incoming call then if an UPDATE message is used for the COT invocation, then it will be treated like a repeat attempt. The same will be valid in vice-versa scenario. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.
8	Cancel Call Waiting	• The user can use the UPDATE message to activate Cancel Call Waiting (CCW) only when the user is already off hook and getting a dial tone or is already on a call (single party or multiparty). • If the user invokes CCW through the UPDATE message while being off hook, then the user will not hear any audible confirmation tone for the invocation. If there's a call billing requirement and an AMASlpId is present. Then an item will be appended to the end of the AMA record. Please refer to the ACC document.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
9	Speed Calling	• GR-1299-Core provides numbers 2 through 9 (for Speed Call Short) or numbers 20 through 39 (for Speed Call Long) as the Speed Calling Code(s) for the Group9 Update Message. Nortel will support these GR required Speed Calling Code range. However, Nortel exceeds the GR-1299-Core standard by supporting the following Speed Call Code(s) (from NTP 297-8021-350, Standard 14.02, May 2001): - single digit Speed Call Cell range 0 to 9 for Speed Call Short (SCS), and - two digit Speed Call Cell range 00 to 69 for Speed Call Long (SCL) or Speed Call User (SCU) • GR-1299-Core does not provide for a Group9 Query message in order to retrieve/query the user's Speed Call data. However, Nortel will utilize the Extension Parm to retrieve/query a Block of 20 DNs (per Group9 Query Message). Each Query Block (of DNs) are labeled 0 to 5. For example: Nortel's Group9 Query Action $Block_X$: where X = 0-5: - Query Action $Block_0$ contains DNs associated with Speed Call Codes 0 to 19 - Query Action $Block_1$ contains DNs associated with Speed Call Codes 00 to 19 - Query Action $Block_2$ contains DNs associated with Speed Call Codes 20 to 39 - Query Action $Block_3$ contains DNs associated with Speed Call Codes 40 to 59 - Query Action $Block_4$ contains DNs associated with Speed Call Codes 60 to 79 - Query Action Block5 contains DNs associated with Speed Call Codes 80 to 99 • Nortel's Group9 Query Action $Block_0$ is utilized for Speed Call Short only. Since Nortel's Speed Call Short list could contain up to a maximum of 10 DNs associated with a Speed Call Code, only the first 10 indexes (0 to 9) of $Block_0$ will be utilized for query. The remaining indexes (10 to 19) will contain NIL DNs. • Nortel's Group9 Query Action Blocks 1-5 (i.e., $Blocks_1$ through $Blocks_5$) are utilized for Speed Call Long only.

Table 1 Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
9	Speed Calling	• GR-1299-Core provides that the Group9 Update Speed Call DN be a maximum of 10 digits per Speed Call Cell. **Note**: Nortel will support the GR-1299-Core requirement for a 10 digit Speed Call DN per Cell. In addition, Nortel will support an AINDigit DN which supports up to 30 digits for a Speed Call DN per Cell. • Nortel's Speed Call Design intent indicates that from the Speed Calling Cell digits provided (from the end user), a single Speed Calling Cell digit indicates Speed Calling Short, and two Speed Calling Cell digits indicate Speed Calling Long or Speed Calling User (SCU)[b]. • Only the Speed Call Controller is allowed to receive or query their Speed Calling List - not a Speed Calling User (SCU). • End to End Speed Call Signaling is not supported. • The Group9 Query Response Extension Parm contains the following fields: - **Count**: the total number of Speed Calling DNs within this $Block_X$ (up to 20). - **DN Bytes**: the number of bytes needed to represent the Speed Calling DN. Note: this range is 1 to 15, where 15 bytes represents 30 Digits. - **SC Cell**: the Speed Calling Cell associated with the Speed Calling DN. - **SC DN**: the Speed Calling DN. **NOTE: *if there's an odd number of Speed Calling Digits, the ending nibble will be hex F*.** • Please reference NTP 297-8021-350, Standard 14.02, May 2001 for all Nortel Speed Call limitations/restrictions. The Group9 Update/Query Event Handler will support the following: • Update Result Causes: - *deniedUnsuccessfulUpdate* - *confServiceActivated* • Update Return Result: - *UPD_UnavailableResources* - *UPD_OK* • Query Result: - *QR_Unavailable_Resources* - *QR_OK* This service does not generate a AMA record.

a. support EXTN DNs is possible given that EXTN is specified in the ADD DN update request - EXTN parm is currently not supported in the protocol but could be added as an extension parm of both group3 and group5 services.
b. SCU - Speed Calling User: this user is allowed (if provisioned with the SCU Servord line option) to have access to a Speed Calling Long list. However for this feature deployment, the SCU user is not allowed to add, change or query the Speed Calling list - only the SCL controller is allowed to modify or to query their SCL list.

118.7 Appendix A: Supplementary Details

This section contains additional details for the encoding and decoding services which are not supported by the GR-1298 and GR-1299. It also contains the details of Nortel's Extension Parameter(s) to support additional services and functionalities.

118.7.1 Make Set Busy Encoding and Decoding

The Make Set Busy service is not described in the GR-1299, Issue 7, Nov. 2001, ASN.1 encoding. The following extension to the GR-1299 ASN.1 encoding provides the Make Set Busy service accessible via update messages (Page 6-17, Section 6.4.2, GR-1299-Core, Issue 7, Nov. 2001):

Service1::=ENUMERATED {

messageWaitingIndicator (0),

visualMessageWaitingIndicator (1),

anonymousCallRejection (2),

automaticCallback (3),

automaticRecall (4),

callScreening (5),

outsideCallingAreaAlerting (6),

callingIdPresentAndSuppress (7),

callWaiting (8),

makeSetBusy (9)

}

The RequestGroup1 in Section 6.114, Page 6-110 of GR-1299-Core, Issue 7, Nov. 2001 refers to above Service1 for the Query request. The above change

also apply to RequestGroup1, Service1 as well to provide the query request of the makeSetBusy service.

The same changes also apply to Page C-57 and C-79, ASN.1 Modules to provide makeSetBusy service under Service1 catagory.

The following is a hex and ASCII representation of the makeSetBusy Query, makeSetBusy Update request without AMASLPID and makeSetBusy Update request with AMASLPID:

makeSetBusy in Query Request:

BF 72

09

A1

07

81 01 09

82 02 07 80

ProvideInfo

(

RequestGroup1

(

Service1(makeSetBusy)

Request1(activationStatus)

)

)

makeSetBusy in Update Request without AMASLPID (Activate Request):

A2

06

81 01 09

82 01 01

UpdateGroup1

(

Service1(makeSetBusy)

Action1(on)

)

makeSetBusy in Update Request without AMASLPID (Deactivate Request):

A2

06

81 01 09

82 01 00

UpdateGroup1

(

Service1(makeSetBusy)

Action1(off)

)

makeSetBusy in Update Request with AMASLPID (Activate Request):

BF 67

11

A1

07

81 05 16 63 12 53 31

A2

06

81 01 09

82 01 01

8A 05 11 11 11 11 01

SSPUserResource

(

SSPUserResourceID

(

DN(6136213513)

)

UpdateGroup1

(

Service1(makeSetBusy)

Action1(on)

)

)

AMASlpID(111111111)

makeSetBusy in Update Request with AMASLPID (Deactivate Request):

BF 67

11

A1

07

81 05 16 63 12 53 31

A2

06

81 01 09

82 01 00

8A 05 21 43 65 87 09

SSPUserResource

(

SSPUserResourceID

(

DN(6136213513)

)

UpdateGroup1

(

Service1(makeSetBusy)

Action1(off)

)

)

AMASlpID(123456789)

118.7.2 Simring Encoding and Decoding

The Simring (simultaneousRinging) service is not described in the GR-1299, Issue 7, Nov. 2001, ASN.1 encoding. The following extension to the GR-1299 ASN.1 encoding provides the Simring service accessible via update messages (Page 6-18, Section 6.4.2, GR-1299-Core, Issue 7, Nov. 2001):

Service3::=ENUMERATED{

distinctiveRingingCallWaiting (0),

selectiveCallRejection (1),

simultaneousRinging (2)

}

The RequestGroup3 in Section 6.114, Page 6-110 of GR-1299-Core, Issue 7, Nov. 2001 refers to above Service3 for the Query request. The above change also apply to RequestGroup3, Service3 as well to provide the query request of the simring service.

The same changes also apply to Page C-59 and C-80, ASN.1 Modules to provide simring service under Service3 catagory.

The following is a hex and ASCII representation of the simring query and update requests:

Simring Query Request:

BF 72

09

A3

07

81 01 02

82 02 07 80

ProvideInfo

(

RequestGroup3

(

Service3(simultaneousRinging)

Request3(activationStatus)

)

)

Simring Update Request:

A4

09

81 01 02

A3

04

9F 69 01 00

UpdateGroup3

(

Service3(simultaneousRinging)

EditSpecificEntry

(

EditListType(addListElement)

)

)

118.7.3 Support of AINDigits Parameter in Call Forwarding and Speed Call

Call Forwarding and Speed Call are not described in GR-1299 Issue 7, Nov.2001, with having the capability to use up to thirty digit DNs (long DN). The following description captures how up to long DNs can now be used.

Service groups 3, 4, 5 and 9 have the ability to send a update request with long DNs. And service groups 3, 4 and 5 have the ability to receive a query request that contain long DNs.

Long DNs are not used to specify the UserResourceID. They're only permitted for example, when updating the ForwardingDN in a Call Forward Variable (CFU) request.

AdministrableObject Changes:

Service Group 3

Entry::=CHOICE {

[1] IMPLICIT Dn.

[2] IMPLICIT SpeedCallingCode,

[3] IMPLICIT MemorySlot,

[4] IMPLICIT AINDigits

}

-- AINDigits parameter supports up to 30 digits.

Service Group 4

Set::=CHOICE {

[1] IMPLICIT Dn,

[4] IMPLICIT SpeedCallingCode,

[5] IMPLICIT AINDigits

}

-- AINDigits parameter supports up to 30 digits.

Service Group 5

The above new definition, SET, is used indirectly by Service Group 5.

Service Group 9

ChangeList::=SEQUENCE {

[1] IMPLICIT Dn,

[2] IMPLICIT SpeedCallingCode,

[3] IMPLICIT AINDigits

}

-- AINDigits parameter supports up to 30 digits.

InfoProvided Changes:

All Service Groups will use this new query definition.

InfoProvided::=[100] IMPLICIT SEQUENCE {

[1] IMPLICIT ActivationStateCode OPTIONAL

[2] IMPLICIT EntireList OPTIONAL

[3] IMPLICIT MemorySlot OPTIONAL

[4] IMPLICIT ListSize OPTIONAL

[5] IMPLICIT ForwardToDn OPTIONAL

[6] IMPLICIT DelayInterval OPTIONAL

[7] IMPLICIT Empty OPTIONAL,

[8] IMPLICIT ListSizeVarDN OPTIONAL,

[9] IMPLICIT ForwardToVarDN OPTIONAL

}

ListSizeVarDN::=SEQUENCE {

AINDigits

}

-- ListSizeVarDN is a new field that uses type AINDigits, which supports up to 30 digits.

ForwardToVarDN::=SEQUENCE {

AINDigits

}

-- ForwardToVarDN is a new field that uses type AINDigits, which supports up to 30 digits.

Example: Call Forward Query Request Response

BF 64

0B

81 01 00

89 06 80 00 27 43 05 00

InfoProvided

(

ActivationStateCode(off)

ForwardToVariableDn(notApplicable odd unknownOrNotApplicable 7234500)

)

Example: Call Forward Update Request

A5

0D

81 01 00

A3

08

84 06 80 00 27 43 05 00

UpdateGroup4

(

Service4(callForwardingVariable)

ForwardingDN

(

VariableDn(notApplicable odd unknownOrNotApplicable 7234500)

)

)

Example: Speed Call Update Request

AA

11

81 01 00

A2

0C

83 06 80 00 27 43 15 00

82 02 32 33

UpdateGroup9

(

Service9(speedCalling)

ChangeList

(

VariableDn(notApplicable odd unknownOrNotApplicable 7234510)

SpeedCallingCode(23)

)

)

118.7.4 Speed Call Query Request Extension Parameter

The Speed Calling Query Request Extension Parmeter contains the following fields:

- AssignmentAuthority: this field is utilized to identify if this particular Extension Parm is appropriate for this vendor's switch.
- NCRSpeedCallQueryRequest(x), where x = 0-5: the non-call response (NCR) parm identifies the Speed Calling Query Action Block request.

Note: the Speed Calling Query Action Block number (0 through 5) dictates which Speed Calling DN(s) will be retrieved:
- Query Action $Block_0$ contains DNs associated with Speed Call Codes 0 to 19
- Query Action $Block_1$ contains DNs associated with Speed Call Codes 00 to 19
- Query Action $Block_2$ contains DNs associated with Speed Call Codes 20 to 39
- Query Action $Block_3$ contains DNs associated with Speed Call Codes 40 to 59
- Query Action $Block_4$ contains DNs associated with Speed Call Codes 60 to 79
- Query Action $Block_5$ contains DNs associated with Speed Call Codes 80 to 99

Listed below are two Speed Calling Query Request examples: one for Speed Calling Short (SCS), and one for Speed Calling Long (SCL):

- Speed Calling Short (SCS) Query Request example:

Figure 1 Speed Calling SCS Example

```
>qlen 0 0 0 13
------------------------------------------------------------------------------
LEN:     HOST  00 0 00 13
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6212233
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  6X17AC    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    67
PM TERMINAL NUMBER :    14
OPTIONS:
DGT SCS
------------------------------------------------------------------------------
```

Figure 1 Speed Calling SCS Example cont.

```
>t ibnsc
TABLE: IBNSC
IBNSCKEY RESULT
---------------
HOST 00 0 00 13 0 SCS 3 8675309 <------ odd number of digits (DN1)
HOST 00 0 00 13 0 SCS 7 9195521200 <--- even number of digits (DN2)


Group 9 Query Request for Action 0:
===================================
MESSAGE
qr9extension0:
QueryWithPermission
(
    OriginationTransactionID(0000029D)
    Components
    (
        InvokeLast
        (
            InvokeID(01 00)
            PrivateTCAP
            QueryRequest
            ParameterSequence
            (
                UserID
                (
                    DN(6136212233) <---Speed Calling Subscriber
                )
                ExtensionParameter
                (
                    AssignmentAuthority(BR549)
                    NCRSpeedCallQueryRequest(0) <---Action Block 0
                )
            )
        )
    )
)
;
```

Figure 1 Speed Calling SCS Example cont.

```
Group 9 Query Response for Action 0:
====================================
MESSAGE
Response
(
    DestinationTransactionID(0000029D)
    Components
    (
        ReturnResultLast
        (
            CorrelationID(01)
            ParameterSequence
            (
                ExtensionParameter
                (
                    AssignmentAuthority(BR549)
                    NCRSpeedCallQueryResponse(020403685703F905071959252100)
                )
            )
        )
    )
)
;

where 020403685703F905071959252100:
02 - Number of Speed Calling DN(s): 2
04 - Number of DN Bytes for DN1: 4 bytes
03 - Speed Calling Cell assignment: 3
685703F9- DN1: 6875309 (Notice the ending hex F for odd number of digits)
05 - Number of DN Bytes for DN2: 5 bytes
07 - Speed Calling Cell assignment: 7
1959252100 - DN2: 9195521200
```

- Speed Calling Long (SCL) Query Request example:

Figure 2 Speed Calling SCL Example

```
>qlen 0 0 0 13
------------------------------------------------------------------------------
LEN:     HOST  00 0 00 13
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6212233
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  6X17AC    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    67
PM TERMINAL NUMBER :    14
OPTIONS:
DGT SCL 0 L30
------------------------------------------------------------------------------
```

Figure 2 Speed Calling SCL Example cont.

```
>t ibnsc
TABLE: IBNSC
IBNSCKEY RESULT
---------------
HOST 00 0 00 13 0 SCL 23 3362921345 <--- even number of digits (DN1)
HOST 00 0 00 13 0 SCL 29 8675309 <------ odd number of digits (DN2)



Group 9 Query Request for Action 2:
===================================
MESSAGE
qr9extension2:
QueryWithPermission
(
    OriginationTransactionID(000002B3)
    Components
    (
        InvokeLast
        (
            InvokeID(01 00)
            PrivateTCAP
            QueryRequest
            ParameterSequence
            (
                UserID
                (
                    DN(6136212233) <---Speed Calling Subscriber
                )
                ExtensionParameter
                (
                    AssignmentAuthority(BR549)
                    NCRSpeedCallQueryRequest(2) <---Action Block 2
                )
            )
        )
    )
)
;
```

Figure 2 Speed Calling SCL Example cont.

```
Group 9 Query Response for Action 2:
====================================
MESSAGE
Response
(
    DestinationTransactionID(000002B3)
    Components
    (
        ReturnResultLast
        (
            CorrelationID(01)
            ParameterSequence
            (
                ExtensionParameter
                (
                    AssignmentAuthority(BR549)
                    NCRSpeedCallQueryResponse(02051733262931540 41D685703F9)
                )
            )
        )
    )
)
;


where 020517332629315404 1D685703F9:
02 - Number of Speed Calling DN(s): 2
05 - Number of DN Bytes for DN1: 5 bytes
17 - Speed Calling Cell assignment: 17 hex, 23 dec
3326293154 - DN1: 3362921345
04 - Number of DN Bytes for DN2: 4 bytes
1D - Speed Calling Cell assignment: 1D hex, 29 dec
685703F9 - DN2: 8675309 (Notice the ending hex F for odd number of digits)
```

Extension Parameter ASN.1 Details:- The following details are based on GR1299 Issue 7 requirements and definitions. They follow the ASN.1 notations for Extension Parameter, Assignement Authority and Special Routing Extension Parameter.

ExtensionParameter:-

The following shall be used for the ExtensionParameter (CR6-334 in GR1299 Issue 7, Page 6-77):

ExtensionParameter ::= [84] IMPLICIT SEQUENCE {

assignmentAuthority OBJECT IDENTIFIER,

parameters ANY DEFINED BY assignmentAuthority

}

-- The maximum length of the assignmentAuthority is 15 octets

The parameters field is to be defined by individual service providers. See ITU-T Recommendation X.209 for the encoding rules of OBJECT IDENTIFIERs.

assignmentAuthority:-

The following shall be used for the assignementAuthority (same as EnvelopeEncodingAuthority - R6-332 in GR1299 Issue 7, Page 6-76):

assignmentAuthority ::= [98] IMPLICIT OBJECT IDENTIFIER

-- Maximum of 15 octets

The following is bit encoding of the assignementAuthority:

Table 2 Bit and Octet Encoding of assignmentAuthority

TCAP INFORMATION		ENCODING	In Hex
		HGFEDCBA	
Parameter Identifier	assignmentAuthority (1st octet	10011111	9F
	assignementAuthority (2nd octet)	01100010	62
Parameter Length		00000111	07
Contents	1st sub-identifier	00101010	2A
	2nd sub-identifier	10000110	86
	3rd sub-identifier	01001000	48
	4th sub-identifier	10000110	86
	5th sub-identifier	11110110	F6
	6th sub-identifier	01111101	7D
	7th sub-identifier	00100100	24

NCRSpeedCallQuery Request:-

The following shall be used for the as NCRSpeedCallQueryRequest (As per ITU-T Recommendation X.209):

NCRSpeedCallQueryRequest::= [2] CHOICE {

[1] IMPLICIT ActionBlock

}

ActionBlock::=INTEGER (0 .. 5)

-- used to convey to the switch

-- association of Speed Call Codes.

-- 0 indicates that the Speed Call Codes for Speed Call short range from 0 to 9

-- 1 indicates that the Speed Call Codes for Speed Call long range from 00 to 19

-- 2 indicates that the Speed Call Codes for Speed Call long range from 20 to 39

-- 3 indicates that the Speed Call Codes for Speed Call long range from 40 to 59

-- 4 indicates that the Speed Call Codes for Speed Call long range from 60 to 79

-- 5 indicates that the Speed Call Codes for Speed Call long range from 80 to 99

118.7.5 Speed Call Query Response Extension Parameter

The Speed Calling Query Response Extension Parmeter contains the following fields:

- AssignmentAuthority: this field is utilized to identify if this particular Extension Parm is appropriate for this vendor's switch.
- NCRSpeedCallQueryResponse: the non-call response (NCR) parm contains the Speed Calling DN(s) associated with the Query Action Block request.

The NCRSpeedCallQueryResponse contains the following fields:

- **Count**: the total number of Speed Calling DNs within this Action Block$_X$ (up to 20).
- **DN Bytes**: the number of bytes needed to represent the Speed Calling DN. Note: range is 1 to 15, where

  1 byte - supports 1 or 2 Digits
  2 bytes - supports 3 or 4 Digits
  3 bytes - supports 5 or 6 Digits
  4 bytes - supports 7 or 8 Digits
  5 bytes - supports 9 or 10 Digits
  6 bytes - supports 11 or 12 Digits
  7 bytes - supports 13 or 14 Digits

8 bytes - supports 15 or 16 Digits
9 bytes - supports 17 or 18 Digits
10 bytes - supports 19 or 20 Digits
11 bytes - supports 21 or 22 Digits
12 bytes - supports 23 or 24 Digits
13 bytes - supports 25 or 26 Digits
14 bytes - supports 27 or 28 Digits
15 bytes - supports 29 or 30 Digits

- **SC Cell**: the Speed Calling Cell associated with the Speed Calling DN.
- **SC DN**: the Speed Calling DN.

  Note: if there's an odd number of Speed Calling Digits, the ending nibble will be hex F.

Please reference Figure 1, on page 1653 and Figure 2, on page 1655 for Speed Calling Query Response examples.

NCRSpeedCallQueryResponse:-

The following shall be used for the as NCRSpeedCallQueryRequest (As per ITU-T Recommendation X.209):

NCRSpeedCallQueryResponse::= [3] IMPLICIT HEX

-- Maximum of 361Octets.

118.8 Applicable customer facing sections

Fault Management	
Logs	_____X
Alarms	___N/A
Configuration	
Data Schema	___N/A
User Interface	___N/A
Element Management	___N/A
Security	___N/A
Service Order	___N/A
Office Parameters	___N/A
Software Optionality Control (SOC)	_____X
Accounting (includes AMA billing)	_____X

Performance (includes operational measurements) _____X

118.9 Glossary

Term	Description
CM	Computing Module
SOC	Software Optionality Control
AIN	Advanced Intelligent Network
ASN.1	Abstract Syntax Notation 1
SS7	Signaling System No. 7
TCAP	Transaction Capabilities Application Part
IP	Internet Protocol
SCP	Service Control Point
IBN	Integrated Business Network
KSET	Key Set
SDF	Service Data Function
DN	Directory Number
SIMRING	Simultaneous Ringing
SCS	Speed Calling Short
SCL	Speed Calling Long
SCU	Speed Calling User
SC	Speed Calling
PC	Personal Computer
EO	End-Office
STD	Stutter Dial Tone
RES	Residential
MWT	Message Waiting
CMWI	Class Message Waiting Indicator
ACRJ	Anonymous Caller Rejection
ACB	Automatic Call Back
AR	Automatic Recall

Term	Description
CSMI	Call Screening, Monitoring and Intercept
LDA	Long Distance Alerting
LDAE	Long Distance Alerting Enhancement
SUPPRESS	Calling Identity Delivery and Suppression
CWT	Call Waiting
MSB	Make Set Busy
PRN	Periodic Ringing Notification
DRCW	Distinctive Ringing/Call Waiting
SCRJ	Selective Call Rejection
ISDN	Integrated Services Digital Network
SCA	Selective Call Acceptance
RDT	Remote Digital Terminal
COT	Customer Originated Trace
CCW	Cancel Call Waiting
AMA	Automatic Message Accounting
PPS	Permanent Presentation Status

129: Functional Description (FN): A00004037

129.1 Feature name

USNBD - FSK CDC Over Trunks

129.2 Description

129.2.1 Background Information

Currently there are three types of delivery mechanisms available for CDC messaging; X25, SCTP (supported only on CS2Kdelivery) or call data delivery via Frequency Shift Keying (FSK supported on DMS or in a CS2K hybrid configuration with TDM LTC/LGCs.) over a dedicated POTs line. X25 and SCTP mechanisms require Law Enforcement agencies to purchase additional hardware in order to receive the call data messages. Nortel has provided an inexpensive mechanism for the delivery of call data over a dedicated line. This feature will allow a mechanism for delivery of call data over a Switched Remote trunk.

129.2.2 Functional Description

Currently, FSK supports 2 access types, SL (switched local) and DE (Dedicated). This feature will add a third access type called SR (Switched Remote).

The DTC/SPM or other trunking peripheral does not support the CMR card. In order for the call data to be delivered over a trunk, an LGC/LTC peripheral containing the CMR will allocate a p-side loop around to the trunk. This will allow the data sent from the CM to be looped from the CMR peripheral to the trunk peripheral and out over the trunk.

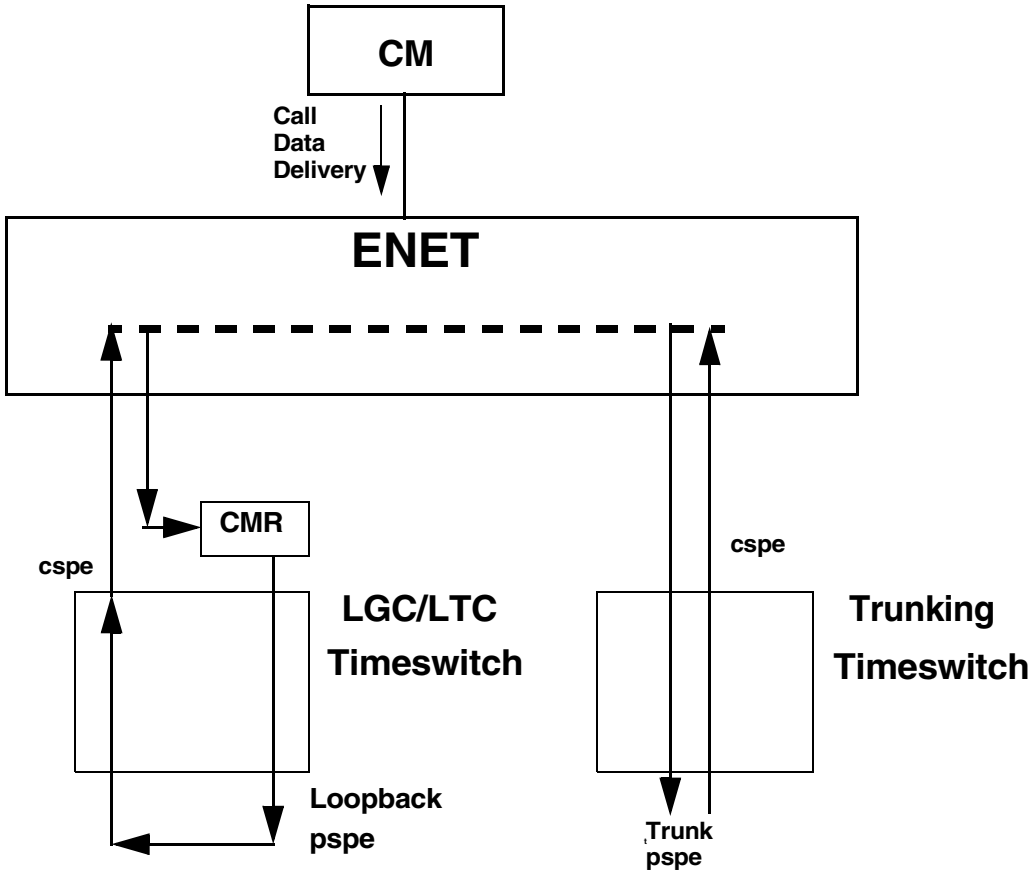
This feature will also support equal access dialing/routing for both Switched-Remote trunk CDCs and Switched CCRs (Note: Switched CCR or dial-out CCR functionality was initially provided in NA014 without equal access support).

To provide support of Equal Access, USNBD Agency command is modified to allow for the provisioning of a PIC and LATA which will be used for all equal access calls to Trunk CDCs and switched CCRs for that agency. If equal access dialing is not desired, the PIC and LATA fields should be set to NILCAR and NILLATA respectively.

Supported trunk types for equal access calls on SR CDCs and Switched CCRs are ISUP IT and ATC trunks with FGD signalling only.

Figure 1 below shows how the connections are made between the CMR card and the outgoing trunk.

Figure 1 CMR card to DTC connection



129.2.2.1 Modifications to USNBD CI commands

The USNBD CDC and AGENCY commands will be enhanced to allow a new type of transport protocol, SR (switched remote) for FSK CDC over trunks. Figure 2 illustrates the CDC list command with an SR CDC link added

Figure 2 Trunk

```
cdc list all
Index Type  Access CDC DN       Agency
    [Associated SINs]
-------------------------------------------------------------------------------
 1 FSK DE    6136211004          TEST
 2 FSK  SL   6136211005          TEST
 3 FSK SR    16136211006         FBI_WITH_EA
CDC LIST DONE
```

The Switched Remote CDC type will utilize Agency data just like the Switched CCRs, for billing information and digit translation.

The Agency command ADD and LIST will be enhanced to add the PIC and LATA fields. Figure 3 shows the agency list display.

Figure 3 Agency List Display

```
>agency list
AGENCY-NAME   STS   PRETRANSLATOR   LCANAME   BILLNO
                    PIC                       LATA
-------------------------------------------------------------------------------
FBI_NO_EA          613   P621                 L613          6135551000
                    NILCAR                    NILLATA
FBI_WITH_EA        613   P621                 L613          6135551001
                    ITT                       LATA1
AGENCY   LIST   DONE.
```

The Switched Remote CDC will utilize Agency data just like the existing Switched CCRs, for billing information and digit translation.

Figure 4 showis a calldump of the 110 and 119 billing records which are output for each CCR or CDC call utilizing EA translations.

Figure 4 110 and 119 CALLDUMP logs

*HEX ID:AA STRUCTURE CODE:40625C CALL CODE:110C SENSOR TYPE:036C
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C
DATE:31215C TIMING IND:00000C STUDY IND:0200000C CLD PTY OFF-HK:0C
SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C
ORIG NPA:613C ORIG NUMBER:5551000C OVERSEAS IND:0C
TERM NPA:00345C TERM NUMBER:8882400C CONNECT TIME:1016181C
ELAPSED TIME:000000465C IC/INC PREFIX:04881C CC DATE:31215C CC TIME:1016165C
ELAPSED CC:000000482C IC/INC EVENT STATUS:010C TRUNK GROUP NUMBER:40639C
ROUTING INDICATOR:1C DIALING INDICATOR:1C ANI INDICATOR:1C
MODULE CODE:306C OLIP:031C MODULE CODE:000C

*HEX ID:AA STRUCTURE CODE:40625C CALL CODE:119C SENSOR TYPE:036C
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C
DATE:31215C TIMING IND:00000C STUDY IND:0200000C CLD PTY OFF-HK:0C
SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C
ORIG NPA:613C ORIG NUMBER:5551000C OVERSEAS IND:0C
TERM NPA:00345C TERM NUMBER:8882400C CONNECT TIME:1016180C
ELAPSED TIME:000000465C IC/INC PREFIX:04881C CC DATE:31215C CC TIME:1016163C
ELAPSED CC:000000482C IC/INC EVENT STATUS:010C TRUNK GROUP NUMBER:30639C
ROUTING INDICATOR:0C DIALING INDICATOR:FF ANI INDICATOR:1C
MODULE CODE:306C OLIP:031C MODULE CODE:000C

129.2.2.2 CDC Link Establishment/Termination/Retries

The same rules which apply to Switched Local CDC lines, will be followed for Switched Remote trunks. A detailed list is in the DID section of this document.

129.3 Hardware Requirements or Dependencies

Availability of a CMR card in any LGC/LTC on the switch.

129.4 Software Requirements or Dependencies

Soc options NBD00003 and NBD00004 turned “ON” for USNBD functionality.

129.5 Limitations and restrictions

CM portion of this feature requires the XPM portion of this feature.

129.6 Interactions

The feature does not modify the way USNBD interacts with other features. It adds an additional CDC type.

129.7 Logs (LG)

129.7.1 New/modified logs

The existing UNB error and secret logs are enhanced to report the problems specific to Switched Remote CDCs during administration or audits. UNB306 logs will be output if the PIC or LATA fields are deleted.

129.8 Data schema (DS)

No new tables are created by this feature and none of the existing tables are modified by this feature.

129.9 Office parameters (OP)

No office parameter related changes are made by this feature.

129.10 Service orders (SO)

No Service order changes are made by this feature.

129.11 Alarms (AL)

No new alarms are added by this feature and none of the existing ones are modified by the feature.

129.12 Glossary

Term	Description
CALEA	Communications Assistance for Law Enforcement Act
CLASS	Custom Local Area Signaling Services
CMR	CLASS Modem Resource
FSK	Frequency Shift Keying
LEA	Law Enforcement Agencies
LI	Lawful Interception
PCM	Pulse Code Modulation
USNBD	United States Network Broadcast Delivery

130: Functional Description (FN): A00004045

130.1 Feature name

UCS20: A00004045 - Calling Line Identification Directory Number (CLIDN) for DMS-250

130.2 Description

The CLIDN call tracing capability captures call data based on the Called number. Called numbers that require tracing are entered into table CLIDN. Call data is captured during trunk termination and output in a TRK605 log. The TRK605 log contains the call origination number (e.g. Calling Party Number) and additional call information for tracing malicious, threatening or otherwise harassing calls.

Prior to this activity, the CLIDN table existed only in the DMS-100/200 product line as one option for providing CLI call tracing functionality. This feature implements similar DMS-100/200 CLIDN call tracing capability into the UCS DMS-250 product line and uses the same CLIDN table. The UCS DMS-250 functionality supports originations and terminations on the following DMS-250 trunk types: EANT (PTS and SS7), PRI, DAL, ONAL, ONAT and IMT (PTS and SS7). Availability of TRK605 log information is dependent on trunk and signaling type at the time the call information is captured.

Please refer to the following sections for additional information on this capability:

- Software Optionality Control (SOC): UTRS0012
- Table CLIDN
- TRK605 Log
- TRK605 Log Data Capture (Call Processing)

130.2.1 Software Optionality Control (SOC): UTRS0012

The new SOC code UTRS0012 ‘CLIDN for DMS-250’ is introduced by this feature. When UTRS0012 is ON, call attempts on a supported incoming trunk to a called number marked for tracing in table CLIDN will generate a TRK605 log. When UTRS0012 is IDLE, call attempts on a supported incoming trunk to a called number marked for tracing in table CLIDN will not generate a TRK605 log. Figure 1 shows an example of SOC UTRS0012 in the ON state.

Figure 1 UTRS0012 SOC option

```
>SOC
SOC:
>SELECT OPTION UTRS0012

GROUP:UTRS
OPTION   NAME              RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------   ----              --- -----   -----   -----    -----  --------
UTRS0012  UCS CLIDN on DMS-250   Y    ON      -      -       -  03/08/28
```

If ACTPATCH KGL03 is active, then SOC UTRS0012 will be set to RTU "Y" and STATE "ON" on ONP to the sourced release.

130.2.2 Table CLIDN

This feature makes table CLIDN functionality available for the UCS DRU. Table CLIDN allows for a maximum of 67 ten-digit directory number (DN) (area code + office code + DN) tuples for which CLI call tracing is provided. For a service code (i.e., 411, 911, etc.) or a seven-digit DN, the letter N (internally translated to 0) must be prefixed to make the total digit count equal to 10.

Table CLIDN is not changed by this feature and is associated with the TRK605 log. When the called number is datafilled in table CLIDN, UTRS0012 SOC option is ON and the incoming trunk is a supported trunk type, the TRK605 log is generated. Figure 2 shows example datafill for table CLIDN.

Figure 2 Table CLIDN datafill

```
>table clidn
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DIGITS:
>6136215015
TUPLE TO BE ADDED:
6136215015
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>list all
TOP
DIGITS
------
NNNNNNN411
NNN8765000
6136215015
BOTTOM
```

130.2.3 TRK605 Log

This feature makes TRK605 log functionality available for the UCS DRU. The existing TRK605 log was introduced in the DMS-100/200 by the Inter-Switch Call Trace (ICT) feature AN1658. The TRK605 log is used in a tandem switch to identify the origination number when the called number is being traced. The TRK605 log contains the fields: Incoming trunk, Outgoing trunk, Called number, Originating number, Source, Call ID and Time.

130.2.3.1 TRK605 Format

This feature does not change the format of the existing TRK605 log. The log report format for TRK605 is as follows:

* TRK605 mmmdd hh:mm:ss ssdd ALARM INFO ICT Calling Line Ident
INCOMING TRUNK = <CKT CLLI>

OUTGOING TRUNK = <CKT CLLI>

CALLED NUMBER = NXXNXXXXXX

SOURCE = CALLING NUMBER/CHARGE NUMBER/
UNAVAILABLE

CALLID = XXXXXX

TIME: MONTH: DAY HH:mm:ss

An example of log report TRK605 follows:

```
* TRK605 SEP27 14:23:29 5908 INFO ICT Calling Line Ident
    INCOMING TRUNK = CKT     DCEA20C7DR01    1
    OUTGOING TRUNK = CKT     DCEA21C7DR02    1
    CALLED NUMBER  = 2018212345
    ORIGINATION NUMBER = 8146119871
    SOURCE =           CALLING NUMBER
    CALLID =      852346
    TIME:    SEP27 14:23:29
```

130.2.3.2 TRK605 Log Field descriptions

Table 1 describes each field in the TRK605 log report.

Table 1 TRK605 Log Field descriptions

Field	Value	Description
*	Alarm	One asterik indicates that the generation of this log report represents a minor alarm condition.
INCOMING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the incoming trunk.
OUTGOING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the outgoing trunk.
CALLED NUMBER	Digits 0-9	This field identifies the called number that is being traced.
ORIGINATING NUMBER	Digits 0-9 or '$'	This field identifies either the calling number, charge number or billing number from the incoming trunk call information. The CLIDN for DMS-250 feature attempts to get the calling number first. If the calling number is not available, the charge number is used. If the charge number is not available, the billing number is used. If neither the calling, charge nor billing number is available, this field will display '$'.

Table 1 TRK605 Log Field descriptions

Field	Value	Description
SOURCE	Calling Number, Charge Number or Unavailable	This field identifies from what the originating number is derived. If the originating number cannot be derived, '$' will appear in the ORIGINATING NUMBER field and the SOURCE field will display "UNAVAILABLE".
CALLID	6 digit number; Digits 0-9 used	This field identifies the call process id number.
TIME	Month, Day, Hour, Minute and Second	This field identifies the date and time the call was logged.

130.2.4 TRK605 Log Data Capture (Call Processing)

When a supported incoming trunk with the called number datafilled in table CLIDN attempts to terminate on an outgoing trunk, a TRK605 log message is generated. The TRK605 log data is captured from the call information depending on the type of call and incoming trunk call data.

The following three call types may impact the Called number used to index table CLIDN on incoming DMS-250 calls:

- For typical calls, the Called number from the incoming trunk is used to index table CLIDN for DN tracing.
- Incoming calls in which a ported number Generic Address Parameter (GAP) is signaled in or returned from the database query, the ported number is used to index table CLIDN for DN tracing, otherwise the Called number is used.
- For all CAIN calls that receive a Called number from the database, the returned Called number from the database is used to index table CLIDN for DN tracing.

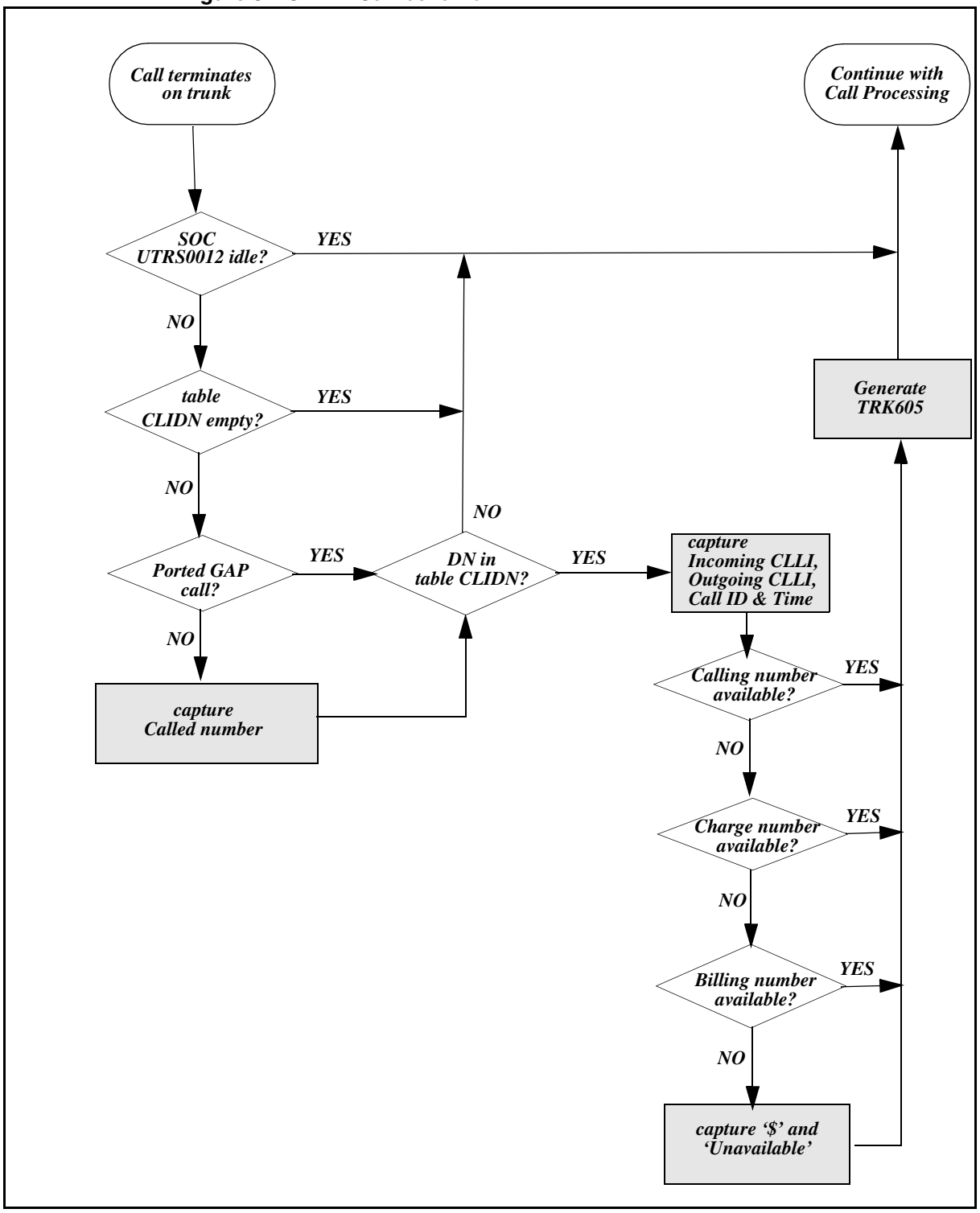
If the Called number is located in table CLIDN, the TRK605 log is generated with the incoming trunk captured call data. Table 2 gives a breakdown of how the TRK605 log data is derived. The flow chart in Figure 3 describes the call processing behavior of this feature.

Table 2 TRK605 log data

TRK605 log field	Information received from
Incoming Trunk	CLLI of incoming trunk

TRK605 log field	Information received from
Outgoing Trunk	CLLI of outgoing trunk
Called Number	Ported number GAP, if ported number is signaled in. The number returned from query, if CAIN alters called number. Called number present in the incoming trunk call data, if typical call.
Origination Number	Calling party number, charge number or billing number. If none of the above info is available, this field will be '$' (left blank).
Source	'CALLING NUMBER' if Origination number field is calling party number. 'CHARGE NUMBER' if Origination number field is charge number or billing number. 'UNAVAILABLE' if Origination number field is '$'.
Callid	Call data information
Time	Call data information time

Figure 3 CLIDN Call behavior



130.3 Hardware Requirements or Dependencies

None.

130.4 Software Requirements or Dependencies

SN07 (UCS20).

130.5 Limitations and restrictions

- This functionality will not support the following UCS trunk types: AXXESS.
- Only standard In-switch routed CAIN calls will be supported.
- This feature is patched in SN06 under ACTPATCH KGL03.

130.6 Interactions

None.

130.7 Applicable customer facing sections

Fault Management	
Logs	__X___
Alarms	__N/A_
Configuration	
Data Schema	__X___
User Interface	__N/A_
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	__N/A_
Accounting (includes AMA billing)	__N/A_
Performance (includes operational measurements)	__N/A_

130.8 Glossary

Term	Description
ANI	Automatic Number Identification
CAIN	Carrier Advanced Intelligent Network
CLI	Calling Line Identify
CLIDN	Calling Line Identify Directory Number
CLLI	Common Language Location Identification
DAL	Dedicated Access Line
DN	Directory Number
EANT	Equal Access Network Trunk
GAP	Generic Address Parameter
IAM	Initial Address Message of the SS7 signalling
IMT	Inter Machine Trunk
ISUP	Integrated Services digital network User Part
ICT	Inter-Switch Call Trace
LNP	Local Number Portability
ONAL	Off Network Access Line
ONAT	Off Network Access Trunk
ONP	One Night Process
PRI	Primary Rate Interface
RTU	Right to Use
SS7	Signalling System No. 7
SOC	Software Optionality Control
UCS	Universal Carrier Service

131: Functional description (FN): A00004046

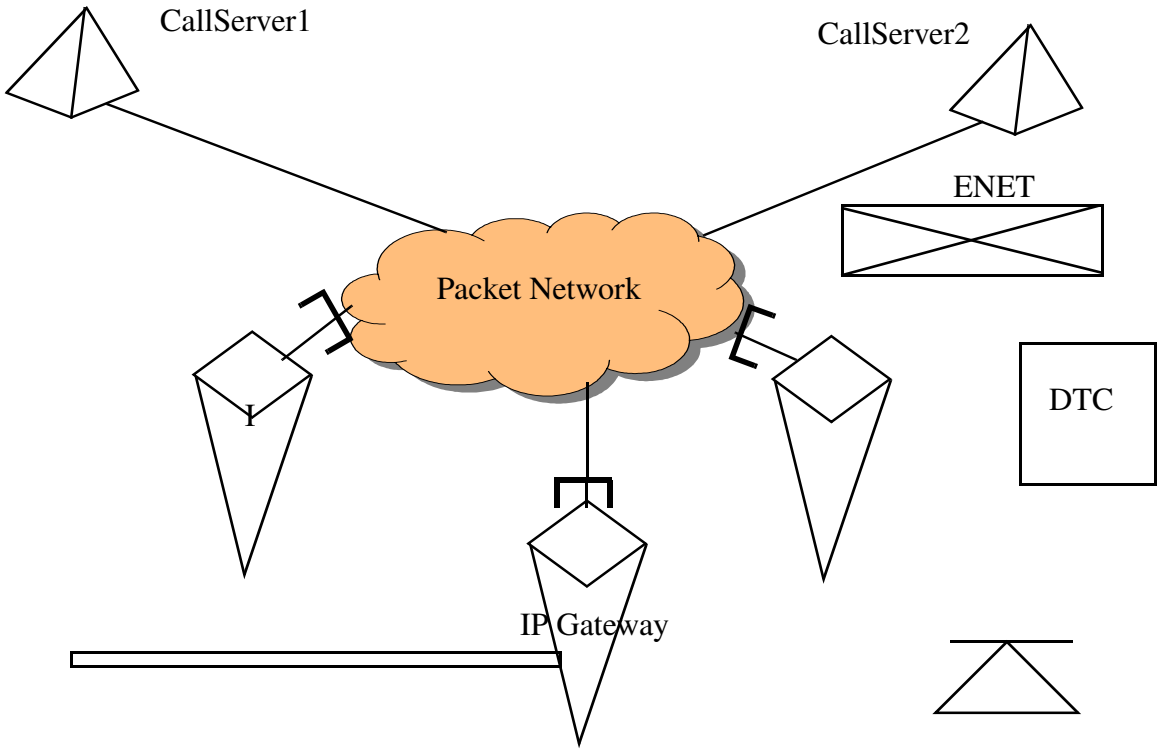
131.1 Feature name

This feature is titled Echo Cancellation Support for TriModal Call Server 2000.

131.2 Description

The TriModal call model allows for legacy, AAL1 and IP bearer fabrics to co-exist in the same Call Server VPN. This activity is responsible for ensuring that ECAN resources can and are allocated appropriately within the CallServer VPN. The goal is to ensure that ECAN resources are always applied in IP networks and are applied according to the selected strategy for AAL1 fabric. This entails implementation of an Edge Strategy for IP Networks and either an Edge or Region strategy for AAL1 networks. Edge Strategy requires that ECAN resources are always allocated at the point of entry into a packet network. Region strategy uses a provisioning model that allows the customer to dictate where ECAN resources should be deployed throughout the network.

Figure 1 Edge Strategy



The diagram above is an illustration of how an edge strategy could be employed. The salient point is that every point of entry into the network is covered by an ECAN resource.

Conversely, a region strategy is dictated by provisioning. The customer, using knowledge of network parameters, provisions the strategic locations within their network where ECAN resources should be applied. It is not assumed that a network device with a packet interface will automatically utilize ECAN resources.

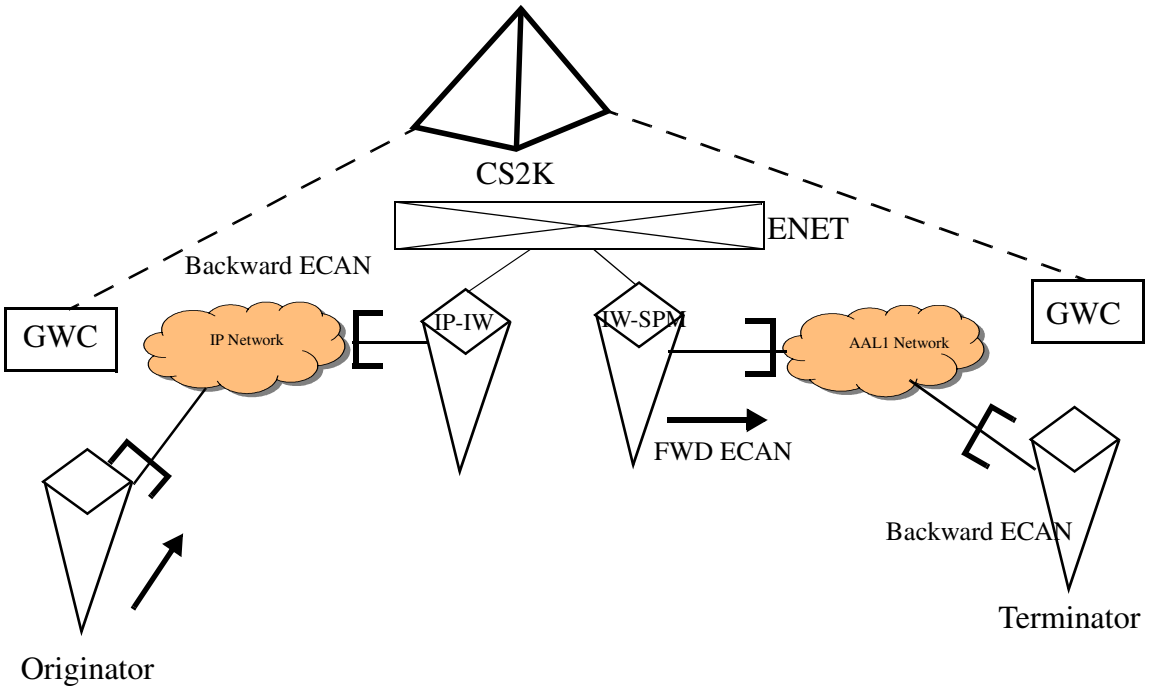
In SN06, feature A89007309, introduced support for an ECAN_EDGE_STRATEGY office parameter which would be used to differentiate between EDGE and REGION strategies on IP and AAL1 networks. A primary goal of activity A00004046 is to ensure that in the TriModal implementation, this strategy continues to be effective.

In SN07, IP, AAL1 and ENET bearer fabrics all co-exists on the same CS2K callserver. At a minimum, every call in this topology must have sufficient ECAN resources. These resources may be provided locally or optimized out of the call if it is subsequently determined that the resource is not required.

Fortunately, the SN06 strategy extends itself quite well to the TriModal architecture, ensuring that ECAN is applied consistent with this strategy.

The ECAN edge strategy will be assumed for all packet network types except AAL1. The ECAN strategy for AAL1 will be determined by the value of the EDGE_ECAN_STRATEGY office parameter. Currently, there are scenarios where ECAN resources in a TriModal switch will be duplicated.

Figure 2 TRI-MODAL IP-AAL1 Call



In the call scenario above, 4 ECAN resources will be allocated in the call, depending upon the ECAN_EDGE_STRATEGY value for the AAL1 side. The IP side of the call will always allocate both ECAN resources, however, if the REGION strategy is deployed, the ECAN resource on the AAL1 side of the call, utilizing the IW-SPM, will be deallocated. The manner in which ECAN resources are allocated in this TriModal topology is unchanged from the manner in which the resources would be allocated if both IP and AAL1 were not converged.

Therefore, in summary, the ECAN_EDGE_STRATEGY parameter will continue to be used in the CS2K to control ECAN allocation in the AAL1 bearer fabric. All other packet bearer fabrics will assume the edge strategy.

131.2.1 Trunk Provisioning

In summary, support for TriModal CS2K should be transparent to the customer. Support for this activity will be provided by the existing infrastructure, developed in the previous release for support of Next Generation Networks.

131.3 Hardware Requirements or Dependencies

There are no additional hardware requirements in support of this feature.

131.4 Software Requirements or Dependencies

There are no additional software requirements in support of this feature.

131.5 Limitations and restrictions

Trunk provisioning pertaining to ECAN is limited to provisioning ECAN resources against a specific trunk sub-group. There are 2 fields in TRKSGRP where this is done. On SPM peripherals, the SPMECIDX option is used to connect a specific ECAN provisioned value with a subgroup. For all other trunks, the ECSTAT field is used to determine whether or not ECAN resources are available, internally or externally.

This mode of operation is unchanged in this activity, however, customers should be aware of the following limitation (once MG4K-IP is available) when determining the ECAN characteristics of SPM based trunk members constituting a trunk group. TRKSGRP table only allows 2 subgroup tuples to be added per trunk group. There are currently 3 bearer fabrics that could potentially differ in their ECAN provisioning requirements in this table.

- Legacy Trunks i.e DMSCP SPM.
- AAL1 Trunks i.e. MG4K
- IP Trunks i.e. MG4K-IP (not available in SN07)

Since only 2 trunk subgroup tuples are allowed per trunkgroup, if the strategy for a trunkgroup contains all three component types, 2 of these types must share the same SPMECIDX value. This constraint should be considered during trunk datafill planning.

131.6 Interactions

There should be no visible effect in support of ECAN allocation in a TRI-MODAL call server. The extensibility of existing Next-Generation-Networks ECAN support makes the application of these resources transparent on a TRI-MODAL CS2K.

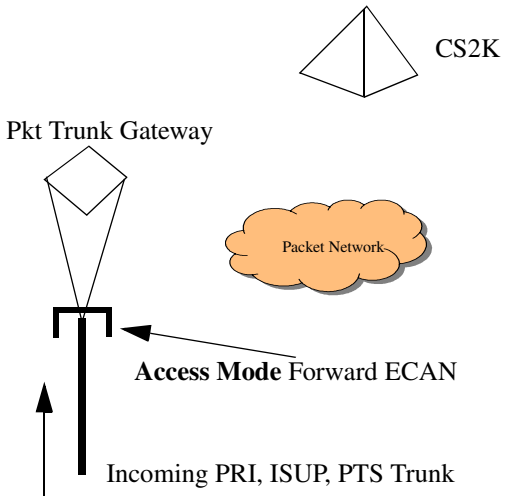
131.6.1 ECAN Terminal Type Cross Matrix

The allocation of resources are described in terms of Forward and Backward ECAN and Network vs. Access Mode allocation. In order to facilitate the understanding of table data, an explanation of these terms is in order.

Forward ECAN refers to ECAN resources that prevent echo from traversing in the forward direction of the call from originator to terminator. Backward ECAN refers to ECAN resources that prevent echo from traversing the call in a backwards direction from terminator to originator.

This concept in conjunction with Access vs. Network mode echo cancellation provides the exact direction and location in the CS2K that the echo cancellers are applied. Access mode ECAN refers to echo cancellers applied towards the facility i.e. The Line or the Trunk entity that is the source of the echo. Network mode ECAN applies echo cancellers toward the ENET. “Towards the ENET” or “Towards the Facility” applies to the “tail of the echo”. The “tail of the echo” can be thought of as the round-trip path from the echo canceller to the source of the echo. The echo cancellers are deployed in the direction of the tail. The following diagrams are provided to help the reader to understand how echo cancellers are applied in conjunction with these concepts.

Figure 3 Access Mode ECAN Example

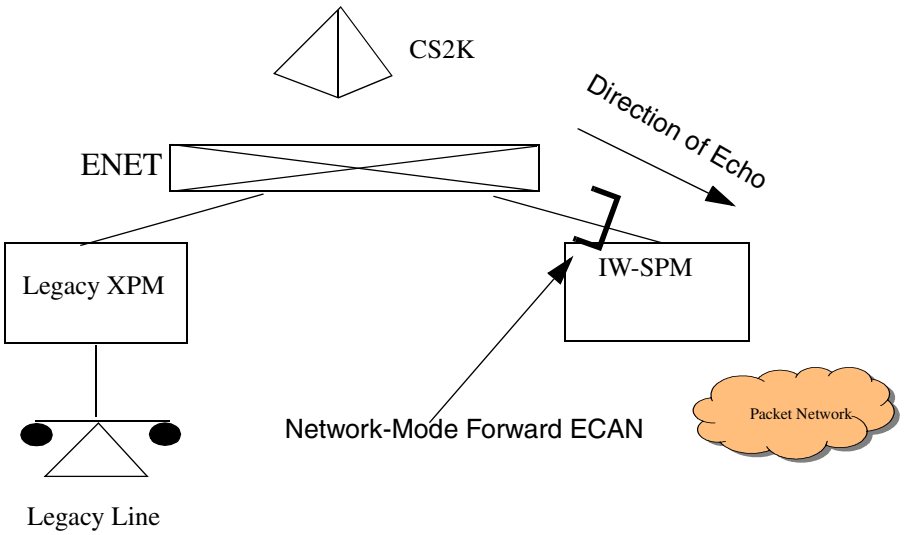


As Figure 3 illustrates, the echo canceller is applied to the incoming trunk, before packetization. It is Access Mode because it is applied to control echo

from the Facility. It is “forward” because it is blocking echo in the forward direction towards the terminating side of the call.

Network-Mode echo cancellers are applied toward the ENET. This is the defining characteristic of Network-Mode ECAN. Figure 4 below illustrates this concept.

Figure 4 Network Mode Forward ECAN

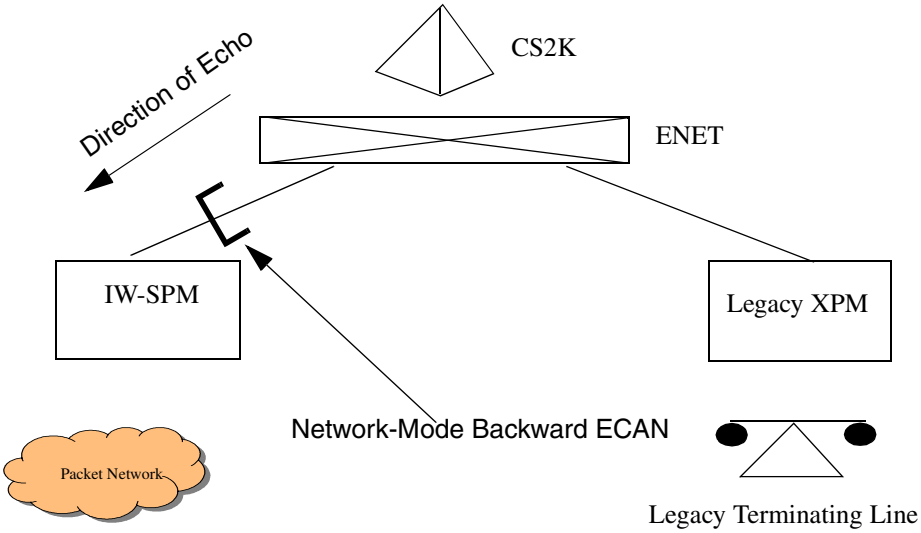


In Figure 4, the echo canceller is forward, due to the direction of the echo that is being cancelled. Echo cancellation is applied prior to packetization. However, the same ECAN resource applied in a different configuration can be Network-Mode **Backward** ECAN due to it’s position within the CS2K VLAN. This is the reason that Forward and Backward are not sufficient to determine the location of an echo canceller in the VLAN.

If the IW-SPM is positioned on the originating side of the CS2K VLAN, as opposed to the terminating side of the CS2K as it is shown in Figure 4, it is providing Backward ECAN.

Figure 5 below illustrates an IW-SPM providing ECAN resources in this capacity.

Figure 5 Network-Mode Backward ECAN



The following tables provides a high level view of ECAN allocation for different terminal types. Note that ABI lines and trunks have the same ECAN behavior as a packet line of the same network type. For example, an AAL1 ABI trunk would have the same ECAN behavior as listed in the following tables for an AAL1 line.

Table 1 ECAN Location for Legacy and IP Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW
IP line to Legacy agent	Backward ECAN		Forward ECAN	
Legacy agent to IP line	Forward ECAN		Backward ECAN	
IP MG4K trunk to Legacy agent	Backward ECAN	Forward ECAN		
Legacy Agent to IP MG4K trunk	Forward ECAN	Backward ECAN		
IP GWC trunk to Legacy agent	Backward ECAN			Forward ECAN
Legacy Agent to IP GWC trunk	Forward ECAN			Backward ECAN
Legacy Agent to SIPT GWC trunk	Forward ECAN			
SIPT GWC trunk to Legacy Agent	Backward ECAN			
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN.			

Table 2 ECAN Location for AAL1 agent Interworkings

Call Type	ECAN_EDGE_STRATEGY = N			ECAN_EDGE_STRATEGY = Y		
	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to AAL1 line			Forward & Backward ECAN			Forward & Backward ECAN
AAL1 line to MG4K trunk		Forward & Backward ECAN**	Forward ECAN		Backward ECAN	Forward ECAN
AAL1 line to AAL1 BICC trunk			Forward ECAN			Forward ECAN
MG4K trunk to MG4K trunk		Forward & Backward ECAN			Forward & Backward ECAN	
MG4K trunk to AAL1 line		Forward & Backward ECAN**	Backward ECAN		Forward ECAN	Backward ECAN
MG4K trunk to AAL1 BICC trunk		Forward & Backward ECAN**			Forward ECAN	
AAL1 BICC trunk to AAL1 BICC trunk						
AAL1 BICC trunk to AAL1 line			Backward ECAN			Backward ECAN
AAL1 BICC trunk to AAL1 MG4K trunk		Backward ECAN			Backward ECAN	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. ****Note:** calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.					

Table 3 ECAN Location for Legacy and AAL1 Interworkings

Call Type	ECAN_EDGE_STRATEGY = N			ECAN_EDGE_STRATEGY = Y		
	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to Legacy agent			Forward ECAN	Backward ECAN		Forward ECAN
Legacy agent to AAL1 line			Backward ECAN	Forward ECAN		Backward ECAN
MG4K trunk to Legacy agent		Forward & Backward ECAN**		Backward ECAN	Forward ECAN	
Legacy Agent to MG4K trunk		Forward & Backward ECAN**		Forward ECAN	Backward ECAN	
Legacy Agent to DPT GWC trunk	Forward ECAN			Forward ECAN		
DPT GWC trunk to Legacy Agent	Backward ECAN			Backward ECAN		
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. ****Note:** calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.					

Table 4 ECAN Location for IP and AAL1 (edge) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
IP line to AAL1 line	Backward ECAN		Forward ECAN		Forward ECAN		Backward ECAN
IP line to AAL1 BICC trunk	Backward ECAN		Forward ECAN		Forward ECAN		
IP line to AAL1 MG4K trunk	Backward ECAN		Forward ECAN		Forward ECAN	Backward ECAN	
IP GWC trunk to AAL1 line	Backward ECAN			Forward ECAN	Forward ECAN		Backward ECAN
IP GWC trunk to AAL1 BICC trunk	Backward ECAN			Forward ECAN	Forward ECAN		
IP GWC trunk to AAL1 MG4K trunk	Backward ECAN			Forward ECAN	Forward ECAN	Backward ECAN	
IP MG4K trunk to AAL1 line		Forward ECAN			Forward ECAN		Backward ECAN
IP MG4K trunk to AAL1 BICC trunk	Backward ECAN	Forward ECAN			Forward ECAN		
IP MG4K trunk to AAL1 MG4K trunk		Forward ECAN				Backward ECAN	
IP SIPT trunk to AAL1 line	Backward ECAN				Forward ECAN		Backward ECAN
IP SIPT trunk to AAL1 BICC trunk	Backward ECAN				Forward ECAN		
IP SIPT trunk to AAL1 MG4K trunk	Backward ECAN				Forward ECAN	Backward ECAN	
AAL1 line to IP line	Forward ECAN		Backward ECAN		Backward ECAN		Forward ECAN
AAL1 line to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		Forward ECAN
AAL1 line to IP MG4K trunk		Backward ECAN			Backward ECAN		Forward ECAN
AAL1 line to IP SIPT trunk	Forward ECAN				Backward ECAN		Forward ECAN

Table 4 ECAN Location for IP and AAL1 (edge) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 BICC trunk to IP line	Forward ECAN		Backward ECAN		Backward ECAN		
AAL1 BICC trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		
AAL1 BICC trunk to IP MG4K trunk	Forward ECAN	Backward ECAN			Backward ECAN		
AAL1 BICC trunk to IP SIPT trunk	Forward ECAN				Backward ECAN		
AAL1 MG4K trunk to IP line	Forward ECAN		Backward ECAN			Forward ECAN	
AAL1 MG4K trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN	Forward ECAN	
AAL1 MG4K trunk to IP MG4K trunk		Backward ECAN				Forward ECAN	
AAL1 MG4K trunk to IP SIPT trunk	Forward ECAN				Backward ECAN	Forward ECAN	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN.						

Table 5 ECAN Location for IP and AAL1 (region) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
IP line to AAL1 line	Backward ECAN		Forward ECAN				Backward ECAN
IP line to AAL1 BICC trunk	Backward ECAN		Forward ECAN		Forward ECAN		
IP line to AAL1 MG4K trunk	Backward ECAN		Forward ECAN			Forward & Backward ECAN**	
IP GWC trunk to AAL1 line	Backward ECAN			Forward ECAN			Backward ECAN
IP GWC trunk to AAL1 BICC trunk	Backward ECAN			Forward ECAN	Forward ECAN		
IP GWC trunk to AAL1 MG4K trunk	Backward ECAN			Forward ECAN		Forward & Backward ECAN**	
IP MG4K trunk to AAL1 line		Forward ECAN					Backward ECAN
IP MG4K trunk to AAL1 BICC trunk	Backward ECAN	Forward ECAN			Forward ECAN		
IP MG4K trunk to AAL1 MG4K trunk		Forward ECAN				Backward ECAN	
IP SIPT trunk to AAL1 line	Backward ECAN						Backward ECAN
IP SIPT trunk to AAL1 BICC trunk	Backward ECAN				Forward ECAN		
IP SIPT trunk to AAL1 MG4K trunk	Backward ECAN					Forward & Backward ECAN**	
AAL1 line to IP line	Forward ECAN		Backward ECAN				Forward ECAN
AAL1 line to IP GWC trunk	Forward ECAN			Backward ECAN			Forward ECAN
AAL1 line to IP MG4K trunk	Forward ECAN	Backward ECAN					Forward ECAN

Table 5 ECAN Location for IP and AAL1 (region) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to IP SIPT trunk	Forward ECAN						Forward ECAN
AAL1 BICC trunk to IP line	Forward ECAN		Backward ECAN		Backward ECAN		
AAL1 BICC trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		
AAL1 BICC trunk to IP MG4K trunk	Forward ECAN	Backward ECAN			Backward ECAN		
AAL1 BICC trunk to IP SIPT trunk	Forward ECAN				Backward ECAN		
AAL1 MG4K trunk to IP line	Forward ECAN		Backward ECAN			Forward & Backward ECAN**	
AAL1 MG4K trunk to IP GWC trunk	Forward ECAN			Backward ECAN		Forward & Backward ECAN**	
AAL1 MG4K trunk to IP MG4K trunk		Backward ECAN				Forward ECAN	
AAL1 MG4K trunk to IP SIPT trunk	Forward ECAN					Forward & Backward ECAN**	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. ****Note:** calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.						

131.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters __X____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

131.8 Glossary

Term	Description
Forward ECAN	Echo Cancellers blocking echo from traversing from originator to terminator
Backward ECAN	Echo Cancellers blocking echo from traversing from terminator to originator

132: Functional description (FN): A00004096

132.1 Feature name

North America (NA) H.323 Support for Networked Meridian Customer Defined Network (MCDN) Services - ActId A00004096: SN07 Release, North American CS2K Load

132.2 Description

This feature allows interworking of MCDN based PBXs with certain hosted NA CS2K centrex lines for use within the Enterprise network.

Therefore, this feature activity A00004096 addresses the development associated with providing the NA CS2K switch the ability to support a specified set of MCDN services for its hosted centrex lines (i.e., CICM and Mediatrix 1104) within a carrier hosted H.323 network.

This feature activity A00004096 supports a specific set of MCDN services based upon the following Network Configurations:

- **interworking on a per nodal basis**
  These specific set of MCDN services are supported and interworked over a PRI_{H323} Trunk facility between either a Succession 1000M or BCM, and a hosted centrex line on a NA CS2K switch. Please reference Figure 2, on page 1695 .
- **interworking on a per inter-Call Server basis**
  These specific set of MCDN services are supported and interworked over a SIP-T[1] Trunk facility between either a Succession 1000M or BCM, and a hosted centrex line on a NA CS2K switch. Please reference Figure 3, on page 1697 .

MCDN is a Nortel proprietary PRI Q.931 protocol that allows Nortel PBXs to support a set of Networked Services between them within a Private Network. Within the H.323 IP network, the Enterprise PBX (i.e., Succession 1000M or BCM) tunnels this MCDN data in the nonStandardData field within the User-user Information Element (IE) of an H.225 message.

Currently, the CS2K Succession switch does not generate nor interpret this H.323 tunneled MCDN data.

[1]Within this document and/or activity A00004096, SIP-T is defined as an ANSI ISUP Trunk facility which contains Tunneled MCDN data.

In order to support these specific set of MCDN services on the CS2K Succession switch, design development maybe required to interpret or generate this tunneled MCDN service data within the H.323 packet.

> ***Note:*** if necessary, MCDN interpretation or generation is done within the Gateway Controller (GWC), not the CS2K Core.

This development allows the CS2K Succession switch to support (a limited set of) MCDN Services to Enterprise customers transparently. Therefore, if the Service Provider's Network contains more than one CS2K switch, an Enterprise customer can be spread across multiple CS2Ks.

132.3 $PRI_{H.323}$ Deployment

Throughout this FN document, a $PRI_{H.323}$ Trunk denotes a H.323 Nortel North American (NTNA) PRI Trunk which is utilized to connect a GWC with an H.323 profile to the CS2K on an NA CM load. This $PRI_{H.323}$ trunk type will be provisioned on the CS2K within the LTDATA table with the **PRI_IP_PROT** option, and **H323** VOIP_ PROTOCOL_TYPE. For example:

Figure 1 $PRI_{H.323}$ datafill trunk type example

```
TABLE: LTDATA
LTDKEY LTDRSLT
--------------
ISDN 867 SERV SERV Y Y ALWAYS ALWAYS (PRI_IP_PROT H323) $
```

Messaging on a $PRI_{H.323}$ trunk is formatted as per the H.323 NTNA PRI standard, and may carry tunneled MCDN private information pertaining to the H.323 endpoints. Currently, this tunneled MCDN data within the H.323 NTNA PRI Facility IE is transported transparently, without MCDN content verification/interpretation by either the GWC H.323 or GWC TPT tasks, up to the CS2K Core.

As indicated before, based upon this specific set of MCDN Services, development may be done within the GWC H.323 in order to interpret this tunneled MCDN data received from either a Succession 1000M or BCM Enterprise, and then pass this extracted interpreted MCDN data onto the GWC TPT.

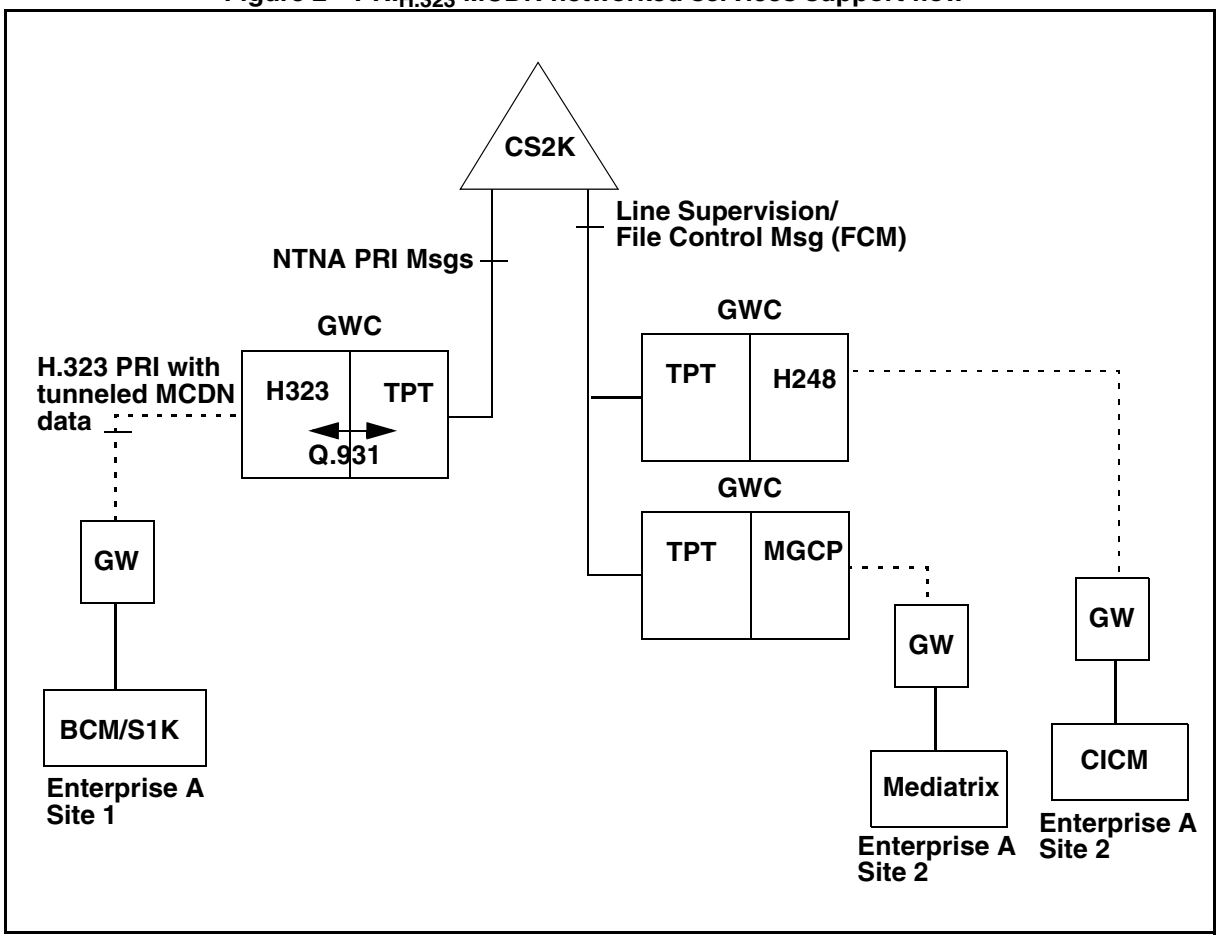
For example, at present, the Succession 1000M does not include Calling Name within the H.323 Setup message IEs, only Calling and Called Number in the H.323 IEs. The Succession 1000M Enterprise places the Calling Name IE within the tunneled MCDN data, not the H.323 IE. Therefore, development is required within the H.323 GWC to interpret this tunneled MCDN data in order to extract the Calling Name IE, and then pass this Calling Name text onto the GWC TPT. By doing this, the CS2K Core will receive Calling Name information from GWC TPT in order to provide Calling Name display.

In the CS2K to Succession 1000M call direction, the CS2K does provide Calling Name (as well as Calling and Called Number) within the H.323 Setup message IEs; however, the Succession 1000M displays only the Calling Number if tunneled MCDN data is not present (within an H.323 Setup Message). At present, the Succession 1000M expects the Calling Name to be contained within a tunneled MCDN H.323 packet. Therefore, the Succession 1000M does not display Calling Name from a CS2K switch. Hence, development is necessary within the GWC H.323 to build tunneled MCDN data which contains the Calling Name IE in order for the Succession 1000M to display Calling Name.

Note: for NTNA PRI name display, the Calling Name Presentation is linked to the Calling Number Presentation which requires the network to apply the Network Presentation Indicator (NPI) (“public” or “private”) value for the Calling Party Number to the Calling Name presentation status.

Figure 2, on page 1695 outlines the $PRI_{H.323}$ callserver topology in which this feature is being developed.

Figure 2 $PRI_{H.323}$ MCDN networked services support flow



132.3.1 SIP_$T_{H.323}$ (Tunneled ANSI ISUP) CS2K Deployment:

Throughout this document, a SIP_$T_{H.323}$ Trunk denotes tunneling of ANSI ISUP data via a SIP-T Trunk for support of the H.323 protocol on an NA CM load. This SIP_$T_{H.323}$ trunk type will be provisioned on the CS2K within the following existing CS2K Tables:

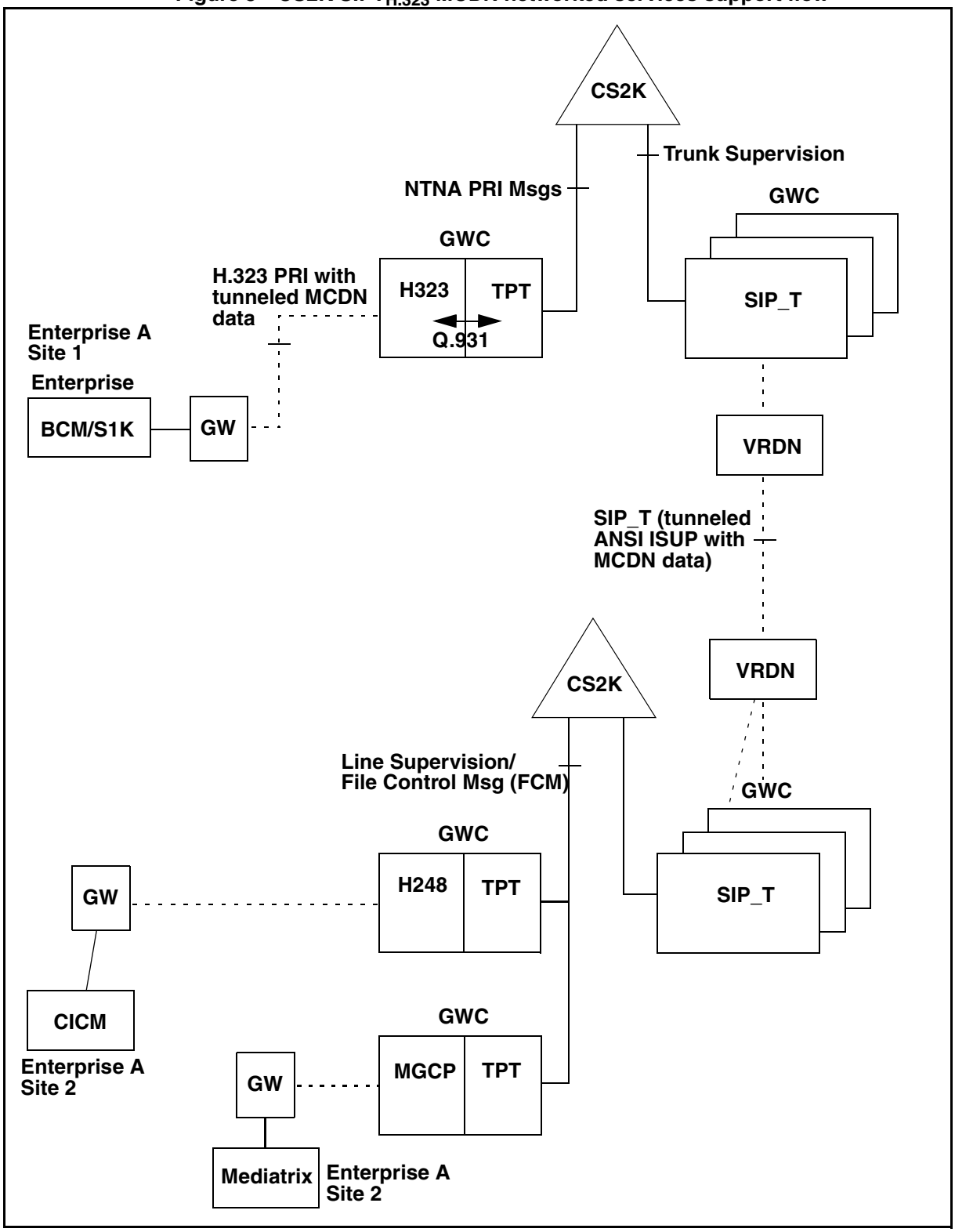
- CLLI
- TRKGRP
- TRKSGRP
- MGCINV
- TELEPROF
- VRINV
- TRKOPTS
- DPTRKMEM

MCDN private data will be mapped to ISUP Remote Operations Service Element (ROSE) Information Elements.

Like $PRI_{H.323}$, MCDN data contained with the ANSI ISUP ROSE parm(s) are transported transparently without verification of the MCDN content by the SIP_T GWC up to the CS2K Core.

Figure 3, on page 1697 outlines the SIP_$T_{H.323}$ callserver topology in which this feature is being developed.

Figure 3 CS2K SIPT$_{H.323}$ MCDN networked services support flow



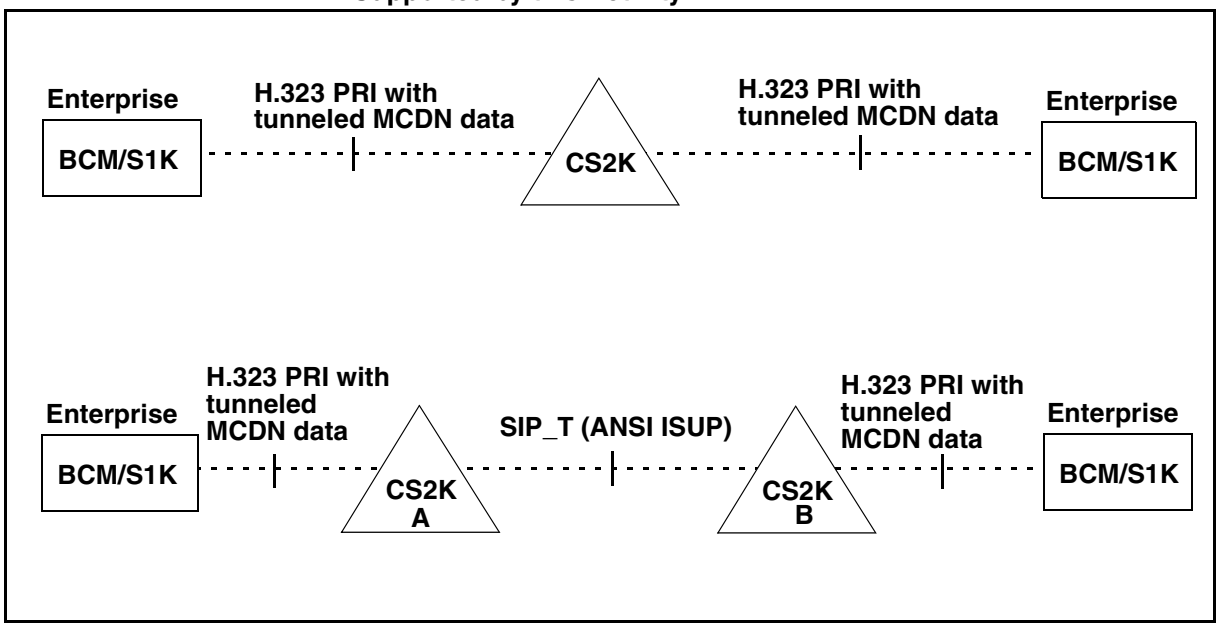
132.3.2 Supported MCDN Services

Only those MCDN services which are supported on either a P-Phone agent (via CICM) or an IBN line agent (via Mediatrix) are supported by this activity.

This feature supports a specific set of MCDN services on a per Enterprise nodal basis where the Originating and Terminating centrex line are connected to the same Call Service (i.e., CS2K). Also, these specific set of MCDN Services are supported across multiple Call Services via a SIP-T (ANSI ISUP).

Support of MCDN Services between different Enterprises (via a CS2K switch) is outside the scope of this feature (please reference Figure 4, on page 1698).

Figure 4 Enterprise to Enterprise MCDN Services via a CS2K is Not Supported by this Activity



Please reference the following activities for MCDN Tunneling through a CS2K:

- A00002206 *H.323 NTNA PRI Support*
- A00004568 *H.323 NA Network CAS SIP_T (Tunneling with MCDN)*

Following interworkings are supported:

- H.323 GW (BCM) <--> H.248 GW (CICM, P-phone)
- H.323 GW (BCM) <--> MGCP GW (Mediatrix, IBN lines)
- H.323 GW (Succession 1000M) <--> H.248 GW (CICM, P-phone)
- H.323 GW (Succession 1000M) <--> MGCP GW (Mediatrix, IBN lines)

Table 1 lists supported MCDN services for BCM interworking to CICM and Mediatrix for nodal calls and through SIP-T.

Table 2 lists supported MCDN services for Succession1000M interworking to CICM and Mediatrix GW for nodal calls and through SIP-T.

Each table should be read as following:

yes MCDN service interworking exists already and has been verified by other activities in SN06.

Yes MCDN service interworking is implemented and verified by this SN07 activity.

- low priority service (priority 2, 3, 4) not captured by this activity

Table 1 Supported MCDN Services

MCDN Services	BCM interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (SIP-T)
Basic Call	yes	yes	yes	yes
Calling Line Identification (CLID)				
- Calling Number Delivery	Note 3	Note 3	Yes	Yes
- Connected Number Delivery	Note 2	Note 2	Note 2	Note 2
- Called Number Delivery	Note 3	Note 3	Yes	Yes
Network Call Party Name Display				
- Calling Party Name Delivery	Note 3	Note 3	Yes Note 4	Yes Note 5
- Connected Party Name Delivery	-	-	-	-
- Original Called Party Name Delivery	-	-	-	-
- Called Party Name Delivery	-	-	-	-
- Redirecting Party Name Delivery	-	-	-	-
- Redirection Party Name Delivery	-	-	-	-
Network Call Redirection				
- Network Call Forward All Calls	Note 3	Note 3	Yes	Yes
- Network Call Forward No Answer	Note 3	Note 3	Yes	Yes
- Network Call Forward Busy	Note 3	Note 3	Yes	Yes

- Network Hunting	-	-	-	-
- Call Transfer	Note 3	Note 3	Yes	Yes
- Call Pickup	-	-	-	-
Network message services				
- Message Waiting Indication	Note 1)			
Network Camp-on	-	-	-	-
Network Break-In	-	-	-	-
Trunk Anti-Tromboning (TAT)	-	-	-	-
Multi-location business groups (MBG)	Note 1)			
Virtual Access to Private Networks (VAPN)	-	-	-	-
Direct Inward System Access (DISA)	-	-	-	-

yes: service is already supported and tested by other SN06 activities
Yes: service is supported by this SN07 activity
- : low priority service, not captured by this activity
Note 1): Priority 1 service, not supported by this activity. Further investigations are needed.
Note 2): Priority 1 service, not supported by this activity, but according to Enterprise Architect, it is supported as a MCDN Service interworking between two H.323 GWs.
Note 3): Currently, CICM GWs are unavailable to test with; however, this is a supported Service.
Note 4): For this activity's CS2K to Succession-1000M direction, only private calls contain the MCDN private data (for displaying Calling Name). For CS2K to Succession-1000M direction, public calls do NOT contain private MCDN data. Therefore, for public CS2K to Succession-1000M direction calls, Calling Display is not applicable/displayed.
Note 5): Calling Name Delivery within the Core remains unchanged by this activity to either line agents or trunk agents; therefore, whatever existing functionalities, restrictions or limitations of Calling Name Delivery remain applicable.

Connected Number identifies the number in which the parties are connected to if the call had been changed (i.e., call redirection) during the lifetime of the call.

Even though Connected Number (CN) is a priority 1 service, it is not supported by this activity because the following:

- if the call has been redirected, CS2K expects that the Connected Number to be contained within a NOTIFY message. However, Nortel's *H.323 Interoperability Specification* does not support H.323 NOTIFY messaging.

  Succession 1000M/BCM expects this NOTIFY message, along with its Connected Number IE and other IEs, to be tunneled within the MCDN nonStandardData portion of a H.323 FACILITY message.
- in order to properly derive the Connected Number upon call redirection, multiple NOTIFY messages are required in order to request and provide

Connected Number bi-directionality (please reference Figure 5). The complexity of either tunneling the entire NOTIFY message and its IEs within the nonStandardData portion of an H.323 FACILITY message or extraction and interpretation of incoming MCDN data to a NOTIFY message to the CS2K Core requires sufficient time. According the an Enterprise Architect, for example, if the CS2K does not correctly build a tunneled MCDN Notify message within an H.323 FACILITY packet, it could cause call processing issues/problems for the Enterprise.

- because this activity came extremely late within the SN07 design cycle, this activity simply does not have a lot of design time (as well as testing time) in order to adequately provide high quality for this particular complicated messaging exchange.

Figure 5, on page 1702 , illustrates how the CS2K expects Connected Number to be contained within a NOTIFY message, but Nortel's H.323 Specifications do not support H.323 NOTIFY messaging. In addition, Figure 5 indicates the multiple messaging necessary to fully support/implement Connected Number.

Figure 5 CS2K Notify messaging Example for Connected Number

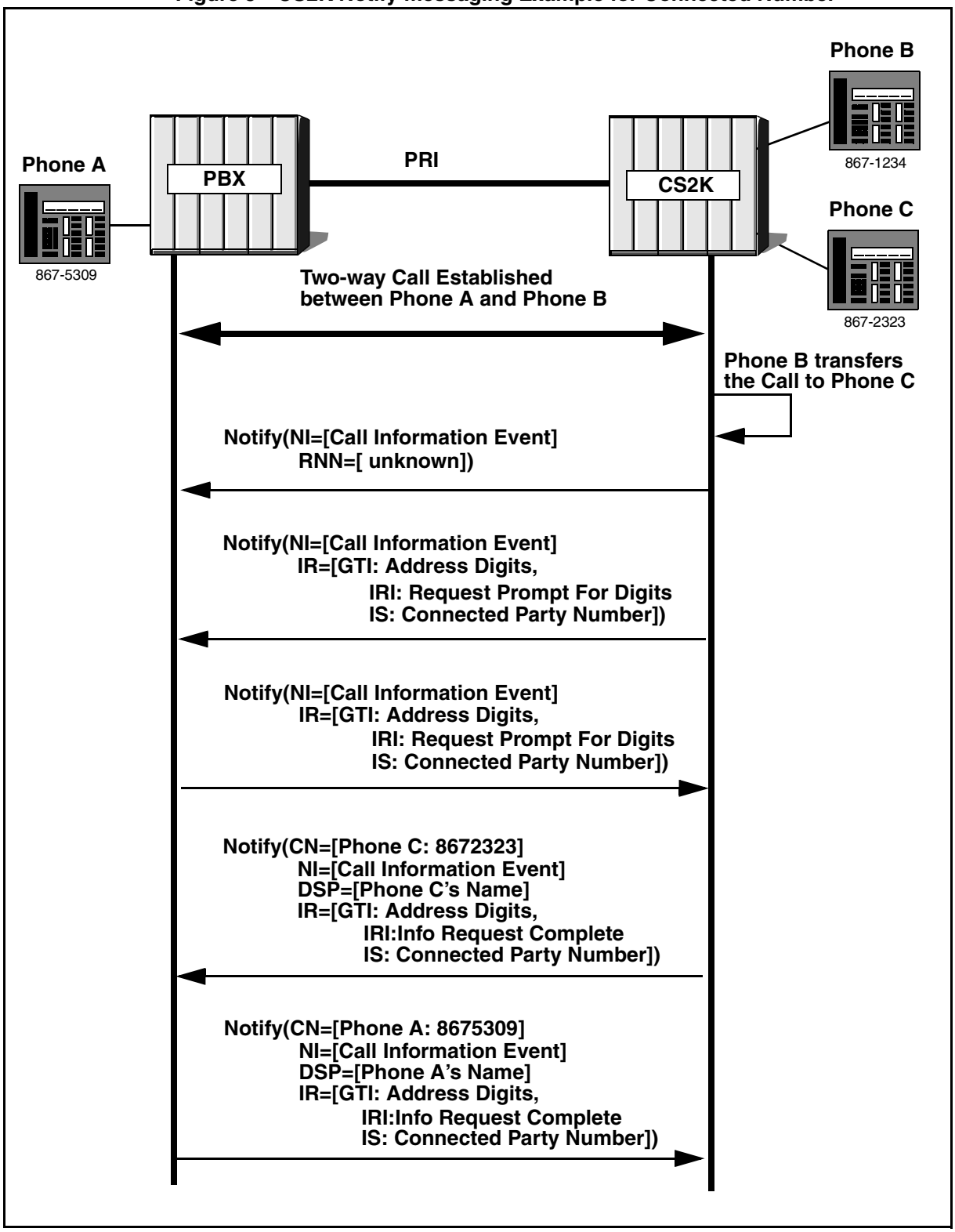


Table 2 lists supported MCDN services for Succession1000M interworking to CICM and Mediatrix GWs for nodal calls and through SIP-T.

The table should be read as following:

yes MCDN service interworking exists already and has been verified by other activities in SN06.

Yes MCDN service interworking is implemented and verified by this SN07 activity.

- low priority service (priority 2, 3, 4) not captured by this activity

Table 2 Supported MCDN Services

MCDN Services	Succession1000M interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (SIP-T)
Basic Call	yes	yes	yes	yes
Calling Line Identification (CLID)				
- Calling Number Delivery	Note 3	Note 3	Yes	Yes
- Connected Number Delivery	Note 2	Note 2	Note 2	Note 2
- Called Number Delivery	Note 3	Note 3	Yes	Yes
Network Call Party Name Display				
- Calling Party Name Delivery	Note 3	Note 3	Yes Note 4	Yes Note 5
- Connected Party Name Delivery	-	-	-	-
- Original Called Party Name Delivery	-	-	-	-
- Called Party Name Delivery	-	-	-	-
- Redirecting Party Name Delivery	-	-	-	-
- Redirection Party Name Delivery	-	-	-	-
CLID in Call Detail Record (CDR)	Note 1)			
ISDN Signaling Link (ISL)	-	-	-	-
Network Ring Again	Note 1)			
Network Call Redirection				
- Network Call Forward All Calls	Note 3	Note 3	Yes	Yes

Table 2 Supported MCDN Services

- Network Call Forward No Answer	Note 3	Note 3	Yes	Yes
- Network Call Forward Busy	Note 3	Note 3	Yes	Yes
- Network Hunting	-	-	-	-
- Call Transfer	Note 3	Note 3	Yes	Yes
- Call Pickup	-	-	-	-
Network Automatic Call Distribution (NACD)				
- Make Set Busy Key	-	-	-	-
- Not Ready Key	-	-	-	-
- Individual DN Key	-	-	-	-
- Dialed Number Identification Service and Name Display	-	-	-	-
- ACD-C and ACD-D reports	-	-	-	-
Network message services	-	-	-	-
- Message Waiting Indication	Note 1)			
Network Authorization Code	-	-	-	-
Network Speed Call	-	-	-	-
Network Class of Service (NCOS)	-	-	-	-
Remote Virtual Queuing	-	-	-	-
Attendant and Network Wide Remote Call Forward	-	-	-	-
Flexible Numbering Plan	-	-	-	-
Network Wide Calling Party Privacy	-	-	-	-
Display of Calling Party Denied	-	-	-	-
Trunk Anti-Tromboning (TAT)	-	-	-	-
Calling Party Privacy Enhancements	-	-	-	-
Integrated Services Access (ISA)	-	-	-	-
Network Alternate Route Selection				
- NARS Access Codes	-	-	-	-
- Uniform Dialing Plan	-	-	-	-
- Coordinated Dialing Plan	-	-	-	-

Table 2 Supported MCDN Services

- Time of Day Routing	-	-	-	-
- Network Routing Control	-	-	-	-
- Satellite link control	-	-	-	-
- Digit screening	-	-	-	-
- Digit manipulation	-	-	-	-
- Auto on-net to off-net overflow	-	-	-	-
- Automatic least cost routing	-	-	-	-
- Automatic OCC access	-	-	-	-
- Expensive Route Warning Tone	-	-	-	-
Data packet network Access	-	-	-	-
Customer Network Manipulation	-	-	-	-
Direct Private Network Access	-	-	-	-
Electronic Tandem Network	-	-	-	-
Meridian Switched Network Variable Types of Outpulsing on Same Call	-	-	-	-
Network CLID and NCOS Display Interaction with 3WC	-	-	-	-
Network Dial Plan Display	-	-	-	-
Network Reason Display	-	-	-	-
Network Information Signals	-	-	-	-
Network Queuing, Main Network Signaling (NSIG)	-	-	-	-
Network Traffic Measurement	-	-	-	-
Time-of-Day Network Class of Service (NCOS)	-	-	-	-
Multi-location business groups (MBG)	Note 1)			
Virtual Access to Private Networks (VAPN)	-	-	-	-
Direct Inward System Access (DISA)	-	-	-	-

Table 2 Supported MCDN Services

yes: service is already supported and tested by other SN06 activities
Yes: service is supported by this SN07 activity
- : low priority service, not captured by this activity
Note 1): Priority 1 service, not supported by this activity. Further investigations are needed.
Note 2): Priority 1 service, not supported by this activity, but according to Enterprise Architect, it is supported as a MCDN Service interworking between two H.323 GWs (if tunneled through a CS2K).
Note 3): Currently, CICM GWs are unavailable to test with; however, this is a supported Service.
Note 4): Succession 1000M requires Calling Name to be tunneled within a H.323 Setup message (please reference See "PRIH.323 Deployment" on page 1693.) - hence, this design activity. In addition, for this activity's CS2K to Succession-1000M direction, only private calls contain the MCDN private data (for displaying Calling Name). For CS2K to Succession-1000M
direction, public calls do NOT contain private MCDN data. Therefore, for public CS2K to Succession-1000M direction calls, Calling Display is not applicable/displayed.
Note 5): Calling Name Delivery within the Core remains unchanged by this activity to either line agents or trunk agents; therefore, whatever existing functionalities, restrictions or limitations of Calling Name Delivery remain applicable.

132.4 Hardware Requirements or Dependencies

Please reference section “132.5 Software Requirements or Dependencies” on page 1707.

132.5 Software Requirements or Dependencies

- CM/GWC with SN07 load
- Business Communication Manager (BCM) with release 3.5
- Succession-1000M with release 4
- Centrex IP Client Manager (CICM) release 6.2
- Mediatrix 1104
- i2004 IP phone with release 1.5x
- Softclient M6350 with release 6.1

132.6 Limitations and restrictions

- A subset of MCDN services are supported by this feature. For supported services see chapter “132.3.2 Supported MCDN Services” on page 1698.
- Line side development (P-phone, IBN lines) is not part of this feature.
- Development on the H.323 agents (BCM, Succession1000M) is not part of this feature.
- MCDN Services which are not supported either by an H.323 agent or the line agent, will not be supported by this feature.
- Tunneling of MCDN data between Enterprises is outside of scope of this feature.
- Verification of MCDN services is done using Succession1000M. Omitting verification on Succession1000 GW is acceptable, because both GWs use the same software load.
- Testing is done on the North American CS2K load only.
- For Calling Name and Number delivery, the appropriate feature must be provisioned against the subscriber (i.e., CND - Calling Number Delivery, CNAMD - Calling Name Delivery, etc.)
- In the Mediatrix/CICM (CS2K) to Succession-1000M direction, only private Numbering Plan Indication (NPI) calls will contain this privately built MCDN tunneled data - public calls will not contain MCDN tunneled data.
- In the Mediatrix/CICM (CS2K) to Succession-1000M direction, private NPI with Local Type of Number (TON) is coded as an UIPE ESN CDP TON.

- CS2K Core Calling Name Delivery remains unchanged by this activity to either line agents or trunk agents; therefore, existing functionalities, restrictions or limitations of Calling Name Delivery remain applicable.

132.7 Applicable customer facing sections

Fault Management

Logs ___N/A___

Alarms ___N/A___

Configuration

Data Schema __N/A____

User Interface __N/A____

Element Management __N/A____

Security __N/A____

Service Order __N/A____

Office Parameters __N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) __N/A____

132.8 Glossary

Term	Description
BCM	Business Communication Manager
CICM	Centrex IP Client Manager
CS2K	Call Server 2000
EBS	Electronic Business Set (P-phone)
GW	Gateway
GWC	Gateway Controller
IE	Information Element
SN07	Succession Product Release 7

Term	Description
ISUP	ISDN User Part
MCDN	Meridian Customer Defined Network
MGCP	Media Gateway Control Protocol (IETF 3435)
NA	North American
NTNA	Nortel North American
SIP-T	Session Initiation Protocol - Telephony ITU-T based standard, that encapsulates ISUP messaging as payload within SIP messages.

133: Functional Description (FN): A00004109

133.1 Feature name

A00004109: MG9K Hardware Upgrade and Call Processing Changes

133.2 Description

Note: This feature doesn't provide customer-facing changes. Any changes that will be visible to the customer will be done by feature A00003571.

This activity will implement call processing and resource management level software changes to support the new MG9000 ITP and ABI cards, which will be introduced in SN07.

Prior to this new ITP card, there were two separate ITP cards. One for the UA-IP product and one for the UA-AAL1 product. With the introduction of the new ITP, the same hardware will be used to support both IP and ATM applications. Previously, since the hardware was different for IP and ATM, the software could determine which application was to be run on the ITP. Since the new ITP supports IP and ATM, this is no longer the case. Customer interaction is necessary to provide the 'Bearer Type' of the VMG.

At VMG provisioning time, the end-user must select the 'Bearer Type' (UA-IP or UA-AAL1). This will be done via a GUI at the Element Manager. Feature A00003571 - "MG9000 MANAGER - NEW MG9000 CARD SUPPORT" will provide the functionality for the GUI and downloading the data to the MG9K. This feature will provide a new MIB which will hold the 'Bearer Type,' along with the VAD and CNG information.

Also, a 'Bearer IP Address' will be stored in this MIB. This address will be used for the bearer channels and will be used by ABI. The ABI handling of this address, along with ABI specific functionality will be provided by feature A00003729. This new MIB will be the 'Media Gateway Bearer Capabilities' MIB.

133.3 Hardware requirements

The functionality introduced by this feature doesn't have a requirement to explicitly run on the new ITP cards (NTNY30CA), but is being developed to support the new cards. The implementation of this feature will still execute on the 'old' ITP cards (NTNY30BA - UA-IP; NTNY30AB - UA-AAL1).

133.4 Limitations and restrictions

None.

133.5 Interactions

As described above, the customer will be required to provide a ‘Bearer Type’ and ‘Bearer IP Address’ at the time of VMG provisioning. For specific customer interactions please reference feature A00003751.

133.6 Logs & Alarms

There are no new logs or alarms being implemented with this feature.

133.7 Applicable customer facing sections

Fault Management	
Logs	__N/A____
Alarms	__N/A____
Configuration	
Data Schema	__N/A____
User Interface	__N/A____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A____

133.8 Glossary

AAL1	ATM Adaptation Layer 1
ABI	Access Bridge Interface

ATM	Asyncronous Transfer Mode
CNG	Comfort Noise Generation
IP	Internet Protocol
MIB	Management Information Base
MG9K	Media Gateway 9000
VAD	Voice Activity Detection
VoIP	Voice over IP
VMG	Virtual Media Gateway

133.9 References

A00004109	Design Intent & Design Summary
A00003571	Design Intent & Design Summary
A00003729	Design Intent & Design Summary

134: Functional description (FN): A00004126

134.1 Feature name

A00004126 - SPM ECAN Control Enhancement

134.2 Description

134.2.1 Introduction

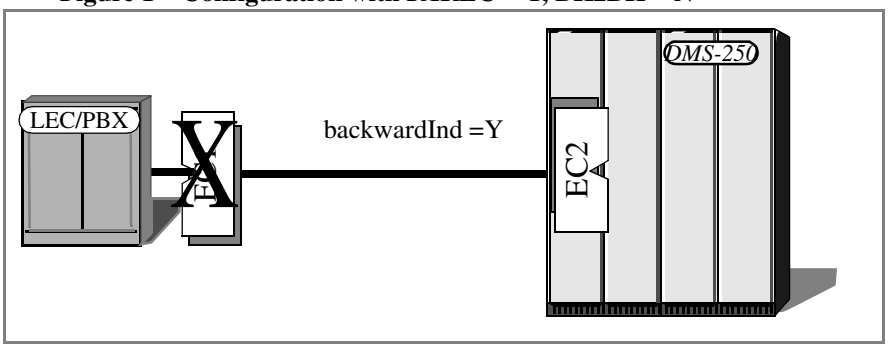
Currently, ECANs for ISUP trunks are allocated according to the ECAN control (EC) bits sent in the IAM and ACM/ANS message. If the far end switch incorrectly sets the EC bits then the near end will incorrectly allocate or not allocate an ECAN accordingly. This feature provides code changes in the CM and SPM that support backward and forward echo cancellation on an ISUP trunk regardless of the ECAN control bit setting of the far end by ignoring the echo bits sent in the IAM and ACM/ANS message.

This will offer the host SPM customer the flexibility of controlling the software decision making process to provide forward and backwards echo cancellation on a per trunk group basis. If the craftsman desires to control how ECANs are allocated the trunk option SPMECIDX in table SPMECAN can be datafilled to ignore the ISUP EC bits by setting a new bool IGNOREEC to TRUE. **However, ignoring the EC bits can cause more than two ECANS per call.**

Case : FAREC = Y, BK2BK = N

In this scenario, an external ECAN is expected at the distant end of the trunk. However, if the backward indicator indicates an ECAN is allocated when one is not allocated the DMS switch is provisioned with only one ECAN to cancel the backward echo. Therefore, a backward ECAN is needed to cancel the echo from the PBX/LEC. Please refer to figure 1.

Figure 1 Configuration with FAREC = Y, BK2BK = N



134.3 Hardware Requirements or Dependencies

There are no new hardware requirements for this feature.

134.4 Software Requirements or Dependencies

This feature requires the SPM and the CM to loaded simultaneously with SP20 and SN07, respectively, to activate this feature.

134.5 Limitations and restrictions

The following restrictions apply to the SPMECAN Table Control operations only:

- When changing the IGNOREEC bit from N to Y, it cannot be set Y if there are existing TRKSGRP tuples that use this SPMECAN index (tuple) and support any signaling type other than CCS7.
- When changed to Y, the new setting of the IGNOREEC bit will apply to all TRKSGRP CCS7 tuples that use the SPMECAN index.
- When changing the IGNOREEC bit from Y to N, it can be set N even if there are tuples in Table TRKSGRP that use this SPMEC index. The setting of the bit to N will be applied to all Trunk Subgroups that use this SPMECAN index.

134.6 Interactions

134.7 Applicable customer facing sections

Fault Management

- Logs ___NA___
- Alarms ___NA___

Configuration

- Data Schema ____X___
- User Interface ___NA___
- Element Management ___NA___
- Security ___NA___
- Service Order ___NA___
- Office Parameters ___NA___

Accounting (includes AMA billing) ___NA___

Performance (includes operational measurements) ___NA___

134.8 Glossary

Term	Description
ONP	One Night Process
DDM	Data Distribution Manger
BK2BK	Back to Back Ecan deployment
FAREC	Far End Ecan deployment

135: Functional description (FN): A00004131

135.1 Feature name

UCS PRI B-Channel Negotiation

135.2 Description

This feature provides the ability for DMS 250 Universal Carrier Services (UCS) Primary Rate Interface (PRI) trunks to perform B-Channel negotiation. This functionality is implemented only for PRI trunks using either NTNA or N449PRI protocol. This feature is supported on both SPMs and GWCs.

135.2.1 B-Channel Negotiation Overview

The B-Channel Negotiation feature is provisioned on a PRI trunk group basis. With PRI B-Channel Negotiation active, the DMS-250 switch delivers an ISDN PRI Call SETUP message with the B-channel ID specified as "preferred" (see **Figure 1** below). The ISDN PRI customer premises equipment (CPE) user response to the Call SETUP message can include a request that the call be connected on a different B-channel from the one that was offered by the switch. If the CPE elects to change the B-channel to a different channel, the CPE's first response to the SETUP message must be a Call Proceeding, Alerting, or Connect message with the channel identification IE specified with the desired channel number. After receiving the message with the new channel, the switch completes the setup of the call using the B-channel that the CPE specified.

Figure 1 Preferred/Exclusive field of Channel Identification IE

The preferred/exclusive field is **Bit 4** of **Octet 3** of the **Channel Identification IE**
Values:

- **0 : preferred** - the indicated channel is preferred.
- **1 : exclusive** - only the indicated B-channel is acceptable.

135.2.2 B-Channel Negotiation Procedures

This section describes the B-Channel Negotiation procedures used by the DMS-250 to support delivery of a Call SETUP message to the terminating CPE with the B-Channel Negotiation feature active. **Note that the SOC option NPRI0003 - UCS B-Channel Negot must be enabled as specified in section 2.2.5 for B-Channel Negotiation to function properly as described in this section.**

If PRI B-Channel Negotiation is active for the B-Channel trunk group, the DMS-250 codes the preferred/exclusive bit of the channel identification IE of the SETUP message as "preferred". If the PRI B-Channel Negotiation is inactive, the switch marks the B-channel identification bit to its default value of “exclusive”.

If the called CPE responds with the same channel identification in the first CALL PROCeeding, ALERTing, or CONNect response to an incoming SETUP message as was indicated by the DMS-250 in the SETUP message, the DMS-250 continues with call processing to the terminating CPE as if the B-Channel Negotiation was not enabled.

If the first response to the outgoing SETUP message with channel identification specified as “preferred” is a Call Proceeding, Alerting, or Connect message containing a channel identification IE whose channel number differs from the offered channel ID, and if the received B-channel trunk group member is available for a call, B-Channel Negotiation is activated. DMS allocates the channel indicated by the CPE to the call and continues with call processing.

The DMS-250 does not distinguish whether the CPE specifies the channel as "preferred" or "exclusive" in the channel identification response of the first CPE Call PROCeeding, ALERTing, or CONNect message response to a terminating Call SETUP message.

There is no restriction on the direction or speech capability of the PRI trunks to which this feature can be assigned.

135.2.3 Errors Invoked by PRI B-Channel Negotiation

If the SETUP message from the DMS-250 specifies the channel identification as “exclusive” and the CPE first response message specifies a different B channel identification, the DMS-250 initiates call clearing by sending to the CPE a RELease message containing the cause: "channel unacceptable" (encoded 0000110)and location: “public network serving the local user” (encoded 0010).

If PRI B-channel Negotiation is active and the CPE's first response to a SETUP message with channel identification specified as "preferred" is a Call Proceeding, Alerting, or Connect message containing a channel identification IE whose channel number differs from the offered channel ID, but the received B-channel trunk group member is not available for a call, then the switch initiates call clearing by sending to the CPE a RELease message containing a cause: "channel unacceptable" (encoded 0000110)and location: "public network serving the local user" (encoded 0010).

If PRI B-channel Negotiation is active and the first response to the outgoing SETUP message with channel identification specified as "preferred" is a Call Proceeding, Alerting, or Connect message containing a channel identification IE whose channel number differs from the offered channel ID but does not exist or is not valid for the offered PRI Group, then the switch initiates call clearing by sending to the user a RELease message with cause: "channel unacceptable" (encoded 0000110)and location: "public network serving the local user" (encoded 0010).

If channel identification is not included in a CALL PROCeeding, ALERTing, or CONNect message received as the first response to the SETUP message, then B-Channel negotiation is not invoked and the treatment of the call is the same as the treatment of a basic call in the same scenario. Specifically, no state transition should occur and the DMS-250 should respond with a STATUS message containing the cause: "mandatory information element missing" (encoded 1100000) and location: "public network serving the local user" (encoded 0010).

135.2.4 B-Channel Negotiation Service Provisioning Options

NOTE : The SOC option NPRI0003 - UCS B-Channel Negot must be enabled as specified in section 2.2.5 before B-Channel Negotiation is provisioned. Otherwise, any call attempting to perform B-Channel Negotiation will fail.

B-Channel Negotiation is activated by setting BCHNEG field in table TRKSGRP to 'Y'. It activates B-channel Negotiation on a PRI trunk group basis. This functionality is turned off by default, as indicated by BCHNEG field setting of 'N'.

This is existing functionality for NTNA. This feature will add the ability to assign B-channel Negotiation to N449PRI by allowing the associated BCHNEG field to be set to 'Y' for trunks supporting the N449PRI protocol variant.

135.2.5 Software Optionality Control

The SOC code for this feature is: NPRI0003 - UCS B-Channel Negot.

When SOC is ‘IDLE’, B-Channel negotiation can be provisioned, but the call processing functionality is not available. Likewise, with the state set to ‘ON’, the functionality is available.

135.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced by this feature.

135.4 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced by this feature, but both Core and peripheral loads for SPMs and GWCs must be at SN07 or higher for this feature to work.

135.5 Limitations and restrictions

This functionality is implemented only for UCS PRI trunks using either NTNA or N449PRI protocol.

PRI B-channel Negotiation is limited to members of the same PRI trunk group.

Setting field ‘BCHNEG’ to ‘Y’ in Table TRKSGRP to activate this feature requires that field ‘BCHGLARE’ controlling glare is set to ‘STAND’.

The following originating agents are supported :

- EANT (MF & ISUP)
- DAL
- PRI
- ONAL
- ONAT

Setting field ‘BCHNEG’ to ‘Y’ in Table TRKSGRP to activate this feature causes the preferred/exclusive bit of channel identification field in the outgoing SETUP message to be set to ‘preferred’. However, the SOC option NPRI0003 - UCS B-Channel Negot controls the call processing functionality of this feature, thus must be enabled as specified in section 2.2.5 before B-Channel Negotiation is provisioned. Otherwise, any attempt to perform B-Channel Negotiation by far-end trying to use a different channel will cause the call to fail, even though the outgoing SETUP msg contained ‘preferred’.

135.6 Interactions

None known.

135.7 Applicable customer facing sections

Fault Management

- Logs _N/A_____
- Alarms _N/A____

Configuration

- Data Schema _X_____
- User Interface _N/A_____
- Element Management _N/A_____
- Security _N/A____
- Service Order _N/A____
- Office Parameters _N/A_____

Accounting (includes AMA billing) _N/A_____

Performance (includes operational measurements) _N/A_____

135.8 Glossary

Term	Description
UCS	Universal Carrier Services
NTNA	DMS PRI
CPE	Customer Premises Equipment

136: Functional description (FN): A00004137

136.1 Feature name

A00004137 - ANI Billing

136.2 Synopsis

This feature introduces a new AMA module, Module Code 838 (MC838). MC838 is appended to a Structure Code 0220 (SC0220) record when the Calling Party Number (CPN) or the Billing Number (BN) is delivered to the terminating party on a PRI connection.

Additionally, the feature enhances the FAR message to indicate to the previous office that the CPN/BN was delivered to the terminating party when the terminating switch is different from the originating switch.

136.3 Description

This feature provides the following functionality:

- If the DMS switch is doing the billing for the call and the call terminates on a PRI trunk, and the PRI trunk is provisioned to deliver Calling Party Number (CPN) or Billing Number (BN), then Module Code 838 will be appended to the AMA record to indicate that the CPN or the BN was delivered to the terminating PRI party. This will only apply for Structure Code 0220. This is the case when the DMS switch is both the originating and terminating switch. Please refer to “Figure 1 - The DMS is both the originating and terminating switch” on page 1722.
- If the DMS switch is the originating switch, but not the terminating switch, then the DMS switch will generate a Module Code 838 based on the FAR message received from the terminating switch indicating that the CPN/BN was delivered to the terminating party. Please refer to “Figure 2 - The DMS is the originating switch, but not the terminating switch” on page 1722. This will be accomplished via a new Facility Indicator in the FAR message.
- If the DMS switch is the terminating switch, but not the originating switch, then the DMS will send a FAR in the backwards direction (to the originating switch) indicating that the CPN/BN was delivered to the terminating party. Please refer to “Figure 3 - The DMS is the terminating switch, but not the originating switch” on page 1723.
- If the DMS is neither the originating or the terminating switch, but an intermediate switch, then the DMS will just pass the FAR message received on the terminating trunk in the backward direction to the previous

switch. Please refer to "Figure 4 - The DMS is neither the terminating switch or the originating switch" on page 1723.

This ANI Billing functionality only applies to calls terminating on PRI trunks. Additionally, this functionality is controlled via SOC UTRS0014.

Figure 1 - The DMS is both the originating and terminating switch

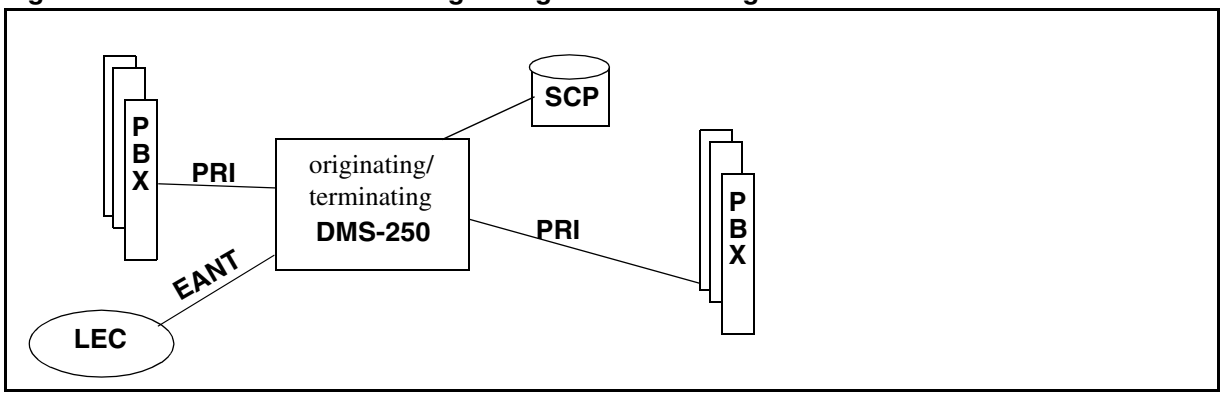


Figure 2 - The DMS is the originating switch, but not the terminating switch

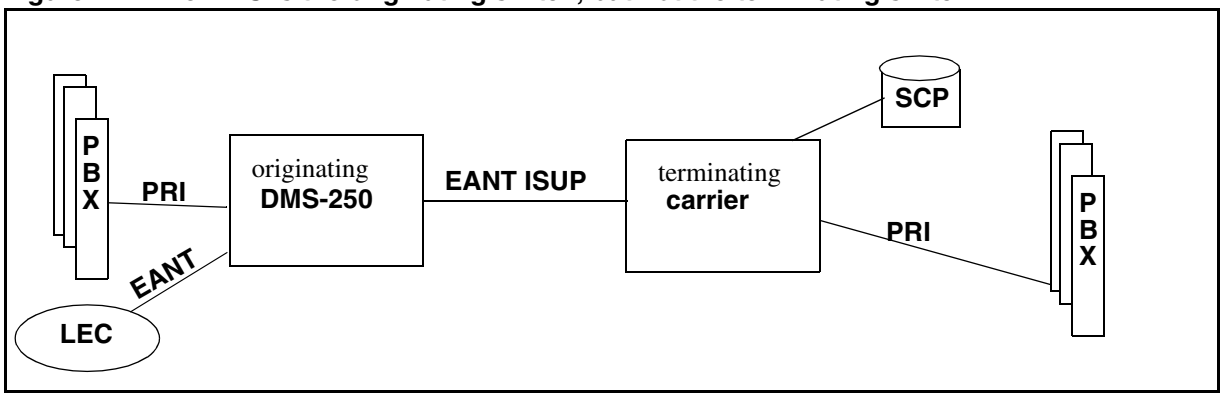


Figure 3 - The DMS is the terminating switch, but not the originating switch

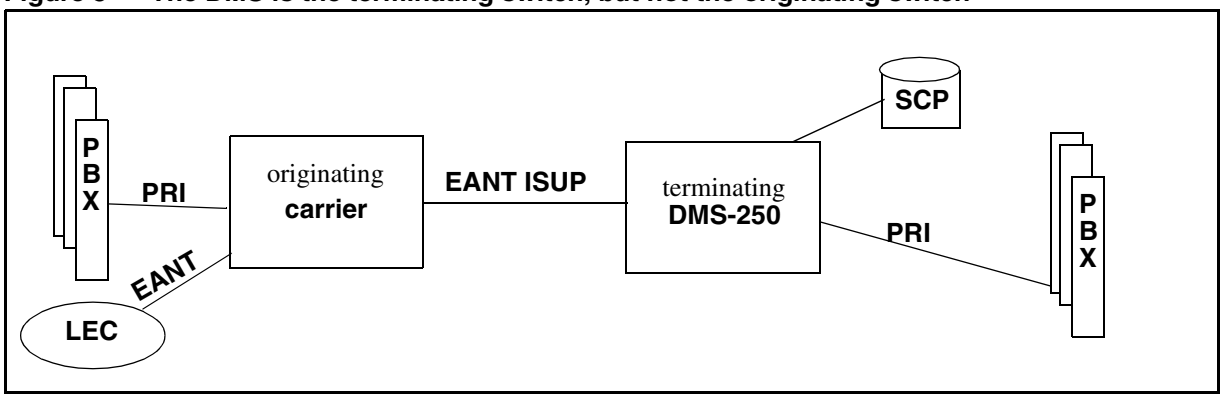
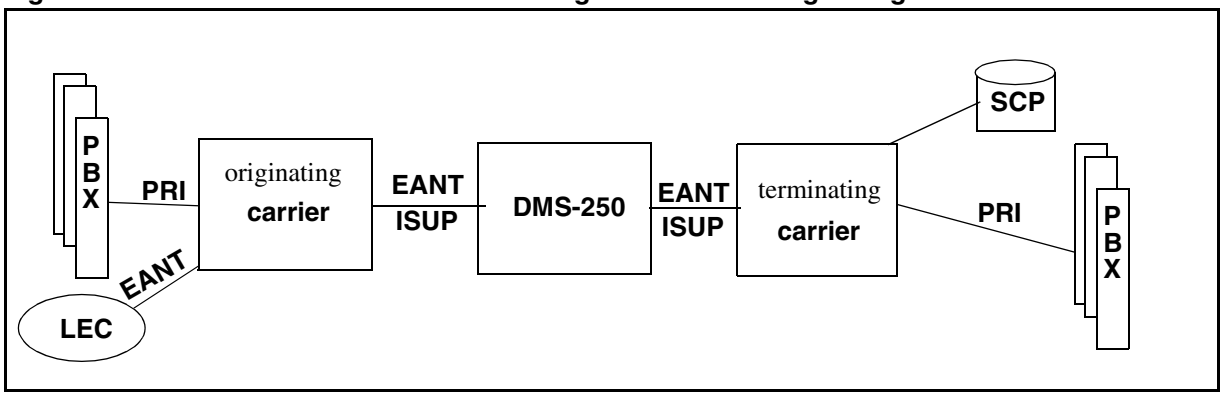


Figure 4 - The DMS is neither the terminating switch or the originating switch



136.3.1 AMA Module

A new module is introduced by this activity, Module Code 838[1]. This module will only be appended to Structure Code 0220 (triggered by the AMASlpID in the Analyze_Route CAIN response) for calls terminating on PRI trunks for which CPN or BN as been delivered to the terminating party.

Table 1 Module Code 838 - Egress Data Module

Field Name	Table Number	Number of Characters
Module Code	88	4
Communications ISDN (ACI)/ISDN Features	344	4

[1]Module Code 838 is not a Bellcore defined module in GR-1100-CORE.

Table 2 Table (Field) 344 characters - values and meaning

Character	Value	Meaning
1-2	00	Constant
3	1	CPN/BN has been delivered to the terminating end.
	2-9	unassigned
4	C	SIGN character (HEX C)

136.3.2 UCP ISUP Protocol Changes

This activity defines a new Facility Indicator for the FAR message.

The Facility Indicator parameter is a mandatory, fixed-length parameter in the FAR message.

Table 3 Facility Indicator Parameter

8	7	6	5	4	3	2	1	
Facility Indicator								Octet 1

The value in bold (11111010) in the following table is added by this feature.

Table 4 Facility Indicator Field

Field	Codes and Description
Facility indicator	00010000=Release link for third-party interaction call (#10)
	00010001=Release link for redirect (#11)
	00010010=Request information from remote (#12)
	00010011=Start billing time (#13)
	00010100=Cancel billing time (#14)
	00010101=Restart billing at zero, no accumulation #(15)
	00010111=Billing information only (#17)

Table 4 Facility Indicator Field

Field	Codes and Description
	00011000=Reorigination information only (#18)
	00011001=AIN IP Connection (#19)
	00011010=Context Block (#1A)
	00011011=Request Context Block (#1B)
	11111011 = ISDN Facility (#FB)
	11111010 = CPN/BN Delivered (#FA)

136.3.3 Call Flows

136.3.3.1 DMS is both originating and terminating switch

In the call flow below (also refer to Figure 5, on page 1726), the DMS-250 is both the originating switch and the terminating switch. In this scenario, the DMS-250 will be performing the billing for the call since it is the originating switch.

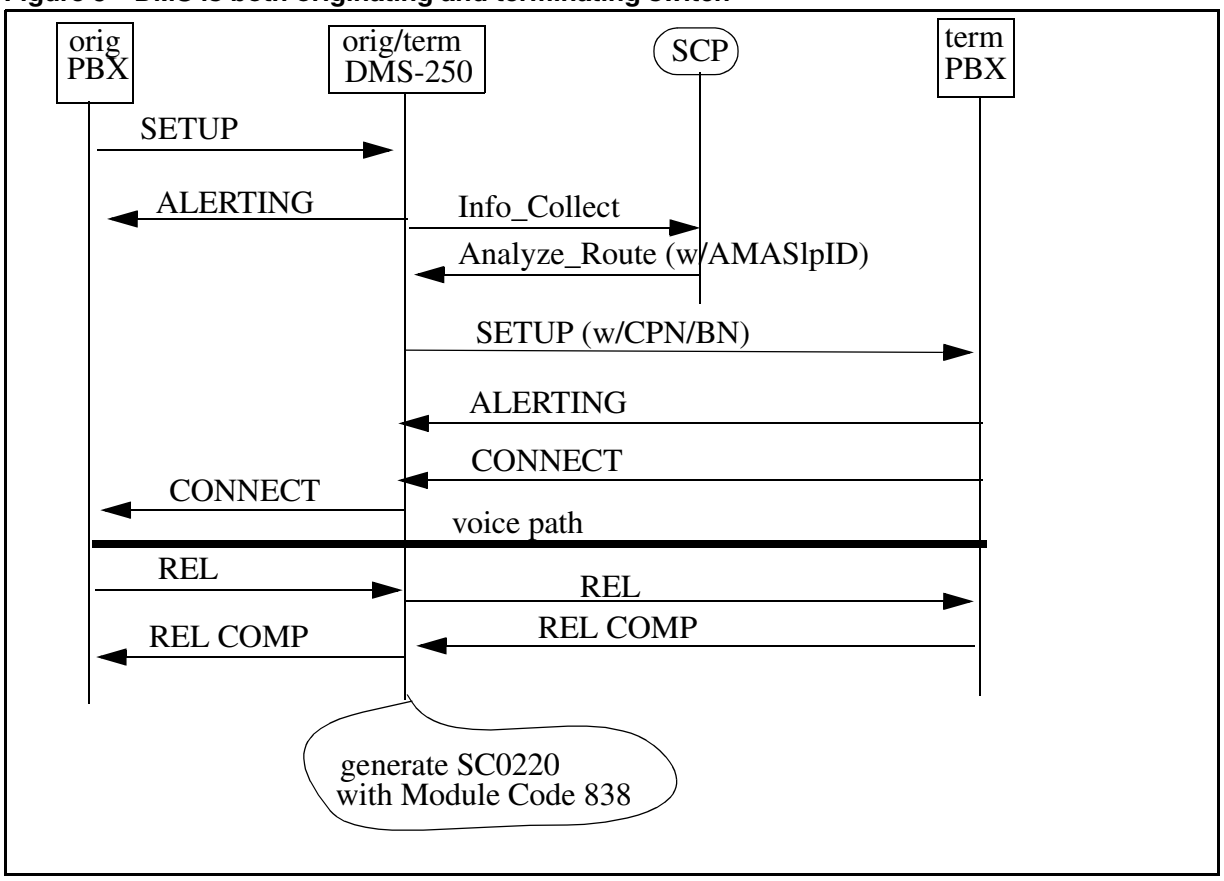
The scenario assumes the following:

- The incoming trunk is an NTNA PRI[1] Trunk
- The outgoing trunk is an NTNA PRI trunk provisioned to send CPN/BN information (via table CALLATTR, field ANIDELV[2])
- This feature is active (i.e., SOC UTRS0014 is ON).
- The Analyze_Route returned a AMASlpID, which causes a SC0220 to be generated for the call.

When the call completes, a SC0220 is generated and MC838 is appended to indicate that the CPN/BN was delivered to the terminating party.

[1]The call flow shows an incoming PRI trunk; however, it doesn't have to be incoming PRI.
[2]ANIDELV option can be set to any one of the following values: CPNPREF,CPNONLY,CGN-PREF,CGNONLY.

Figure 5 DMS is both originating and terminating switch



136.3.3.2 DMS is originating switch, but not terminating

In the call flow below (refer to Figure 6, on page 1727), the DMS-250 is the originating switch, but not the terminating switch. In this scenario, the DMS-250 will be performing the billing for the call since it is the originating switch; however, whether or not to append a MC838 will depend on the FAR message sent by the terminating switch.

The scenario assumes the following:

- The incoming trunk into the DMS-250 is an NTNA PRI[1] Trunk
- The outgoing trunk to the carrier is an EANT trunk and the ISUPIDX field is set to UCS2FE.
- This feature is active (i.e., SOC UTRS0014 is ON).
- The Analyze_Route returned a AMASlpID, which causes a SC0220 to be generated for the call.

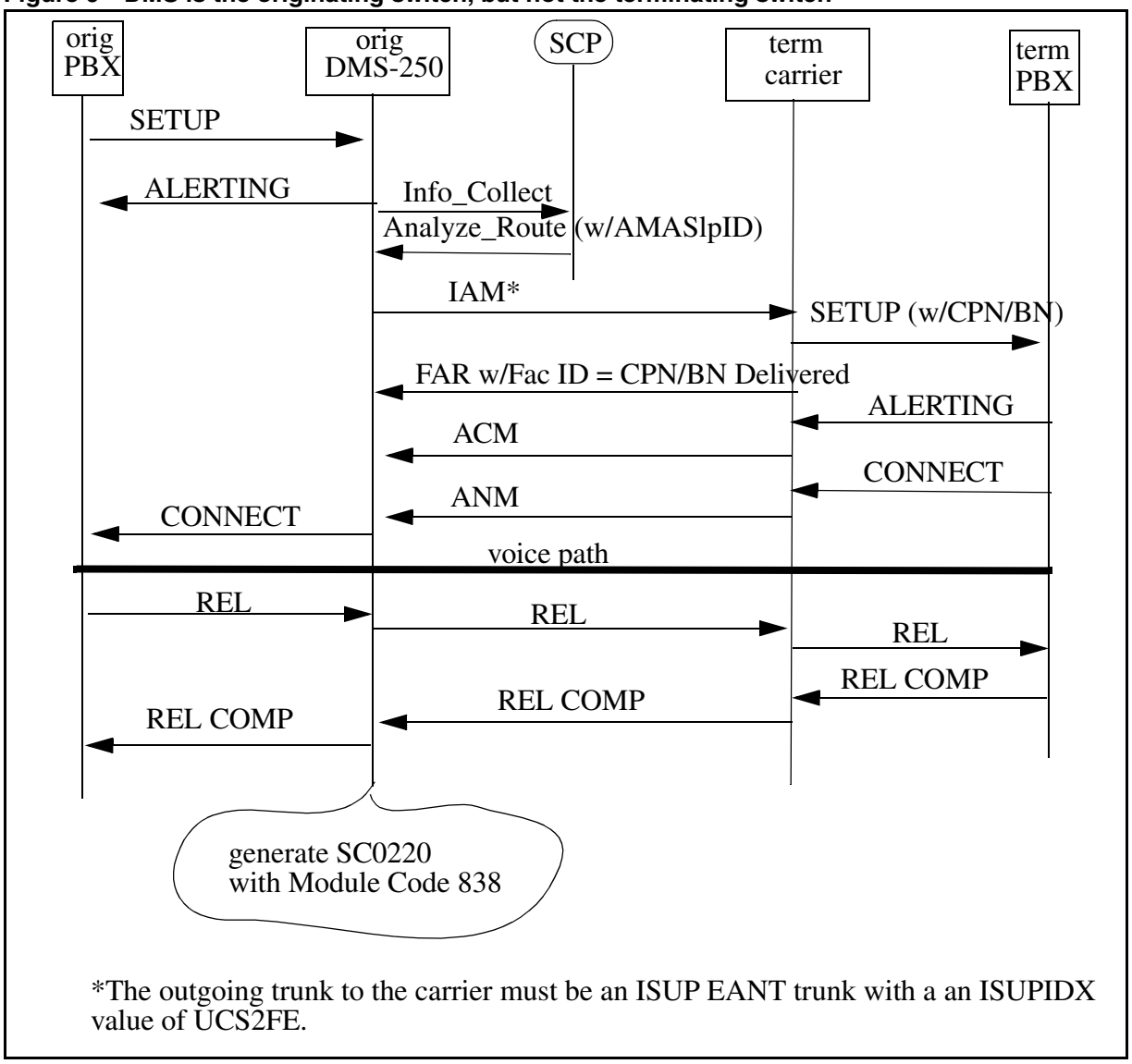
The call is routed to the carrier for completion. The carrier routes the call to the terminating party and sends CPN/BN in the SETUP message.

[1]The call flow shows an incoming PRI trunk; however, it doesn't have to be incoming PRI.

The carrier sends back a FAR message before an ACM to the DMS-250. The FAR message will contain a Facility Indicator value of #FA (CPN/BN Delivered). When the DMS-250 receives the FAR message, it will check to ensure that the trunk is datafilled with an ISUPIDX of UCS2FE and if so, it will append MC838 when the call ends.

If the EANT trunk group field ISUPIDX in table TRKGRP is set to anything other than UCS2FE, then the FAR message will be ignored. The call will complete successfully and a SC0220 AMA record will be generated; however, it will not contain an MC838 module.

Figure 6 DMS is the originating switch, but not the terminating switch



136.3.3.3 DMS is terminating switch, but not originating

In the call flow below (refer to Figure 7, on page 1729), the DMS-250 is the terminating switch, but not the originating switch. In this scenario, the DMS-250 will NOT be performing the billing for the call since it is not the originating switch. In this scenario, the DMS-250 will build a FAR message with a Facility Indicator of #FA and send it back on the originating trunk group back to the carrier.

The scenario assumes the following:

- The incoming trunk to the DMS-250 is an EANT trunk and the ISUPIDX field is set to UCS2FE.
- This feature is active (i.e., SOC UTRS0014 is ON).
- The outgoing trunk is an NTNA PRI trunk provisioned to send CPN/BN information (via table CALLATTR, field ANIDELV[1])

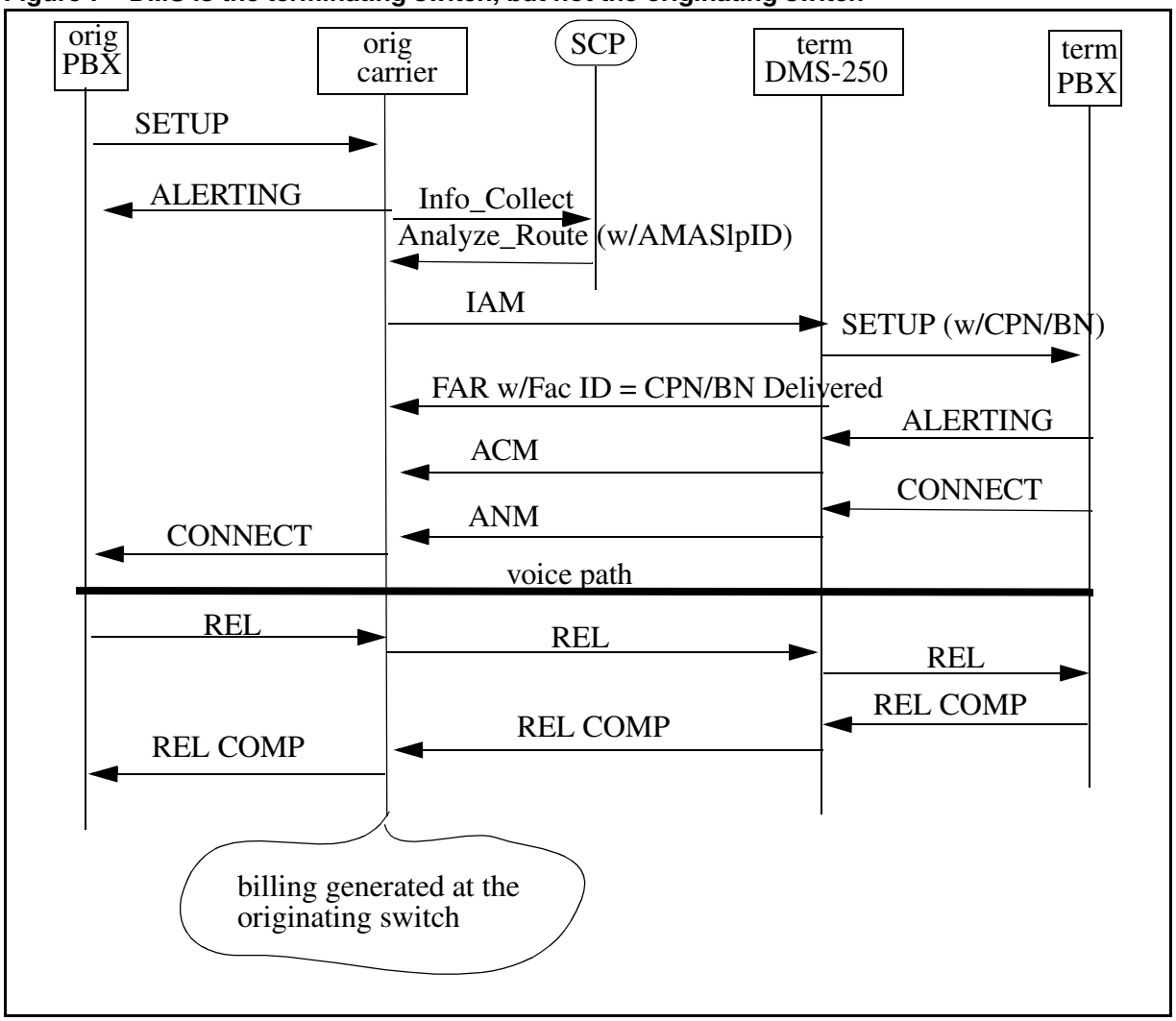
The call is routed to the DMS-250 for completion. The DMS-250 routes the call to the terminating party and sends CPN/BN in the SETUP message.

The DMS-250 check to ensure that the originating trunk is datafilled as a UCS2FE trunk and if so it will send back a FAR message **before sending an ACM** to the carrier. The FAR message will contain a Facility Indicator value of #FA (CPN/BN Delivered). In this scenario, the carrier is responsible for billing for the call.

If the EANT trunk group field ISUPIDX is set to anything other than UCS2FE, then the FAR message will not be sent. The call will complete successfully; however, there will be no indication sent back to the carrier to indicate that CPN/BN was delivered to the terminating party.

[1]ANIDELV option can be set to any one of the following values: CPNPREF,CPNONLY,CGN-PREF,CGNONLY.

Figure 7 DMS is the terminating switch, but not the originating switch



136.3.3.4 DMS is neither originating nor terminating

In the call flow below (refer to Figure 8, on page 1731), the DMS-250 is neither the terminating switch nor the originating switch. In this scenario, the DMS-250 will NOT be performing the billing for the call since it is not the originating switch. In this scenario, the DMS-250 merely passes the FAR message in the backwards direction if received.

The scenario assumes the following:

- The incoming trunk to the DMS-250 is an EANT trunk and the ISUPIDX field is set to UCS2FE.
- The outgoing trunk from the DMS-250 is an EANT trunk and the ISUPIDX field is set to UCS2FE.

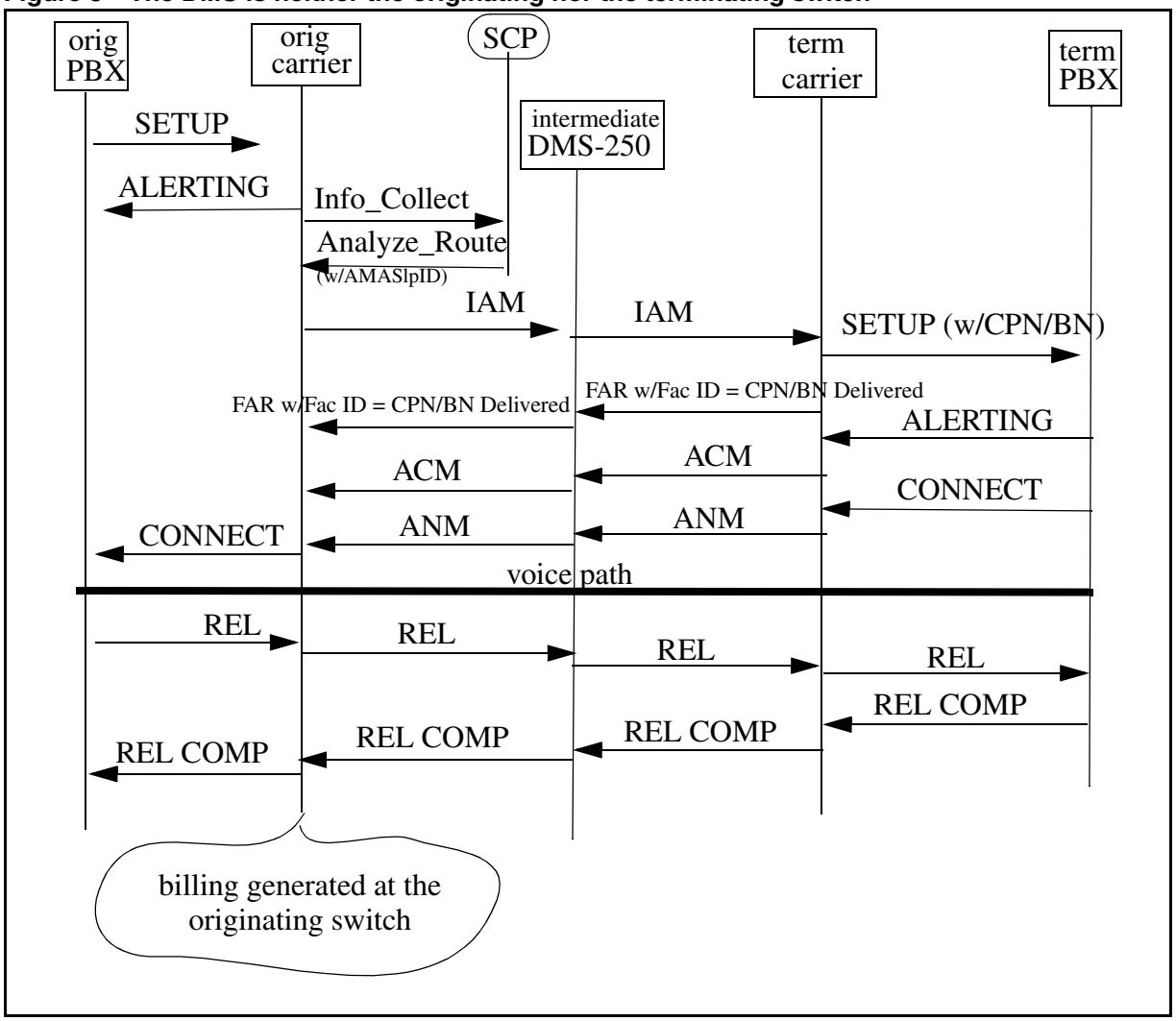
- This feature is active (i.e., SOC UTRS0014 is ON).

The call is routed to the DMS-250 for completion. The DMS-250 routes the call out on an EANT trunk to the carrier. The carrier terminates the call to the PBX and sends CPN/BN to the terminating party via the SETUP. The carrier then sends a FAR message in the backwards direction to the DMS-250 before it sends an ACM on the call.

The DMS-250 check to ensure that the terminating trunk is datafilled as a UCS2FE trunk and if so it will check to see if the incoming trunk group is also EANT with ISUPIDX set to UCS2FE. If so, it will pass the FAR message in the backward direction back to the originating carrier switch before it sends ACM.

If the EANT trunk group field ISUPIDX is set to anything other than UCS2FE, then the FAR message will be ignored and/or not sent. The call will complete successfully; however, there will be no indication sent back to the carrier to indicate that CPN/BN was delivered to the terminating party.

Figure 8 The DMS is neither the originating nor the terminating switch



136.3.4 Supported trunk group types

The FAR message with Facility Indicator set to “11111010 = CPN/BN Delivered (#FA)” is only supported on EANT trunk groups that are datafilled with an ISUPIDX value of UCS2FE.

When a FAR message is received on an EANT trunk group with an ISUPIDX other than UCS2FE, it will be ignored if the switch is the originating switch. If the switch is a terminating or an intermediate switch, it will not be passed in the backwards direction unless the ISUPIDX on the originating trunk is set to UCS2FE

136.3.5 Sending the FAR message

The FAR message will be sent in the backwards direction (on the originating trunk) before the ACM is sent. The one exception to this will be CGETS calls

that queue with announcement or queue without announcement, but are provisioned to send back ACM.

136.3.6 MC838 and trigger events

If a call sets trigger events such as ‘user busy’ and outpulses the CPN/BN on first terminating attempt, but encounters a user busy condition that results in another query/response (Analyze_Route) from the SCP and the second attempt terminates over a trunk group not provisioned to send CPN/BN, MC838 will still be included on the AMA record since it was sent on the first termination attempt.

A maximum of one MC838 will ever be appending to a SC0220 AMA record.

136.3.7 Generating MC838

Module Code 838 will not be generated for calls that terminate on PRI trunks with the following options:

- PRI trunks with the SNTRUNK option datafilled in table CALLATTR
- PRI trunks with the IPTRUNK option datafilled in table TRKGRP

Module Code 838 will not be generated for calls that terminate on DAL trunks.

136.3.8 Sending ISUP FAR in the backward direction

The ISUP FAR message will not be sent in the backwards direction if any of the following conditions occur:

- The terminating PRI trunk has the SNTRUNK option datafilled in table CALLATTR
- The terminating PRI trunk has the IPTRUNK option datafilled in table TRKGRP.
- The terminating trunk group in a non-PRI trunk (i.e., DAL)
- The originating trunk group is not an EANT trunk group.
- The originating EANT trunk group has an ISUPIDX value set to something other than UCS2FE.

136.4 Hardware Requirements or Dependencies

Not applicable.

136.5 Software Requirements or Dependencies

Not applicable.

136.6 Limitations and restrictions

This feature is only supported for the AMAREC template as defined in table CDRTMPLT. Additionally, the EDGE_SWITCH parameter in table OFCVAR must be set to Y.

This feature is not supported over SIP (Session Initiation Protocol) regarding usage of the FAR message.

136.7 Interactions

This feature does not do any work to actually deliver the CPN/BN. That is existing functionally and is controlled via the ANIDELV option in table CALLATTR.

136.8 Applicable customer facing sections

Fault Management

- Logs ___n/a___
- Alarms ___n/a___

Configuration

- Data Schema ___x___
- User Interface ___n/a___
- Element Management ___n/a___
- Security ___n/a___
- Service Order ___n/a___
- Office Parameters ___n/a___
- Software Optionality Control __ x___

Accounting (includes AMA billing) ___x___

Performance (includes operational measurements) ___n/a___

136.9 Glossary

Term	Description
ACM	Address Complete Message
AMA	Automatic Message Accounting
ANM	Answer

Term	Description
BN	Billing Number
CAIN	Carrier AIN
CPN	Calling Party Number
FAR	Facility Request Message
IAM	Initial Address Message
REL	Release
REL COMP	Release Complete
SOC	Software Optionality Control
UCP	Universal Carrier Protocol

137: Functional Description (FN): A00004260

137.1 Feature name

XPKT301 Alarm Banner for MG4K/IW/DPT

137.2 Description

This feature introduces a new MAP banner alarm that is generated when the number of XPKT301 logs crosses (i.e. meets or exceeds) thresholds controlled by the customer. XPKT301 logs are currently generated whenever a call fails SVC setup thru the ATM fabric. The new banner alarm will be displayed as “nn PKT” with major severity, where “nn” is the number of SMG4, IW, and DPT gateways (i.e. nodes) that have crossed the threshold for XPKT301XPKT301 logs. “PKT” is an abbreviation for Packet. The customer can modify the threshold parameters via Table OFCENG. A new XPKT806 log, with major alarm, is generated when a node crosses its threshold. A new XPKT807 log is generated when the node alarm clears. A new option allows suppressing further XPKT301 logs while the XPKT806 alarm is present for a SPM impacted by the XPKT301.

Note that “SMG4 node” refers to a SPM tuple in MNNODE with a CLASS of SMG4. “IW node” refers to a SPM tuple in MNNODE with a CLASS of IW and a DPT_INFO of BRDG_ONLY (Bridged). “DPT node” refers to a SPM tuple in MNNODE with a class of IW and a DPT_INFO of DPT_ONLY.

The new Map functions are documented in the OPTCN section. The new logs and alarms are documented in the OPTFM section. The office parameters that control the thresholds are documented in the OPTCN section.

Motivation for this feature is to allow the customer to respond quickly to ATM CallP failures (indicated by XPKT301 logs) by having a visual display at the MAP banner. There are cases where XPKT301 logs can occur due to problems in the ATM fabric that are not indicated elsewhere on the MAP (e.g. when there are no SMG4 equipment failures reported on the MAP).

137.3 Hardware Requirements or Dependencies

None.

137.4 Software Requirements or Dependencies

This feature will impact the MSH20 stream that is being delivered in SN07 loads. Feature will be patched to SN06. This feature does not impact any firmware or Local loads.

Here are the BLM and customer requirements for this feature:

1. Provide a new “nn PKT” MAP banner alarm for SVC failures on these ATM gateways: SMG4 (MG 4000), IW, and DPT-SPM. The SVC failures are indicated by the current XPKT301 log. The “nn PKT” will be displayed with major priority under the APPL MAP banner, where “nn” is the current number of nodes with the XPKT806 alarm.
2. A new XPKT806 log with major alarm will be **raised** on a per node basis when the number of XPKT301 logs for that node crosses (i.e. reaches or exceeds) RAISE_THRESHOLD number of XPKT301 logs within RAISE_CYCLE number of minutes, where RAISE_THRESHOLD and RAISE_CYCLE are office parameters provisionable on a per node class basis. The three supported Succession node classes will be SMG4, IW, and DPT. The XPKT806 log info will include node number (i.e. SPM number), node class type (i.e. SMG4, IW, DPT), number of SVC failures for that node, time interval, and threshold values.
3. Likewise, the alarm will be **cleared** on a per node basis via XPKT807 log when the number of XPKT301 logs for that node does not exceed CLEAR_THRESHOLD number of XPKT301 logs within CLEAR_CYCLE number of minutes, where CLEAR_THRESHOLD and CLEAR_CYCLE are office parameters provisionable on a per node class basis. There will be no severity for the XPKT807 log. The XPKT807 log will show the same type of info as the XPKT806 log.
4. The new alarm will be raised instantly once the raise threshold is crossed for a node (i.e. will not wait for the time interval to expire).
5. Provisioning changes to the feature’s office parameters that control raising and clearing the alarm will be activated immediately and not require a Restart. To immediately activate the changes, it will be necessary to reset the raise and clear cycles on the impacted node class type. For example, if a raise cycle is running on a SMG4 and any of the office parameters for the SMG4 are changed, then the raise cycle will be aborted by zeroing its XPKT301 hit counter and starting the raise cycle fresh with the updated threshold and cycle duration values.
6. Alarms and fault counts must persist over local node SWACTs and local S/W Upgrades, but not over ONPs. If the new alarm is present before an ONP, it will disappear after the NoRestartSWACT and will then be raised again if the fault condition persists.
7. An XPKT301 log for a failed **intra-office** gateway call (i.e. SMG4 to SMG4 call) will peg both gateways as long as the originating and terminating gateways are supported node classes (i.e. SMG4, IW, or DPT).
8. An XPKT301 log for a failed **inter-office** gateway call that terminates to a DPT will only peg the terminating node. Note that in this case, the originating node is not on the CS2K so the terminating info is all that is available to the CS2K.

9. New MAP commands will be provided to allow the craftsperson to query the status of any single node, or to query the status of all nodes in the CS2K office. The status information displayed will include node number, node class type, number of SVC failures, time interval, the threshold values, etc. MAP commands will also be provided to manually clear the alarm and to zero the failure counters.
10. The alarm status can be viewed at the APPL MAP level under a new PKT column (same place where all other APPL alarms can be viewed).
11. A new MAP level will dynamically display the alarm status for every supported node (SMG4, IW, DPT) in the CS2K office.
12. The feature will default to “off”. Customer must turn the feature on via the new office parameters to see the new XPKT806 alarms reported.
13. Introduce a new option to suppress further XPKT301 logs that impact a XPKT806-alarmed Succession node. This new option is “off” by default, meaning the customer must turn this option “on” before any XPKT301 logs will be suppressed. Once the XPKT806 alarm clears for a Succession node via an XPKT807 log, that node will no longer suppress any XPKT301 logs.

137.5 Limitations and restrictions

1. MG9K is not a supported node type for this feature.
2. While alarm raising is immediate per requirement #4 above, the clearing of the alarm can take an extra minute beyond the clear cycle completion. For example, consider a SMG4 that raised an XPKT806 alarm and is now running a 5 minute clear cycle; if the number of XPKT301 hits does not exceed the CLEAR_THRESHOLD, then the alarm will be cleared via XPKT807 between 5 and 6 minutes after the alarm was initially raised. This slower clearing of the alarm helps to minimize the real time impact of the new software.
3. This limitation is only applicable if XPKT301 suppression is “on” per requirement #13 above. If an XPKT301 log impacts two Succession nodes and only one of the nodes has the XPKT806 alarm raised, then the XPKT301 will still be suppressed even though one of the nodes does not have the XPKT806 alarm raised.
4. This feature will be dormant in MTXP/MSH20 Combo load since there is no room available for PKT in the dynamic alarm status of the MAPCI;MTC;APPL level.

137.6 Interactions

137.6.1 SPM Nodes Impacted by XPKT301 - Rules for Node Pegging

Feature A00004430 is being developed to deliver new OMs for XPKT301 logs. A0004430 is dependent on the A0004260 feature for the functionality of determining which SPM nodes are impacted by an XPKT301 log. To determine which SPM nodes are impacted, these fields from the XPKT301 log will be examined:

1. **Orig agent:** if this is a trunk hosted by a SMG4, then the XPKT301 log will be pegged against that SMG4 node.
2. **Term agent:** if this is a trunk hosted by a SMG4,, then the XPKT301 log will be pegged against that SMG4 node.
3. **Location:** if this SPM number is not the same as the SPM node hosting the originating or terminating agent, then the XPKT301 log will be pegged against the SPM in this Location field. .

In some cases, the SMG4 node will be the host for the originating or terminating agent and appear in the “Location” field; in these cases, following the above rules will avoid double-pegging the SMG4 node. Note that intra-switching at the SMG4 will prevent the same SMG4 node from hosting the originating and terminating agents (i.e. trunks).

For calls involving IW or DPT, those node types will never be the host of the originating or terminating agent since IW and DPT nodes do not provide trunks. When a IW of DPT node is involved with an XPKT301 failure, the node will only appear in the “Location” field.

137.6.2 Pegs during XPKT301 Suppression

While XPKT301 logs are being suppressed for any node with an XPKT806 alarm raised, all Succession nodes impacted by the XPKT301 will continue to be pegged for the purposes of OM (A00004430) and raising/clearing XPKT806/807 (A00004260).

137.7 Applicable customer facing sections

Fault Management	
Logs	___X__
Alarms	__X_
Configuration	
Data Schema	__N/A_
User Interface	___X__

Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	___X__
Accounting (includes AMA billing)	__N/A_
Performance (includes operational measurements)	__N/A_

137.8 Glossary

Term	Description
New term	Definition

138: Functional Description (FN): A00004271

138.1 Feature name

SIP App Server SOC

138.2 Description

This activity implements a mechanism to control the maximum number of SIPT calls that utilize the Next Generation Session Server (NGSS) platform when the far end is a non-CS2K, referred to here as an Application Server. A usage SOC, CS2B0009, is implemented to limit these types of calls (abreviated as CS2AS in this document).

Another activity, A00004414 SIP Call Server SOC, implements a similar mechanism to control the maximum number of SIPT calls that utilize the NGSS platform when the far end is another CS2K (CS2CS calls). SOC option CS2B0008 is the usage SOC for A00004414.

Both SOC features are part of a set of activities for delivering the Session Server - SIP Gateway application in SN07. The other features are:

- A00003270 SIP Open Interop Call Processing
- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003277 Session Server OM Subsystem
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003281 SIP on Session Server Call Audit
- A00003282 SIP on Session Server Datasync
- A00003933 SIP on Session Server Drop 1 ICAF
- A00003934 Session Server Project ICAF

138.2.1 SOC limiting

The usage-controlled CS2B0009 SOC added by this activity applies to calls that have the following characteristics:

— the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,

— a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK[1],

— the CONNTYPE field of the tuple in table SIPLINK is set to CS2AS

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exeed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming SIPT calls on trunk group NGSSINC and outgoing calls on trunk group NGSSOUT will increment the usage counter for the CS2AS SOC.

```
TABLE: SIPLINK
        LINKNAME CONNTYPE                  AGNTDATA
-------------------------------------------------
        NGSSOUTLK    CS2AS ISUPTRK          NGSSOUT
      NGSSINLINK    CS2AS ISUPTRK          NGSSINC
     LOOPAROUND1    CS2CS ISUPTRK         NGSSLOOP
```

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0009
GROUP:CS2B
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
CS2B0009 CS to AppS Calls         Y   -      127     500      1VC    04/01/19
```

138.2.2 OMs

A new OM group, NGSSOM is introduced for tracking the effects of the CS2B0009 SOC limit setting on CS2AS calls. OM fields in the new group relative to this feature are:

- CS2ASOVF - pegged when a CS2AS NGSS call is deflected because allowing the call would have caused the current CS2AS call count to exceed the SOC limit.
- CS2ASHWM - keeps track of the maximum value reached for the CS2AS call counter.

Two other registers are added for feature A00004414 to keep track of CS2CS calls (SOC CS2B0008):

[1]Table SIPLINK is a new table introduced in feature A00003279

- CS2CSOVF - pegged when a CS2CS NGSS call is deflected because allowing the call would have caused the current CS2CS call count to exceed the SOC limit.
- CS2CSHWM - keeps track of the maximum value reached for the CS2CS call counter.

Sample output for the NGSSOM group:

```
NGSSOM

CLASS: ACTIVE
START:2003/12/01 06:00:00 MON; STOP: 2003/12/01 06:09:10 MON;
SLOWSAMPLES:          6 ; FASTSAMPLES:          55 ;

          CS2CSHW   CS2CSHW2    CS2ASHW   CS2ASHW2
          CS2CSOV   CS2CSOV2    CS2ASOV   CS2ASOV2

    0
                0           0        125           0
                0           0          0           0
```

138.2.3 Logs

The NGSS701 log is a new log added for this feature. It is generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC.

The NGSS700 log is added for feature A00004414 to be output when a CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.

138.3 Hardware Requirements or Dependencies

None

138.4 Software Requirements or Dependencies

None

138.5 Limitations and restrictions

None

138.6 Interactions

The usage SOC introduced by this feature does not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

Calls that peg the new CS2B0009 count will always peg the CS2B0005 count as well.

If the SOC limit set for CS2B0009 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

138.7 Applicable customer facing sections

Fault Management

- Logs __X____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____
- SOC __X____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) __X___

138.8 Glossary

Term	Description
CS2AS	CS2K Call Server-to-Agent Server
CS2CS	CS2K Call Server-to-CS2K Call Server

139: Functional Description (FN): A00004391

139.1 Feature name

ACD Agent Expansion from 9,999 to 30,000 Agents.

139.2 Description

Currently, the maximum number of ACD agents that can be provisioned in a single SL-100 or DMS-100 switch is 9,999. This feature extends that maximum to 30,000 agents.

This activity does not increase the number of ACD groups per switch nor the number of ACD agents per group. It only increases the switch-wide maximum number of total ACD agents.

This feature will be controlled via usage based SOC. The maximum number of ACD agents in the switch will be determined by the level of SOC which has been purchased but cannot exceed 30,000 agents.

139.2.1 Background

The maximum number of ACD agents that can be provisioned in a DMS-100 or SL-100 is currently determined by the value of an office parameter. The parameter MAX_NUM_ACD_AGENTS_PER_SWITCH is found in table OFCOPT and can be set to any value in the range of 0 to 9999.

When an attempt is made to create a new ACD agent, the current count of agents in the switch is compared to the value of the office parameter. If the limit has already been reached, the new agent cannot be created. For this activity, the range of the office parameter will be increased to 30000.

Other factors which contribute to the current maximum of 9,999 ACD agents per switch include the ACD agent position ID (POSID) and login ID (LOGINID). The POSID is defined via SERVORD when a new ACD agent is created, and LOGINIDs are defined via tables ACDLOGIN and ACDENLOG.

The POSID and LOGINID are both four digit values with a range of 0001 to 9999. Though neither POSID nor LOGINID is directly correlated to the number of agents in the switch, it would be impractical to have more than

9,999 agents if the POSID and LOGINID remain limited to 4 digits. Therefore, the range of POSID and LOGINID will be increased to 30000.

The external impact of making these changes is briefly described in the sections that follow. More detailed information can be found in the "Configuration" (CN) section of this document (chapter 13).

139.2.2 Office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH

The office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH currently has a maximum value of 9999. The range of this parameter will be increased to have a maximum value of 30000. The actual value of this parameter can no longer be changed by the end user. In order to change the value of the parameter, the SOC usage limit must be changed. The value in the office parameter will then be automatically updated to reflect the new SOC limit.

See section 13.3 (Office Parms) and 13.7 (SOC) for detailed information.

139.2.3 Table ACDLOGIN

Table ACDLOGIN currently supports a maximum of 9,999 tuples. LOGINIDs between 0001 and 9999 can be datafilled here for use by individual ACD agents. This table will be expanded to support up to 30,000 tuples.

Expansion to 30,000 LOGINIDs requires that the LOGINID field be expanded from a 4 digit value to a 5 digit value. Existing 4 digit LOGINIDs will be padded with a leading 0 during ONP.

See section 13.5 (Data Schema) for detailed information.

139.2.4 Table ACDENLOG

Table ACDENLOG currently supports up to 1024 partitions with a maximum of 9,999 tuples each. LOGINIDs between 0001 and 9999 can be datafilled in each partition for use by individual ACD agents. This table will be expanded to support up to 30,000 LOGINIDs in each partition.

Expansion to 30,000 LOGINIDs per partition requires that the LOGINID field be expanded from a 4 digit value to a 5 digit value. Existing 4 digit LOGINIDs will be padded with a leading 0 during ONP.

See section 13.5 (Data Schema) for detailed information and examples.

139.2.5 Table ACDGRP

This activity adds a new field in table ACDGRP. The new field will be called IDSIZE and will specify the number of login digits to be used by all agents in the group. IDSIZE can be set to a value of 4 or 5. The default value will be 4.

When IDSIZE equals ‘4’, all agents in the ACD group will login using 4 digit login IDs. When IDSIZE equals ‘5’, all agents in the ACD group will login using 5 digit login IDs.

During ONP from a load which does not include this feature to a load which does, IDSIZE will be defaulted to ‘4’ for all ACDGRP tuples.

All existing agents will continue to login using their existing 4 digit login IDs. The operating company can continue to add agents to these groups and/or create new groups with IDSIZE = 4 provided that there are available login IDs in the range of 00001 to 09999. Availability depends on datafill in table ACDLOGIN and/or ACDENLOG.

When login IDs 00001 through 09999 have been exhausted, the next agent added must use a 5 digit login ID. This means that the agent’s entire ACD group must be converted to 5 digit login.

139.2.5.1 Converting a group to 5 digit login

To convert an ACD group from 4 digit login to 5 digit login, field IDSIZE in table ACDGRP must be changed to ‘5’. No other switch based changes will be required. However, all agents in that ACD group must be notified to begin using 5 digit login. Existing agents can simply use their old 4 digit login ID but manually pad it with a leading 0. For example, an agent using a login ID of 1234 will begin using the login ID 01234. If they attempt to login without the leading 0, the login will fail.

New agents that are added to a group already using 5 digit login IDs can use any available login ID in the range of 00001 to 30000. Availability depends on existing datafill in table ACDLOGIN and/or ACDENLOG.

See section 13.5 (Data Schema) for detailed information and examples.

139.2.6 Table KSETLINE

Table KSETLINE defines the DN keys on all keysets. This activity makes a field change for KSETLINE tuples that meet the following criteria:

- FORMAT = ‘ACD’
- ACDKEY = ‘INCALLS’
- IDNUM = ‘Y’

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See section 13.5 (Data Schema) for detailed information and examples.

139.2.7 Table KSETFEAT

Table KSETFEAT defines the feature assignments on keysets. This activity makes a field change for KSETFEAT tuples that meet the following criteria:

- FEATURE = ‘SUPR’
- IDNUM = ‘Y’

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See section 13.5 (Data Schema) for detailed information and examples.

139.2.8 Table IBNFEAT

Table IBNFEAT defines the feature assignments on IBN sets. This activity makes a field change for IBNFEAT tuples that meet the following criteria:

- FEATURE = ‘ACD’ or ‘SUPR’
- IDNUM = ‘Y’

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See section 13.5 (Data Schema) for detailed information and examples.

139.2.9 SERVORD

Some Servord commands used by ACD offer a prompt for POSID. Currently, any value between 0000 and 9999 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be a 5 digit value in the range of 00000 to 30000.

This change affects command prompting for NEW, ADO, NEWACD, and CHF commands.

See section 13.6 (Service Orders) for detailed information and examples.

139.2.10 Tools

ACDDEBUG and ACDSHOW are Command Interface (CI) tools that will require changes by this feature in order to handle a 5 digit position ID. ACDDEBUG is a CI tool created to display ACD data structures. Currently, a ACDDEBUG command uses a 4 digit position ID as an index in order to display ACD agent data. This activity will extend the command so that the data structures of an ACD agent with a 5 digit position will be displayed.

ACDSHOW is a CI tool that displays specific information concerning a current ACD configuration such as the list of agent positions in a ACD group and agent information for a given user login ID. Currently, ACDSHOW commands use a 4 digit position ID as an index in order to display information concerning an ACD configuration. This activity will extend the command so that the information of an ACD agent with a 5 digit position will be displayed.

For more information on ACDDEBUG and ACDSHOW, please refer to section 13.9 (Command Interface changes).

139.2.11 Intelligent Call Management (ICM)

ICM is a product that connects a host computer to a DMS-100 or MSL-100. ICM defines a switch to computer message set and a computer to switch message set that enables services to a telephone subscriber. Call event messages are sent from the switch to the host computer. Whereas call control messages, are sent from the host computer to the switch. Specific ICM call event messages or ICM call control message can contain a ‘positionID’ parameter and/or ‘loginID’ parameter. Currently, the ‘positionID’ parameter and the ‘loginID parameter in ICM messages handle only 4 digits.

This activity will allow the switch to send ICM call event messages to the host computer with a 5 digit ‘positionID’ parameter and/or a 5 digit ‘loginID’parameter’. This activity will also allow call control ICM messages sent from the host computer to the switch to have a 5 digit ‘positionID’ parameter or 5 digit ‘loginID’ parameter. Once the call control message is received on the switch, the 5 digit ‘positionID’ or 5 digit ‘loginID’ will be checked for validity.

139.2.12 ACD Management Information System (MIS)

ACD MIS is a hardware and software option which provides customer premise equipment (CPE) downstream processor (DSP) with information concerning ACD events occurring in an associated DMS-100 switch. The DSP can request and collect ACD information from the switch . There are two types of ACD MIS messages: messages sent from the switch to the DSP and message sent from the DSP to the switch.

The following are categories of messages sent from the switch to the DSP:

- Switch Control messages
- Initialization Data messages
- ACD VFG OM messages,
- ACD call/agent position event messages and
- Load Management Event messages.

Specific ACD MIS messages can contain a ‘positionID’ parameter and/or ‘loginID’ parameter. Currently, the ‘positionID’ parameter and the ‘loginID parameter in ACD MIS messages handle only 4 digits. This activity will allow ACD MIS messages sent from the switch to the DSP to have a 5 digit ‘positionID’ parameter or 5 digit ‘loginID’ parameter.

There following are categories of messages sent from the DSP to the switch:

- DSP Control Messages
- Inquire Switch Data Messages
- Remote Load Management Request messages.

This activity will allow ACD MIS message sent from the DSP to the switch to have a 5 digit ‘positionID’ parameter and/or a 5 digit ‘loginID’ parameter. The 5 digit ‘positionID’ will be checked for validity.

139.2.13 SOC Control

This feature will be controlled by a standard usage based SOC. The usage limit will define the maximum number of agents for the switch (i.e. the total number of lines that can have the ACD option assigned).

The default usage limit will be 0 ACD agents. During ONP from previous loads, the SOC usage limit will be set to match the value of office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH. Thus there will be no impact to existing customers who do not purchase this SOC.

When the SOC is purchased, the usage limit can be increased by any number of agents up to a maximum value of 30,000 agents.

When the usage limit is changed via SOC, the value in office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH will automatically be updated to reflect the SOC usage limit. The value in the office parameter can no longer be changed manually. The SOC usage limit must be changed first.

The SOC will not control the ability to use the optional 5 digit login IDs, nor will it control the ability to datafill extra login IDs for future use.

See section 13.7 (SOC) for detailed information.

139.3 Hardware Requirements or Dependencies

Not applicable

139.4 Software Requirements or Dependencies

Not applicable

139.5 Limitations and restrictions

- Once an ACD group is converted to 5 digit login (see section 2.2.5), all of the agents in that group will be required to login using 5 digits. Pre-existing 4 digit login IDs can be used by dialing a leading zero.
- Once an ACD group is converted to 5 digit login, it cannot be converted back to 4 digit login.

- Login IDs 00001 through 09999 can be used by any ACD agent in the switch. If the agent's group is using 4 digit login (as defined in table ACDGRP), the agent will dial the last 4 digits only. If the agent's group is using 5 digit login, the agent must dial all 5 digits.
- Login IDs 10000 through 30000 can only be used by agents in groups which use 5 digit login.
- Although 5 digit login is optional per ACD group, it should be noted that 5 digit login will be required as soon as the login IDs 00001 through 09999 are exhausted. At that point, the next agent added must use a 5 digit login ID. This means that the entire group to which this agent belongs must be converted to 5 digit login. The other agents in the group can continue to use their previous login IDs, but they must now include a leading zero when logging in.
- Individual ACD agents cannot be moved between two ACD groups which do not use the same number of login digits. Field IDSIZE in table ACDGRP must match for an agent to be moved from group to group by any means.

139.6 Interactions

139.6.1 Load Management / Remote Load Management

Load Management / Remote Load Management allows ACD agents to be moved from one ACD group to another. This activity restricts movement of agents between groups which do not use the same number of login digits. Field IDSIZE in table ACDGRP must match or the agent movement will not be allowed.

139.7 Applicable customer facing sections.

Fault Management	
Logs	__X__
Alarms	_N/A_
Configuration	
Data Schema	__X__

User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	__X__
Office Parameters	__X__
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

139.8 Glossary

Term	Description
ACD	Automatic Call Distribution
ACDMIS	ACD Management Information Systems
ASN	Abstract Syntax Notation
CI	Command Interface
DMS	Digital Multiplex System
DN	Directory Number
DSP	Downstream Processor
IBN	Integrated Business Network
ICM	Intelligent Call Management
ONP	One Night Process
SCAI	Switch Computer Application Interface
SOC	Software Optionality Control

140: Functional Description (FN): A00004414

140.1 Feature name

SIP Call Server SOC

140.2 Description

This activity implements a mechanism to control the maximum number of SIPT calls that utilize the Next Generation Session Server (NGSS) platform when the far end is another CS2K. A usage SOC, CS2B0008, is implemented to limit these types of calls (abreviated as CS2CS in this document).

Another activity, A00004271 SIP App Server SOC, implements a similar mechanism to control the maximum number of SIPT calls that utilize the NGSS platform when the far end is non-CS2K, referred to here as an Application Server. SOC option CS2B0009 is the usage SOC for A00004271.

Both SOC features are part of a set of activities for delivering the Session Server - SIP Gateway application in SN07. The other features are:

- A00003270 SIP Open Interop Call Processing
- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003277 Session Server OM Subsystem
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003281 SIP on Session Server Call Audit
- A00003282 SIP on Session Server Datasync
- A00003933 SIP on Session Server Drop 1 ICAF
- A00003934 Session Server Project ICAF

140.2.1 SOC limiting

The usage-controlled CS2B0008 SOC added by this activity applies to calls that meet the following criteria:

— the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,

— a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK[1],

— the CONNTYPE field of the tuple in table SIPLINK is set to CS2CS.

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exeed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming and outgoing SIPT calls on trunk group NGSSLOOP will increment the usage counter for the CS2AS SOC.

```
TABLE: SIPLINK
        LINKNAME CONNTYPE                  AGNTDATA
-------------------------------------------------
        NGSSOUTLK    CS2AS ISUPTRK          NGSSOUT
      NGSSINLINK    CS2AS ISUPTRK          NGSSINC
     LOOPAROUND1    CS2CS ISUPTRK          NGSSLOOP
```

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0008
GROUP:CS2B
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
CS2B0008 CS to CS Calls           Y -         127     500      1VC  04/01/19
```

140.3 Hardware Requirements or Dependencies

None

140.4 Software Requirements or Dependencies

None

140.5 Limitations and restrictions

None

140.6 Interactions

The usage SOC introduced by this feature does not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

Calls that peg the new CS2B0008 count will always peg the CS2B0005 count as well.

[1]Table SIPLINK is a new table introduced in feature A00003279

If the SOC limit set for CS2B0008 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

Feature A00004271 SIP App Server SOC introduces new OM group NGSSOM for tracking the effects of the CS2B0008 SOC limit setting on CS2CS calls.

Feature A00004271 SIP App Server SOC adds a new NGSS700 log that is generated when a CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.

140.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- SOC ___X__
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

140.8 Glossary

Term	Description
New term	Definition

141: Functional Description (FN): A00004422

141.1 Feature name

ACT.00004422: Enhanced 911 Dynamic Packet Trunks Session Initiation Protocol-Telephony Call Trace.

141.2 Description

This feature provides the ability to trace established intra and inter office calls involving SIP-T DPT for Call Server 2000 (CS2K). Before the development of this feature, CS2K-Core had the ability to trace intra office line to line and inter office line to trunk/line and trunk to trunk/line calls for emergency situations (police, fire, hospital etc.) for only TDM trunks.

This feature enhances the trace abilities of CS2K to identify which SIP-T DPT (originating and/or terminating) is associated with an active call within the call server by means of SIP-T DPT callid.

This feature works for all calls and not just E911 calls.

The trunk information is provided through a new man-machine command interpreter (CI) command "SIPTRACE"[1]. The syntax and permissible input and output parameters of SIPTRACE are described below.

The input trunk information consists of:-

- trunk group and trunk member for TDM trunks.
- SIP-T DPT call-id for SIP-T DPT.

This command tool utility is limited to SIP-T DPT and TDM trunks as input to this command, while the output can be SIP-T DPT, TDM trunks or lines.

The new CI command "SIPTRACE" has the following syntax:-

SIPTRACE <Input trunk> {

{T <TDM trunk group> STRING

<TDM trunk member> {0 TO 9999}},

{D <DPT SIP-T call-id> STRING}}

Output on the CI prompt for the above command is of the following format:-

[1]Henceforth, in this document, all references to new CI command utility would refer to new CI command "SIPTRACE".

<input> is currently connected to ***<output>***

where

<input> is either

- "TDM trunk <trkgrp> <trkmem>" if a TDM trunk was entered or
- "SIP-T DPT <trkgrp> callid <SIP-T callid>" if a SIP-T callid was entered. The SIP-T callid entered on the command prompt during SIPTRACE command execution, is enclosed in single quotes.

<output> is one of the following:

- "TDM trunk <trkgrp> <trkmem>" if the connected party is a TDM trunk member
- "SIP-T DPT <trkgrp> callid <SIP-T callid>" if the connected party is a SIP-T DPT.
- "LINE <lineid>" DN is displayed, if the connected party is a line terminal.

For call scenarios in which the output TDM agent is found to be a C7ISL member, the tool automatically traverses the ISL and presents the final agent of the call. In such cases, multiple output lines are displayed on the CI.

Call scenarios involving SIP-T loop-arounds where SIP-T DPT looped around on the same or different GWC(s), are also supported by the new CI command SIPTRACE. In cases when the output agent for a SIPTRACE command execution is found to be SIP-T DPT, the output SIP-T call-id retrieved from the GWC is used to recursively trace the final output agent of the call and hence multi-line outputs are displayed on the CI.

Calls involving IW-SPM between legacy TDM agents connected to XPM (e.g. LTC in a North American lab. setup and PLGC in an International lab. setup) and succession agents in hybrid offices are also supported by SIPTRACE.

The new CI command utility is at the top level of CI and the user is able to invoke this new command, at any level built over CI (e.g. MAPCI, LOGUTIL etc.)

The following are the error/information messages to be displayed on the CI:-

Table 1 Error/Information messages displayed on the CI

Sr. No.	Error/Information messages displayed on the CI	Cause of the error/information message
1	<Input trunk>[a] is currently connected to a line whose DN is not available	The output end-point is found to be a line but its Tid is not mapped to a DN datafilled in tables on the Core

Sr. No.	Error/Information messages displayed on the CI	Cause of the error/information message
2	TDM trunk group not datafilled in table CLLI	Invalid TDM trunk group entered
3	TDM trunk group not datafilled in table TRKGRP	TDM Trunk group not datafilled in table TRKGRP
4	TDM trunk group not datafilled in table TRKSGRP	TDM Trunk group not datafilled in table TRKSGRP
5	SIP-T DPT <SIP-T DPT trkgrp> callid <SIP-T call-id> not associated with any active call	SIP-T callid does not exist within the GWC(s) and when the SIP-T DPT trunk group is available.
6	<Input trunk> is currently connected to an un-supported agent type <CP selector>	Output agent is not supported by this feature
7	TDM trunk <trkgrp> <trkmem> not associated with any active call	The input TDM trunk member information entered at the CI does not map to a live call
8	SIP-T DPT callid <SIP-T call-id> not associated with any active call	CS2K-Core is unable to send broadcast message to GWC(s) to retrieve associated DPT Tid(s) or when the GWC response messages have arrived in the Core but unable to determine the output agent details and the SIP-T DPT trunk group is not available.
9	Unable to identify far-end C7ISL member for TDM trunk (C7ISL) <trkgrp> <trkmem>	The output agent is found to be a TDM C7ISL agent but the far end TDM C7ISL trunk group and trunk member details datafilled in table C7ISL are not available.
10	Trunk group datafilled as DPT in Table DPTRKMEM	DPT trunk group entered using option T while SIPTRACE command execution
11	Number of SIP-T DPT loop-arounds exceeded allowed limit	For call scenarios in which the number of SIP-T to SIP-T loop-arounds in the same call server has exceeded 9 (highly unlikely)

a. <Input trunk> refers to: {T <Input TDM trunk group> <Input TDM trunk member>, D <SIP-T DPT trkgrp> callid <SIP-T call-id>}

The snap-shots of various combinations of call scenarios involving TDM and SIP-T DPT trunks is shown below; the SIPTRACE command execution is shown on the CI prompt for simplicity purpose but same can be executed on any level built over CI (e.g. MAPCI, LOGUTIL, etc.):-

Note: A brief description of the call scenario is provided only for some complex call scenarios.

1. TDM to line inter-working in CS2K

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 is currently connected to LINE 1158206005
```

2. SIP-T DPT to line inter-working in CS2K

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K4SIP1LOOPFR3 callid 0026.4030-10-16-49-02.67@CS2K4_84
is currently connected to LINE 1158206007
```

3. TDM to TDM inter-working in CS2K

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM trunk
UKISUPLPA 10
```

4. TDM to SIP-T DPT inter-working in CS2K

```
Call Scenario: Line 1158206007 -> TDM ETSILPA 2
               TDM ETSILPB 2 -> SIP-T -> Line 1158206008v
```

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to SIP-T DPT
K4SIP1LOOPFR3 callid 0026.4030-10-16-49-02.67@CS2K4_84
SIP-T DPT K4SIP1LOOPFR3 callid 0026.4030-10-16-49-02.67@CS2K4_84
is currently connected to LINE 1158206008
```

5. SIP-T DPT to TDM inter-working in CS2K

```
Call Scenario: Inter-Call Server posted SIP-T -> TDM ETSILPA 2
               TDM ETSILPB 2 -> Line 1158206008
```

Note: The SIPTRACE command will not be able to determine the other agent for an inter-call server SIP-T DPT as it involves another call server; hence the second line of output shows that SIPTRACE command execution in this call server could not determine the connected agent for the SIP-T DPT leg belonging to another call server domain.

In order to determine the complete path of the call, the SIPTRACE command has to be executed in successive call servers also.

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to TDM trunk ETSIV1LPA 2
SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84 not
associated with any active call
```

6. Output TDM identified as C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM trunk (C7ISL)
ETSIV1LPA 3
TDM trunk (C7ISL) UKISUPLPA 4 is currently connected to LINE
1158206005
```

7. Input TDM identified as C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk (C7ISL) ETSIV1LPB 2 is currently connected to TDM trunk
UKISUPLPA 8
```

8. SIP-T DPT loop-arounds - Auto-traversal of SIP-T callid encountered as output of a SIPTRACE command execution

```
Call Scenario: Line 1158206005 -> SIP-T -> SIP-T (posted) -> Line 1158206007
```

Note: The order of displaying output agents for SIPTRACE command executions involving SIP-T DPT callid may not be in the same order as depicted in the snap-shot because this depends on the way in which the DPT Tid(s) are returned by the SIP-T GWC.

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1UK3 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-
49-02.95@CS2K4_84
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.95@CS2K4_84 is
currently connected to LINE 1158206005
SIP-T DPT K1SIP1UK3 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to LINE 1158206007
```

9. Invalid input option

```
CI> SIPTRACE abcd

Next par is: <Input trunk> {T <TDM trunk group> <TDM trunk
member>,
D <DPT SIP-T call-id>}


Enter: <Input trunk>
CI>
```

10. No option entered with new CI command

```
CI> SIPTRACE

Next par is: <Input trunk> {T <TDM trunk group> <TDM trunk
member>,
D <DPT SIP-T call-id>}


Enter: <Input trunk>
CI>
```

11. Incomplete input entered with option T

```
CI> SIPTRACE T ETSIV1LPA

Next par is: <TDM trunk member> {0 TO 9999}


Enter: <TDM trunk member>
CI>
```

12. Incomplete input entered with option D

```
CI> SIPTRACE D

Next par is: <DPT SIP-T call-id> {STRING}


Enter: <DPT SIP-T call-id>
CI>
```

13. Invalid input TDM trunk group name

```
CI> SIPTRACE T ABCD 2

TDM trunk group not datafilled in Table CLLI
```

14. TDM trunk group not datafilled in table TRKGRP

```
CI> SIPTRACE T UASBLDNANN 2

TDM trunk group not datafilled in Table TRKGRP
```

15. TDM trunk group not datafilled in table TRKSGRP

```
CI> SIPTRACE T ETSIV2LPB 2

TDM trunk group not datafilled in Table TRKSGRP
```

16. Invalid input TDM trunk member number

```
CI> SIPTRACE T ETSIV1LPA -2

Out of range: <TDM trunk member> {0 TO 9999}
Enter: <TDM trunk member>

CI>
```

17. SIP-T callid does not exist / does not map to any live call.

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 not
associated with any active call
```

18. Input TDM parameters do not map to any live call.

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 not associated with any active call
```

19. Output agent is not supported for TDM input

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 is currently connected to an un-supported
agent type 10
```

20. Output agent is not supported for SIP-T DPT inputs

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to an un-supported agent type 12
```

21. Output line DN not identifiable for TDM inputs

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 is currently connected to a line whose DN
is not available
```

22. Output line DN not identifiable for SIP-T DPT inputs

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to a line whose DN is not available
```

23. Output agent is TDM C7ISL but unable to find far-end C7ISL agent

```
CI> SIPTRACE T ETSILPB 2

TDM trunk ETSILPB 2 is currently connected to TDM trunk (C7ISL)
UKISUPLPA 3
Unable to identify far-end C7ISL member for TDM trunk (C7ISL)
UKISUPLPA 3
```

24. Input DPT trunk group entered with option T

```
CI> SIPTRACE T K2SIP1CZ1 2

Trunk group datafilled as DPT in Table DPTRKMEM
```

25. Unable to send GWC request message or unable to determine output agent for SIP-T DPT input

```
CI> SIPTRACE D ‘0026.4030-10-16-49-02.67@CS2K4_84’

SIP-T DPT callid 0026.4030-10-16-49-02.67@CS2K4_84 not
associated with any active call
```

26. Number of SIP-T loop-arounds exceed 9 within the same CS2K

```
CI> SIPTRACE D ‘0026.4030-10-16-49-02.67@CS2K4_84’

SIP-T DPT K4SIPTLOOPV3 callid 0026.4030-10-16-49-02.67@CS2K4_84
is currently connected to SIP-T DPT K3SIPTDPTLOOP1 callid
0026.4030-10-16-49-02.33@CS2K4_84

... (printing total of 9 output lines for more than 9 SIP-T loops)

SIP-T DPT K2SIPTLOOPV6 callid 0026.4030-10-16-49-02.04@CS2K4_84
is currently connected to SIP-T DPT K8LOOPV8 callid 0026.4030-10-
16-49-02.15@CS2K4_84
Number of SIP-T DPT loop-arounds exceeded allowed limit
```

141.3 Hardware Requirements or Dependencies

None.

141.4 Software Requirements or Dependencies

Software load from SN07 onwards.

141.5 Limitations and restrictions

— The new command interpreter (CI) command “SIPTRACE” is supported only for SIP-T DPT. It is not supported for networks using BICC protocol.

— TDM trunks and SIP-T DPT are the only input parameters allowed. Line is not allowed as input parameter.

— TDM trunks, SIP-T DPT and Line DNs are the only output parameters.

— If a line directly maps to a DN, the DN is displayed as <lineid> with area-code, office-code and station-number as datafilled in table DNINV.

— Lines, discovered as output agents, not mapped to DNs are not supported by the new CI command SIPTRACE.

— Feature interactions like 3WC or any other multi-linked calls with the new CI command SIPTRACE, are not supported by the new CI command SIPTRACE.

141.6 Interactions

Features supported by the new CI command SIPTRACE include, but not limited to, 3WC, CFB, CFU, CFDA, SDN, MLH.

141.7 Applicable customer facing sections

Fault Management	
Logs	__N/A____
Alarms	__N/A____
Configuration	
Data Schema	__N/A____
User Interface	__X____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____
Accounting (includes AMA billing)	__N/A____
Performance (includes operational measurements)	__N/A____

141.8 Glossary

Term	Description
3WC	Three way conference
BICC	Bearer Independent Call Control
CI	Command Interpreter
C7ISL	CCS7 ISUP Signalling Loop-back
CFB	Call Forward Busy
CFD/CFDA	Call Forward Don’t Answer
CFU	Call Forward Universal
CS2K	Communication Server 2000
DMS	Digital Multiplex System
DN	Directory Number
DPT	Dynamic Packet Trunking
E911	Enhanced 911 services
ISUP	ISDN User Part
ISDN	Integrated Services Digital Network
GWC	GateWay Controller
MLH	Multi Line Hunt-group
SIP-T	Session Initiation Protocol-Telephony
SDN	Secondary Directory Number
TDM	Time Division Multiplexing
VRDN	Virtual Routing Distribution Node

142: Functional Description (FN): A00004430 (AL1SVCOM)

142.1 Feature name

A00004430 - SVC Failure OMs

142.2 Description

This SN07 feature provides two main functional components:

- Introduces new OM group AL1SVCOM.
- Replaces the ATM606 log report with XPKT301 and XPKT302 logs.

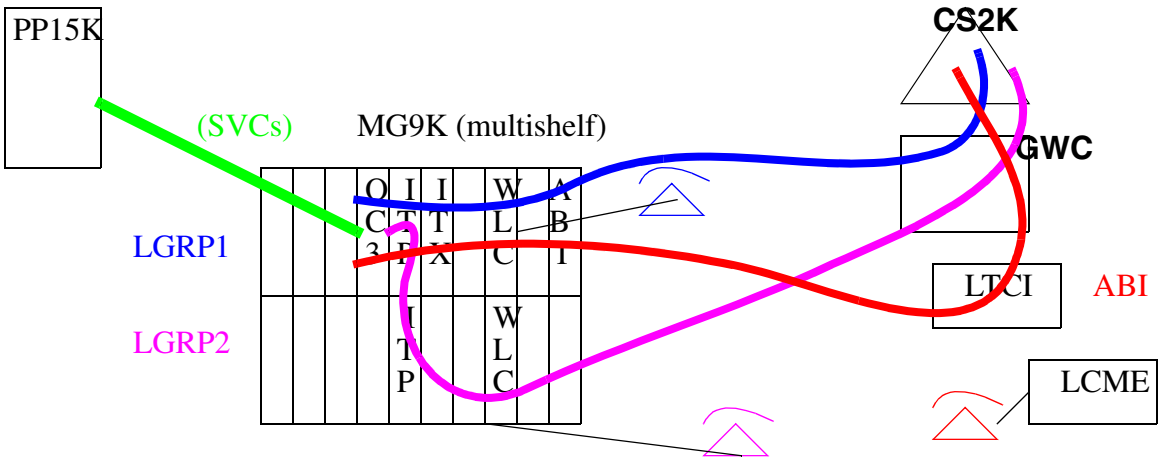
OM group - AL1SVCOM - is used to provide OM registers for ATM switched virtual circuits (SVC) external network connection bearer path call origination attempts and call failures. Prior to this feature, ATM external network bearer path connection failures were only captured with ATM606 log reports for (SPM IW, DPT SPM and SMG4)[1] nodes and also for MG9K[2] nodes.

Prior to SN07, an ATM606 log report was generated when either a node failed to get an SVC connection through the ATM network during initial call setup, or when an established call was taken down due to an ATM external network connection failure.

In SN07, when an ATM SVC failure occurs, this feature increments registers in OM group AL1SVCOM, on a nodal basis, for UA-AAL1 nodes: SMG4, IW SPM, DPT SPM, MG9K ABI (LTC, SMA1, LGC, RCC2, SMSR, SMS, RCC) and on a logical group basis for MG9K. An XPKT301 or XPKT302 log report is output for the SVC failure also. The XPKT301 log report is for UNI connection failures. The XPKT302 log report is for UNI Mid-call connection failures.

[1]SN05 feature A59035937 - ATM Failure Log
[2]SN06.2 feature A00001934 - ATM Troubleshooting Log Support for MG9K AAL1

Figure 1 CS2K identification of MG9K and ABI lines



MG9Ks are identified as ‘logical groups’ because the CS2K is not aware of MG9Ks on a nodal basis. SN06.2 feature A00002607 - ABI XPM SITE and MG9K Location support on the Core - provided the first step towards providing management on the CS2K of ABI XPM and MG9K lines in the Succession network, however, there is no distinction between an MG9K ‘master’ shelf (for multi-shelf MG9K configurations) and ‘subtending’ shelves.

Refering to figure 1 above, the physical ATM bearer path for a multi-shelf MG9K, (or a single-shelf MG9K) is between the ATM switch (which is a Passport 15000 in the example above) and the OC3 Supercore card on the MG9K master shelf. At the time of this writing, the CS2K has no concept of ‘master’ shelf for the MG9K. The ATM bearer path connection data is only maintained in the MG9K Element Manager. The CS2K maintains information in Table LGRPINV for each MG9K shelf. OM group AL1SVCOM will therefore output each MG9K shelf as a separate logical group, rather than identify one Master Shelf, where the actual physical ATM fiber connects the MG9K OC3 pack to the ATM network.

The MG9K logical group names displayed by OM group AL1SVCOM are the MG9K shelf names listed in Table LGRPINV.

Table 1 below lists the registers for OM group AL1SVCOM and a description of each register. External network origination connection attempts and connection failures are tracked by this OM group in SN07.

This feature increments OM group AL1SVCOM registers for both originating and terminating nodes, when the Core attempts to set up an external network connection.[1] Thus one ATM606 logged ATM SVC failure event will in most cases increment two OM AL1SVCFL registers - once for the SVC originating call agent node, and once for the SVC terminating agent node.

When an ATM external network connection failed prior to SN07, the Gateway node that requested the connection - the master of the ATM connection - reported an ATM SVC failure message to the Core which then generated an ATM606 log report.

With ths feature, an XPKT301 or XPKT302 log is generated for external network connection failures, depending upon if the connection failure occured during initial call setup, or after the call was established, and then OM group AL1SVCOM failure registers are also pegged.

Table 1 Registers for OM group AL1SVCOM

Register	Description
NOSVCAT	Number of SVC call attempts.
NOSVCAT2	Extension register for nosvcatt.
NOSVCFL	Number of SVC call failures.
ISSVCAT	Number of intraswitched (local) SVC call attempts
ISSVCAT2	Extension register for issvcsat.
ISSVCFL	Number of intraswitch (local) SVC call failures.
DPTSVCA	Number of interswitch (DPT) SVC call attempts.
DPTSVCA2	Extension register for dptsvca.
DPTSVCF	Number of interswitch (DPT) SVC call failures.
NRTEDEST	ATM cause code 3 - no route to destination - SVC call failures.
NOUSRRES	ATM cause code 18 - no user responding - SVC call failures.
VPCINAVL	ATM cause code 35 - requested VPI/VCI not available - SVC call failures.
BWTHNAVL	ATM cause code 37 - user cell rate not available - SVC call failures.
TEMPFAIL	ATM cause code 41 - temp failure - SVC call failure reference.
RESUNAVL	ATM cause code 47 - Resource unavailable SVC call failure reference
OTH_CC	All other ATM cause codes SVC call failures.

[1]Inter-office MG9K calls using BICC GWC, have only an originating node to report for the SVC call failure. The terminating side of the bearer path through the ATM network is located in another office. The local office is only aware of the originating agent on the ATM bearer path connection.

Figure 2 below shows the OM register peg flow chart for group AL1SVCOM..

1. (Originating registers): nosvcat, issvcat, dptsvca

All external network connection attempts peg register ***nosvcat*** (number of svc attempts)

If the external network connection attempt is an 'intra' switched call, register ***issvcat*** (interswitch svc attempt) is pegged along with the nosvcat register.

If the external network connection failure is an 'inter' switched call, register ***dptsvca*** is pegged along with the nosvcat register.

2. (Failure registers): dptsvcf, issvcfl, dptsvcf

All connection failures peg register ***nosvcfl*** (number of svc failures).

If the connection fails and the call is intra-switched, register ***issvcfl*** is pegged along with the nosvcfl register.

If the connection fails and the call is inter-switched, register ***dptsvcf*** is pegged along with the nosvcfl register.

3. (Failure registers):
nrtedest, ***nousrres***, ***vpcinavl***, ***bwthnavl***, ***tempfail***, ***resunavl***, ***oth_cc***

Depending upon what ATM cause code is reported to the Core from the Gateway, will determine which of the above registers are then pegged. Ony one of the above registers will be pegged to provide further categorization for connection failures. If the ATM cause code is not one of 3, 18, 35, 37, 41, or 47, register oth_cc (all other cause codes) is pegged.

Figure 2 AL1SVCFL OM Group Register Flow

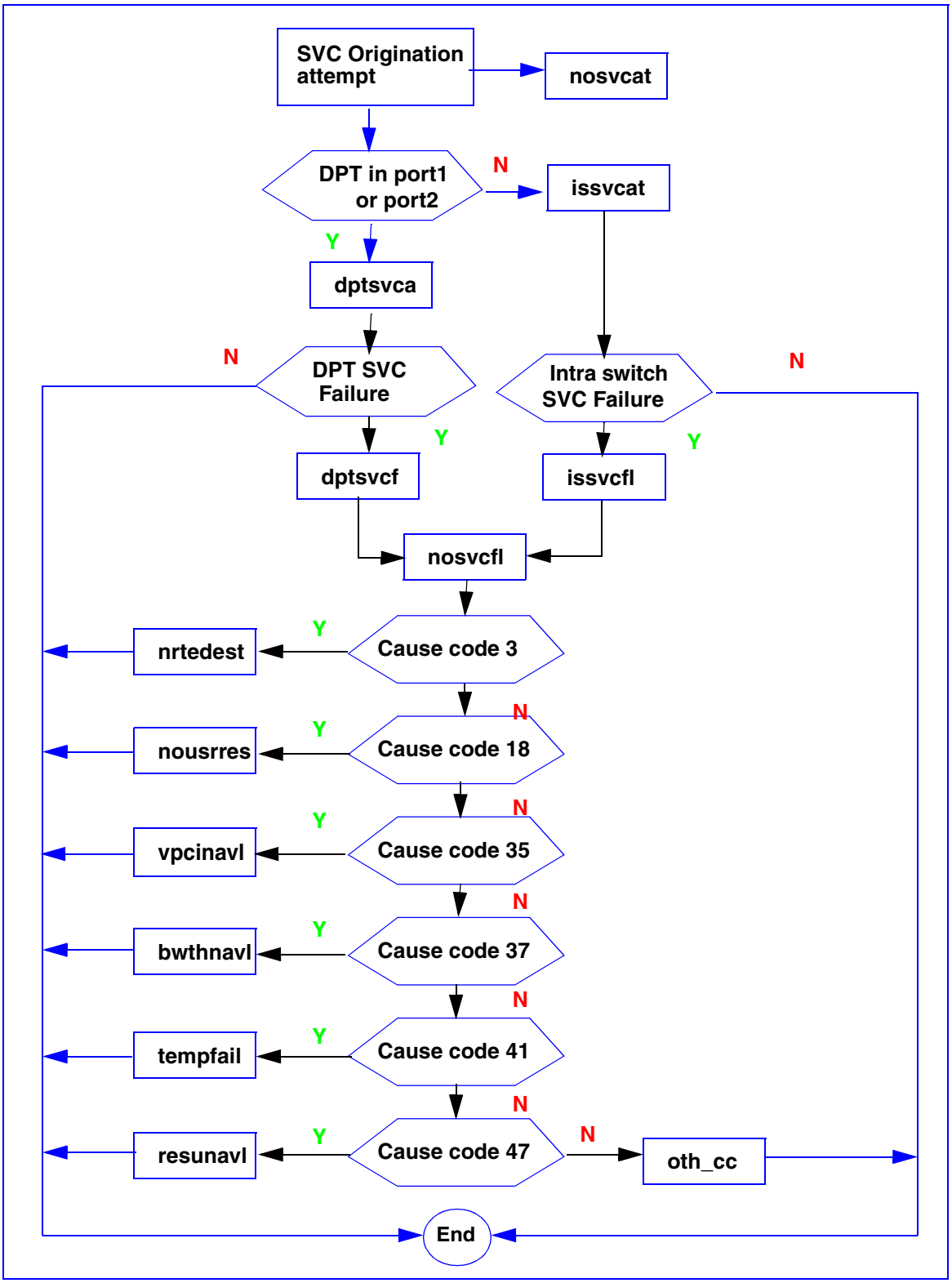


Figure 1 below displays OMSHOW command output for the new AL1SVCFL OM group.

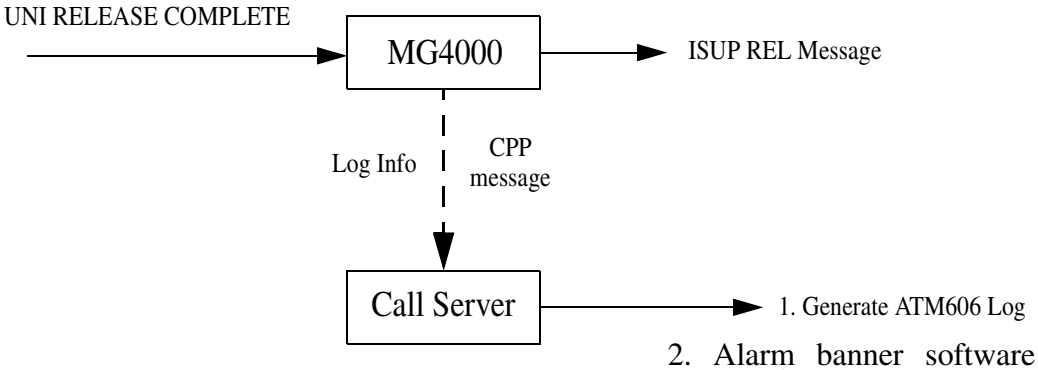
Figure 3 OM group AL1SVCFL with registers

```
omshow al1svcom active 60 120
AL1SVCOM

CLASS: ACTIVE
START:2004/02/03 15:30:00 TUE; STOP: 2004/02/03 15:31:26 TUE;
SLOWSAMPLES:        1 ; FASTSAMPLES:         9 ;

    KEY (SVC_OM_PM_INFO)
    INFO (SVC_OM_TUPLE_DATA)
      NOSVCAT   NOSVCAT2   NOSVCFL   ISSVCAT
     ISSVCAT2   ISSVCFL   DPTSVCA   DPTSVCA2
      DPTSVCF   NRTEDEST   NOUSRRES   VPCINAVL
     BWTHNAVL   TEMPFAIL   RESUNAVL    OTH_CC

  66
    SMG4 SPM    0
          0        0        0        0
          0        0        0        0
          0        0        0        0
          0        0        0        0
  108
  MG9K ABI LGC 0
          0        0        0        0
          0        0        0        0
          0        0        0        0
          0        0        0        0
  112
  MG9K ABI SMA2 0
          0        0        0        0
          0        0        0        0
          0        0        0        0
          0        0        0        0
  118
    MG9K SLOA 23 3
          2        0        0        2
          0        0        0        0
          0        0        0        0
          0        0        0        0
```

142.2.1 SPM based AAL1 SVC Failure OM generation Functionality

When the ATM606 log is generated for SPM IW, DPT SPM or an SMG4, new software introduced by this feature pegs the appropriate OM AL1SVCOM registers as shown in Figure 2.

SPM based AAL1 Functionality



[1]A00004260 - SN07

The operations relevant to an ATM bearer path failure scenario are as follows:

- During call setup time, the MG 4000 sends a UNI Setup message to the Passport ATM switch. Instead of receiving a UNI Connect, a UNI Release Complete is received with a cause value indicating some failure to set up the ATM SVC, or bearer path.
- When the MG 4000 receives the UNI Release Complete message, it gathers data needed for the new log and sends it to the Call Server.
- The Call Server receives the message from the MG 4000 and formats it into a new log, increment the appropriate alarm banner counter[1], and pegs the appropriate OM group AL1SVCOM register for the ATM failure cause code event.
- The Supernode Data Manager uses the existing log delivery capabilities to transfer the new log and OM to the OSS.
- The MG 4000 builds an ISUP RELease message and inserts the ISUP release cause value of 47. The ISUP RELease message is sent to the Ingress Succession Network in case of inter-working calls.

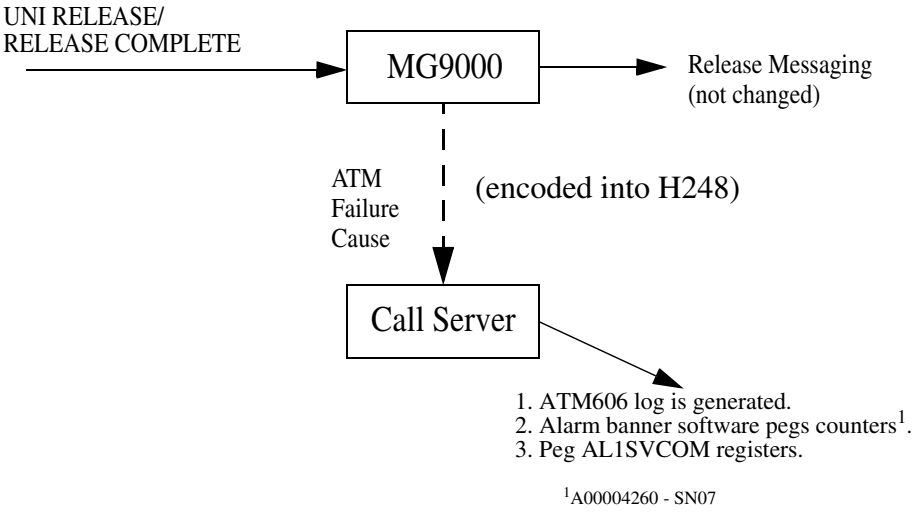
[1]SN07 - A00004260 - Alarm Banner.

142.2.2 MG9K AAL1 SVC Failure OM generation Functionality

The functionality shown in figure 2 shows the SN06.2 generation of ATM606[1] logs for MG9K gateways, and the OM pegging functionality introduced by this feature.

The functionality of this feature is depicted in Figure 1.

Figure 4 Functional Behavior Diagram



- During call setup time, the MG 9000 sends a UNI Setup message to the Passport ATM switch. Instead of receiving a UNI Connect, a UNI Release/ release Complete is received with a cause value indicating some failure to set up the ATM SVC, or bearer path.
- When the MG 9000 receives the UNI Release/release Complete message, it encodes the UNI release cause into an H248 message and sends same to the Call Server.
- The Call Server receives the message from the MG 9000 and formats it into an XPKT301 or XPKT302 log, and pegs the appropriate AL1SVCOM OM register for the ATM failure cause code[2].
- The Supernode Data Manager uses the existing log delivery capabilities to transfer the new log to the customer's OSS.
- For the affected call, the Call Server will detect integrity lost and process release messages to the other agent (line or trunk) in its usual way.

[1]ATM606 logs are replaced by the XPKT301 and XPKT302 log in SN07, see DSUM and FM sections.
[2]The alarm banner feature in SN07 is for SMG4/IW/DPTs only.

142.2.3 XPKT301 and XPKT302 logs

This feature eliminates the ATM606 log, replacing it with XPKT301 and XPKT302 logs. The XPKT301 and XPKT302 logs contain all the existing fields and formatting of the replaced ATM606 log, and also introduce three new fields:

- Orig Node field:
  This field lists the node name for the originating calling agent.
- Term Node field:
  This field lists the node name for the terminating calling agent.
- Debug field:
  This field introduces a debug area that provides space to capture Gateway application information that would be useful to help troubleshoot external network failure conditions. This information will be useful to Nortel Neworks engineers in a later release. The values in SN07 are NIL.

The XPKT301 log is generated for ATM external network connection failures that fail during initial call setup.

The XPKT302 log is generated for ATM external network connection failures that occur for established connections.

Figure 5 XPKT301 and XPKT302 logs

```
RTP7          XPKT301 FEB01 11:44:12 7100 INFO UNI Connection Failure
      Location: SPM 4
      Type: SMG4
      Orig Agent: GRP      BICCINTRA1
      Orig Node: SPM 4
      Term Agent: GRP      BICCINTRA2
      Term Node: SPM 4
      Called Number:          9686930
      CallID: 28705228
      Cause: 31 NORMAL_UNSPEC
      Debug: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      Location: SPM   4  Type: SMG4     Fabric: ATM

RTP7     XPKT302  FEB02 12:26:21 9100 INFO UNI Mid-call Failure
      Location: SLOA 23 3
      Type: MG9K
      Orig Agent: HOST 00 0 00 08    DN 6136211002
      Orig Node: SLOA 23 3
      Term Agent: SLOA 23 3 04 00    DN 6137202340
      Term Node: SLOA 23 3
      Called Number:          7202340
      CallID: 37224882
      Cause: 41 TEMP_FAILURE
      Debug: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      Location: SLOA 23 3   Type: MG9K     Fabric: ATM
```

142.3 Hardware Requirements or Dependencies

None

142.4 Software Requirements or Dependencies

SN07 - feature A00004260 - ATM606 Alarm Banner for SMG4/IW/DPT-SPM.

142.5 Limitations and restrictions

None

142.6 Interactions

Node

142.7 Applicable customer facing sections

Fault Management

- Logs ___X___
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) __X___

142.8 Glossary

Term	Description
New term	Definition

Term	Description

143: Functional Description (FN): A00004449

143.1 Feature name

ACT ID - A00004449 : OP_E911-TRUNK_SUPPORT.

143.2 Description

This feature supports the provisioning of OP and E911 MF trunks for DMSCP SPM for North American market.

E911 emergency service is a distinct product from the Basic 911 emergency service (B911). A DMS100 or DMS100/200 office with the E911 product, known as an E911 tandem, provides centralized emergency service that is capable of serving many end offices. An E911 tandem receives 911 calls from end offices and routes the calls to the appropriate PSAP (Public Safety Answering Point).

This feature enables the provisioning of E911 MF trunk for DMSCP SPM in table TRKMEM.

143.3 Hardware Requirements or Dependencies

None.

143.4 Software Requirements or Dependencies

None.

143.5 Limitations and restrictions

None.

143.6 Interactions

The intent of this activity is to support the provisioning of E911 MF trunks for DMSCP SPM. All the applicable interactions supported by this trunk group for DTC shall be supported on DMSCP SPM.

143.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

143.8 Glossary

Term	Description
MF	Multi Frequency
DMSCP SPM	Digital Multiplex System Call Processing, Spectrum Peripheral Module
E911	Enhanced 911
PSAP	Public Safety Answering Point.

144: Functional Description (FN): A00004500

144.1 Feature name

A00004500 - IN TCAP Messaging on IP

144.2 Description

This document is a Functional Description for the support of the AIN TCAP (Transaction Capability Application Part) messaging in Open Standards Protocol. This activity is provided on the DMS / CS2K - CORE. It is intended to transport the IN messages via the IP fabric - using the Simple Control Transport Protocol[1] (SCTP). Control SOC INW0003 is used to control the IN Messaging over IP functionality.

With the converging of PSTN and IP networks, the existing transfer protocols (e.g.: TCP) has some major limitations. SCTP (Stream Control Transmission Protocol) is designed to overcome the limitations of TCP as well as supporting the extra requirements of PSTN signalling over IP networks.

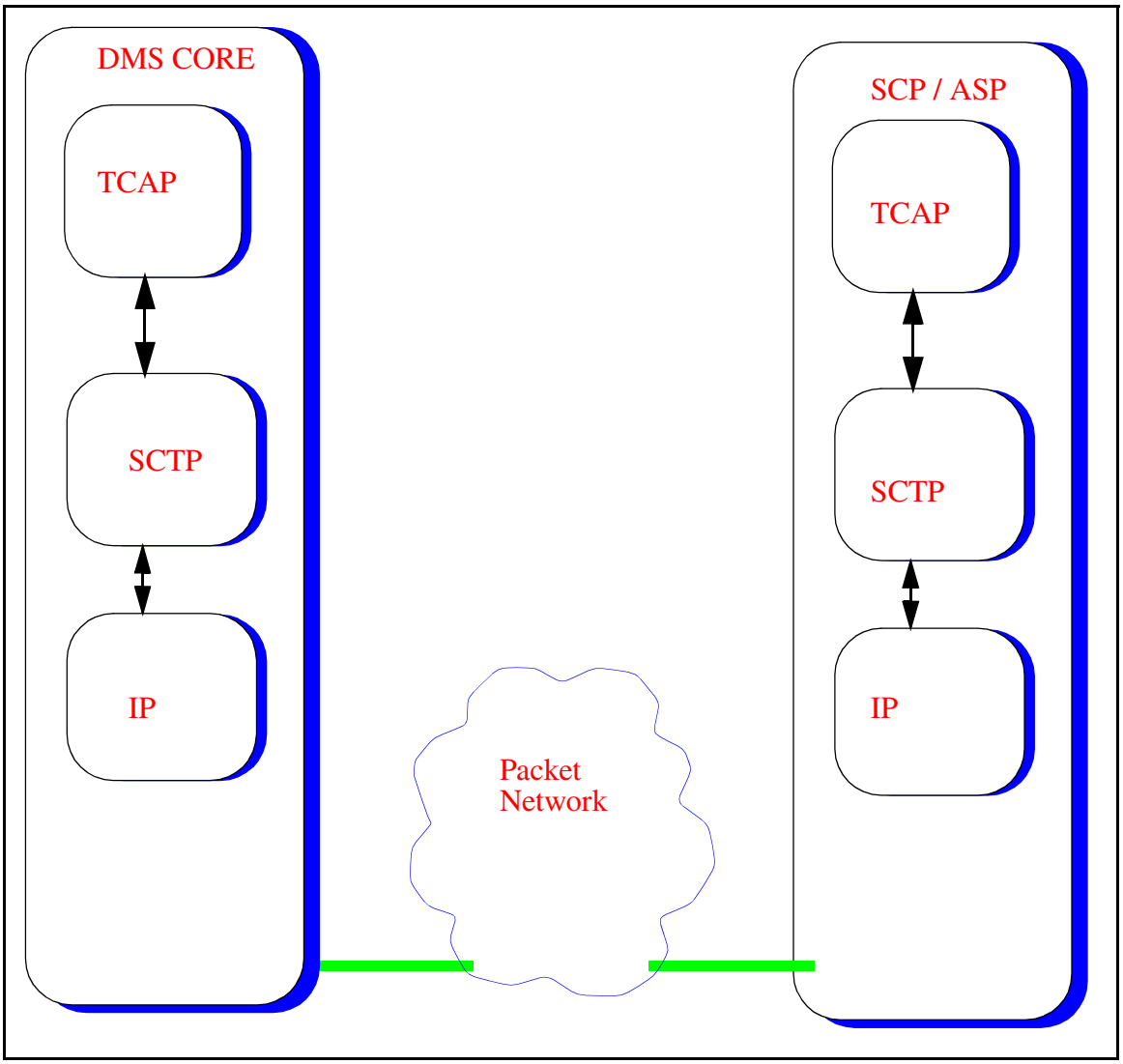
This activity provides the following functionality:

- Supporting AIN (IN) and LNP messages to / from the DMS / CS2K - CORE over SCTP / IP. Please note that the message sets supported for NA markets are only supported.

[1] It should be noted that version 5 RFC is titled “Simple Control Transmission Protocol” and the original RFC2690 is titled “Stream Control Transmission Protocol”. Throughout this document SCTP is “Stream Control Transmission Protocol”.

144.2.1 Functional Behavior

Figure 1 Functional Behavior



The IN TCAP messages will use the SCTP as a transport layer over IP networks. The hardware at the DMS-Core / CS2K may be either EIU or HIOP depending upon the required bandwidth.

Note: HIOP card is available only over XA-CORE platform for high bandwidth IP access.

This feature provides an Interface to the IP network via SCTP, which enables an Advanced Intelligent Network (AIN) Application to access services offered by an Application Service Provider (ASP) located on an Offboard Processor (OP) on an Ethernet / Local Area Network (LAN). The AIN Application uses the services of the Signalling System Number 7 (SS7) Transaction Capability Application Part (TCAP) Application Layer Protocol. This feature also provides the software to manage the SCTP association between the AIN Application in the Computing Module (CM) and the Application Service Provider in the Offboard Processor.

144.2.1.1 TCAP Background

Transaction Capability Application Part (TCAP) provides a common protocol for remote operations across the CCS7 network. The protocol consists of message formatting and contains rules and exchange procedures.

Transactions are functions which control non-circuit related information transfer between nodes in a CCS7 network. The TCAP protocol format is separated into two parts, the *Transaction and Component portions*.

The *Transaction Portion* provides a means of associating messages with a specific Application Process transaction. A transaction consists of one or more messages exchanged between Application Processes on the same or different Network Nodes.

The *Component Portion* ensures that Components are formatted an exchanged properly. A Component is a unit of information within a transaction. The Component Portion utilities provide all TCAP users with a common set of component encoding and decoding procedures. This eliminates the need for individual Applications that implement message formatting procedures thereby reducing development time and minimizing the risk of protocol errors.

A TCAP message consists of a Package containing a Transaction Portion plus one or more Components in any order.

TCAP enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the ***SCCP connectionless service***. An SSP uses TCAP to query an SCP to determine the routing number(s) associated with a dialed LNP, 800, 888, or 900 number. The SCP uses TCAP to return a response containing the routing number(s) (or an error or reject component) back to the SSP. Calling card calls are also validated using TCAP query and response messages.

In the CCS7 layered architecture, TCAP lies between the Application Processes using the CCS7 signalling network and the Signalling Connection Control Part (SCCP) which provides the message transfer capabilities.

Since IN TCAP messaging uses connectionless service, IN TCAP messages can be embedded in a transport layer function and transported across IP.

144.2.1.2 SCTP Background:

The limitations of TCP as a transport protocol for SS7 was the direct motivation for the using of SCTP as a new transport protocol. SCTP is a new IP transport protocol, which exists at an equivalent level with TCP and user datagram protocol (UDP) and which currently provides transport layer functions to many Internet-based applications. SCTP has been approved by the IETF as a proposed standard, and is specified in RFC 2960. Nortel Implementation of the SCTP transport protocol on the CORE was implemented by feature activity A59023997.

The SCTP transport service can be fragmented into several functionalities:

1. **Association Startup and Teardown** --An association is initiated by a request from the SCTP user. A cookie mechanism is employed during the initialization to provide protection against security attacks.
2. **Sequenced Delivery within Streams** --The SCTP user can specify at association startup time the number of streams to be supported by the association.
3. **User Data Fragmentation** --SCTP supports fragmentation and reassembly of user messages to ensure that the SCTP packet passed to the lower layer conforms to the path multiple-tenant unit (MTU).
4. **Acknowledgement and Congestion Avoidance** --SCTP assigns a transmission sequence number (TSN) to each user data message (fragment or unfragmented). The receiving end acknowledges all TSNs received, even if there are gaps in the sequence.
5. **Chunk Bundling** --The SCTP packet delivered to the lower layer consists of a common header followed by one or more chunks. The following table depicts the general structure of an SCTP packet:
6. **Packet Validation** --A mandatory verification tag field and a 32-bit checksum field are included in the SCTP common header.
7. **Path Management** --The SCTP path-management function chooses the destination transport address for each outgoing SCTP packet based on the SCTP user's instructions and the currently perceived reachability status of the eligible destination set.

The feature activity that implemented the SCTP stack on the core provides the above SCTP advantages and a framework for developing an Application Program Interface.

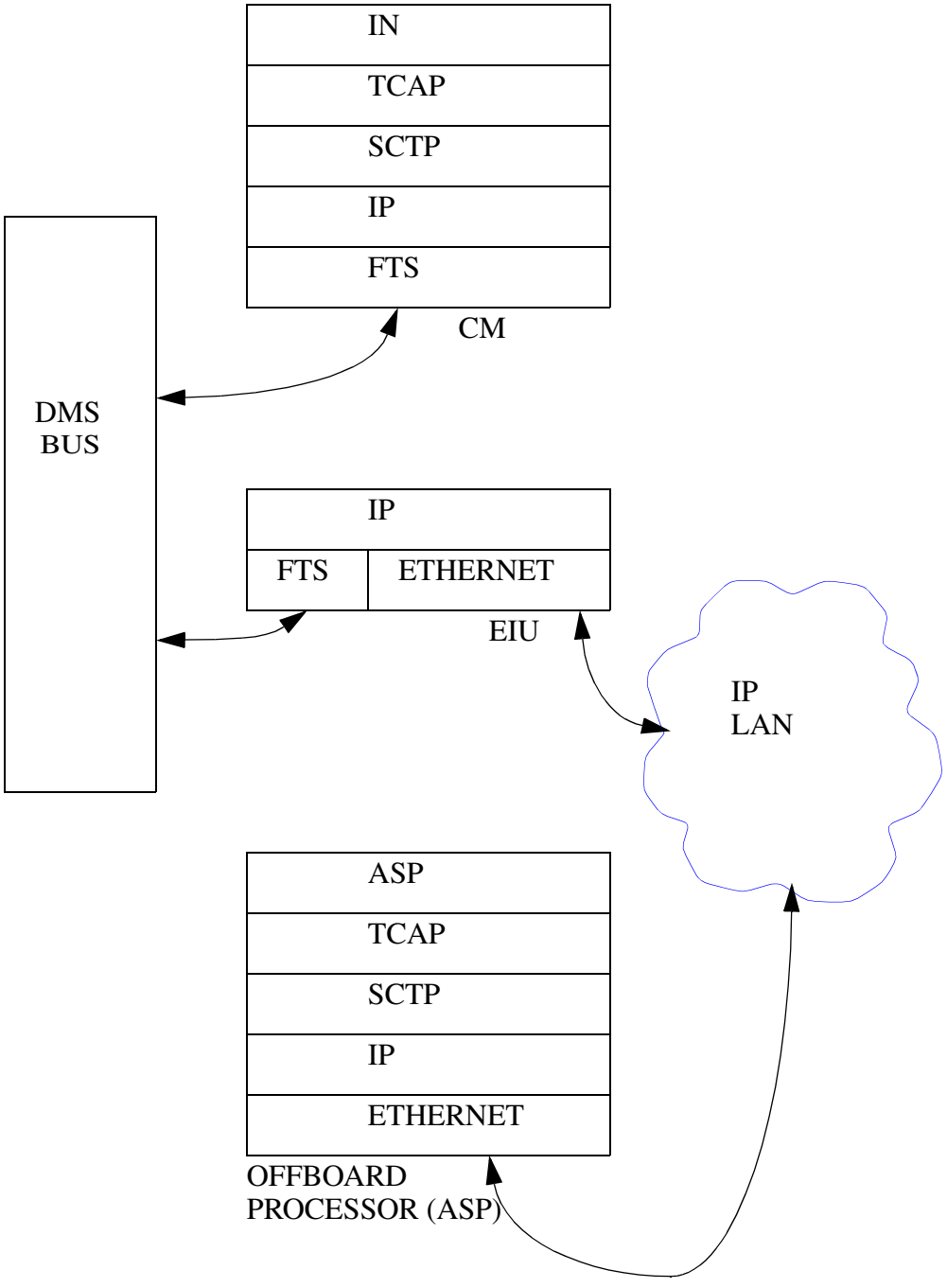
144.2.1.3 System Flow

Following Figure (Figure 2, on page 1786) shows the message flow between the AIN Application (located in the CM) and the ASP (connected on an Ethernet LAN). An IN/TCAP message is encoded and passed to SCTP for delivery to the ASP.

The SCTP transport hands over the TCAP Message to IP. IP forwards the Message to an Ethernet Interface Unit (EIU) through the Supernode Frame Transport System (FTS).In the EIU, the Message is received by FTS which passes it on to IP.

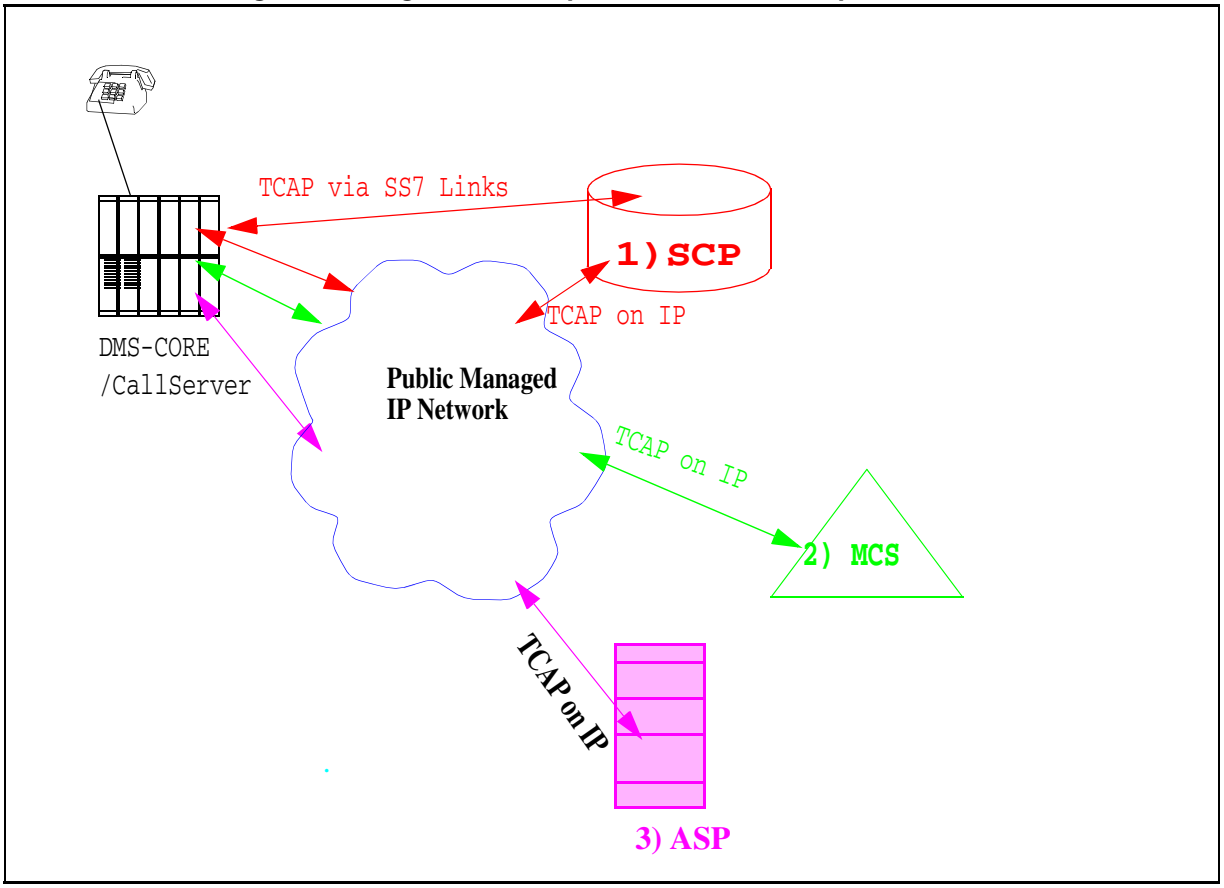
IP delivers the message to the Ethernet LAN which forwards it to the Appropriate Offboard Processor. On the ASP, the message is delivered to IP which passes it on SCTP transport which hands it over to the Application Service Provider. A Response Message from the ASP to the AIN Application follows the exact same path but in reverse order.

Figure 2 System Flow using EIU on DMS



Below is a diagrammatic representation of different nodes that could use the SCTP/IP interface. Figure 3, on page 1787

Figure 3 Diagrammatic representation of Examples

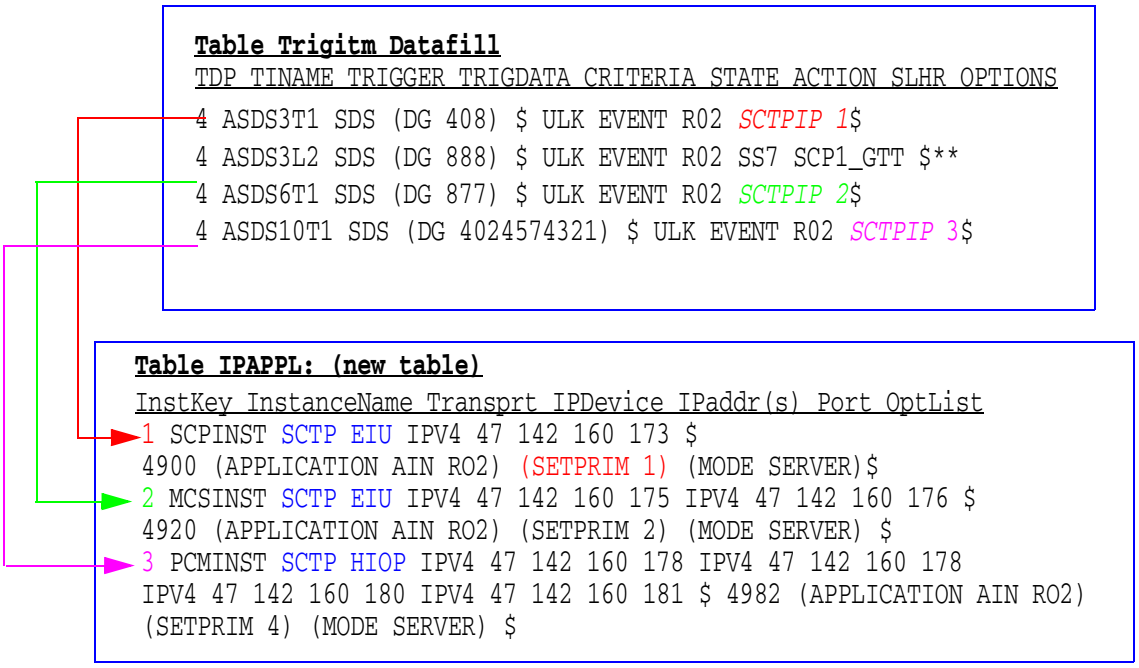


144.2.2 Provisioning

Only the TRIGITM model of subscription supports IN messaging over IP. The TRIGGRP model of subsrcription is not supported by this activity. Following datafill is required to allow IN messages over IP.

144.2.2.1 Table IPAPPL

Figure 4 Table Control Changes



** Note that SCP1_GTT points to the existing GTT for SS7 translations.

New **Table IPAPPL** datafill provides separation of various connections to the DMS. The use of SCTP transport requires that the application store the specific remote IP addresses and local Port number. Therefore table IPAPPL is datafilled in order to provide these details.

InstKey is datafilled in order to map this instance with an internally assigned instance number. This field is the unique key to the tuple. This field is used in the tuples in trigitm that uses SCTP as transport.

InstanceName is datafilled in order for the telco personnel to be able to distinguish one connection from the other.

Transprt is datafilled in order to classify the instance to which transport protocol be used. Currently the table will support SCTP functionality ONLY.

IPDevice is datafilled to indicate which IP interface hardware will be used. This table currently supports EIU and HIOP.

IP addresses (upto 4 addresses) are allowed in one instance tuple. This may be used to support multihoming. Please refer to Section “144.6.1 MultiHoming” on page 1792. The first IP address in the list will be used as the primary address. IPV4 type IP addresses are supported.

Port Number is the local port number at which the DMS-Core will expect to receive messages from this instance. (Note that the remote port is received during the INIT message from the far-end). Valid range of Source port allowed to be configured on the CORE is from **4900 to 4982**.

The IN Messaging application using SCTP allows for multiple associations to an ASP on the same IP address, but using a different port number. Care must be taken to datafill a different portnumber in the source port field on the DMS Core. This method may be used by service providers that use the GTT or SSN in SS7 for translating to different applications.

OptList field may be datafilled with "**SETPRIME**" to set any of the IP address in an instance to be used as to set the primary destination address. The field is designed so as to support any future enhanced options. The setprime option is mandatory for AIN on SCTP.

This option has been used along with the position of the ipaddress as in above examples,(Please refer to "Figure 4 Table Control Changes" on page 1788.), where in the SCTPINST the ipaddress "`47 142 160 173`" is set as the primary IP address.

Optlist sub-field "**APPLICATION**" can be datafilled to specify the application eg:AIN. This field is further augmented by **Msgset** eg: R01, R02. The application option is mandatory for AIN on SCTP.

Optlist sub-field "**mode**" is currently defaulted to the SERVER mode for AIN on SCTP. The IN TCAP messaging on IP requires the SCTP application runs in SERVER mode on the CORE.

Optlist sub-field "**multihoming"** is used to specify if the remote node supports multihoming. This option is currently only supported on the HIOP ipdevice.

144.2.2.2 Table Trigitim

In the trigitm model of AIN, the Trigitm table stores the trigger item definitions. Each trigger item also contains the Service Logic Host Route, which currently allows SS7 as transport and the datafill of a GTT per trigger item. The SLHR entry for each trigger specifies the ASP (Application Service Provider) destination (instance) to which this trigger query / messages will be sent.

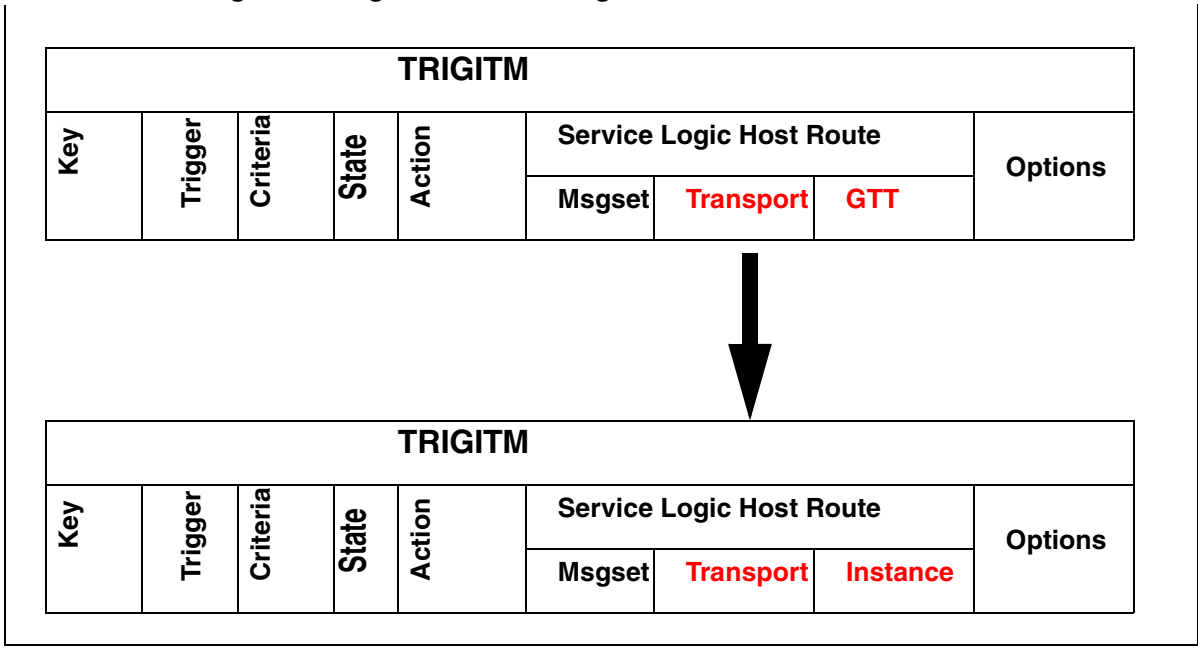
When the transport mechanism is changed to SCTP, this entry needs to be changed for transport and GTT fields for each trigger item. It should be replaced with the transport as SCTP with an instance number.

Field **SLHR's** sub-field transport in table trigitm is modified to allow the following transports:

- TCP (Lab-only)
- SCTP
- SS7

The Table trigitm changes are shown below.Please refer Figure 5, on page 1790

Figure 5 Trigitm Datafill Changes



144.3 Logs and OMs

New OMS are added by this activity. Please refer to the OMs section(optpf) of this document for new OMs introduced by this activity.

144.4 Hardware Requirements or Dependencies

The DMS core usually carries out most of the IP traffic over EIU. CS2K assumes XA-Core and may use EIU, but most CS2Ks are equipped with HIOP card for higher bandwidth IP traffic. This feature will support IN messages over IP for both EIU as well as HIOP. The bandwidth limitations posed by EIU in general will apply. For detail Engineering Information please refer to EI section(optei) of this document.

From the IN Messaging application perspective, it will serve different instances using HIOP and EIU simultaneously on the same switching core. However, Please refer to appropriate hardware procedures when operating with HIOP card as well as EIU peripheral on the CORE.

Note: The CORE platform can either be an XA-Core or Brisc.

144.5 Software Requirements or Dependencies

Limit SOC INW0003 will be used with this functionality. The limit in SOC must be set to atleast the number of tuples datafilled in the table IPAPPL. For more instances to be added in the table IPAPPL limit of this SOC must be increased by additional number of tuples.

Initial limit of this SOC will be zero. When limit is zero no tuples can be added to the IPAPPL table. Tuples can be added only when a non-zero limit is set. Maximum limit that can be set will be 32.

Adding, deleting and modifying do not impact the value of the SOC limit. The value of the current usage counter is however changed accordingly

If SOC limit is reduced after adding tuples, IN messaging on IP functionality will not be affected, but no further tuples will be allowed to be added to the table IPAPPL.

If the SOC limit set is less than or equal to the current number of tuples in table IPAPPL, no further tuples will be allowed to be added to the table IPAPPL. An attempt to add a tuple will result in the following message being displayed:

“SOC option INW0003: Usage limit exceeded”
“ERROR: Table IPAPPL is under SOC usage control.”
“ACTION: SOC Limit must be increased before adding further tuples.”

144.6 Limitations and restrictions

For Engineering Information on the

- bandwidth,
- Message Size,
- SCTP/IP Link Messaging Rate,
- Normal Throughput,
- Failure ThroughPut,
- Link Capacity as Call Attempts Per Hour, Messages Per Second and others,

Please refer to the EI section of this Document.

For EIU and HIOP being shared between various IP applications, For EIU configurations across subnets, etc. please refer to specific hardware guidelines

as well as the EI documentation referring to the bandwidth allotted to application sharing the hardware.

144.6.1 MultiHoming

Mutlihoming is not supported for IN Messaging using the SCTP on EIU configuration. Multihoming is supported by SCTP on the HIOP configuration.

144.6.2 Simultaneous HIOP and EIU

Please refer to appropriate hardware procedures when operating with HIOP card as well as EIU peripheral on the CORE.

144.7 Sample EIU Configurations

Please refer to NTP 297-8991-910, DMS-100 Family Ethernet Interface Unit User Guide TELECOM12 Standard 03.01 August 1999, EIU documentation(LANCOMM) for recommended EIU configurations.

144.8 Interactions

Tools such as AINTRACE and TRAVER will be supported to be able to refer to SCTP instances for the transactions using this transport.

144.9 Applicable customer facing sections

Fault Management	
Logs	_X_____
Alarms	_ ___
Configuration	
Data Schema	__X____
User Interface	__X____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	__X____

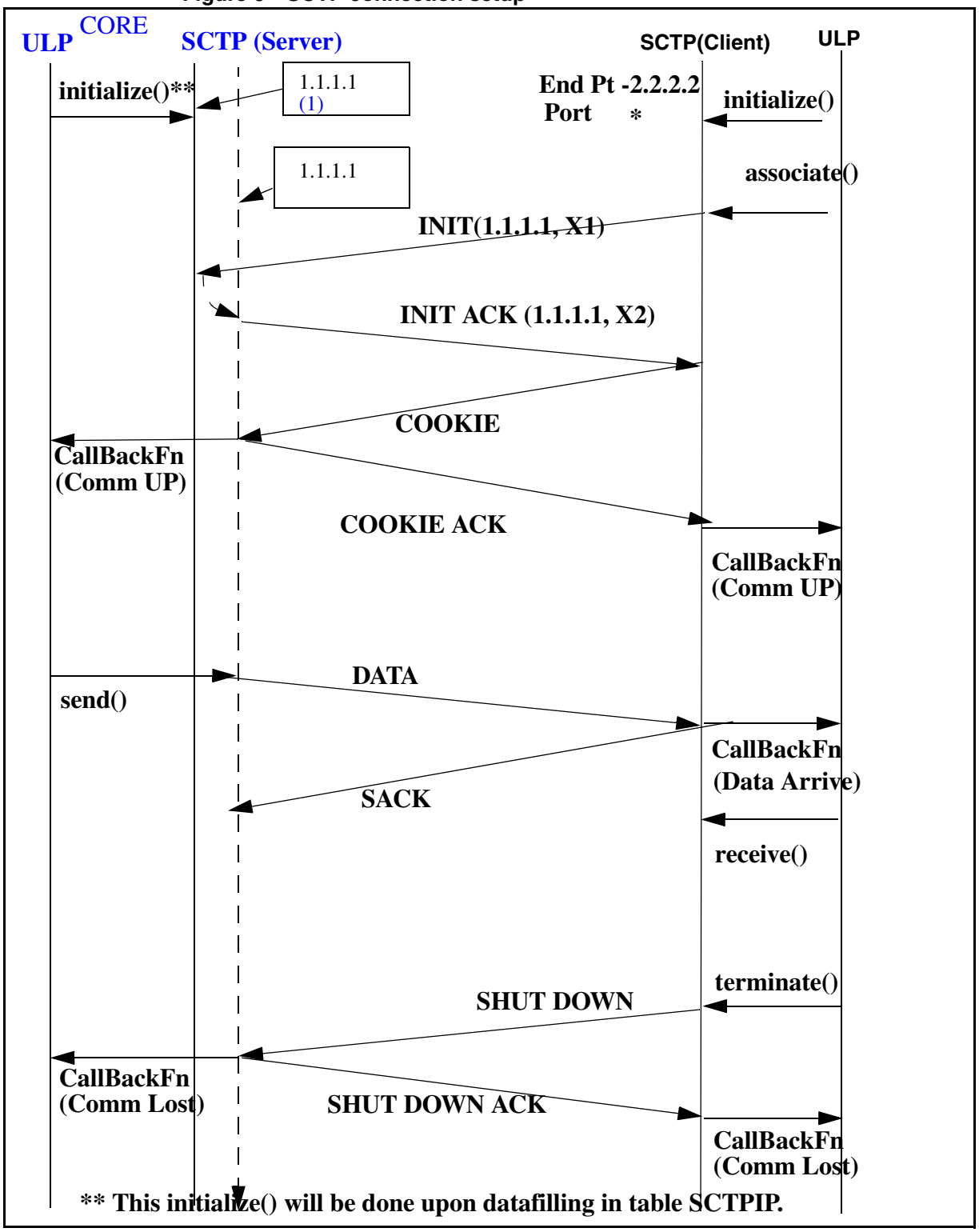
144.10 Glossary

Term	Description
New term	Definition
ASP	Application Service Provider
CS2K	Call Server 2000
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
PSTN	Public Service Telephone Network
AIN	Advanced Intelligent Network
IP	Internet Protocol
IN	Intelligent Networks
CCS7	Common Channel Signalling 7
TCAP	Transaction Capabilities Application Part
SCCP	Service Connection Control Part
HIOP	High Performance I/O Peripheral
MCS	Multimedia Call Server
EIU	Ethernet Interface Unit
FTS	Frame Transport System

144.11 Appendix A

144.11.1 Sample SCTP instance setup

Figure 6 SCTP connection setup



145: Functional Description (FN): A00004554

145.1 Introduction

SDM FX System Backup Enhancements

This feature (A00004554) implements scheduling of the system image backup to both SDM tape drives and the capability to configure the "Backup Required Alarm".

145.2 Purpose

The following are the purposes of this activity.

- Automate the backup process and allow the user to schedule the backups for each drive (Dat 0 and Dat 1).
- Allow the user to Configure "Backup required "alarm, so that he can Enable/Disable the backup required alarm.

145.3 Subject Matter Experts Agreement List

Table 1 Table 1 Agreement List

Name	Role/Title	DRU,ArchID, Module, or Functional Area	Mandatory Reviewer (Y/N)
Reid,Bob	Manager/	SDM Evolution and Architecture	Y
Feijun Ma	FX Base Architect	SDM Base	Y

145.4 Problem Symptoms

In the existing SDM environment, if somebody wants to take the backup of the system, he has to go to the sdmmtc level and issue the backup command manually. There is no method avilable to take the backup automatically. So, the customer needs a method to schedule the backup.

Currently whenever a change happens to the SDM environment, like patch applying, logical volume changes, etc.. , a “Backup Required” alarm will be triggered. To clear this alarm the customer needs to issue "Backup clear" command or initiate a system backup. This constitute a heavy load for the cutomer.

145.5 Requirements

The existing backup code is designed only to support adhoc backup execution. No scheduling possible for backups. The Requirements for this activity are the Following

- A utility to schedule backup to write avilable tape drives on the SDM. This utility will provide a mechanism to automate the backup process in a scheduled interval.
- An option to configure the "Backup required" alarm. This will allow the user to Enable/ Disable the "Backup required" alarm.

145.6 Description of Code Churn

This will be a small tool for scheduling the backup and configure the "Backup Required" alarm. By implementing this tool, the customer will have an option to automate this backup process. The tool will allow the user to schedule each drive separately for taking the backups.

This tool will provide an option to configure the “Backup Required” alarm. It will have various options like, Disable (or) Enable this alarm, show only when backup fails, etc...

145.7 Scheduling Interface

This is the interface the user employs to add new schedules and disable or modify existing schedules.

The options provided by this interface are:

- Schedule Dat 0
- Schedule Dat 1

These two options allow the user to add new schedules and disable or modify an existing schedule.

- List Schedules

The List Schedule option will show all the schedule details for each drive.

145.8 Other features

The other features are:

- Incase of a failure it will raise a "Backup Failure "alarm.
- It won’t start the system image backup if a “Backup Failure” alarm exists.
- Necessary customer logs will be generated during the execution of the scheduled backup.
- It will support the existing way of taking the backup also.

145.9 Alarm Configure Interface

This is an interface for setting the “Backup Required” alarm status. The options provided by this interface are:

- Disable the “Backup Required” alarm
- Enable the “Backup Required” alarm
- List the Current status of “Backup Required” alarm

Note: The existing backup “InProgress” alarm will be there even if the “Backup Required” alarm status is Disabled.

145.10 Screen Captures for the Main Menus

145.10.1 Main Menu

```
***    ******************************************
***            SuperNode Data Manager
***
***       System Image Backup and Restore Menu
***    ******************************************
***
***
***  0. Exit
***
***  1. Help
***
***  2. Backup & Restore System image
***
***  3. Alarm Configure
***
***
***
***
***  Please enter your selection (0 to 3) ? ==>
```

145.10.2 Backup and Restore Menu

```
***    ******************************************
                    ***            SuperNode Data Manager
                    ***
                    ***       System Image Backup and Restore Menu
                    ***    ******************************************
                    ***
                    ***
                    ***  0. Exit
                    ***
                    ***  1. Previous Menu
```

```
***
***   2. Create a System Image on Tape (S-tape)
***
***   3. List Contents of the System Image Tape (S-tape)
***
***   4. Restore Files from the System Image Tape (S-tape)
***
***   5. Schedule Backup
***
***   Please enter your selection (0 to 5) ? ==>
```

145.10.3 Scheduled Backup Menu

```
***     ******************************************
***             SuperNode Data Manager
***
***         Schedule Backup Configure Menu
***     ******************************************
***
***
***   0. Exit
***
***   1. Previous Menu
***
***   2. Schedule Dat 0
***
***   3. Schedule Dat 1
***
***   4. List Backup Schedules
***
***
***   Please enter your selection (0 to 4) ? ==>
```

146: Functional description (FN): A00004568

146.1 Feature name

H.323 NA Network CAS Tunneling - A00004568

146.2 Description

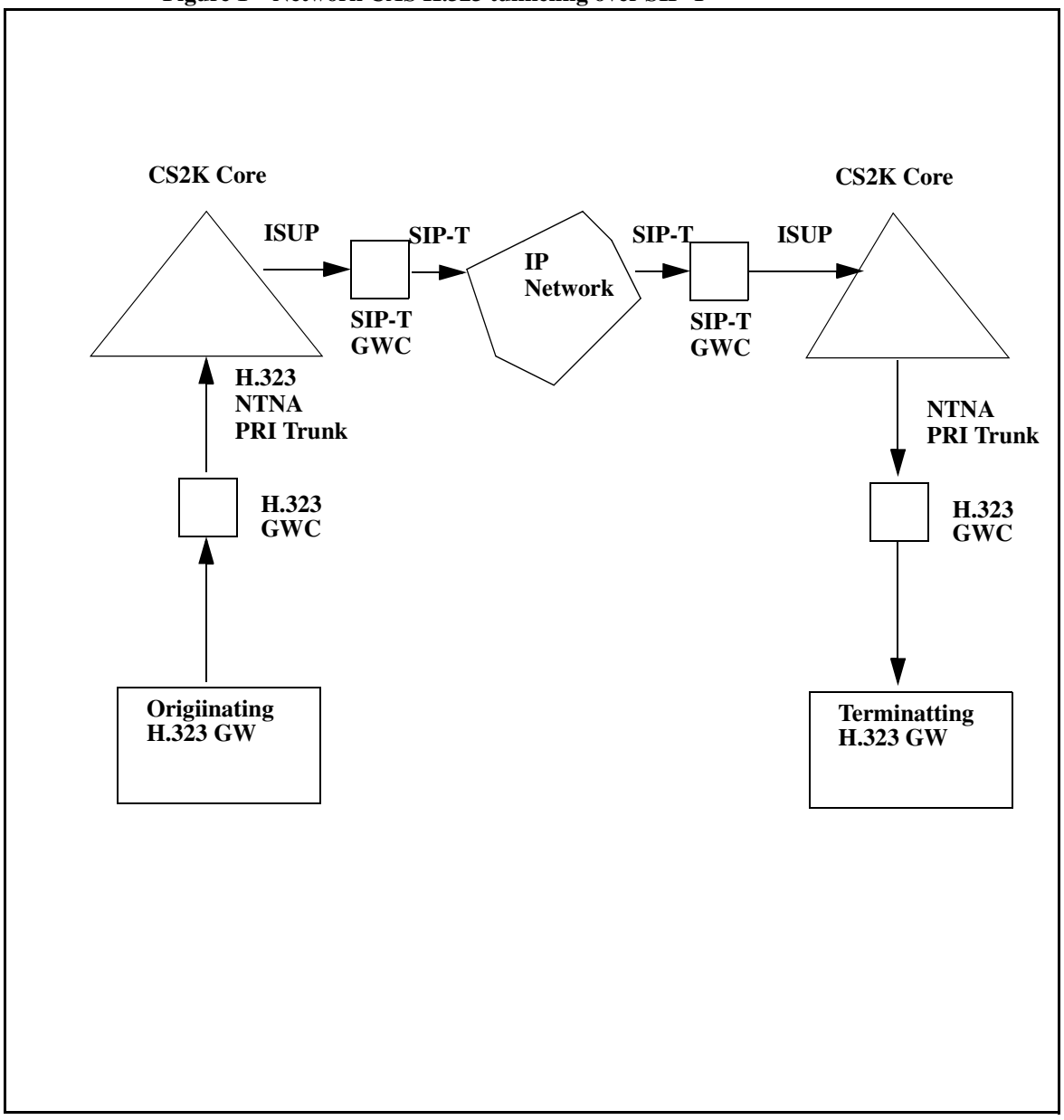
This activity provides the functionality to support the tunneling of ANSI Call Associated (CAS) messages between 2 CS2Ks via SIP-T, in support of the H.323 protocol.This activity provides the functionality to support the tunneling of ANSI Call Associated (CAS) messages between 2 CS2Ks via SIP-T, in support of the H.323 protocol.

Support is required both for North American ANSI and International ETSI message protocols, this activity covers the development required in the CS2K core for Network ANSI CAS, activity A00002358 covers ETSI.

The activity is part of a suite of features which support H.323 on the Succession CS200 Call Server. A00002206 provides the equivalent functionality for NA nodal CAS calls, and A00002261 the functionality for NA nodal and network NCAS (Non CAS) calls.

The following diagram shows the network configuration. A CAS message is routed from the Originating GW via a GWC to the core at the originating node. The message is then tunneled across the network via SIP-T to the Terminating Node where it is tunneled in a PRI Facility message to the terminating GW.

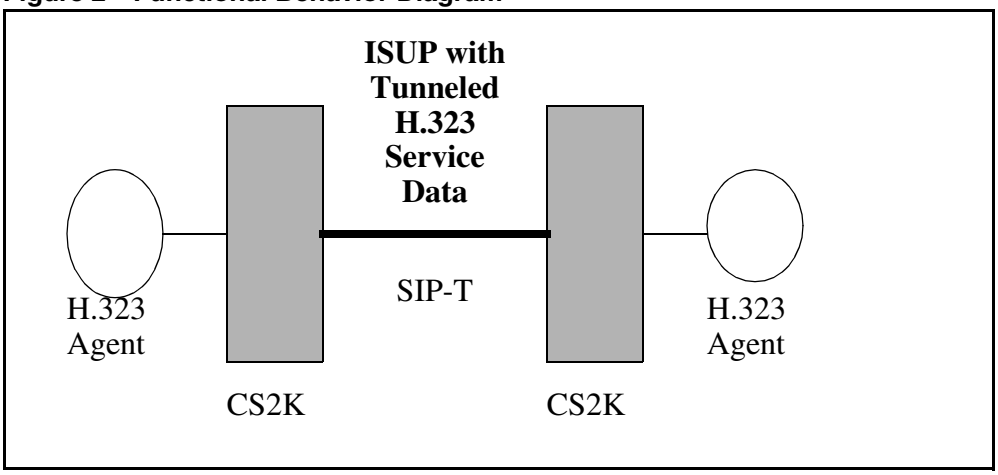
Figure 1 Network CAS H.323 tunneling over SIP-T



146.2.1 Call Processing Overview

This feature provides a mechanism to allow 2 H.323 agents to tunnel end to end service data to each other when they are interworked through the SIP-T protocol. The H.323 payload is tunneled within ISUP messages, which is in turn tunneled within the SIP-T messages, hence the references to ISUP, even though SIP-T is the only network protocol supported.

Figure 2 Functional Behavior Diagram



For ANSI, when a H.323 message is received from a H.323 gateway (GW) by the Gateway Controller (GWC) it is mapped to a NTNA PRI Q.931 message and sent via a H.323 NTNA PRI trunk signaling channel to the CS2K core for processing.

For CAS messages, the GWC will extract the tunneled payload from the UUIE in the H.323 message and include it in the Facility Information Element (FAC IE) of a corresponding NTNA PRI message. If the payload is destined for a local CS2K it is routed to the appropriate NTNA PRI trunk per feature A00002206. If the payload is destined for a gateway at a remote CS2K the payload is then extracted from the PRI message and tunneled within a ISUP message to the destination switch using the SIP-T protocol via the IP network

At the terminating switch the reverse occurs. The payload received within the ISUP message is tunneled within the FAC IE of a NTNA PRI message and sent to the GWC via a NTNA PRI H.323 trunk signaling channel, which then tunnels the payload within the UUIE of a H.323 message via the appropriate gateway.

This activity covers the development within the CS2K core to enhance the PRI/ISUP interworking to tunnel the H.323 payload within a appropriate ISUP parameter to the destination CS2K where the payload is extracted and presented in such a way that the existing PRI functionality developed by A00002206 will tunnel that payload and route it to the terminating GW.

146.2.2 Tunneling of H.323 Data

- The tunneling of H.323 data within an ISUP message can be divided into two components
  Mapping PRI Fac IE's to ISUP Parameters
- **The Segmentation of Large Payloads**

146.2.2.1 Mapping PRI Fac IEs to ISUP Parameters

This component covers determining that there is H.323 data to tunnel, creating the appropriate ISUP parameter and adding the H.323 data. At the terminating CS2K, determining there is H.323 data tunneled and ensuring that existing PRI functionality tunnels the data to the destination gateway. The following list shows the mapping of PRI to ISUP messages that can tunnel the data (the SC_X messages are sent from the GWC, SCP_C to the GWC):

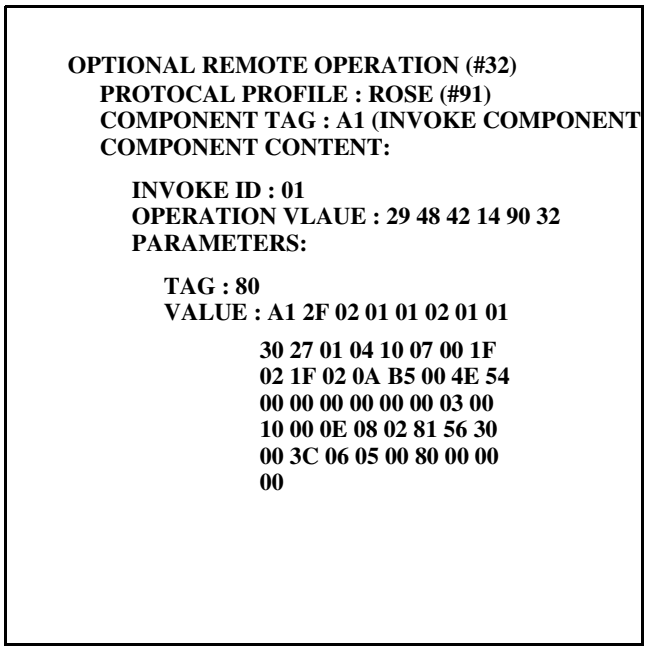
- Setup (maps to SCP_X_Origination/SCP_C_Origination) -> ISUP IAM
- Alerting (maps to SCP_X_Alerting/SCP_C_Alerting or SCP_X_Progress/ SCP_C_Progress) -> ISUP ACM
- FAC (maps to SCP_X_FAC/SCP_C_FAC) -> ISUP FAC
- Connect (maps to SCP_X_Progress ppi=Connect/SCP_C_Progress ppi=Connect) -> ISUP ANM
- Release (maps to SCP_X_Release/SCP_C_Release) -> ISUP REL

Note: for messages with large payloads the “long” version of the above SCP messages will be used.

In each of the listed ISUP messages the H.323 payload is tunneled in the ISUP Remote Operation (RO) parameter. The H.323 payload is tunneled within the Value field of the RO.

The following figure shows the structure of an RO parm containing a H.323 payload

Figure 3 Format of ISUP RO Parameter for H.323 Tunneling



146.2.2.2 The Segmentation of Large Payloads

The originating H.323 GWC will segment the payload based on a preset maximum, currently 180 bytes from the GW. The first 180 bytes is sent in the applicable PRI message. This data is then tunneled in the RO of the appropriate ISUP message. The remainder of the data is sent in a PRI FAC message. This data is tunneled in the RO of the ISUP FAC. For this case the GWC controls segmenting the payload and restoring it at the remote office.

The CS2K will segment the payload when it receives greater than 100 bytes. For the PRI SETUP message the first 100 bytes is tunneled in the RO of the ISUP IAM. The remainder of the data is tunneled in the RO of the ISUP FAC. This allows room for the other optional parameters of the ISUP IAM. For all other PRI messages with greater than 115 bytes the data is tunneled in multiple ROs of the applicable ISUP message. For both of these cases the CS2K controls segmenting the payload and restoring it at the terminating office.

146.3 Hardware requirements

There are no hardware requirements specifically for this feature. This feature applies to any H.323 North American GateWay currently supported.

146.4 Software Requirements or Dependencies

A00002206 - H.323 NTNA PRI

A00001895 - H.323 Base Application

146.5 Limitations and restrictions

None

146.6 Applicable customer facing sections

Fault Management

- Logs _N/A__
- Alarms _N/A_____

Configuration

- Data Schema _N/A_____
- User Interface _N/A_____
- Element Management _N/A_____
- Security _N/A_____
- Service Order _N/A_____
- Office Parameters _N/A____

Accounting (includes AMA billing) _N/A_____

Performance (includes operational measurements) __N/A____

146.7 Glossary

Term	Description
ACM	Address Complete Message
ANM	Answer Message
ANSI	American National Standards Institute
CAS	Call-Associated Signaling
CS2K	Call Server 2000

ETSI	European Union Telecommunications Standards Institute
FAC	Facility
GW	Gateway
GWC	Gateway Controller
H.323	Packet based multimedia communications systems protocol
IAM	Initial Address Message
IE	Information Element
ISUP	ISDN User Part
NCAS	Non-Call-Associated Signaling
PRI	Primary Rate Interface
REL	Release Message
RO	Remote Operations
SIP-T	Session Initiation Protocol - Telecommunications
SS7	Signaling System #7
TCAP	Transaction Capabilities Application Part
UUI	User to User Information
UUIE	User to User Information Element

147: Functional description (FN): A00004713

147.1 Feature name

1+1 Speedometer Support

147.2 Description

This feature updates the Speedometer to support 1+1 configuration in release CSP20. It provides capacity prediction for 1+1 configuration within the accuracy target of +/-10% when the utilization is above 15%. It allows the users to change the value of Rated Power to 1 through table OFCENG.

147.3 Hardware Requirements or Dependencies

N/A

147.4 Software Requirements or Dependencies

N/A

147.5 Limitations and restrictions

None

147.6 Interactions

In the releases without this feature, the smallest value of Rated Power allowed is 2. In this feature, the users are able to modify the value of Rated Power to the smallest of 1.

147.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	X

Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

148: Functional description (FN): A00004772

148.1 Feature name

Destination ACD DN MIS Reporting

148.2 Description

This activity will allow reporting of the Dialed Digits of the Destination ACD Group in the ACDMIS CallOffered, CallAnswered, CallAbandoned, CallBlocked, RemoteOffered, RemoteAbandoned and CallNetworkAnswered messages on an office-wide basis. The Dialed Digits of the destination ACD Group that the call was CTI redirected to or immediate overflowed to, will replace the Original Dialed ACD DN in these messages.

Currently the original Dialed DN is reported in the CallOffered, CallAnswered, CallAbandoned, CallBlocked, RemoteOffered, RemoteAbandoned and CallNetworkAnswered ACDMIS messages. This is the DN that was dialed to enter the ACD environment. As long as the call remains in the ACD environment, this DN is preserved and reported in the ACDMIS messages. This DN is used by Call Center customers for generating various statistics.

This activity will provide new optional functionality (via SOC) for CTI redirected calls and Immediate overflowed calls that will report the Dialed Digits of the Destination ACD Group that the call was redirected to or immediately overflowed to. This information will be carried in the existing ACD DN field of the ACDMIS messages. There will be no change required to the ACDMIS Protocol.

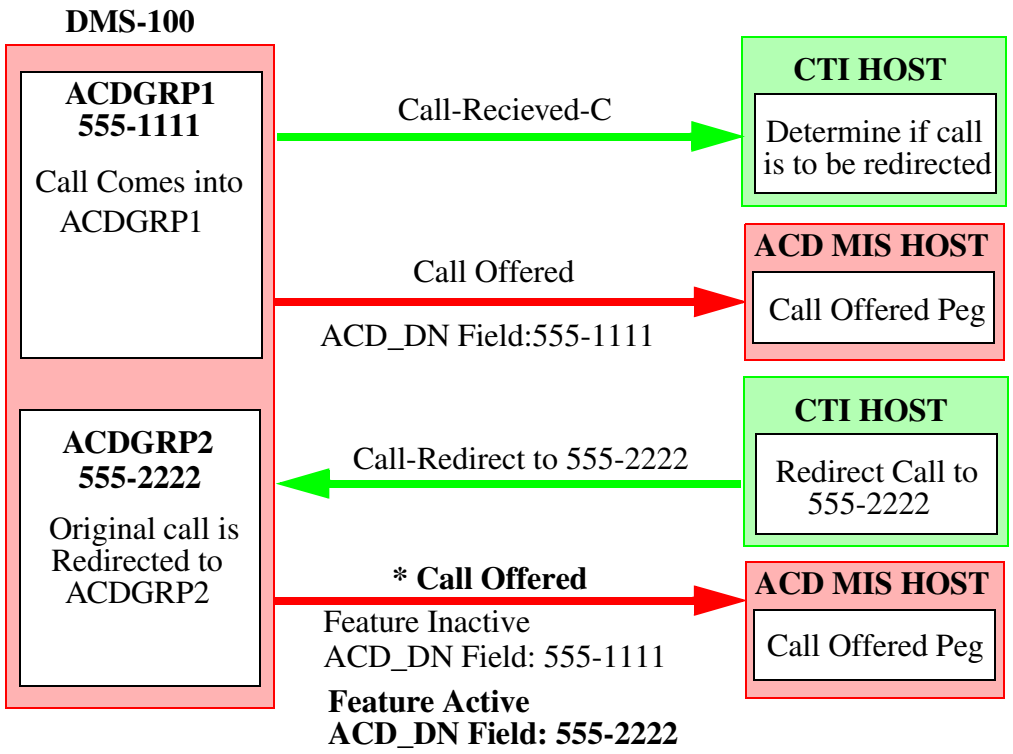
148.2.1 Supported ACD MIS Protocol Versions

Tuples in the ACDMISPL table on the DMS contain a field named PROTOCOL which uniquely identifies the version of ACD MIS messages that will be used for the session.

This activity will not require a new ACD MIS Protocol version. This activity will be supported by the existing ACD MIS Protocol versions BCS31 through BCS43 and newer.

148.2.2 Destination ACD DN MIS Reporting Functionality

As illustrated below, when activated via SOC, this activity will report the destination DN in the ACD_DN field of the CallOffered, CallAnswered, CallAbandoned, CallBlocked, RemoteOffered, RemoteAbandoned and CallNetworkAnswered ACD MIS messages for immediate overflowed and CTI redirected calls. If this functionality has not been activated via SOC, the Original Dialed DN will be populated in the ACD_DN field of the affected ACD messages.



** Diagram illustates CallOffered ACD MIS Message, however the same functionality will apply for the CallAnswered, CallAbandoned and CallBlocked etc. ACD MIS messages.*

148.2.3 ACD Call Offered Message Example

For this activity the ACD_DN fields of the CallOffered, CallAnswered, CallAbandoned CallBlocked, RemoteOffered, RemoteAbandoned and CallNetworkAnswered ACD MIS messages will be affected.

In this example the fields of ACDCallOffered message are shown with the affected ACD_DN field highlighted:

ACDCallOffered Message:

CALL_OFFERED_SGRP_DN
CALL_OFFERED_SGRP_DN_COUNT
CALL_OFFERED_DGRP_DN
CALL_OFFERED_DGRP_DN_COUNT
CALL_OFFERED_TOD
CALL_OFFERED_CSTATUS
CALL_OFFERED_NUMICQ_P
CALL_OFFERED_NUMICQ_L
CALL_OFFERED_ACD_DN
CALL_OFFERED_ACD_DN_COUNT
CURRENT_P_CALL_Q_WAIT_TIME
CURRENT_L_CALL_Q_WAIT_TIME
CALL_OFFERED_DGRP_AGPOSNID
CALL_TRANSFER_STATUS
CALL_TRANSFER_DIFF_CUST_GROUP
CALL_XFERING_PARKING_DN
CALL_XFERING_PARKING_DN_CNT
CALL_XFERING_PARKING_AGPOSNID
CALL_OFFERED_CALLING_NUMBER
CALL_OFFERED_CALLING_NUMBER_CNT
CALL_OFFERED_RECALL_DN
CALL_OFFERED_RECALL_DN_CNT

148.2.4 Software Optionality Control (SOC)

Order code ***ACD00102 - "Destination ACD DN MIS Reporting"*** provides Destination Dialed Digits reporting via the ACD_DN field of the CallOffered, CallAnswered, CallAbandoned and CallBlocked ACD MIS messages on a office-wide basis. When ACD00102 SOC is in the IDLE state, the ACD_DN field for the above stated ACD MIS messages will reflect the Orignal Dialed DN as it did prior to this activity.

148.3 Hardware Requirements or Dependencies

Not Applicable

148.4 Software Requirements or Dependencies

Not Applicable

148.5 Limitations and restrictions

- This activity will be supported by the existing ACD MIS Protocol versions BCS31 through BCS43 and newer.
- This activity only pertains to the CallOffered, CallAnswered, CallAbandoned, CallBlocked, RemoteOffered, RemoteAbandoned and CallNetworkAnswered ACD MIS messages.

148.6 Interactions

No new interactions are introduced by this activity. However it should be noted that when this new functionality is activated the Original Dialed DN will no longer be provided in the ACD_DN field of the affected ACDMIS messages on an office-wide basis for CTI redirected and immediate overflowed ACD calls. Conversely, when not activated the Original Dialed DN will be provided in the ACD_DN field of the affected ACDMIS messages.

148.7 Applicable customer facing sections

Fault Management

- Logs __N/A__
- Alarms __N/A__

Configuration

- Data Schema __N/A__
- User Interface __N/A__
- Element Management __N/A__
- Security __N/A__
- Service Order __N/A__
- Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

148.8 Glossary

Term	Description
ACD	Automatic Call Distribution
BCS	Batch Change Supplement
CTI	Computer Telephone Integration
DN	Directory Number
MIS	Management Information System

149: Functional Description (FN): A00004859

149.1 Feature name

T1400 to N240 migration procedure

149.2 Description

The intent of this document is to describe the procedure to be used to migrate the CMT, MG9KEM and MG9KMT element managers from the existing T1400 platforms to the new COAM frame using Netra 240 High Availability servers.

This document contains all the necessary steps to accomplish the following:

- Migrate CMT SN07(T1400) to CMT-COAM SN07 (N240)
- Migrate MG9KEM SN07 (T1400) to MG9K-COAM SN07 (N240)
- Migrate MG9KMT SN07 (T1400) to MG9K-COAM SN07 (N240)

Refer to individual sections for the details. The user is referred to additional documentation when appropriate.

This procedure requires that the existing servers (T1400) have been upgraded to the SN07 software release.

.

149.3 Precautions

Contact GTAC if assistance is required with this section.

- Read this document in its entirety before attempting any individual procedure.
- The person(s) performing these procedures must be thoroughly familiar with the UA-AAL1 NA solution. The user is expected to have knowledge of the DMS MAP interface and be able to manipulate datafill and navigate the menu system.

- Certain procedures in this document are GTAC Interactive. Individual procedures will indicate this requirement. Use the 801 Scheduling procedures to obtain online GTAC support when required.
- Using the Core Management Tools, SAM21 Element Manager GUI, and MG9000 Element manager GUI, ensure the system is alarm free. Do not proceed until all alarms are either cleared or explained.
- Monitor logs in the XA Core and ensure the system is stable. Pay special attention to XAC logs.
- All procedures in this document require close coordination and prior approval from the customer. IP addressing changes must be clearly communicated to the customer.
- Obtain the latest copy of all referenced documentation the day of the actual activity. This will ensure the latest copy of each document is being used.
- Before performing any configuration changes on the Passport 8600 units, ensure direct physical connection to the console port is available. Locate a console port cable before the start of procedure.
- Ensure all REX tests are suspended when performing procedures in this document.
- Ensure Auto-patching is disabled when performing procedures in this document.
- Ensure no image dumps in XAC are scheduled when performing procedures in this document.
- No provisioning changes are allowed during this procedure.

149.4 Preparations

Contact GTAC if you require assistance with these preparation steps.

- Create backups for CMT, MG9KEM, MG9KMT
- Obtain and verify Userid/password information for all elements that will be accessed.
- Obtain and verify the IP addresses for all elements that will be accessed. These will include console port access.
- There are further preparation steps detailed in each procedure and/or the referenced documentation. Ensure those preparations are followed.
- The following tables are provided as a place to write down the information needed. Fill these out before continuing with the procedure.

149.5 Info Sheets

	Hostname	**IP addresses**	
CMT			
MG9KEM			
MG9KMT			

Table 1: Information to configure CMT-COAM

Hostname		This hostname is also called the original hostname later in this document	
3 IP Addresses	Cluster IP – new N240_0 IP – new N240_1 IP – new	Must be on same subnet as existing T1400 servers	
Subnet mask			
Default Router IP			
DNS Config			
Timezone	US/Central		
Server Installation Type “cs2kaps”, “cs2kmt”, “mg9kem”, or “csen”	cs2kaps		
NTP Server (s)			
Syslog setup			

Table 2: Information to configure MG9K-COAM

Hostname		This hostname is also called the original hostname later in this document	
3 IP Addresses	Cluster IP – new N240_0 IP - new N240_1 IP - new	Must be on same subnet as existing T1400 servers.	

Subnet mask			
Default Router IP			
DNS Config			
Timezone	US/Central		
Server Installation Type "cs2kaps", "cs2kmt", "mg9kem", or "csen"	mg9kem		
NTP Server (s)			
Syslog setup			

149.6 High Level Approach

The following approach will be used to make the transition from SN07 (T1400) to SN07 (N240).

1. Backup the CMT T1400 server
2. Install SSPFS and applications on the CMT-COAM server
3. Move data from the CMT T1400 server to the CMT-COAM server
4. Shutdown the CMT T1400 server
5. Reconfigure the CMT-COAM server with the IP address and host name of the CMT T1400
6. Reconfigure applications on the CMT-COAM server
7. Clone the CMT-COAM server to its mate server

The steps above will be repeated for the MG9K EM server if one exists in the office.

149.7 Detailed Steps

The following approach will be used to make the transition from T1400 to N240.

149.7.1 Migrate CMT from T1400 to N240

See Table 1 for CMT-COAM config settings.

The CMT-T1400 and the CMT-COAM will be configured with the same Hostname and IP address. Therefore, only one of these can be connected to the CS-LAN at any one time. The strategy is used so as to ensure that any other system referencing the CMT IP address will not be affected.

1. Follow the installation procedures for SSPFS installation defined in IM 241621.

2. Follow the installation procedures for CMT applications defined in IM 241623, **but don't perform the cloning step for this server. It will be done later.**

3. Ensure/Perform complete backup of required CMT oracle databases, patches, NPM, APS files etc. (must be backed up to file, not tape, since the N240 does not have a tape drive)

   Backup Oracle DB and critical data

   a) NN10281-600; Procedure-Performing a critical data backup;
   b) **Perform steps 2,3,4,5**
   c) Backup the CMT oracle database and critical data to a file using the following command: **/opt/nortel/sspfs/bks/bkdata –f /backup**

   Backup APS files if APS is running on same server with CMT

   d) NN10281-600; Procedure-Backing up APS application files; Instead of backup to tape, we modify the command to backup to file as follows:
      - Perform step 2
      - **Tar –cvf /aps_backup.tar /PROV_data /audio_files /user_audio_files / opt/uas/uas_conf_backup**

   Backup NPM patch files

   e) FTP all files in the **/data/npm/Au** from the CMT-T1400 to the CMT-COAM server
   f) FTP the **/backup** file from the CMT-T1400 to the CMT-COAM server
   g) FTP the **/aps_backup.tar** from the CMT-T1400 to the CMT-COAM server

4. Record any NPM customer specific configurations.
   a) NN10261-450v2; Procedure-**Saving user-defined NPM data using the NPM**; Perform steps 1-37 (Using the NPM GUI)

5. Shutdown the CMT-T1400 server

a) This is done by logging in as root, and issuing the **init 0** command.

At this point all commands are done on the CMT-COAM (N240) server

6. Change the virtual IP address of the CMT-COAM server
   a) Login as root
   b) Run the cli command
   c) Select option "Configure"
   d) Select option "IP Configuration"
   e) Select option "config_data"
   f) You will be prompted for the hostname and IP address to use. Enter the hostname of the CMT-T1400 and IP address of the CMT-T1400

7. Configure CS2M applications on the unit 0 N240

Configure Patching Server Element (PSE)

a) NN10276-500; Procedure- Configure Patching Server Element (PSE); **Perform steps 1-13.**

Configure APS

b) IM 24-9082 **(Need SN07 version);** Procedure 10 – **APS Configuration**; Perform steps 1-16. (Not required for this customer)

Configure SESM

c) IM 24-9082 **(Need SN07 version);** Procedure 11 – **SESM Configuration**; **Perform steps 1-17**. **(Skip steps 18-21) (Do not initialize or restore the database)**

Configure NPM (PFRS)

d) IM 24-9082 **(Need SN07 version);** Procedure 12 – **NPM Configuration**; Perform steps 1-14.

Configure SAM21

e) IM 24-9082 **(Need SN07 version);** Procedure 13 – **SAM21 Configuration**; Perform steps 1-24.

Configure SNMP Agent

f) NN10261-450v2; Procedure – **Configuring the SNMP Agent**; Perform steps 1-21.

g) Need Fred to provide the IM here

8. Ensure that no applications are running prior to restoring database
   a) Stop NPM with the command: servstop NPM
   b) Stop PTM with the command: servstop SESMservice
   c) Stop SAM21 with the command: servstop SAM21EM
   d) Stop APS with the command: servstop APS
   e) If QCA is configured on the server: Stop QCA with the command: servstop QCA

9. Restore all required CMT oracle databases, patches, NPM, APS files

   Restore Oracle DB and critical data

   a) NN10281-600; Procedure-Performing a data restore
      Perform steps 2,3,4,5
   b) Restore the CMT oracle database and critical data from a file using the following command: **/opt/nortel/sspfs/bks/rsdata -f /backup**
   c) NN10281-600; Procedure-Performing a data restore
      Perform steps 9,11

   Restore APS files

   a) **Tar –xvf aps_backup.tar (Will restore the files /PROV_data /audio_files / user_audio_files /opt/uas/uas_conf_backup)**

10. Start applications (SESM, SAM21, NPM)
    a) Start SESM with: serstart SESMserver
    b) Start NPM with: servstart NPM
    c) Start APS with: servstart APS
    d) Start SAM21 EM with: servstart SAM21EM
    e) If QCA is configured on this server: Start QCA with: servstart QCA

11. Restore any NPM customer specific configurations.
    a) NN10261-450v2; Procedure-Restoring the NPM patch files; **Perform steps 14-15**

12. Reboot the CMT-COAM
    a) sync;sync;init 6

13. Test all element Managers and equipment to ensure everything is operating correctly

NN10261-450v2; Procedure-Verifiying upgrade was successful; **Perform steps 1-9**

14. If there are problems at this point and a back-out is desired, execute the steps in the back-out procedure in the next section.

15. Clone Master N240 to Mate N240 (Approx 1 hour)
    IM 24-9082 **Perform steps 23-28**
    a) Copy MAC address into command into installed server
    b) Boot clone N240 from network with <ip address> of master
    c) Disk replication will occur
    d) Fred to provide new IM number and procedure number

16. Re-test all element Managers and equipment to ensure everything is still operating correctly
    a) NN10261-450v2; Procedure-Verifiying upgrade was successful; **Perform steps 1-9**

17. Remove CMT (T1400) physically from network

149.7.2 Back-out procedure for CMT from N240 to T1400

1. Change the virtual IP address of the CMT-COAM server
    a. Login as root
    b. Run the cli command
    c. Select option “Configure”
    d. Select option “IP Configuration”
    e. Select option “config_data”
    f. You will be prompted for the hostname and IP address to use. Enter the original hostname of the CMT-COAM and original IP address of the CMT-COAM. Leave the rest alone.
2. Take the CMT-COAM server down by doing the following as the root user:
    a. **init 0**

3. Reboot the CMT-T1400 server by issuing the following command from the console port of the CMT-T1400 server: **boot**
    a. The system will come up at this point

149.7.3 Migrate MG9KEM and MG9KMT from T1400 to N240

See Table 2 for MG9K-COAM config settings

1. Follow the installation procedures for SSPFS installation defined in IM 241621.

2. Follow the installation procedures for MG9KEM and MG9KMT applications defined in IM 240674, **but don't perform the cloning step for this server. It will be done later**.

3. Shutdown the MG9KEM-T1400
    a. This is done by logging in as root, and issuing the **init 0** command
4. Shutdown the MG9KMT-T1400
    a. This is done by logging in as root, and issuing the **init 0** command

At this point all commands are done on the MG9KEM-COAM (N240) server

5. Change the virtual IP address of the MG9KEM-COAM server
    a. Login as root
    b. Run the cli command
    c. Select option "Configure"
    d. Select option "IP Configuration"
    e. Select option "config_data"
    f. You will be prompted for the hostname and IP address to use. Enter the hostname of the MG9KEM-T1400 and IP address of the MG9KEM-T1400. Do NOT use the hostname and IP address of the MG9KMT-T1400 server.

6. Configure MG9K Server applications on master N240
    a. IM 24-0739 **(Need SN07 version)**; Procedure 8 – **EM Server Software Installation and Configuration**; Perform steps 8-10, 14-18.

7. Start MG9K server application
    a. IM 24-0739 **(Need SN07 version)**; Procedure 8 – **EM Server Software Installation and Configuration**; Perform steps 19-21.

8. Configure MG9K Midtier application on master N240

a. IM 24-0739 **(Need SN07 version)**; Procedure 9 – **Mid-Tier Software Installation and Configuration**; Perform steps 8-23.

9. Start MG9K Midtier application
    a. IM 24-0739 (Need SN07 version); Procedure 9 – Mid-Tier Software Installation **and Configuration**; Perform steps 8-23.
    b. NN10048-461; Procedure –Importing MG9000 Manager Data; Perform steps 1-4

10. Configure OM Collector
    a. Configure OM Collector. Follow the procedure to configure OM collector

11. Reboot the MG9K-COAM
    a. sync;sync;init 6

12. Test all MG9KEM/MT functions to ensure everything is operating correctly
    a. IM 24-0739 **(Need SN07 version)**; Section 4.13 – **Client Verification**; Perform procedure.

13. If there are problems at this point and a back-out is desired, execute the steps in the back-out procedure in the next section.

14. Clone Master N240 to Mate N240 (Approx 1 hour)
    IM 24-9082 **Perform steps 23-28**
    a. Copy MAC address into command into installed server
    b. Boot clone N240 from network with <ip address> of master
    c. Disk replication will occur
    d. Fred to provide new IM number and procedure number

15. Re-test all element Managers and equipment to ensure everything is operating correctly

16. Perform Failover Tests
    a. On master N240, issue “sync;sync;init 6”
    b. Check that the backup server takes over
    c.

17. Remove MG9KEM-T1400 and MG9KMT-T1400 physically from the network

149.7.4 Back-out procedure for MG9KEM and MG9KMT from N240 to T1400

4. Change the virtual IP address of the MG9KEM-COAM server
    a. Login as root
    b. Run the cli command
    c. Select option “Configure”
    d. Select option “IP Configuration”
    e. Select option “config_data”
    f. You will be prompted for the hostname and IP address to use. Enter the original hostname of the MG9KEM-COAM and original IP address of the MG9KEM-COAM. Leave the rest alone.
5. Take the MG9KEM-COAM server down by doing the following as the root user:
    a. **init 0**

6. Reboot the MG9KEM-T1400 server by issuing the following command from the console port of the MG9KEM-T1400 server: **boot**
    a. The system will come up at this point

7. Reboot the MG9KMT-T1400 server by issuing the following command from the console port of the MG9KMT-T1400 server: **boot**
    a. The system will come up at this point

149.8 References

NN10048-461 – SN06.2 Draft#2 05.01a – Upgrading the MG9000 – October 2003
NN10062-461 – SN06.2 Draft 05.02 – Upgrading the CS 200 Management Tools – October 2003
IM 24-9082 – CS2000 Management Tools Commissioning – SN06 August 25, 2003
IM 24-0739 – MG9000 Element Manager Commissioning – SN06 August 25, 2003

149.9 Glossary

GTAC - Global Technical Assistance Center
SSPFS – Succession Server Platform Foundation Software

150: Corrective CAF, Functional Description (FN): A00004860

150.1 Title

SSPFSHA Cluster & Application Upgrade Procedures

150.2 Purpose

In Succession SN06.2 release, we have introduced two-node SSPFSHA cluster. As we moved to SN07, one of the direct requirements is to provide a SN06.2-SN07 cluster and application upgrade and migration strategy. Both SSPFS and SSPFS client applications have already done most preparatory work in SN06.2 in anticipation of this procedure.

150.3 Problem symptoms

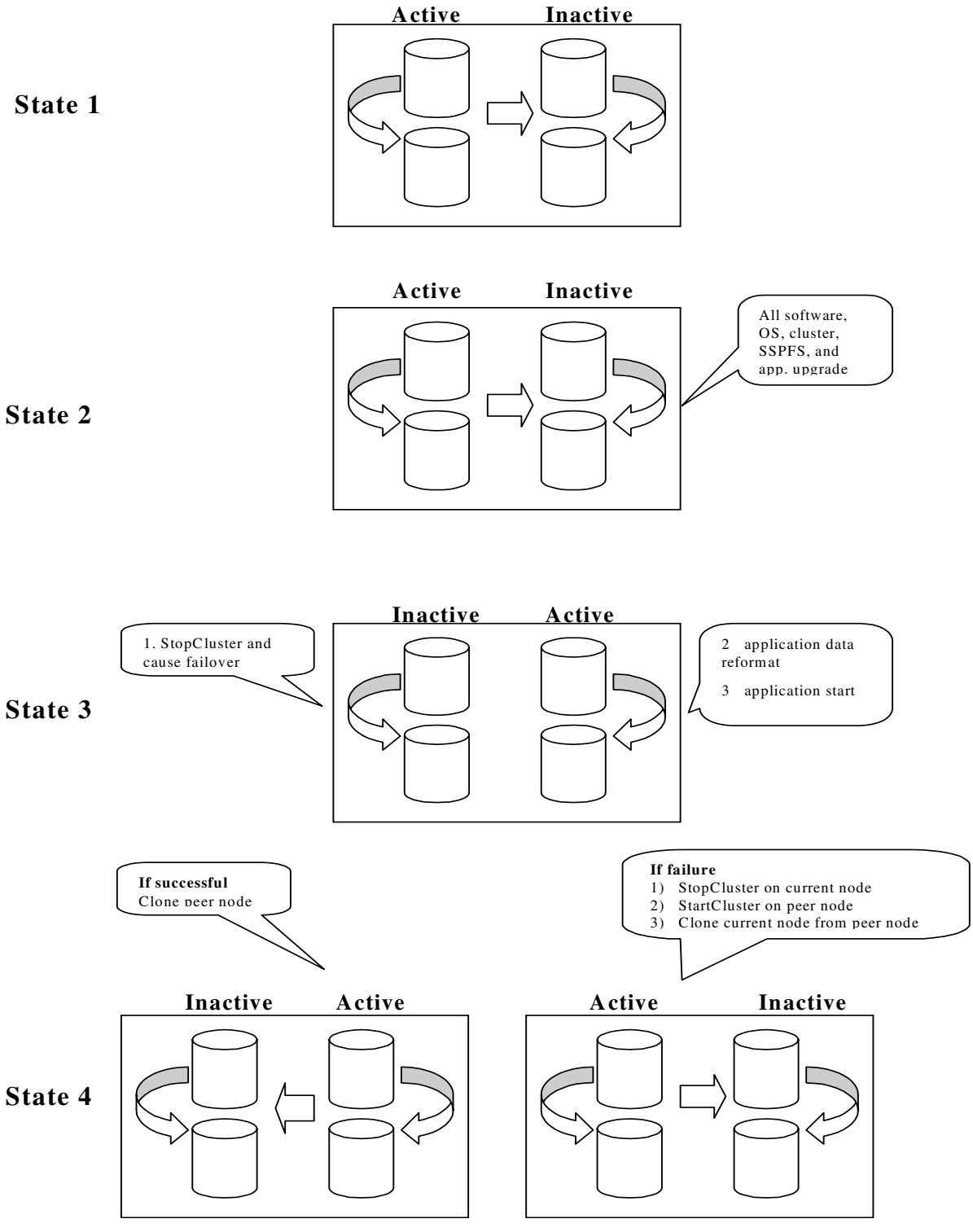
In SN07, none of the SSPFSHA clustered applications that have been running since SN06.2 have any explicit requirement on continuous network data replication between the cluster nodes during upgrade. Being able to quickly move back to previous SN06.2 running environment in case of upgrade failure is the only requirement.

150.4 Resolution

This procedure will concentrate on SSPFSHA SN06.2 cluster to SN07 cluster upgrade. There may be other issues relating to SSPFSHA simplex to cluster or dual-server profile configuration. They will be addressed separately.

For SSPFSHA Cluster SN06.2 to SN07 upgrade, we will separate the cluster in order to preserve the one of the cluster node in its previously, before-upgrade environment. If the upgrade is successful, a normal cloning procedure will create the secondary node and sync up the cluster. If the upgrade fails, we will quickly shutdown the newly upgraded node and restate the previous active cluster node.

Cluster upgrade takes place in four distinct stages:


State 1
Active
Inactive
State 2
Active
Inactive
All software, OS, cluster, SSPFS, and app. upgrade
State 3
Inactive
Active
1. StopCluster and cause failover
2 application data reformat
3 application start
If successful
Clone peer node
If failure
1) StopCluster on current node
2) StartCluster on peer node
3) Clone current node from peer node
State 4
Inactive
Active
Active
Inactive

Same upgrade procedure described in state tables:

	Active	*Inactive*
1		Upgrade software including OS, SSPFS middleware, upSuite, and OAM&P applications. See URLs below.
2	$StopCluster	
	Inactive	*Active*
3		Application reformat data Application start
4(successful)		$Clone
4(failure)		$StopCluster
	$StartCluster	
	$Clone	

Note: We will have a new command Clone, which when typed on the local machine, will go ahead and clone the peer node from the local machine image.

SSPFS

http://sspfs/LabBulletins/SN04_SN06.2_UpgradeGuide.html

SESM

http://znc0s0p1.us.nortel.com:8100/pnm/bin/ptm-docs.pl?op=sendFile&filename=/view/pnmdoc_www/pnm/documents/Activity/SN06.2/CS2M_Product_Specification/SN06_2_Upgrade.html

CBM

http://sdm.ca.nortel.com/sw_delivery/documents/

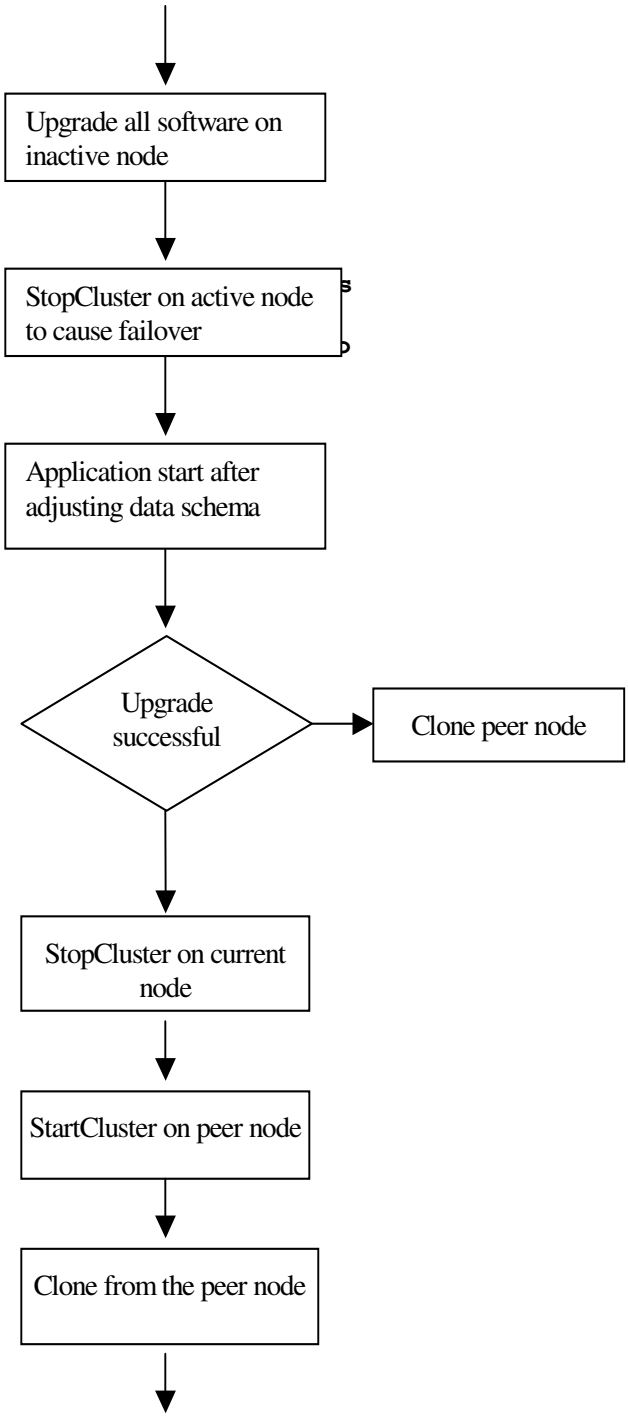
MG9KEM

http://sdm.ca.nortel.com/sw_delivery/documents/

IEMS

http://livelink.us.nortel.com/livelink/livelink.exe/fetch/2000/2743299/2894744/5685304/5693238/6080225/6086765/6180994/6692253/a0000366_iems_ha_coresidency_cn_v3.pdf?nodeid=6697481&vernum=0

Same upgrade procedure expressed in data flow chart.


Upgrade all software on inactive node
StopCluster on active node to cause failover
Application start after adjusting data schema
Upgrade successful
Clone peer node
StopCluster on current node
StartCluster on peer node
Clone from the peer node

5.13 Related documentation

SSPSF-HA-Enhancement-DSUM.pdf

SSPSF-HA-Enhancement-FN.pdf

151: Design Description excerpts: A00004868

151.1 Feature name

FTP Proxy for SDM and DBM

151.2 Description

151.2.1 Purpose

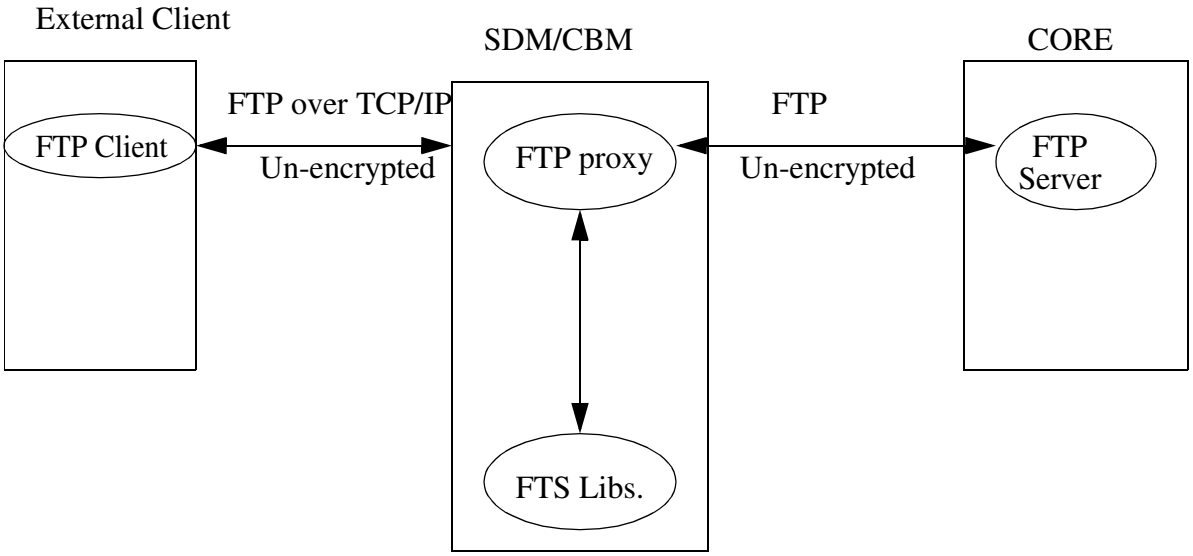
The purpose of this feature is to provide passthrough (file transfer) to the CM from the ftp client (downstream machine) via SDM/CBM in a Non-DCE environment.

FTPProxy will be used by an external ftp client for transferring files between client and CORE, client and SDM/CBM (In case of CORE it will be without the files ever residing on the SDM/CBM). Certain amount of security will be provided by giving the passthrough (file transfer) facility to the ftp users based on their unix groups. FTP Proxy will provide all of the facility provided by the current File transfer Service(SDM_BASE.fts) implementation on SDM19.

On SDM, SFT application provides the passthrough capability to the ftp users. So, the FTPProxy and SFT application will be mutually exclusive, at one point only either of them can reside on SDM. Whereas on CBM, SFT is not available, so the FTPProxy can reside independent of other CBM applications, but it will be mutually exclusive with SSPFS's ProFTPD service.

FTPProxy feature will be provided to the customer as an optional application on SDM and CBM. It will also include the functionalities such as creating ftp users dynamically and deleting them after the file transfer is over, and parallel sessions will also be supported.

Refer to the following figure for FTP functionality.



151.2.2 Logs

New customer logs will be generated to provide information regarding the file transfers between FTP Client and CORE, and who ftp-users are logged on to CORE.

151.2.2.1 Log format for file transfers

```
Feb 16 02:24:52 sspfs_server ftpd[20103]: SDM739 NONE
INFO FTS ftp-user request for file PML successful
```

151.2.2.2 Log format for login information

```
Feb 16 02:24:40 sspfs_server ftpd[20103]: SDM739 NONE
INFO FTS ftp-user hari logged on to CORE
successfully.
```

151.3 Glossary

Term	Description
AIX	IBM UNIX operating system on the SDM FX
CBM	Core and Billing Manager
CM	Command Module (the CPU of the DMS)
CMFT	Command Module File Transfer Script
Core	DMS switch computing engine
DCE	Distributed Computer Environment
FTP	File transfer protocol
FTS	File transfer System (Nortel proprietary code)
IP	Internet Protocol
SCFT	SSH Core File Transfer
SDM	SuperNode Data Manager
SSH	Secure Shell protocol
SSHD	Secure Shell protocol Daemon

152: Functional Description (FN): A00004872

152.1 Feature name

SN07 Services Support for the Universal Access-Internet Protocol (UA-IP) Solution

152.2 Description

This SN07 activity provides support in both the North American and International markets for the following services:

- Automatic Call Distribution Observe (ACD OBS): allows an ACD supervisor to monitor the quality of service offered to callers. As an option, an observe warning tone may be provided to the agent prior to the observation. The tone is heard when the observation is invoked and at the start of each new call while an observation is in effect. This tone is heard by the ACD agent and not the caller.

  There are various types of observe:

  a. Basic - Basic observe allows the supervisor to monitor an agent within its group that is involved in an active call. To activate OBS, a supervisor presses the OBS key and enters the INCALLS DN of the agent to be monitored. The supervisor is provided with a one way listen path into a call between an ACD agent and caller. A two way speech path can be achieved by pressing the CAG key.

  b. Extended - Extended Observe enhances the observe functionality to allow a supervisor to observe any agent that has an INCALLS key in any ACD group within the same customer group.

  c. Enhanced - When the ACD observe agent enhanced feature is in effect, the supervisor can observe the INCALLS key and a datafilled SDN using the AGENT key. Once the supervisor enters the observe mode, pressing the AGENT key after dial tone is received allows the supervisor to switch back and forth between observing the INCALLS key and the SDN as the agent switches between talking on the two keys.

  d. Flexible Call Observing (FOBS) - FOBS enhances the current ACD feature by providing an ACD OBS means for ACD supervisors to begin monitoring service given to a call before an agent has answered the call. The basic OBS feature imposes the restriction that a call must be in the talking state in order for OBS to be used. FOBS allows observation of a call to begin from the time it is first queued in the ACD system. This gives the supervisor an opportunity to gain knowledge of the overall handling of the incoming call. The supervisor continues to

monitor the call if it is rerouted under enhanced overflow or NACD, if it is presented to an agent, and if the agent answers the call. Activation of FOBS instigates the monitoring of the next call to the ACD group, ACD subgroup or ACDDN. Monitoring ceases when the caller disconnects, or if the call is routed outside the ACD environment

NOTE: ASL functionality cannot be supported at this time. Although the provisioning of this functionality is not restricted, the behavior is not supported in solutions using an audio server. Solutions using an MTM to provide this observe conferencing should work with ASL. Furthermore, OBS and 3WC interactions are supported using the AMS for conferencing, but it is not supported on the UAS due to protocol restrictions on the UAS.

- Automatic Call Distribution Emergency Key, Emergency Key Backup (ACD EMK)- The EMK feature enables an ACD agent to immediately conference in a supervisor and/or an auxiliary device in the event of threatening or abusive calls. When the EMK key is pressed, the lamp flashes on the agent set if the supervisor is available. The supervisor set rings and the Answer Emergency Key (AEMK) lamp flashes. When the supervisor answers the AEMK key the supervisor is conferenced into the call. The EMK and AEMK lamps are steadily lit. If the call is not answered by the supervisor within 30 seconds the feature is taken down. The EMK key can only be activated while the agent is active on an ACD call. The agent who initiates the emergency call must remain on the call for the duration of the feature. Emergency Key Backup provides a method for redirecting EMK calls made from an ACD agent position to a supervisor set AEMK key when the supervisor set is already active on an AEMK call, or the supervisor set is unavailable (i.e. supervisor does not answer the EMK call.) Redirection is accomplished by placing ACD supervisor AEMK (Answer Emergency) DNs in a hunt group via tables HUNTGRP and HUNTMEM.
- Camp-on for MDC lines (MBSCAMP) - this feature allows a MBS set to “camp-on” to a busy group member. When the MBSCAMP subscriber receives a call and attempts to transfer to another member of the customer group, if that line is busy so that the call would normally receive busy treatment, the MBSCAMP feature provides a call-waiting type indication to the busy line and camps onto the busy line. The MBSCAMP line is provided ringback or audio as an indication of the camping.
- Music on Hold (LMOH, KSMOH, pre-recorded music announcement on hold for ACD) - this feature provides an audio source to a line placed on hold by a line with this option (either on the line or the customer group).
- Executive Busy Override/Executive Busy Override Exempt (EBO/EBX) - the EBO feature allows a member of a customer group to override a busy indication from a called line in the group and connect into the call in progress. The EBO line can be connected as a third party or can either flash

(on an IBN set) or press an EBO key again (on an MBS set) to drop the extra party and only be connected to the called party. Just prior to connecting the EBO party into the call, an EBO warning tone is provided to both parties of the current call. The EBX feature prevents a line with EBO from barging into a call. That is, when a subscriber with EBO attempts to override a call to another subscriber with EBX, the EBO feature is denied.

- Directed Call pick-up Barge In (DCBI) - this feature allows a member of a customer group to pickup an incoming call to a member of a customer group and also allows the member to barge-in to that call if it is answered prior to the completion of the pickup attempt. In that case, the DCBI line is connected as a third party to the call, and prior to the connection, an optional DCBITONE barge-in indication tone is provided to both parties of the initial call.

This activity requires mapping of EBO tone for the EBO, DCBI, and ACD OBS services. MBSCAMP actually sends an EBS opcode to physically buzz a pset and therefore does not send an actual tone signal.

These services should have the same basic functionality in Succession as in the Legacy environment, but it must be noted that in Succession the tones associated with the services are supplied by another device and therefore are a product of those elements.The following table describes the signals and associated GW tone mapping for these tones. For this activity, the tones are only required for the H.248 protocol although they are mapped to existing supported tones in other protocols in order to provide some sort of tone if ever required.

Table 1 Tones for services

Tone service	Tone is provided by	H.248 signal sent	GW signal and market supported with typical tone characteristics
EBO, DCBI	conferencing source (MTM or UAS/AMS)	(int/int) if package supported otherwise (cg/wt)	The UAS and AMS support cg/wt in North America and international packages. This is typically defined as a single 1400 hz tone for most markets but this is dependant upon the physical tone characteristics actually downloaded to the device.
ACD OBS	lines GW for packet agent; MTM for legacy agent	(int/int) if package supported otherwise (cg/wt)	MG9K North American V1 toneset supports int/int as 3 100msec on/100 msec off bursts of 440 hz at -13 db. CICM international int/int tone supported with same tone characteristics as above.

152.3 Hardware Requirements or Dependencies

No new hardware is introduced by these services. However, as noted above, in Succession the tones required for these services are requested of a gateway (GW), either a network audio server (i.e. Universal Audio Server (UAS) or Audiocodes Media Server (AMS)) or a local GW.

Note there is a limitation with respect to the UAS. See the limitations section for more information.

For hybrid testing, the MTM tone circuit is required along with table STN datafill for cases where EBO tone is played into an MTM conference or to a legacy ACD agent.

152.4 Software Requirements or Dependencies

The SN07 software loads are required of the Succession elements.

152.5 Limitations and restrictions

These services function in Succession as they do in Legacy; that is, any limitations existing in Legacy also exist in Succession. An exception is that ASL functionality cannot be supported at this time. Although the provisioning of this function is not restricted, the behavior is not supported in solutions using an audio server. Solutions using an MTM to provide this observe conferencing should work with ASL.

The UAS does not support some of the signalling used for the ACD OBS interactions with 3WC (a null events descriptor in the H.248 protocol). Therefore this interaction is not supported with the UAS. This functionality is supported on the AMS.

Tones for these services are dependant upon the GWs used. EBO and DCBI services play tones to a conference; therefore EBO tone is played by the conference server. For MTM based conferences, the table STN EBOT tone datafill is used to select the MTM for the tone (tone card is required); for the audio servers, the tone is provided by the audio server. For ACD, the tone is played to the agent; therefore for legacy agents the tone is provided by the MTM and for packet agents it is provided by the GW. Therefore the tones can differ based on legacy or succession and type of GW.

For Music On Hold, the music is a pre-recorded music announcement.

152.6 Interactions

There are no new interactions with these services in SN07.

152.7 Applicable customer facing sections

Fault Management

Logs	_n/a__
Alarms	_n/a__
Configuration	
Data Schema	__X___
User Interface	_n/a__
Element Management	_n/a__
Security	_n/a__
Service Order	_n/a__
Office Parameters	_n/a__
Accounting (includes AMA billing)	_n/a__
Performance (includes operational measurements)	_n/a__

152.8 Glossary

Term	Description
ACD	Automatic Call Distribution
AEMK	ACD Answer Emergency key
AMS	Audiocodes Media Server
CAG	Call Agent key
EBO	Executive Busy Override
EBX	Executive Busy Override Exempt
EMK	ACD Emergency key
FOBS	Flexible Call Observe
GW	Gateway
IBN	Integrated Business Network
KSMOH	Keyset Music on Hold
LMOH	Line Music on Hold
MOH	Music on Hold
OBS	ACD Observe
PRECONF	Preset Conference

Term	Description
SDN	Secondary Directory Number
UA-IP	Universal Access - Internet Protocol
UAS	Universal Audio Server

153: Functional Description (FN): A00004873

153.1 Feature name and Feature ID

A00004873 - MS2000 CLUI Enhancements

153.2 Description

In SN06.2, the MS2000 (Media Server 2000) Series Node CLUI was introduced to configure the MS2010 device. The CLUI is delivered to the customer as part of the SESM load that is bundled as part of the CS2M load. The tool requires that the SESM server is in service.

The tool is launched with the command:
/opt/nortel/NTsesm/bin/ms2000.sh

The existing MS2000 Series Node CLUI will be enhanced in SN07 to handle configuration for the MS2020 ATM device. The tool will handle both SN06.2 MS2010 nodes as well as SN07 MS2010 and MS2020 nodes.

The following new functionality will be added to the MS2000 CLUI for SN07:

1) Ability to configure MS2020 device

2) Force Lock of a Device

3) Ability to change the SNMP Community Strings

4) Ability to change the MS2000 web interface user name and password.

5) Ability to configure the NTP (Network Time Protocol) settings for the MS2000 device.

6) Ability to set up trusted managers and trap destinations for MS2010 and MS2020 SN07 devices.

7) Ability to change the file transfer (web server) password on an SN07 MS2000 node from the CLUI.

153.2.1 MS2000 Main Menu

The layout of the menus has changed from SN06.2. The main menu that the tool launches into contains items that pertain to all MS2000 nodes. It allows the user to set up the automated ini file backup. Copy files to the SDM/CBM and list the MS2000 nodes datafilled in the SESM database (must be associated with GWCs).

```
wnc0s0jm:/var/tmp/ptm> /opt/nortel/NTsesm/bin/ms2000.sh
*********************************************************
**  Nortel Media Server 2000 Series Configuration Tool  **
**                    version 2.02                     **
*********************************************************
Enter user name > ptm
Enter password  >
ORBWrapper orb initialized


***** Media Server 2000 Series CLUI Main Menu *****
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
Enter Selection (1 - 5, x)
>
```

153.2.2 MS2010 SN06.2 Configuration

From here the “Node Maintenance and Configuration” can be launched for a specific node.The changes to that menu are outlined below.

153.2.2.1 MS2010 with a SN06.2 load

The SN06.2 load operates a little differently than the SN07 versions. In SN06.2

- the trap destination is setup in the general configuration
- the file download password can be set for the tool but CANNOT be changed on the MS2000 node.

Below is a look at the SN06.2 MS2010 maintenance and configuration menu. The maintenance menu is identical to the one used for an SN07 device.

```
***** Media Server 2000 Series CLUI Main Menu *****
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
Enter Selection (1 - 5, x)
> 2

Return to access this node or enter another IP address
>47.142.92.104

*** Main Menu for MS2010 at 47.142.92.104 ***
1) Maintenance Menu
```

```
2) Configuration Menu
x) EXIT
Enter Selection (1 - 2, x)
> 1

*** Maintenance Menu for MS2010 at 47.142.92.104 ***
1) Download load files to this node
2) Backup the INI file for this node
3) Perform a soft reset on this node
4) Lock or Unlock this node
x) EXIT
Enter Selection (1 - 4, x)
> x
```

Below is the configuration menu which does have different selections from the SN07 nodes.

```
***** Main Configuration Menu for MS2010 at 47.142.92.104 *****
1) Display this nodes current configuration
2) General node configuration
3) Change File Upload and Download user and password
x) EXIT
Enter Selection (1 - 2, x)
>
```

153.2.2.1.1 MS2010 SN06.2 File Download password

In SN06.2, the File transfer username and password was setup once and was used for every node. This made the assumption that each node would be setup with the same username and password. In SN07 the username and password is setup on a per node basis. The menu selection below allows for the SN06.2 functionality to remain the same when configuring an SN06.2 MS2010 node. A note is displayed to explain the functionality.

```
***** Main Configuration Menu for MS2010 at 47.142.92.104 *****
1) Display this nodes current configuration
2) General node configuration
3) Change File Upload and Download user and password
x) EXIT
Enter Selection (1 - 2, x)
> 3

This menu selection will allow you to setup the file transfer username and password
for ALL SN06.2 MS2010 nodes. The CLUI will allow you to setup the SN06.2 username
and password in two ways. First, you can setup the CLUI to use the factory default
username and password for all of the SN06.2 MS2010 nodes or second, you can specify
a different username and password for the tool to use when communicating with
SN06.2
MS2010 devices.

This menu selection will NOT actually change the username and password on the node.
In order to change the username and password on an MS2010 SN06.2 node, the MS2010
web interface must be used.

Would you like to change the file transfer username and password that the CLUI uses
when communicating with all SN06.2 MS2010 nodes? (y/n)
```

```
>
```

153.2.3 MS2010 and MS2020 SN07 Configuration

The MS2010 and MS2020 share some common behavior for SN07.

153.2.3.1 Forced Lock Menu change

Below is an example of logging into the device issuing a force lock command.

```
***** Media Server 2000 Series CLUI Main Menu *****
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM
5) Configure CLUI tool
x) EXIT
Enter Selection (1 - 5, x)
> 2

Enter the IP address of the MS 2000 node
> 47.142.134.127

*** MS2020 Maintenance and Configuration Menu for Node : 47.142.134.127 ***
1) Display this nodes current configuration
2) Configure this node
3) Download load files to this node
4) Backup the INI file for this node
5) Perform a soft reset on this node
6) Lock or Unlock this node
x) EXIT
Enter Selection (1 - 6, x)
> 6

*** MS2020 Lock Menu for node : 47.142.134.127 ***
*** Current State : unlocked(2)
1) Graceful Lock Node
2) Force Lock Node
3) Unlock Node
x) EXIT
Enter Selection (1 - 2, x)
> 2

                        *** WARNING ***
Performing a forced lock on the node will take it out of service immediately.
Active calls will be dropped!
Perform forced lock? (y/n)
> y
The MS2020 node has been locked.
Press <enter> to continue
```

153.2.3.2 Setting Network Time Protocol

```
***** AAL1 Main Configuration Menu for MS2020 at 47.142.92.107 *****
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
```

```
4) SNMP configuration and security
5) Configure ATM loopback table
6) Display SVC Connection table
x) EXIT
Enter Selection (1 - 6, x)
> 3
*** NTP configuration for MS2020 at 47.142.92.107 ***
Enter the desired value at the prompt. The current setting is displayed
in brackets. To chose the default setting press Enter. Enter '?' for
help with the format.
NTP Server Address [1.2.3.4]
> 47.1.1.1
Value validated and set to 47.1.1.1

NTP time to offset [0]
> 10
Value validated and set to 10

NTP Update Interval [5000]
>
Using current value 5000


Would you like to write these values to the MS2020 node? (y/n)
> y
Would you like to store the changes by backing up the INI file now? (y/n)
> y

Backup of .ini successful

Would you like to save file 2004-04-12_10:07:53.Board.ini
to the SDM/CBM now? (y/n)
> y
File copied to the SDM successfully.
Press <enter> to continue
```

153.2.3.3 Setting SNMP Community String

SNMP has a password type of security for versions v1 and v2 called the Community String. The CLUI allows you to change the Community String that will be used by the box when communicating via SNMP. This will actually change the Community String on the MS2000 node and then the CLUI will store that password for later use. Any other device that must communicate via SNMP with the MS2000 node will also need to change the community string it uses.

```
***** AAL1 Main Configuration Menu for MS2020 at 47.142.92.107 *****
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
4) SNMP configuration and security
5) Configure ATM loopback table
6) Display SVC Connection table
x) EXIT
Enter Selection (1 - 6, x)
> 4
```

```
*** SNMP Configuration and Password Management Menu for MS2020 at 47.142.92.107
***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and password
?) Help
x) EXIT
Enter Selection (1 - 4, ?, x)
> 3

** SNMP Community String Password Management **
Would you like to change the SNMP Community password
for this node? (y/n)
> y
                          *** WARNING ***
This password will be written to the MS2020 and is the only password
that can be used for either reading from or writing to the node via
SNMP. If there are other managers that must communicate to this MS2020
node then you will need to go to that manager and reconfigure the
community strings it uses to communicate with this MS2020 node. The
password you are entering here will be used for both the read and write SNMP
community strings.

Press <enter> to continue

Enter the SNMP password for the CLUI to use when communicating with
the 47.142.92.107 MS2020 node. Return to exit.

>
Re-enter the Password
>
Save the SNMP password change? (y/n)
> y
```

153.2.3.4 Configuring Trusted SNMP Managers

The definition of a Trusted Manger is defined below in the CLUI help text. An example of adding a trusted manager is defined. Of special note is the proplem that can be created when someone adds the first trusted manager and it is not the IP address of the CLUI. This can cause the MS2000 node to stop responding to the CLUI. A special warning is put into the CLUI to help warn of this problem.

```
*** SNMP Configuration and Password Management Menu for MS2020 at 47.142.92.107
***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and password
?) Help
x) EXIT
Enter Selection (1 - 4, ?, x)
> 1

*** Trusted Mangers Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
```

```
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> ?

A trusted manager is an Element Manager (EM) from which the MS2020
accepts SNMP requests. By default, if there are no trusted managers
defined then the MS2020 accepts requests from any manager that provides
a valid community string. Up to 5 trusted managers can be placed in
the table. After adding a trusted manager, a soft reset will need to
be issued.
                        *** WARNING ***
Once a single trusted manager is configured, requests from any IP
address not in the trusted managers table will be rejected. Since
the MS2000 CLUI acts as the EM for the MS2000 devices, it should be
entered into the table BEFORE adding any other entries. The IP address
entered for the CLUI should be the IP address of the server that the
MS2000 CLUI is running on.


*** Trusted Mangers Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
>1

List of Trusted Managers
========================

There are no Trusted Managers defined
Press <enter> to continue

*** Trusted Mangers Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> 2
*** Adding new Trusted Manager Entry for 47.142.92.107 ***

Enter the desired value at the prompt. Enter '?' for help with
the format or carriage return to exit from the add entry

Enter the IP address of the node that you would like to set up
as a Trusted Manager.
> 1.1.1.1

                        *** WARNING ***
You are adding the first trusted manager to this MS2020 node. As soon
as this trusted manager is added to the node, the node will ONLY accept SNMP
requests from the 1.1.1.1 address. Other trusted managers can be added from the
CLUI (up to 5) but in order to add more trusted managers, the CLUI server's IP
address must be the first trusted manager in the table in order to communicate
with the node.

The CLUI sees the server IP address as 47.142.94.81 and if this is correct
then if you proceed with adding the 1.1.1.1 address as the first trusted manager,
the CLUI will NO LONGER BE ABLE TO COMMUNICATE WITH THE DEVICE!
```

```
It is STRONGLY recommended that you NOT proceed with adding 1.1.1.1 as
the first trusted manager until you are positive that it is the IP address that
the MS2020 will recognize as the CLUI.

Continue with add of trusted manager? (y/n)
> n

*** Trusted Mangers Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> 2
*** Adding new Trusted Manager Entry for 47.142.92.107 ***

Enter the desired value at the prompt. Enter '?' for help with
the format or carriage return to exit from the add entry

Enter the IP address of the node that you would like to set up
as a Trusted Manager.
> 47.142.94.81


Would you like to add this Trusted Manager to the MS2020 node? (y/n)
> y
                            *** NOTE ***
The changes that have been made to the MS2020 require a soft reset of the
node in order for the changes to take effect. A soft reset of the node will
take it out of service for several minutes.
Perform soft reset now? (y/n)
> n
Would you like to store the changes by backing up the INI file now? (y/n)
> y

Backup of .ini successful

Would you like to save file 2004-04-12_10:18:17.Board.ini
to the SDM/CBM now? (y/n)
> y
File copied to the SDM successfully.
Press <enter> to continue

*** Trusted Mangers Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> 1

List of Trusted Managers
========================
  IP = 47.142.94.81

Press <enter> to continue
```

NOTE : At this point the ONLY way that the MS2000 node configured above will responde to an SNMP request is if it comes from the IP address configured

in the Trusted Managers list (in our case it is 47.142.94.81) AND it provides the correct community string.

NOTE: If the situation arises where the CLUI cannot communicate with the node because a trusted manager is defined and it is NOT the IP address of the CLUI then the MS2000 node will need to reboot via bootp and loaded with an INI file that clears out the trusted managers.

153.2.3.5 SNMP Trap Destinations

The trap destinations menu will allow the customer to configure up to 5 trap destinations. This will allow for multiple logging locations for traps generated by the box.

```
*** SNMP Configuration and Password Management Menu for MS2020 at 47.142.92.107
***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and password
?) Help
x) EXIT
Enter Selection (1 - 4, ?, x)
> 2

*** Trap Destinations Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trap destinations
2) Add a trap destination
3) Delete a trap destination
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> ?

Most of the traps originating from the MS2020 are alarm related. The
MS2020 is capable of routing these traps to multiple destinations
should the user want the traps logged by different trap collection systems.

*** Trap Destinations Configuration Menu for MS2020 at 47.142.92.107 ***
1) List configured trap destinations
2) Add a trap destination
3) Delete a trap destination
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
> 1

List of Trap Destinations
=========================
  IP = 47.142.94.81  Port = 162

Press <enter> to continue
```

In the configuration above. The traps are only sent to the 47.142.94.81 port 162 adress.

153.2.4 MS2020 devices specific Configuration

The following menu items are specific to the MS2020 nodes.

153.2.4.1 Configure ATM loopback table (AAL1 & AAL2)

This menu allows the user to display and edit the ATM loopback entry. Please see the AudioCodes documentation for the meaning of the settings.

```
***** AAL1 Main Configuration Menu for MS2020 at 47.142.92.107 *****
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
4) SNMP configuration and security
5) Configure ATM loopback table
6) Display SVC Connection table
x) EXIT
Enter Selection (1 - 6, x)
> 5

***** ATM Loopback Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit Port Entry
x) EXIT
Enter Selection (1 - 2, x)
> 1

*** LoopBack Table for MS2020 at 47.142.92.107 ***

    Table Entry 1
    ************
    Is Used               : yes(1)
    Action                : none(0)
    Action Result         : none(0)
    Port Number           : port0(0)
    Mode                  : vp(2)
    OutBound Virtual Path : 2
    InBound Virtual Path  : 1
    Vci Range First       : 100
    Vci Range Last        : 400
    Service Category      : rtVbr(2)
    PCR                   : 5000
    SCR                   : 5000
    MBS                   : 1

***** ATM Loopback Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit Port Entry
x) EXIT
Enter Selection (1 - 2, x)
>
```

153.2.4.2 Display SVC Connection table (AAL1 & AAL2)

This menu allows the user to display and edit the SVC Connection table. Please see the AudioCodes documentation for the meaning of the settings.

```
***** AAL1 Main Configuration Menu for MS2020 at 47.142.92.107 *****
```

```
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
4) SNMP configuration and security
5) Configure ATM loopback table
6) Display SVC Connection table
x) EXIT
Enter Selection (1 - 6, x)
> 6

***** SVC Connection Display Menu for MS2020 at 47.142.92.107 *****
1) List current table
x) EXIT
Enter Selection (1, x)
> 1

*** SVC Connection Table for MS2020 at 47.142.92.107 ***

    Empty table returned.

Press <enter> to continue

***** SVC Connection Display Menu for MS2020 at 47.142.92.107 *****
1) List current table
x) EXIT
Enter Selection (1, x)
>
```

153.2.4.3 Configure ATM port table (AAL1 & AAL2)

This menu allows the user to display, add and delete from the ATM port table. Please see the AudioCodes documentation for the meaning of the settings.

```
***** ATM Port Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit Port Entry
x) EXIT
Enter Selection (1 - 2, x)
> 1

*** Port Table for MS2020 at 47.142.92.107 ***

    Table Entry 1
    ************
    Administrative State  : unlocked(2)
    Operational State     : enabled(1)
    Port Number           : port0(0)
    Port Admin Address    :
    Operational Address   : 39345678901234567890a4a4a400908f045ce700
    Alarm Status          : 0
    Port Address Mode     : addrModeILMI(2)

***** ATM Port Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit Port Entry
x) EXIT
Enter Selection (1 - 2, x)
```

153.2.4.4 Configure Remote Gateway table (AAL2 only)

This menu allows the user to display add and delete from the Remote gateway table. Please see the AudioCodes documentation for the meaning of the settings.

```
***** Remote Gateway Configuration Menu for MS2020 at 47.142.92.107 *****
1) List Remote Gateway table
2) Add Remote Gateway entry
3) Delete Remote Gateway entry
x) EXIT
Enter Selection (1 - 3, x)
> 1

*** Remote Gateway Table for MS2020 at 47.142.92.107 ***

    Table Entry 1
    ************
    Row Status          : active(1)
    Action              : 0
    Action Result       : 0
    Index               : 0
    Name                : rtp7_gw
    NSAP Address        : 39345678901234567890a4a4a400908f045ce701
    ALCAP InstanceNum   : 0

***** Remote Gateway Configuration Menu for MS2020 at 47.142.92.107 *****
1) List Remote Gateway table
2) Add Remote Gateway entry
3) Delete Remote Gateway entry
x) EXIT
Enter Selection (1 - 3, x)
>
```

153.2.4.5 Configure AAL2 PVC table (AAL2 only)

This menu allows the user to display add and delete from the Port table. Please see the AudioCodes documentation for the meaning of the settings.

```
***** AAL2 PVC Configuration Menu for MS2020 at 47.142.92.107 *****
1) List PVC table
2) Add PVC entry
3) Delete PVC entry
x) EXIT
Enter Selection (1 - 3, x)
> 1

*** AAL2 PVC Table for MS2020 at 47.142.92.107 ***

    Table Entry 1
    ************
    PVC RowStatus            : active(1)
    Action                   : none(0)
    Action Result            : none(0)
    PVC Remote Gateway Index : 0
    PVC VCCI Path ID         : 1
    PVC PortNumber           : port0(0)
    PVC Vpi                  : 3
    PVC Vci                  : 54
    PVC MaxNumOfCid          : 5
```

```
    PVC NumOfCidInUse        : 0
    PVC ServiceCategory      : cbr(1)
    PVC PCR                  : 5
    PVC SCR                  : 0
    PVC MBS                  : 0

***** AAL2 PVC Configuration Menu for MS2020 at 47.142.92.107 *****
1) List PVC table
2) Add PVC entry
3) Delete PVC entry
x) EXIT
Enter Selection (1 - 3, x)
>
```

153.2.4.6 Configure SVC Profile table (AAL2 only)

This menu allows the user to display and edit the SVC Profile table. Please see the AudioCodes documentation for the meaning of the settings.

```
***** SVC Profile Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit SVC Profile Entry
x) EXIT
Enter Selection (1 - 2, x)
> 1

*** SVC Profile Table for MS2020 at 47.142.92.107 ***

    Table Entry 1
    ************
    Is Profile used   : yes(1)
    Profile Index     : 1
    Maximum # of CIDs : 4
    PCR               : 800
    SCR               : 800
    MBS               : 1
    Persistence       : 180
    Service Category  : rtVbr(2)

***** SVC Profile Configuration Menu for MS2020 at 47.142.92.107 *****
1) List current table
2) Edit SVC Profile Entry
x) EXIT
Enter Selection (1 - 2, x)
>
```

153.3 Applicable customer facing sections

Fault Management

Not applicable	__X___
Logs	_____
Alarms	_____

Configuration

Not applicable	_____
Data Schema/MIBs	_____
User Interface	__X___
GUI	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	__X___
Billing changes	_____
Performance	__X___
Not Applicable	_____
Operational Measurements	_____
Performance Measurements	_____
Realtime	_____
Not applicable	__X___
Engineering Information	_____
Not applicable	__X___

153.4 Hardware Requirements or Dependencies

153.5 Software Requirements or Dependencies

153.6 Limitations and restrictions

153.7 Interactions

153.8 Glossary

Term	Description
MS2020	Media Server 2020, ATM Media Server

154: Functional description (FN): A00004922

154.1 Feature name

A00004922 DMS-250 N449 PRI Enhancements - GWC

A00004923 DMS-250 N449 PRI Enhancements - SPM

154.2 Synopsis

This FN documents the functionalities provided by features A00004922 (DMS-250 N449 PRI Enhancements - GWC) and A00004923 (DMS-250 N449 PRI Enhancements - SPM) in Succession environment.

A00004922 covers the functionalities required to support the following N449 Primary Rate Interface (PRI) enhancements:

- Support of CodeSet 0 (CS0) parameterized Network Specific Facilities Information Element (NSF IE) with Out-Of-Band (OOB) data in Facility message.
- Support of CS6 Facility IE, Billing IE, and Item IE in Facility message.
- Support of CS0 and CS7 User-to-User Information (UUI) if present in PRI Disconnect message.

A00004923 covers the functionalities required to support the following N449 PRI enhancements:

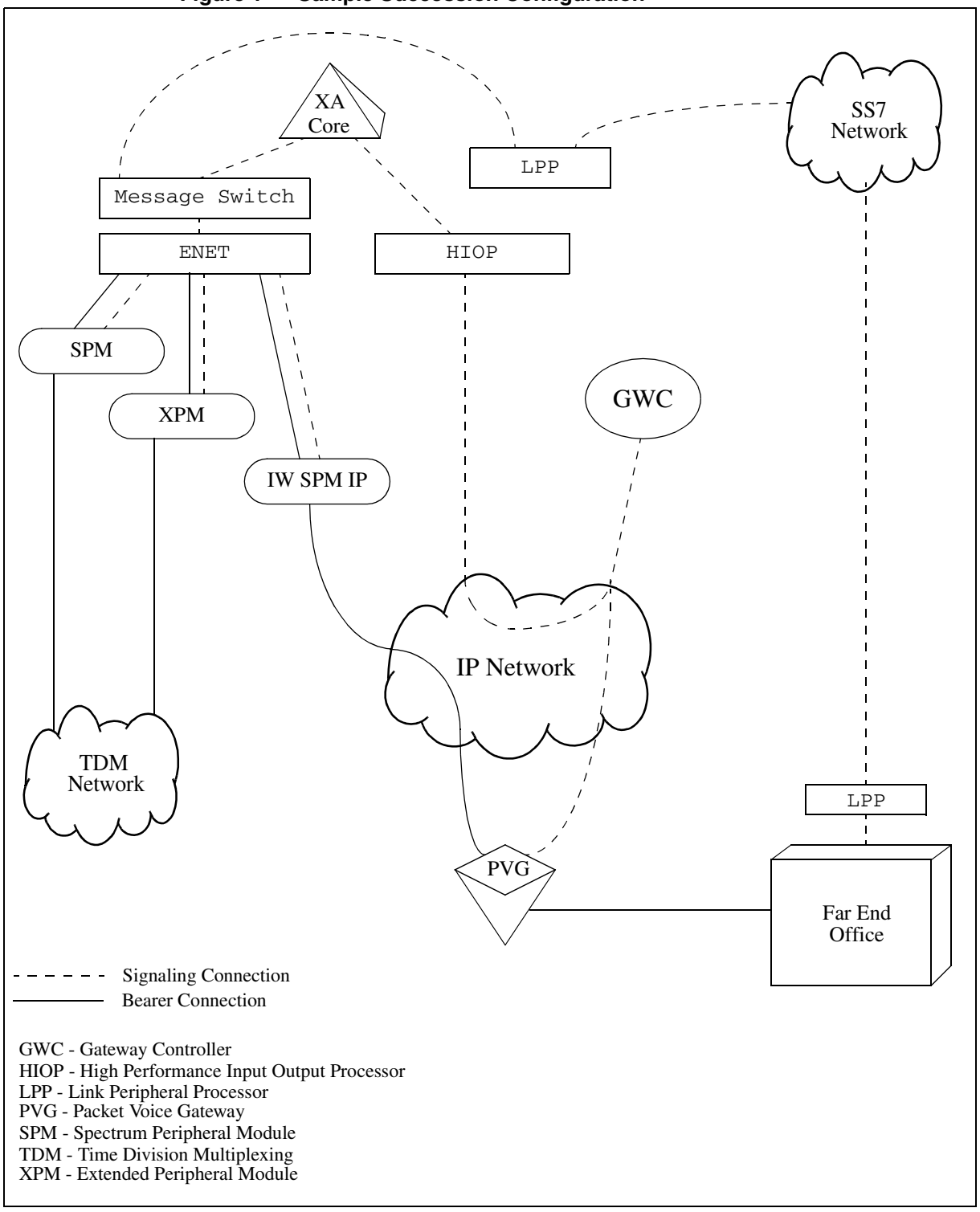
- Support of CS0 parameterized NSF IE with OOB data in SETUP and Facility messages.
- Support of CS6 Facility IE in Facility message.

154.3 Background

A brief description of Succession environment and its components is presented in this section as the background information.

Figure 1 - Sample Succession Configuration on page 23, shows a switch that is capable of Time Division Multiplexing (TDM) as well as Succession environment.

Figure 1 - Sample Succession Configuration



A description of the IP components are presented in “Table 1 - IP Components” on page 1855:

Table 1 - IP Components

IP Component	Explanation
XA-Core	Performs the call processing functions for a TDM and/or IP based solution. Also known as the computing module (CM).
Gateway Controller	Functions as the interface between the XA-Core and gateways such as the PVG. The GWC handles signaling from the core that was previously handled by the TDM SPM/XPM. Examples of this include Integrated Services Digital Network User Part (ISUP) and PRI. To communicate with gateways; the GWC also supports protocols such as ASPEN, ISDN User Adaptation Protocol (IUAP), and H.248.
Interworking SPM IP	Provides trunking capability from a TDM network to the IP network. TDM voice flows in the IW SPM IP from the ENET and is sent to the PVG in the form of IP packets. The reverse function is also performed. It is important to note that trunks do not hang off the IW SPM IP as they do with TDM SPMs.
Packet Voice Gateway	Functions as a gateway to the network for the bearer (i.e. speech) path. Bearer voice over IP packets are received from peripherals such as the IW SPM IP and sent to the outside network in the form of IP packets or TDM voice.
Link Peripheral Processor	This SS7 entity is the switch’s link to the SS7 network. It functions in the IP world exactly as it does in the TDM world. In a TDM environment, the SPM/XPM sends an ISUP Initial Address Message (IAM) to the destination switch by bouncing the IAM through the core to the LPP to the SS7 Network. In an IP environment, the GWC sends an ISUP IAM to the destination switch in exactly the same way.
High Performance Input Output Processor	Provides the XA-Core a 100 Base ethernet access to the IP network. This allows communication between the core and the gateway controller.

154.4 Feature Description

154.4.1 A00004922 DMS-250 N449 PRI Enhancements - GWC

The functionalities provided by GWC for N449 PRI are documented in the following subsections.

154.4.1.1 Support of CS0 Parameterized NSF IE with OOB data in Facility Message

This feature supports three new NSF service identifiers in CS0 for the N449 PRI. The service identifier is sent in the Service Parameter field of the NSF IE in a Facility message. The new service identifiers are:

- OOB triggers and data allowed (0001100)
- Only OOB triggers allowed (0001101)
- Network Managed Data (NMD) (0001110)

The GWC supports the receipt of the following parameterized values in a Facility message.

Table 2 - Parameterized Network Specific Facilities Information Element.

Octet	Values
Octet 1	00100000 (NSF IE identifier)
Octet 2	Length of NSF IE
Octet 3:	00000000 (Length of network identification)
Octet 4: Bit 8	**0 (Parameterized)**
Octet 4: Bit 7	1 (Extension)
Octet 4: Bit 6	**0 (Feature)**
Octet 4: Bit 5-1	01001 (Available Feature Indicator)
Octet 5: Bit 8	0 (Spare)
Octet 5:Bits 7-1	Service Parameter Field
	0001100 OOB Triggers Allowed - Data Allowed **0001101 OOB Triggers allowed - Data Not Allowed** **0001110 Network Managed Data (NMD)**

154.4.1.2 Support of CS6 Facility IE in Facility Message

This feature supports a CS6 Facility IE length of up to 200 octets in an N449 PRI Facility message. A sample format of CS6 Facility IE supported is shown below. The highlighted operation values are the new values supported.

Table 3 - Parameterized Network CS6 Facility IE

Octet	Values
Octet 1	Service Discriminator = 10001
Octet 2	Component Type Tag = 10100001 (Invoke)

Octet	Values
Octet 3:	Component Length
Octet 4: Bit 8	Invoke ID Tag = 00000010 (Invoke ID tag)
Octet 4: Bit 7	Invoke ID Length
Octet 4: Bit 6	Invoke ID
Octet 4: Bit 5-1	Operation Value Tag = 00000010 (Operation Value Tag)
Octet 5: Bit 8	Operation Value Length
Octet 5:Bits 7-1	**Operation Value**
	11001110 (Redirect Call)
	11001111 (Put Calling Party on Hold)
	11010000 (Retrieve Calling Party From Hold)
	11010001 (Drop TP)
	11010011 (User Data Transfer)
	11001100 (Billing Operation)
	11010010 (Application Specific Call Status)
	10001111 (Request Feature)
	Q.931 IE tag = 01000000

154.4.1.3 Support of CS6 Billing IE, and Item IE in Facility Message

This feature provides the capability to receive and transmit an N449 PRI Facility message containing CS6 Billing Service Data IE, and/or CS6 Item IE.

The Billing Service Data IE can be received in a Facility message on a call after a Call Proceeding message has been received or sent.

The content of the Billing Service Data IE is presented in “Table 4 - Billing Service Data Information Element” on page 1857. Up to 100 octets of billing service data is supported. The Billing Service Data IE may appear in a Facility message as long as the total number of octets within the message does not exceed the maximum.

Table 4 - Billing Service Data Information Element

Octet	Values
Octet 1	01011000 (Billing Service Data IE identifier)
Octet 2	Length of Billing Service Data IE
Octet 3: Bit 8	1 (Extension)
Octet 3: Bits 7-5	000 (spare)

Octet	Values
Octet 3: Bits 4-1	Type of Billing Service Data 0011 Append To Record: Non-Mutilated Data 0100 Append To Record: Mutilated Data
Octet 4 - 103	Billing Service Data

The content of the Item IE is presented in “Table 5 - Item Information Element” on page 1858.

Table 5 - Item Information Element

Octet	Values
Octet 1:bit 8	0 Set value
Octet 1:bits 7-1	1001101 (Item IE Identifier)
Octet 2	Length of Item IE
Octet 3: Bit 8	1 (Extension)
Octet 3:Bits 7-1	Item 0100001 Billing Closure 0101001 Send Close Message

154.4.1.4 Support of CS0 and CS7 UUI IE

This feature provides the capability to receive and transmit CS0 and/or CS7 UUI IE if present in an N449 PRI Disconnect message.

The content of UUI IE is presented in “Table 6 - User-to-User Information Element” on page 1858.

Table 6 - User-to-User Information Element

Octet	Values
Octet 1:bit 8	0 Set value
Octet 1:bits 7-1	1111110 (UUI IE Identifier)
Octet 2	Length of UUI IE
Octet 3+	User Information (See notes)

Notes: The contents of user information are structured according to the user application.

154.4.2 A00004923 DMS-250 N449 PRI Enhancements - SPM

The functionalities provided by SPM for N449 PRI are documented in the following subsections.

154.4.2.1 Support of CS0 Parameterized NSF IE with OOB data in SETUP and Facility Message

This feature supports three new NSF service identifiers in CS0. The service identifier is sent in the Service Parameter field of the NSF IE in a SETUP and Facility message.

Refer to “154.4.1.1 Support of CS0 Parameterized NSF IE with OOB data in Facility Message” on page 1856 for more information.

154.4.2.2 Support of CS6 Facility IE in Facility Message

This feature supports a CS6 Facility IE length of up to 200 bytes in a Facility message.

Refer to “154.4.1.2 Support of CS6 Facility IE in Facility Message” on page 1856 for more information.

154.5 Hardware Requirements or Dependencies

Not Applicable.

154.6 Software Requirements or Dependencies

Not Applicable.

154.7 Limitations and restrictions

Not Applicable.

154.8 Interactions

Not Applicable.

154.9 Applicable customer facing sections

Fault Management

Logs	__N/A____
Alarms	__N/A____

Configuration

Data Schema	__N/A____
User Interface	__N/A____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____

Accounting (includes AMA billing) __N/A_____

Performance (includes operational measurements) __N/A____

154.10 Glossary

Term	Description
AMA	Automatic Message Accounting
ASPEN	Nortel's Media Gateway Control Protocol
CM	Computing Module
CS	CodeSet
CS0	CodeSet 0
CS6	CodeSet 6
CS7	CodeSet 7
GWC	Gateway Controller
HIOP	High performance Input Output Processor
H.248	Media Gateway Control Protocol
IAM	Initial Address Message
ISUP	Integrated Services Digital Network User Part
IUAP	ISDN User Adaptation Protocol
IW-SPM IP	Interworking Spectrum Peripheral Module IP
LPP	Link Peripheral Processor
NMD	Network Managed Data
NSF IE	Network Specific Facility Information Element
OOB	Out-Of-Band
PRI	Primary Rate Interface
PVG	Packet Voice Gateway
SS7	Signaling System No. 7
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
UUI	User-to-User Information

Term	Description
AMA	Automatic Message Accounting
ASPEN	Nortel's Media Gateway Control Protocol
CM	Computing Module
CS	CodeSet
CS0	CodeSet 0
CS6	CodeSet 6
CS7	CodeSet 7
XPM	Extended Peripheral Module

155: Functional Description (FN): A00004923

155.1 Feature name

AT&T DMS-250 N449 PRI Enhancements - SPM

155.2 Description

Refer to the FN section of feature A00004922 for detailed information.

155.3 Hardware Requirements or Dependencies

155.4 Software Requirements or Dependencies

155.5 Limitations and restrictions

155.6 Interactions

155.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

155.8 Glossary

Term	Description
New term	Definition

156: Functional Description (FN): A00005007

156.1 Feature name

Cause Indicators parameter support for DTAG AMA Enhancement.

156.2 Description

This feature addresses the specific requirements defined by Deutsche Telekom AG (DTAG) for reporting the cause indicator parameter in the AMA records for an Avst (International Gateway Switch).

This feature is in continuation with feature A00003007 AMA Enhancements for DTAG International Gateway.

156.2.1 Functional Overview.

The DTAG specifications states that the cause indicator of the release message be captured in AMA records.

This feature captures the Cause Indicator for ETSI ISUP to ETSI ISUP non-INAP tandem call for the following scenarios.

- GWC sends a Clear Forward Message.
- GWC sends a Clear Back Message.
- GWC reports the Release message to the CM.

In a Tandem (or Gateway) switch, for most of the cases, the release message is bounced on the GWC and not sent to the CM. Upon receiving a release message, the GWC sends a CLEAR_FORWARD or CLEAR_BACKWARD message to the CM to tear down the call.

This feature introduces a mechanism to transport CI parameter from GWC to CM in CLEAR_FORWARD or CLEAR_BACKWARD message. Figure2 explains the mechanism.

A new office parameter REPORT_ISUP_CI_TO_CM will be created in table OFCENG, which will govern the functionality.

- If the office-parameter is set to ‘Y’, functionality is enabled
- If the office-parameter is set to ‘N’, functionality is disabled.

Figure 1 Example datafill of REPORT_ISUP_CI_TO_CM

```
Table OFCENG
REPORT_ISUP_CI_TO_CM    N
```

The Extraction of Cause Indicator will be fully invoked if

- The Office Parameter CAPTURE_TMR_ST_CI of TABLE AMAOPTS is ON.
- The Office Parameter REPORT_ISUP_CI_TO_CM of TABLE OFCENG is set to YES.

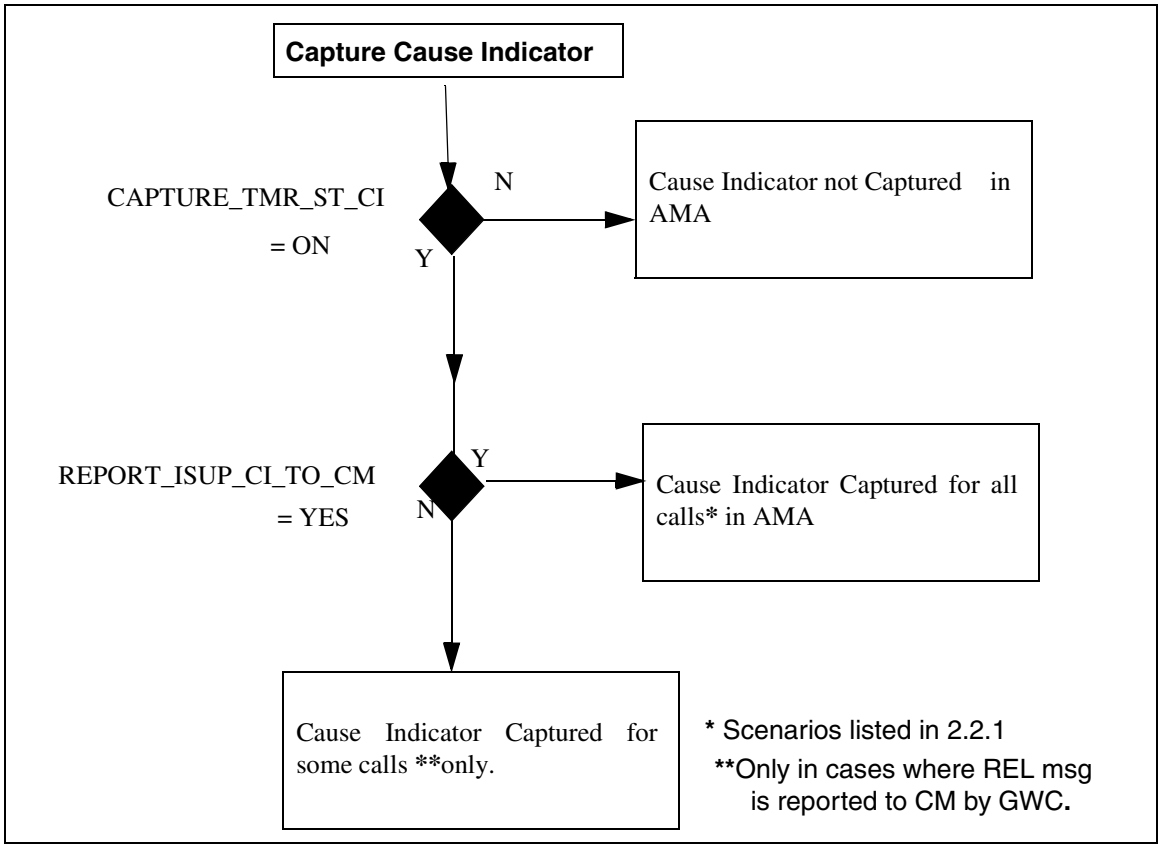
While data filling CAPTURE_TMR_ST_CI in table AMAOPTS, this feature introduces additional **warning** to data fill REPORT_ISUP_CI_TO_CM to YES to ensure complete functionality.

Figure 2 Warning while data filling CAPTURE_TMR_ST_CI.

```
TABLE: AMAOPTS
>pos capture_tmr_st_ci
   CAPTURE_TMR_ST_CI                                OFF
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>ON
TUPLE TO BE CHANGED:
   CAPTURE_TMR_ST_CI                                 ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Note: Additional AMA MC611 (context ID 80100) will be
generated for all ETSI ISUP tandem (non-INAP) calls.
Warning : Please ensure that the office parameter
REPORT_ISUP_CI_TO_CM in table OFCENG is set to YES to
enable full functionality of capturing Cause Indicator.
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

The cause indicator will be stored in AMA record in AMA generic module code 611 with context id 80100 (TMR_ST_CI).

Figure 3 Capturing of Cause Indicator in AMA records

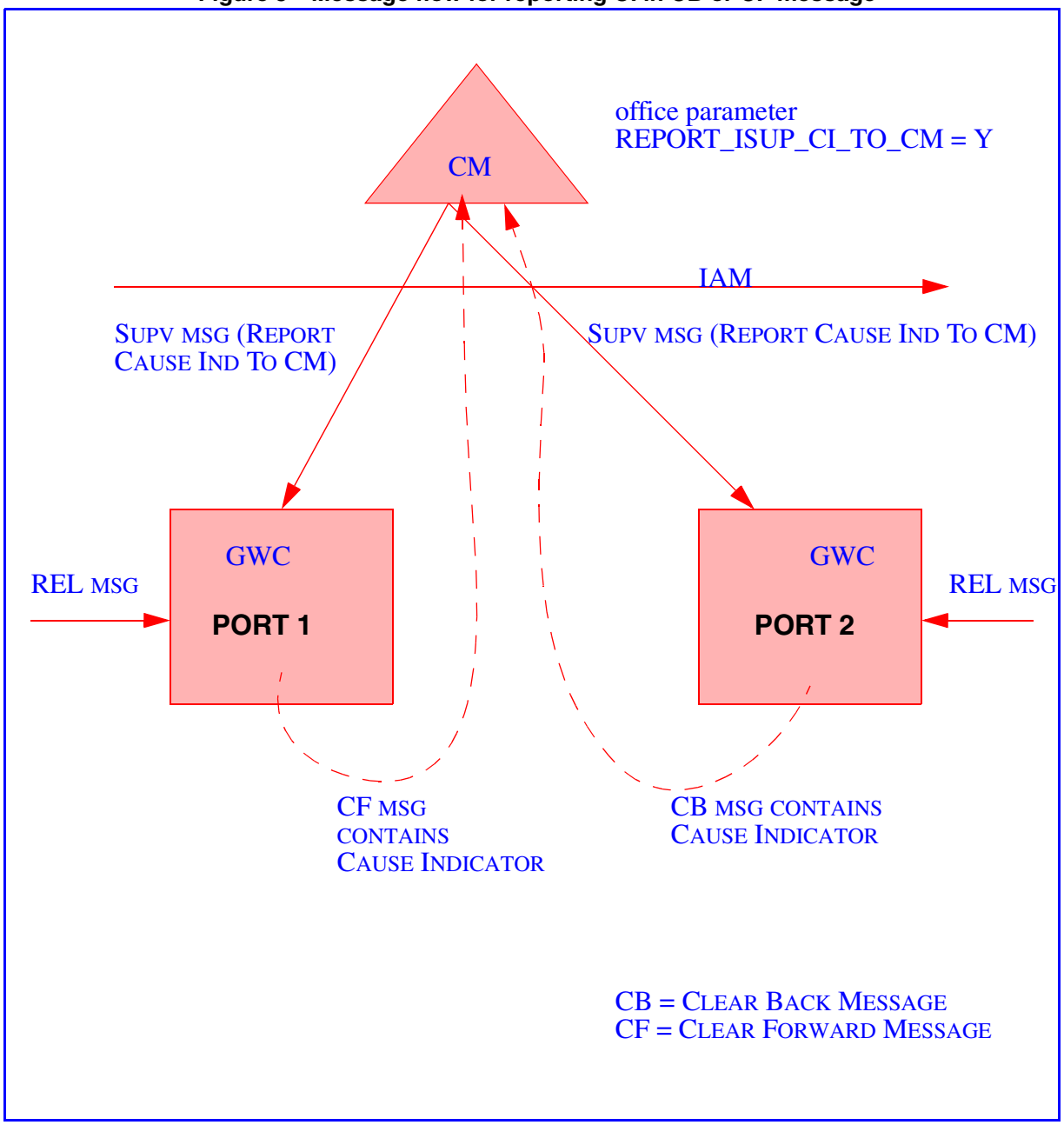


The Cause Indicator will appear in AMA records as below.

Figure 4 Cause Indicator parameter in AMA records.

```
MODULE CODE:                        611C      GENERIC MOD: ONE DGT STR FMT
 GENERIC CONTEXT ID:
     PARSE RULES                    80100     TMR/SERVTYPE/CAUSE IND
     SIGNIFICANT DIGITS              00C       NIL
 GENERIC DIGIT STRING ONE:
     TRANSMISSION MEDIUM REQ          003
    SERVICE TYPE                      000
    CODING STANDARD                   0         ITU-T
     LOCATION                         00        U
     CAUSE VALUE (CLASS PORTION)      1 NORMAL EVENT
     CAUSE VALUE (VALUE PORTION)      00
     UNUSED                           000C
 MODULE CODE:                         000C      FINAL MODULE
```

Figure 5 Message flow for reporting CI in CB or CF message



156.3 Hardware Requirements or Dependencies

-N/A-

156.4 Software Requirements or Dependencies

-N/A-

156.5 Limitations and restrictions

For scenarios in which the CS2K releases the call, cause indicator is not captured in AMA records (Module 611, Context id 80100)

The figure below shows the values of CI which will appear AMA in such scenarios.

Figure 6 Default Cause Indicator in AMA records

```
MODULE CODE:                        611C      GENERIC MOD: ONE DGT STR FMT
 GENERIC CONTEXT ID:
     PARSE RULES                    80100     TMR/SERVTYPE/CAUSE IND
     SIGNIFICANT DIGITS              00C       NIL
 GENERIC DIGIT STRING ONE:
     TRANSMISSION MEDIUM REQ         003
    SERVICE TYPE                     000
    CODING STANDARD                  0         ITU-T
     LOCATION                        00        U
     CAUSE VALUE (CLASS PORTION)     0         NORMAL EVENT
     CAUSE VALUE (VALUE PORTION)     00
     UNUSED                          000C
 MODULE CODE:                        000C      FINAL MODULE
```

156.6 Interactions

156.7 Applicable customer facing sections.

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters ___X___

Accounting (includes AMA billing) ___X___

Performance (includes operational measurements) _____

156.8 Glossary

Term	Explanation
CS2K	Call Server 2000
DTAG	Deutsche Telekom AG
GWC	Gateway Controller
CB	Clear Back
CF	Clear Forward
CI	Cause Indicator

Recommended Reading/References

[1] 163TR75 - DTAG specification for the Telekom-ISUP (T-ISUP)

[2] 163TR76 -DTAG specification for the Gateway-ISUP (G-ISUP)

[3] 163TR80 - DTAG interworking specification (R2, G-ISUP, T-ISUP)

[4] A00003007- AMA Enhancements for DTAG Intl GW

[5] KDS:IN specification, DTAG, release date unknown.

[6] Tarifierung von IN-Verbindungen“, FTZ 163 TL 50 Teil 1/10.94, Anhang AA, DTAG, Oct 1994.

[7] „Beschreibung der Kommunikationsdatenerfassung für IN“, FTZ 163 TL 500 Teil 1200/10.94, Anhang D, DTAG, Oct 1994.

[8] KDS:N specification (163 TL 500 Teil 1202/10.94, Anhang C), DTAG, Oct 1994.

[9] KDS:A specification („Technische Spezifikation MSP-T, Anhang A: Datenformat NAKODA (KDS:A)“, Version 1.0, DTAG, Mar 28th, 2002.

[10] TZ 163 TR 75.97 „T-ISUP“, DTAG, Aug 25th, 1997.

[11] TZ 163 TR 76.98 „Anwendungsspezifikation für das Zeichengabesystem Nr. 7 - G-ISUP“, DTAG, Apr 1998.

[12] TZ 163 TR 78.96 „T-INAP“ Teil 1+3+4, DTAG, Apr 1996.

[13] TZ 163 TR 80.98 Annex 3 „Tarifierung von IN-Verbindungen“, DTAG, Apr 1998.

157: Functional Description (FN): A00005016

157.1 Feature name and Feature ID

A00005016: VMG Out of Service Alarms

157.2 Description

This document provides the functional description for support of additional VMG alarms on the MG 9000 and Media Gateway 9000 Manager.

In SN06.2, there is only one alarm that is raised if a VMG has been provisioned that is in an Out of Service state. Unfortunately, the state of VMG Out of Service is symptomatic of many problems that could be occurring:

missed steps in LCI commissioning

bad IP address input during VMG provisioning

mismatch provisioning between MG 9000 Mgr and the core during ABI provisioning

network router issues

ITP/ABI is locked or disabled

GWC locked

card is still initializing

This feature addresses the problem that resolution of a single VMG OOSV alarm is too complex, especially at VMG provisioning time. Instead of the single fault raised in SN06.2 - VMG300 - VMG OOS, there will instead be a number of faults, each describing a different root cause for why the MG9K is not in service. Raising different alarms helps the user to narrow their resolution /debugging efforts to what is specifically broken.

In addition, because these different alarm reasons are logged, there will now be extra information in the logs when the VMG goes out of service as to why it did so (manually set to out of service vs. GWC unreachable vs. GWC not responding).

As a result of this feature, when a VMG goes out of service, the Alarm Browser will show the VMG300 alarm only in very unusual circumstances - instead, one or more of the following faults will be raised:

rootTermStatusChange (1), -- generic reason

vMGAdminStatusOutOfService (2), - VMG was administratively set to out of service

cardLocked (3), -- card is locked
cardDisabled (4), -- card is disabled
cardInitializing (5), -- card is initializing
lineMtceOnPairNotReady (8), -- Line maintenance is not ready
megacoMtceOnPairNotReady (8), -- Megaco maintenance is not ready
gWCUnreachable (53), -- pings to reach GWC failed
noGWCReply (54), -- GWC didn't reply to ServiceChange
aal1BearerSubsystemOnPairNotReady (56),
ipBearerSubsystemOnPairNotReady (57),

All faults are cleared when a VMG goes to an In Service state.

While the VMG300 alarm was always critical in SN06.2, the following faults will be raised at a severity level of warning instead of critical to indicate that there was a (likely) user-initiated reason the VMG is out of service:

Initializing - this fault will be raised during the initial period after an ITP/ABI card pair has been restarted or when the ITP/ABI is waiting for an initial registration response from the GWC, after which the VMG will either be in service (all faults cleared) or a different alarm will be raised

Card Locked - if the active ITP or ABI has been locked

VMG Admin Status Out Of Service - if the VMG has been set to out of service in the Gateway Status Config tab of the Switched Lines Services GUI

All of the other faults will have a severity of critical.

The Switched Lines Services GUI will show what VMG alarms are currently raised against the VMG in a new field in the GW Status Config screen.

More information on the purpose and clearing procedures of the new faults is in the Fault Management section of this DDOC.

157.3 Applicable customer facing sections

Fault Management

Logs	__X____
Alarms	_X_____

Configuration	
Data Schema/MIBs	__NA____
User Interface	___X___
GUI	___X___
Element Management	____NA__
Security	____NA__
Service Order	____NA__
Office Parameters	____NA__
SOC	____NA__
Upgrades impact	___NA___
Accounting (includes AMA billing)	____NA__
Performance	___NA___
Realtime	___NA___
Engineering Information	__NA____

157.4 Hardware Requirements or Dependencies

N/A

157.5 Software Requirements or Dependencies

N/A

157.6 Limitations and restrictions

After SWACTs and card pair restarts, any alarms that had been raised against the VMG before the restart or SWACT are cleared and new faults are raised to match the present VMG fault state of the active card.

157.7 Interactions

N/A

157.8 Glossary

VMG	Virtual Media Gateway

158: Functional Description (FN): A00005073

158.1 Feature name

SBA Outbound Connection Security

158.2 Description

This feature provides optional secure outbound file transfer using OpenSSH sftp client. The sftp client protects all data including sensitive user s' password by encrypting the data before it leaves SDM/CBM and decrypting the data after it arrives the downstream OSS. The sftp also provides data integrity check to ensure that no one has tampered the data during the transfer.

The SBA user can configure the secure file transfer by adding or changing an existing schedule tuple in billmtc. For SN07, the user has to manually accept the downstream host key for each destintation before configuring secure outbound file transfer to the destintation. The actual configuration details are documented in the configuration section.

This feature also enhances SBA password protection scheme by using SDM/CBM private data manager (documented in A00005074) to store all the passwords for OSS access. The private data manager is responsible for storing the data in an encrypted form.

158.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

158.4 Software Requirements or Dependencies

158.4.1 Software requirements for downstream system

A SSH sftp-server[1] which is compatible with OpenSSH sftp client must be running on the downstream Operations Support System (OSS) in order for SBA to transfer data with OpenSSH sftp client.

158.4.2 Software requirements for SDM.

The OpenSSH and its dependencis should be installed on the SDM/CBM. If this software is unavailable, SBA user will not be able to uses the SFTPW protocol for outbound file transfer. There is no explicity check done by the SBA software to determine if this package/fileset is installed during SFTPW configuration time. If the SBA SFTPW application fail to find the sftp

[1]SFTP server subsystem

program, it raised a SFTPW alarm and terminates the transfer event immediately.

For CBM, this feature depends on the OpenSSH packages as well as NTutil

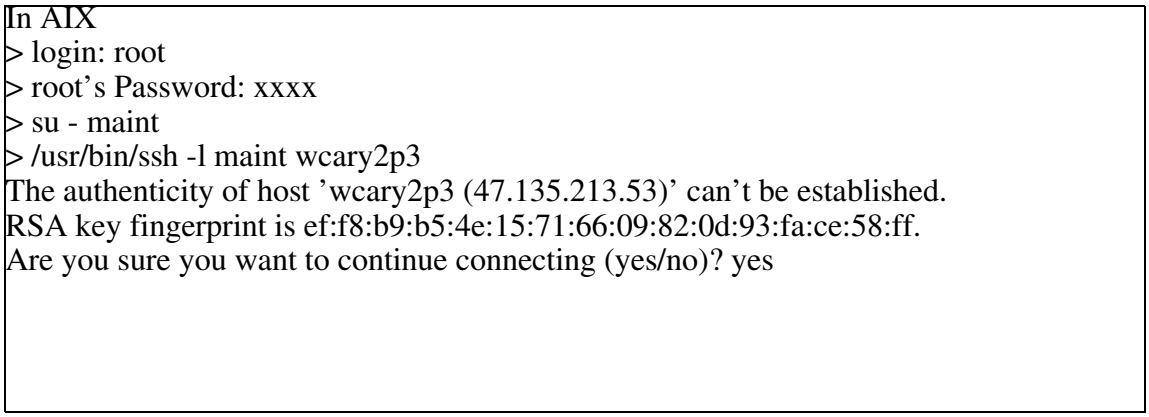
For SDM, this feature depends on SDM_OpenSSH.base and SDM_BASE.util fileset must be installed manually.

158.5 Limitations and restrictions

- As described in Section “158.4 Software Requirements or Dependencies”, that the SFTPW is only available if OpenSSH and the SDM base util software is iinstalled. SBA uses OpenSSH software verion 3.7.1p2 or later for secure file transfer.
- Public keys authentication is not supported in this release. All users are authenticated with userid/password to the dowstream OSS.
- The overall billing data traffic rate is lower than that of a FTPW with a given SBA CPU usage. For more information, please refer to the SDM EI section.
- The initial host key acceptance of the downstream processor should be done manually before it can use the SFTPW[1] to transfer files from SDM/CBM. Figure 1 shows how to accept a host key manually. The .ssh/known_hosts file in maint’s home directory will be edited by SSH software to include the host key. After that SBA can use sftp to send file to the downstream OSS as maint/root. This procedure must be done for each downstream destintation. This step must be done prior to schedule tuple configuration for SFTPW.
- The SSH-2 server running on the downstream OSS must be compatbile with OpenSSH sftp client.
- Due to governement restrictions on export/import of encryption software, secure file transfer will not be available on SDM/CBM loads that shipped to some countries with restrictions on the strength of encryption.
- Does not secure data transfer for AFT, RTB and sendtape applications

[1]SFTPW - Secure File Transfer Protocol Wrapper which controls sftp client to send files using SSH protocol

Figure 1 Host key acceptance



158.6 Interactions

No

158.7 Applicable customer facing sections

Fault Management	
Logs	___X__
Alarms	___X___
Configuration	
Data Schema	__N/A_
User Interface	__X__
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	__N/A__

158.8 Glossary

Term	Description
SDM	Supernode Data Manager

Term	Description
CBM	Core Billing Manager
SBA	SDM/CBM billing application
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol (SSH internal protocol)
OSS	Operations Support System

159: Functional Description (FN): A00005074

159.1 Feature name

OMDD: Outbound Connection Security

159.2 Description

The OM Data Delivery (OMDD) application on the SDM/CBM collectes OM reports from the core, processes them in to CSV files and sends the CSV files to downstream destinations (OSS). Prior to this activity, the outbound transfer of CSV files from SDM/CBM to downstream was always insecure because it used only the standard ftp protocol to do the transfer. The standard ftp protocol sends out user password as well as data in cleartext, making them vulnerable to reading by a thirdparty by interceptiing them in the network.

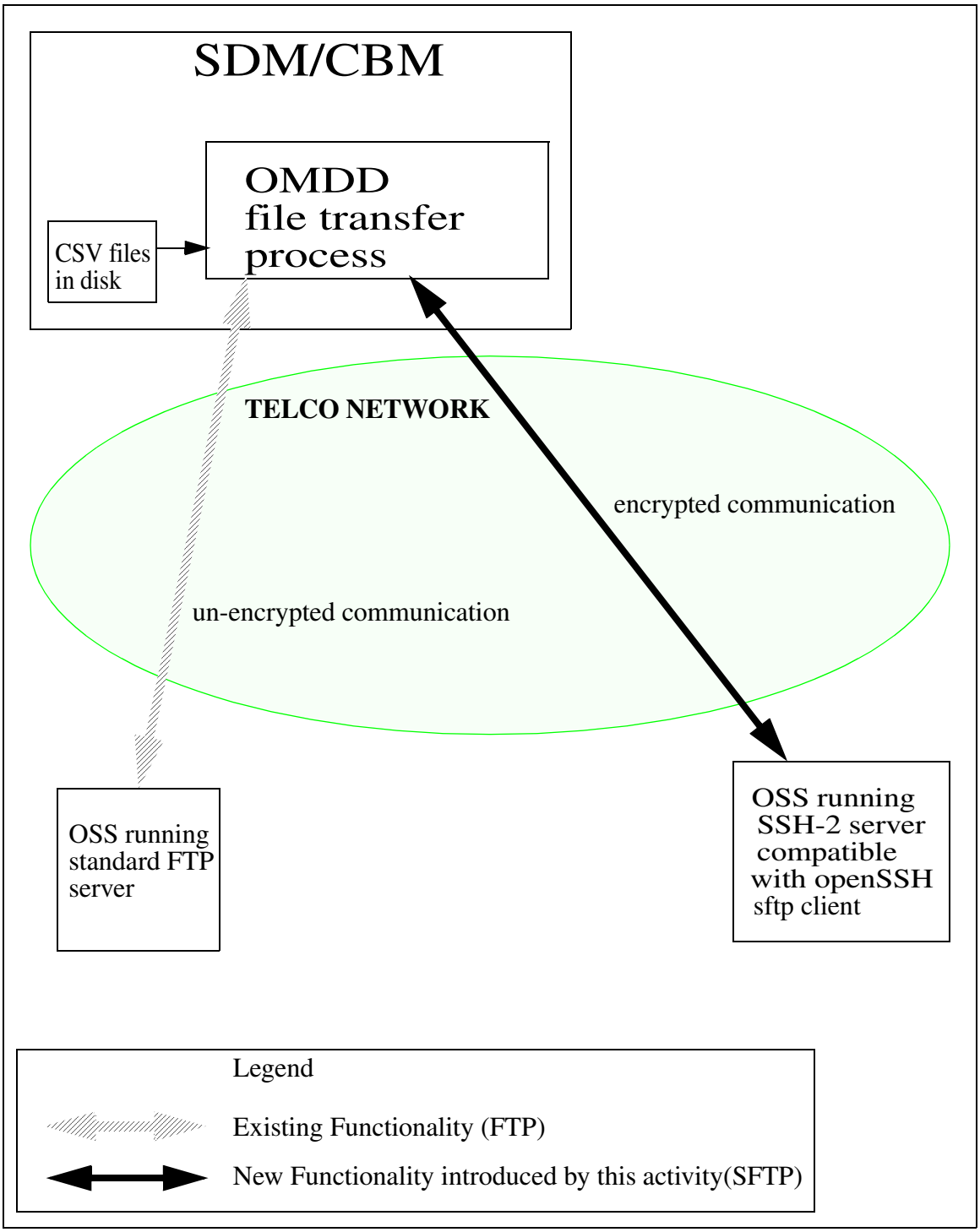
This activity provides an optional mechanism to prevent OMDD outbound transfers from sending out clear text passwords and data in the network. The mechanism uses the OpenSSH secure ftp client for doing outbound filetransfers from SDM/CBM to the downstream destination. OpenSSH encrpyts all data (including passwords) exchanged between the SDM/CBM and downstream, thus making them resistant to reading bya thirdpary by intercepting them in the network.

Figure 1 shows the OMDD outbound file transfer functionality after this activity. It should be noted that secure file transfer is only an optional mechanism and the user can still choose standard ftp for file transfers. This choice can be done while configuring or modifying file transfer destinations.

The user configures file transfer destinations on the SDM/CBM using the OMDD User Interface program (OMUI). It is the configuration tool for OMDD. This activity modifies the Add and Modify File Transfer Destination menus of OMUI. From now on, when a user adds or modifies a file transfer destination, he/she will be asked to select the type of file transfer for the destination in addition to the already existing parameters. The choices for the type of file transfer will be “Standard” and “Secure” . The default choice will be “Standard”.

While doing the actual file transfer, OMDD will invoke either the standard FTP client or the secure FTP client by looking at the choice made by the user at the time of configuration. A customer log SDMO375 will be generated if the OM file transfer fails.

Figure 1 OMDD File Transfer view



Additionally, this feature develops a Private Data Manager on the SDM./CBM for encrypting data by all applications. OMDD will contact the Private Data Manager for storing downstream destination passwords in encrypted format.

159.3 Hardware Requirements or Dependencies

No hardware requirements or dependencies are introduced by this feature.

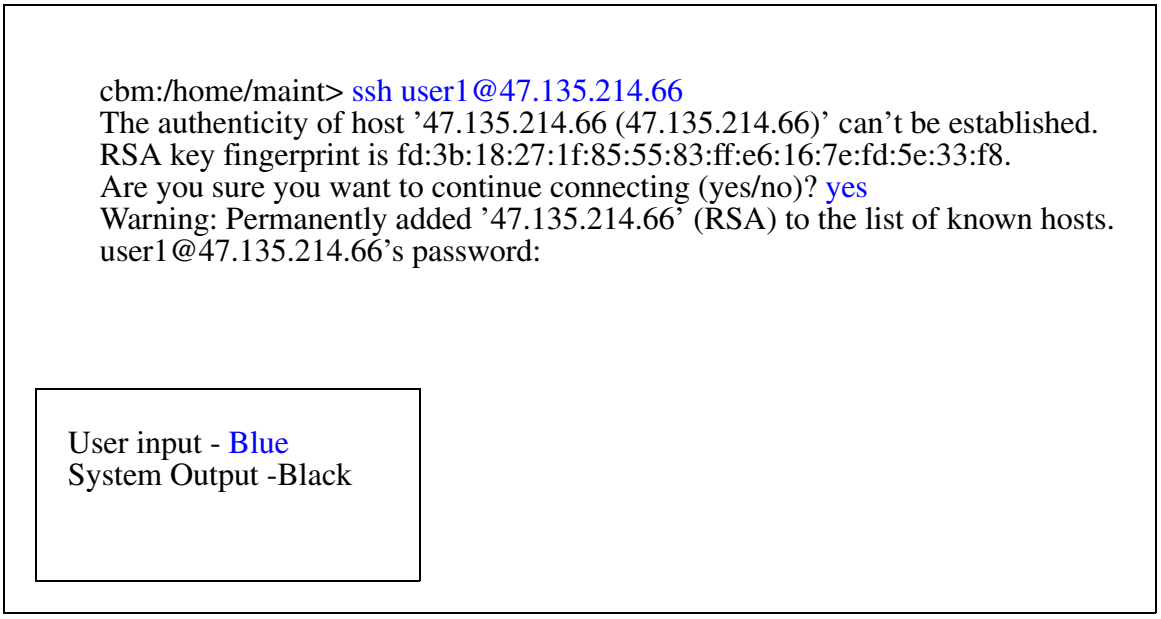
159.4 Software Requirements or Dependencies

The customer's downstream machine (the OSS) should be running a SSH-2 server compatible with SFTP client of OpenSSH.The OpenSSH fileset should be installed on the SDM/CBM too.

159.5 Limitations and restrictions

- The additional overhead of encrypting/decrypting all data will affect the capacity of OMDD if secure ftp is used.
- Public keys authentication is NOT supported in this release. All users are authenticated with userid/password with the downstream OSS.
- The initial host key acceptance of the downstream processor should be done manually before it can use the SSH protocol to transfer file from SDM/CBM. Figure 2 shows an example how to accept a host key. The /home/maint/.ssh/known_hosts file will be edited by ssh to include the host key. After that user can use SSH for OMDD file transfer. OMDD will use the /home/maint/.ssh/known_hosts file when invoking the sftp client.
- The SSH-2 server running on the downstream OSS should be compatible with the OpenSSH sftp client.
- Due to government restrictions on export/import of encryption software, this feature will not be available on SDM/CBM loads shipped to some countires.

Figure 2 Example of adding the host key of downstream processor to the known_hosts file



159.6 Interactions

Not Applicable

159.7 Applicable customer facing sections

Fault Management	
Logs	__X_
Alarms	__N/A_
Configuration	
Data Schema	__N/A_
User Interface	___X__
Element Management	__N/A_
Security	__ N/A_
Service Order	__N/A_
Office Parameters	__N/A_
Accounting (includes AMA billing)	__N/A_

Performance (includes operational measurements) __N/A_

159.8 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
OMDD	Operational Measurements Data Delivery
OMUI	OMDD User Interface
CSV	Comma Seperated Value
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol
OSS	Operations Support System

160: Functional Description (FN): A00005089

160.1 Feature name and Feature ID

A00005089: NOA Routing for IC Agency - TRAVER Enhancement

160.2 Description

Feature A00004192 enhances NOA routing to support CAP and INAP protocols, TRAVER tool is also enhanced to verify NOA routing for CAP and INAP protocols.

TRAVER is enhanced to display the result of a search for a match in table CDNCHAR for CAP and INAP protocol. Only TRACE option B for MS selector is supported.

Additional enhancement makes users can replace LAC, CID/SAC option with a new XLAENTRY option, so that they can directly specify the XLAENTRY INDEX they want without datafilling and looking up table LAC to find it. It's useful when users just want an entry point of UXLA to verify the NOA routing without caring about mobile's LAC and CELL.

The enhancement only works with MS selector. For other selector, TRAVER's behavior is not affected.

For details, please refer to FN and MM document of A00004192 in GSMDOC library.

160.3 Applicable customer facing sections

Fault Management

Not applicable	___X__
Logs	_____
Alarms	_____

Configuration

Not applicable	___X__
Data Schema/MIBs	_____
User Interface	_____
GUI	_____
Element Management	_____

Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	___X__
Billing changes	_____
Performance	_____
Not Applicable	___X__
Operational Measurements	_____
Performance Measurements	_____
Realtime	_____
Not applicable	___X__
Engineering Information	_____
Not applicable	___X__

160.4 Hardware Requirements or Dependencies

None.

160.5 Software Requirements or Dependencies

None.

160.6 Limitations and restrictions

None.

160.7 Interactions

This feature changes the CDNCHAR option which is also used by TR selector. A new parameter PROTOCOL is added, but it is useless for TR selector. If user input PROTOCOL parameter when CDNCHAR option presented with TR selector, TRAVER tool terminate and prompt that it is not permitted.

160.8 Glossary

Term	Description
CAP	CAMEL Application Part
INAP	Intelligent Network Application Part
NOA	Nature of Address
TRAVER	Translation Verify

161: Functional Description (FN): A00005123

161.1 Purpose

In SN07, changes to the SESM upgrade scripts will enhance how the SESM s/w handles upgrades, in particular Database upgrades. These changes will prevent a number of issues frequently observed in labs, and will also be required to correctly handle database upgrades with the introduction of CI and HA.

161.2 Description of Fix

There are several different enhancements as described below:

- Restructured CS2M load
  The CS2M load is being restructured to allow s/w packages to be easily added or removed from the CS2M combo load. The CS2M installer script will be made dynamic so it looks into the packages directory and installs only the loads it finds there. The installation code is being made generic to handle any normal Sun package.
- SESM Data Versioning and DB upgrade enhancements
  SESM database upgrades are being divorced from the s/w installation. During SESM startup, the Database is checked for the current version. If it is not current, a DB upgrade is initiated. The DB upgrade code is being changed so that it no longer relies on s/w versions, but only on internal DB versions.
- SESM Configuration enhancements
  SESM configuration is now being linked into the CLI tool.

161.3 Possible Design Side Effects

SESM s/w upgrades will now occur faster as a result of the DB upgrades being decoupled from s/w upgrades. SESM startup time will be increased slightly due to the check of DB versions and the SESM could take significantly longer to start up if the system determines that the DB needs to be upgraded.

161.4 Customer Facing Document Changes

There will be minor impacts to Installation and Upgrade documents. The area most significantly impacted will be the upgrade process when going from one h/w platform to another.

161.5 Test Instructions

1. Verify CS2M application installation
   a. Download and untar the CS2M Combo load.

b. **cd** to the **bin** directory and run the **appl_mgr.ksh** script and verify that all the applications install.

2. Verify ability to add and remove apps from the CS2M application installation script

a. Download and untar the CS2M Combo load.

b. **cd** to the **pkg** directory and move the NTsesm package to the **/tmp** directory.

c. **cd** to the **bin** directory of the CS2M Combo load and run the **appl_mgr.ksh** script and verify that the SESM application isn't listed.\

d. **cd** to the **/tmp** directory and move the NTsesm package to the **pkg** directory of the CS2M Combo load package.

e. **cd** to the **bin** directory of the CS2M Combo load and run the **appl_mgr.ksh** script and verify that the SESM application is listed.

3. Verify CS2M Upgrade from SN06.2

a. Install the SN06.2 FC SESM load, configure and enter some provisioning data.

b. Using CS2M, upgrade to SN07 load.

c. Verify the SESM installs cleanly and configuration settings survived the upgrade using the **configure** tool.

d. Start the SESM using the **ptmctl –f start** command

e. Verify that SESM detects that the DB needs upgrading.

f. After prompting the system to upgrade the DB, verify that the DB is upgraded successfully with no errors.

g. Verify SESM starts up with no errors.

4. Verify CS2M Upgrade from SN06

a. Install the SN06 FC SESM load, configure and enter some provisioning data.

b. Using CS2M, upgrade to SN07 load.

c. Verify the SESM installs cleanly and configuration settings survived the upgrade using the **configure** tool.

d. Run the **ptmctl diag** command

e. Verify that SESM detects that the DB needs upgrading.

f. After prompting the system not to upgrade the DB, run the **configure** tool. Select Option 2 (SESM database tools). Then select Option 4 (Upgrade SESM database).

g. Verify that the DB is upgraded successfully with no errors

h. Start SESM using the **ptmctl –f** start command.

i. Verify SESM starts up with no errors.

5. Verify CS2M Upgrade from SN05

a. Install the SN05 FC SESM load, configure and enter some provisioning data.

b. Using CS2M, upgrade to SN07 load.

c. Verify the SESM installs cleanly and configuration settings survived the upgrade using the **configure** tool.

d. Start the SESM using the **servman** utility

e. Verify that SESM detects that the DB needs upgrading and upgrades it automatically.

f. Verify that the DB is upgraded successfully with no errors.

g. Verify SESM starts up with no errors.

6. Verify **configure** script binds into **cli**

a. Install the SN07 SESM load.

b. Type **cli** to start the cli tool

c. Select Option 2 (Configuration).

d. Select Option 3 (Succession Element configuration).

e. Verify an option for “SESM Application configuration” exists.

f. Select “SESM Application configuration” and verify that it launches **configure** tool

162: Functional Description (FN): A00005124

This FN is covered under the FN for feature A89008767 3PC Hybrid: Cutover and Upgrades.

162.1 Feature name

Compact Hybrid China Cutover Tools - Production Software

162.2 Description

162.3 Hardware Requirements or Dependencies

162.4 Software Requirements or Dependencies

162.5 Limitations and restrictions

162.6 Interactions

162.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

162.8 Glossary

Term	Description
New term	Definition

163: Functional Description (FN): A00005160

163.1 Feature name

OSSAIN XA-Core Data Messaging Capacity Enhancements.

OSSAIN: Operator Services System Advanced Intelligent Network.
XA-Core: Extended Architecture Core.

163.2 Description

This activity makes it possible for OSSAIN data messaging to use XA-Core Ethernet interfaces such as the HIOP and the new HCMIC card. Prior to this activity, all OSSAIN messaging used the EIU (Ethernet Interface Unit). The EIU has insufficient capacity to support some service providers' requirements for OSSAIN.

163.2.1 Background

This section includes background material on both OSSAIN and XA-Core Ethernet interfaces.

163.2.1.1 OSSAIN background

The OSSAIN product uses a messaging protocol between TOPS (Traffic Office Position System) switches and external service nodes (SNs), allowing the SNs to provide services for and control switch functionality associated with directory and operator services calls. In an OSAC (OSSAIN centralization) configuration, one or more centralized SNs provide services for multiple TOPS switches. These TOPS switches are referred to as OSAC hosts and OSAC remotes, and they exchange messages with each other as well as with SNs. All of this messaging uses the UDP protocol at the transport level.

Until recently, OSSAIN was used mainly for toll and assistance (TA) calls. Now service providers are beginning to use OSSAIN for directory assistance automation (DAA) as well. Since most TOPS switches handle many more DA than TA calls, and since DAA calls may use OSSAIN for both front end and back end automation, service providers are requiring more OSSAIN messaging capacity than EIUs can provide. Throughput of an EIU is between roughly 10 and 40 KBytes/second in each direction, depending on how heavily the LPP or FLIS is used for other applications besides OSSAIN. And because of the way EIU selection is done, adding more EIUs for OSSAIN may not increase the messaging capacity. For more information about EIU capacity, refer to *OSSAIN User's Guide* (297-8403-901) and *Ethernet Interface Unit User Guide* (297-8991-910).

163.2.1.2 XA-Core Ethernet interface background

In the XA-Core architecture, I/O processor cards in the core can be used to provide Ethernet LAN connectivity. These cards communicate directly with the PEs (processing elements) using a shared memory system. The first-generation card was the IOP, a host card that accommodates specialized packlets for different interfaces. An IOP with Ethernet packlet(s) is called an EIOP. The second-generation card is the HIOP. HIOP cards do not host packlets. Three versions of HIOP have been developed—one with only an Ethernet interface, and two with both Ethernet and AMDI (for ATM). Next-generation HCMIC cards with CMIC, RTIF, and Ethernet interfaces are under test at the time of this writing.

XA-Core Ethernet interface cards are datafilled in switch table CMIPADDR. The datafill includes two active host CM IP addresses, which the switch dynamically associates with physical links. As long as at least two links are in-service, the two IP addresses are always associated with different links. If a link fails while another is in-service, the IP address that was associated with the failed link is automatically reassigned to a different one. Unsolicited ARP (Address Resolution Protocol) replies are used to inform the network of the association between IP addresses and physical interfaces.

XA-Core I/O cards are maintained from the switch at MAP level MAPCI;MTC;XAC;IO. Their functional components, including Ethernet ports and links, are maintained at level MAPCI;MTC;XAC;ETHR. *Port* refers to a hardware interface on the card, and *link* represents the transmission medium connecting the XA-Core to other nodes. For more information, refer to documentation for the following features:

A59019176	XA-Core ethernet packlet - OA&M
A59029980	HIOP Maintenance Software
A00002012	XA-Core CMIC/RTIF HIOP Maintenance Software

163.2.2 New functionality

This feature adds new fields to switch table OANODINV, the inventory table for OSSAIN SNs and OSAC nodes, to allow the service provider to specify the data path to be used for messaging with each node. Thus it is possible for a TOPS switch to use EIU for messaging with some OSSAIN nodes and XA-Core Ethernet interface cards for messaging with others. This enables a gradual transition, on a node-by-node basis, to using XA-Core Ethernet interface cards.

Which data path the switch uses is transparent to the far-end node, except that the far-end node must be configured to use a different IP address for the switch depending on which data path the switch uses when messaging with that node.

For the EIU data path, far-end nodes are configured to send messages to the IP address in the CMIPADDR tuple of table IPNETWRK. This is existing functionality, and is unchanged.

For the XA-Core Ethernet interface data path, each far-end node is configured to send messages to one of the two active CM host IP addresses datafilled in table CMIPADDR. That address is also datafilled against the node in table OANODINV, and is used as the source IP address when the switch sends messages to the node.

Under normal conditions of no failure, traffic should be balanced over the physical links. This is accomplished by configuring half of the far-end nodes to use one of the active CM host IP addresses, and the other half to use the other active CM host IP address.

TOPS does not restrict which XA-Core Ethernet interface cards can be used. However, some of the earlier XA-Core I/O cards have been or will soon be manufacture discontinued, and the product platform on which TOPS runs may have restrictions on which cards are supported. Contact your Nortel Networks representative for more information.

This activity also adds a new OM group, TDGTHRU (TOPS Datagram Throughput), which counts the number of UDP messages sent and received in each of several "buckets" or message size ranges. The OM group has tuples for several TOPS applications, and it has separate tuples for OSSAIN using EIU and OSSAIN using XA-Core Ethernet interface. The pegs are meant to help in studies of messaging bandwidth utilization of TOPS applications.

163.2.3 Capacity engineering considerations

Paper studies suggest that if the LPP or FLIS that houses the EIU is used primarily for OSSAIN messaging, an OSAC remote can process roughly 100,000 DA busy hour calls/hour, with DA front and back end automation using Nortel Networks service nodes, before it approaches EIU messaging capacity limits. If the LPP or FLIS is also used heavily for ISUP signaling or other applications, the OSSAIN traffic limit may be closer to 25,000 calls/hour. Capacity decreases if the SNs send a significant number of SMS (Short Message Service) requests to the switch. Other features may also decrease capacity.

Similar studies suggest that a pure OSAC host can process roughly a million busy hour OAP sessions for its remotes if the EIU in the host is used primarily for OSSAIN traffic. Using Nortel Networks service nodes, separate OAP sessions are used for DA front end and back end automation, so this translates to 500,000 DA calls/hour. If the LPP or FLIS housing the EIU in the OSAC host is also used heavily for ISUP signaling or other applications, the OSAC host's limit is closer to 125,000 DA calls/hour from its OSAC remotes. The host's capacity decreases if it is also processing standalone OSSAIN calls.

Note: Messaging patterns may be different if service nodes from other vendors are used. Nortel Networks does not have message flows for calls that are serviced by other vendors' SNs, and does not do capacity engineering for these SNs.

Ethernet throughput capacity of XA-Core interface cards depends on factors such as the extent to which other interfaces on the card are used and the sizes of the individual messages. Committed throughput numbers for NTLX04CA (HIOP) and NTLX17AA (HCMIC) were not available at the time of this writing, but both cards will have Ethernet throughput capacity much higher than the EIU, even if other interfaces on the card are used.

It is anticipated that in offices that are not using XA-Core interfaces for Succession packet call signaling, a pair of NTLX04CA or NTLX17AA cards (for redundancy) can easily accommodate both CBM (Core and Billing Manager, the next-generation Supernode Data Manager replacement) and all existing DA traffic, using OSSAIN for both front and back end automation, with no capacity concerns.

In TOPS CS2000 switches in which OSSAIN messaging is sharing the available Ethernet interface bandwidth with high-runner Succession call signaling, the CS2000 capacity for handling non-TOPS calls is decreased. At the time of this writing, Succession CS2000 capacity numbers published by Nortel Networks were based on office models that did not include OSSAIN. Contact your Nortel Networks representative for the status of capacity engineering work for CS2000 switches that use Ethernet interface cards for both OSSAIN and Succession packet call signaling.

163.3 Hardware Requirements or Dependencies

This functionality is available only on XA-Core equipped with Ethernet interface cards such as HIOP (NTLX04CA) or HCMIC (NTLX17AA).

163.4 Software Requirements or Dependencies

This functionality is first available in the SN07 and ISN07 core software loads.

163.5 Limitations and restrictions

From an end user's perspective, this activity introduces no limitations or restrictions that were not present in OSSAIN using EIU.

From a service provider's perspective, the following limitations and restrictions apply:

- Use of XA-Core Ethernet interface cards is supported only for OSSAIN applications that use the UDP protocol. It is not supported for OSSAIN QMS MIS, which uses TCP.

- Unlike EIUs, XA-Core Ethernet interface cards do not provide screening capabilities. (EIUs can be configured to protect the core by screening out incoming messages from unwanted IP addresses, including addresses that do not match datafilled nodes and addresses of nodes that are off-line or have been declared babblers.)

  Since call processing can be adversely affected if the core is flooded with unwanted messages, it is especially important that the network be properly configured with firewalls and router filters when XA-Core Ethernet interfaces are used.

- In TOPS CS2000 switches in which OSSAIN is sharing the Ethernet interface cards with high-runner Succession calls, OSSAIN decreases the capacity of the CS2000 for non-TOPS calls. CS2000 capacity numbers published by Nortel Networks engineering groups do not apply in this case, unless the office model has specifically included OSSAIN calls.

- The XA-Core does not provide a way to reserve portions of its total Ethernet interface bandwidth for specific applications. All applications compete for the same bandwidth.

- An SN cannot be on the same subnet as a core Ethernet interface if an EIU router is to be used for messaging with the SN. Refer to the Configuration section of this feature for more information.

- This limitation applies when (a) an OSAC remote switch is being changed to use XA-Core Ethernet interface to communicate with a centralized SN, and (b) either the OSAC host is below SN07/ISN07, the centralized SN is at an OAP release below 9, or both. In this situation, if the service node is incorrectly configured (in the service node) to use the wrong IP address for the OSAC remote, the mismatch is not detected when the links to the centralized SN are returned to service in the OSAC remote. The OSAC remote will present calls to the centralized SN. The incorrectly configured SN will probably not attempt to send the switch any messages regarding these calls. Depending on datafill for OSSAIN time-outs and on how quickly callers abandon these calls, there may be no logs in the OSAC remote indicating any problem. However, the incorrectly configured SN should be raising alarms using its own event reporting system if this happens.

  This is not a new problem with XA-Core Ethernet interface; however, the configuration mismatch may be more likely to be introduced with this feature, since the service provider now has to be aware of more than one IP address for any particular switch.

  The OSAC and OAP protocols are enhanced in SN07 and OAP Release 9 to eliminate this limitation. If the SN is at OAP 9 or higher, and both the OSAC remote and host are at SN07 or higher, then the OSAC remote cannot RTS its links to the centralized SN if the SN has incorrect datafill for the OSAC remote's IP address.

163.6 Interactions

Existing OSSAIN services are not affected by the choice of which data path the switch uses for Ethernet connectivity.

163.7 Applicable customer facing sections

An X indicates that the corresponding DDOC section is applicable. N/A indicates it is not.

Fault Management	
Logs	X
Alarms	N/A
Configuration	
Data Schema	X
User Interface	X
Element Management	N/A
Security	X
Service Order	N/A
Office Parameters	N/A
Configuration Walkthrough	X
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	X

163.8 Glossary

This activity does not introduce new or non-standard terms. For convenience, this section expands standard acronyms used in this FN.

Term	Description
AMDI	ATM Multi-mode Data Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Time Multiplexing
CBM	Core and Billing Manager
CM	Computing Module
CMIC	Computing Module Interface Card
CS2000	Communication Server 2000
DA	Directory Assistance
DAA	Directory Assistance Automation

Term	Description
EIOP	Ethernet Input Output Processor
EIU	Ethernet Interface Unit
FLIS	Fiber Link Interface Shelf
HCMIC	High Performance Computing Module Interface Card
HIOP	High Speed Input Output Processor
IOP	Input Output Processor
IP	Internet Protocol
ISUP	Integrated Services Digital Network
LAN	Local Area Network
LPP	Link Peripheral Processor
MAP	Maintenance and Administration Position
OAP	Open Automated Protocol
OSAC	OSSAIN Centralization
OSSAIN	Operator Services System Advanced Intelligent Network
QMS MIS	Queue Management System Management Information System
RTIF	Reset (or Remote) Terminal Interface
SMS	Short Message Service
SN	Service Node
TA	Toll and Assistance
TCP	Transmission Control Protocol
TOPS	Traffic Office Position System
UDP	User Datagram Protocol
XA-Core	Extended Architecture Core

164: Functional Description (FN): A00005190

164.1 Feature name

CBM 800 OC3 Core Node and Link Maintenance

164.2 Description

A market was identified to replace the aging billing storage device known as the DPP (Distributed Processing Peripheral). The function of the DPP is to receive billing records from the core through an IOC interface and store them on redundant hard disks. A modem link is used to poll the DPP for billing records and transfer them downstream to an OSS.

The chosen platform for DPP replacement was the next generation SDM or Core and Billing Manager (CBM) on the SSPFS platform. However core connectivity became a problem since DPP's are connected to BRISC cores via IOC connectivity but the CBM only provided IP connectivity.

A prototype was built to prove that OC3 could be used to connect a CBM 800 to an MS in a similar manner to the SDM FX which is connected through DS512 links to the MS.

The OC3 connectivity resolves several issues including security and capacity.

This solution builds on the existing infrastructure that is used for the SDM FX platform and the Node maintenance infrastructure that was developed for the Ethernet connected SDM and the CBM 850.

This activity provides the modifications in node maintenance on the core to support the OC3 connected CBM 800.

164.3 Hardware Requirements or Dependencies

None

164.4 Software Requirements or Dependencies

None.

164.5 Limitations and restrictions

None.

164.6 Interactions

None.

164.7 Applicable customer facing sections

Fault Management

- Logs _____N/A
- Alarms _____N/A

Configuration

- Data Schema _____X
- User Interface _____X
- Element Management _____N/A
- Security _____N/A
- Service Order _____N/A
- Office Parameters _____N/A

Accounting (includes AMA billing) _____N/A

Performance (includes operational measurements) _____N/A

164.8 Glossary

Term	Description
CBM	Core and Billing Manager

165: Functional Description (FN): A00005192

165.1 Feature name

CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance.

165.2 Description

This feature provides OC3 connectivity between a CBM 800 and the MS of a BRISC or XA-Core. Physical connectivity consists of two OC3 fibers connected between two ATM interface cards on the Solaris Netra-240 and two NTL9X63 paddleboards, one on each MS.

This feature provides the following software components:

- CBM 800 MTS/IP/FTS driver
- CBM 800 link maintenance
- CBM 800 node maintenance

The MTS/IP/FTS driver provides an MTS socket and IP socket interface to allow CBM 800 software components to send and receive MTS and IP messages to and from core software components.

CBM 800 link maintenance sets the conditions of the two OC3 links displayed at the Core level (figure 2) of the cbmmtc UI. Link conditions are set in response to node state change commands invoked from the SDM level of MAPCI (figure 1) and port / card state changes invoked from the MS Card level of MAPCI. Table 1 gives the MAPCI node state and the cbmmtc link conditions for various mtce actions.

Figure 1 MAPCI SDM Level

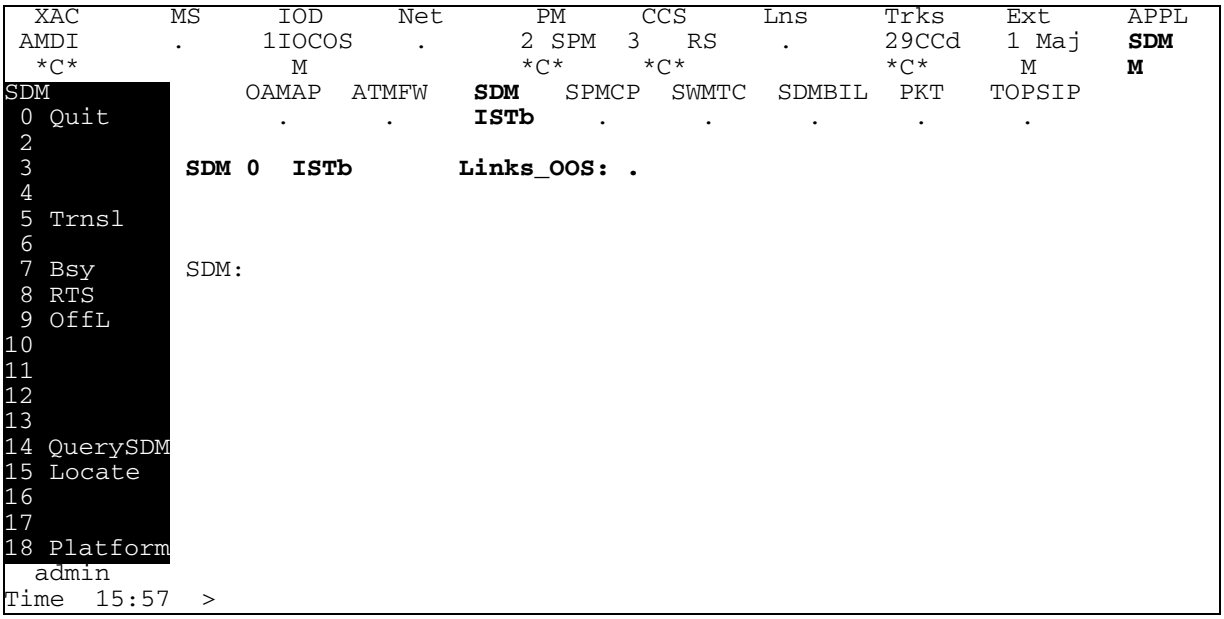


Figure 2 cbmmtc Core Level

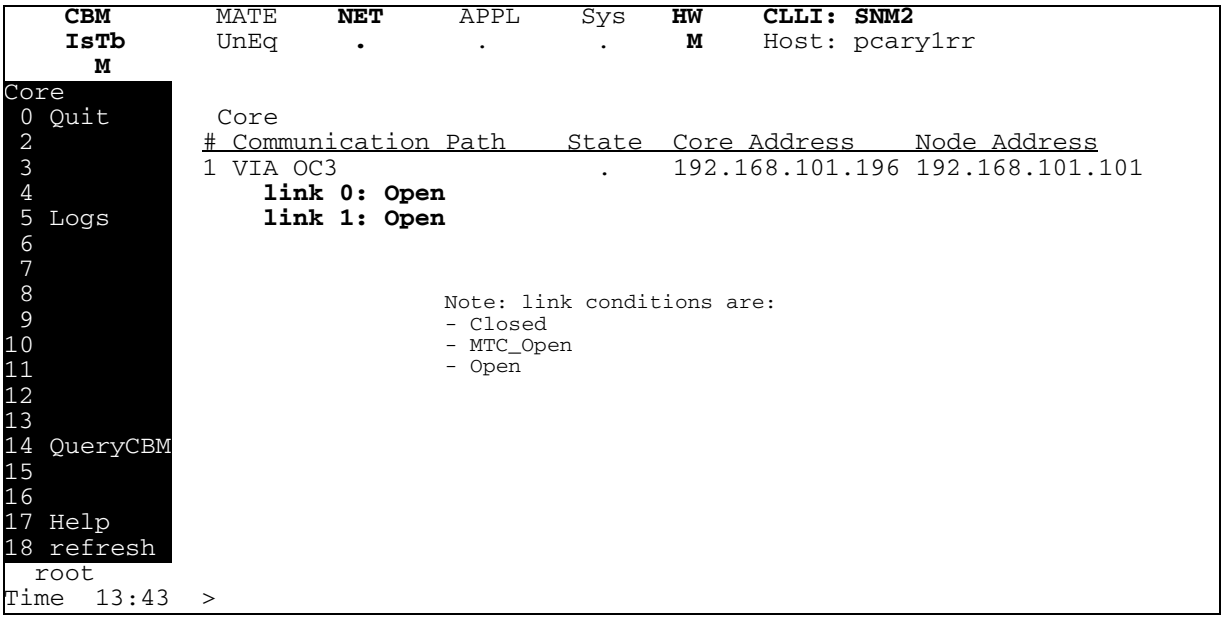


Table 1 Node State and Link Conditions

Mtce Action	Node State	Link 0 Condition	Link 1 Condition
Offline node	Offl	Closed	Closed
Busy node	ManB	Mtc-open	Mtc-open
RTS node	InSv / ISTb	Open	Open
Busy link 0	InSv / ISTb	Closed	Open
Busy link 1	InSv / ISTb	Open	Closed
Busy all links when node state InSv	SysB (NA)	Closed	Closed
Busy all links when node state ManB	ManB (NA)	Closed	Closed
Faults on both links	SysB (NA)	Closed	Closed

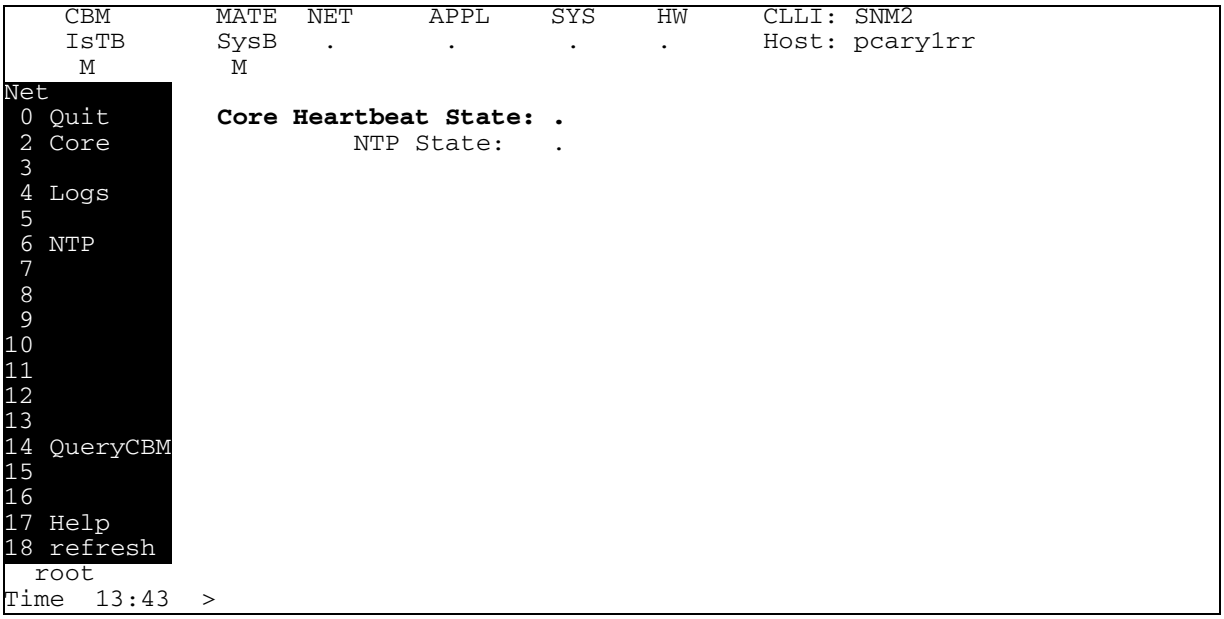
The CBM node state in the banner of figure 2 may **not** be the same as the SDM node state in figure 1 due to the fact that the two node states are different data points. The CBM alarm state in the banner of figure 2 will match the SDM alarm state in figure 1 when the CBM 800 is in-service.

CBM 800 node maintenance sets the Core Heartbeat State at the Net level of the cbmmtc UI (figure 3). The heartbeat state will be InSv if at least one of the OC3 links is in a mtc-open or open condition. If faults are raised on both links, the link conditions will change to closed and the heartbeat state will change to SysB. The NET alarm in the banner will also change to SysB.

If an ATM card alarm is raised, the HW alarm in the banner will indicate a HW problem. The ATM HW alarm can be queried from the HW level of the cbmmtc UI.

CBM 800 link mtce generates cust logs for link condition changes and crossed links.

Figure 3 CBM Net Connectivity Level



165.3 Hardware Requirements or Dependencies

None

165.4 Software Requirements or Dependencies

None

165.5 Limitations and restrictions

None

165.6 Interactions

This feature interacts with the following features:

- A00005337 CBM 800 OC3 BRISC Paddleboard Connectivity
  - provides datafilling of an NTL9X63 paddleboard in a non-cmic slot of a Supernode or SNSE MS shelf.
- A00005190 CBM 800 OC3 Node and Link Maintenance
  - provides core side node and link maintenance components
- A00002822 CBM User Interface Manager
  - provides user interface manager for CBM 800 and CBM 850

165.7 Applicable customer facing sections

Fault Management

Logs ___X___

Alarms	___X___
Configuration	
Data Schema	__NA__
User Interface	__NA__
Element Management	__NA__
Security	__NA__
Service Order	__NA__
Office Parameters	__NA__
Accounting (includes AMA billing)	__NA__
Performance (includes operational measurements)	__NA__

165.8 Glossary

Term	Description
CBM	Core and Billing Manager on SSPFS platform
CBM 800	OC3 connected simplex CBM
CBM 850	IP connected high availability CBM
SSPFS	Succession Solaris Platform Foundation Software

166: Functional description (FN): A00005193

166.1 Feature name

9+1 Performance Measurements Tools Support

166.2 Description

This CSP20 feature implements changes required to support the XA-Core 9+1 configuration. Specifically, this feature will allow a Rated Power of 9.

166.3 Hardware Requirements or Dependencies

N/A

166.4 Software Requirements or Dependencies

N/A

166.5 Limitations and restrictions

None

166.6 Interactions

For releases prior to this feature, the largest value allowed for the office parm Rated_Power in table OFCENG is 7. With this feature, users are able to modify the value of Rated_Power up to a maximum of 9.

166.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	X
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

167: Functional description (FN): A00005268

167.1 Feature name

A00005268: SBA: MULTI-VOLUME SUPPORT FOR CORE BACKUP .

167.2 Description

167.2.1 Architectural Description.

Currently 2 volumes can be assigned on a per stream for SBA on the CM as backup storage.These volumes are used to store the billing records whenever the stream goes to backup mode on the CM.This configuration deos not meet the backup storage requirement for some of the markets.

This feature will focus on increasing the backup storage capacity available for SBA on the CM from current 2 volumes allotted per stream to 69 volumes or the maximum supported by the underlying hardware whichever is less per stream.

167.2.2 High Level Description.

As part of this feature new MAPCI commands will be introduced. The new CI commands will allow user to add / remove more than one volume at a time per stream .

This feature is core only scope and affect TL layer.

167.3 Hardware requirements

Under investigation.

167.4 Limitations and restrictions

None

167.5 Interactions

None.

167.6 Logs (LG)

The following logs have been changed as part of this activity.

167.6.1 SDMB531 :

The conf log (SDMB531) has been changed. Following shows a sample output of the current SDMB531 log format.

3PC_TDM07CD SDMB531 MAY06 09:43:32 0500 INFO SDM BILLING CONFIG

STREAM= SBA0:

NEWVOLUMES =

SD00AMA1 SD00AMA2 SD00AMA3 SD00AMA4 SD00AMA5

SD00AMA6 SD00AMA7 SD00AMA8 SD00AMA9 SD00AMA10

SD00AMA11 SD00AMA12 SD00AMA13 SD00AMA14 SD00AMA15

SD00AMA16 SD00AMA17 SD00AMA18 SD00AMA19 SD00AMA20

SD00AMA21 SD00AMA22 SD00AMA23 SD00SNS SD00AMA

SD01AMA1 SD01AMA2 SD01AMA3 SD01AMA4 SD01AMA5

SD01AMA6 SD01AMA7 SD01AMA8 SD01AMA9 SD01AMA10

SD01AMA11 SD01AMA12 SD01AMA13 SD01AMA14 SD01AMA15

OLDVOLUMES =

SD00AMA1 SD00AMA2 SD00AMA3 SD00AMA4 SD00AMA5

SD00AMA6 SD00AMA7 SD00AMA8 SD00AMA9 SD00AMA10

SD00AMA11 SD00AMA12 SD00AMA13 SD00AMA14 SD00AMA15

SD00AMA16 SD00AMA17 SD00AMA18 SD00AMA19 SD00AMA20

SD00AMA21 SD00AMA22 SD00AMA23 SD00SNS SD00AMA

SD01AMA1 SD01AMA2 SD01AMA3 SD01AMA4 SD01AMA5

SD01AMA6 SD01AMA7 SD01AMA8 SD01AMA9 SD01AMA10

SD01AMA11 SD01AMA12 SD01AMA13 SD01AMA14 SD01AMA15

SD01AMA16 SD01AMA17 SD01AMA18 SD01AMA19 SD01AMA20

167.6.2 SDMB820

The logs raised when any of BAK** alarms are raised have also been changed. Following is a sample output of the log generated.

3PC_TDM07CD *** SDMB820 MAY06 11:20:51 2876 SDM BILLING BACKUP
STREAM= SBA0: WARNING, 50% or less of Backup space is free.
VOLUMES=
SD00AMA13 SD00AMA15 SD01AMA11 SD01AMA12 SD01AMA13

167.7 Data schema (DS)

167.7.1 New/modified tables

Table 1 New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
SDMBILL	Changed	Unchanged

167.8 Office parameters (OP)

None.

167.8.1 New/modified office parameters

167.9 Service orders (SO)

No change.

167.10 Alarms (AL)

No change.

167.10.1 New/modified directories

167.11 Command interface (CI)

167.11.1 New/modified commands

Table 2 New or modified commands

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/MAP level name	MENU/NON-MENU /HIDDEN
CONF	changed		SDMBIL	Menu
ADDVOL	new		SDMBIL	Menu
REMVOL	new		SDMBIL	Menu

167.12 Operational measurements (OM)

167.12.1 New/modified OM groups

No change.

167.13 AMA/Billing information (AM)

167.13.1 New/changed AMA/billing information

No change.

167.14 Software optionality control (SOC)

No change.

167.15 Glossary

Term	Description
New term	definition
SBA	Supernode Billing Application

SDM	Supernode Data Manager
CM	Computing Module

167.16 References

168: Functional Description (FN): A00005317

168.1 Feature name

WanBuilder Heartbeat Ping

168.2 Description

This feature adds robustness to the WanBuilder inband messaging links by allowing the subsystem to perform corrective actions when communication fails. WanBuilder Heartbeat Ping monitors the inband messaging links (OAM, CallControl and DS512) and reacts to failure by raising an alarm, swapping SVCs or causing a SWACT, for example.

168.3 Problem Correction

In some cases, the UEMG's primary SVC is to the inactive Shelf Controller but the SAM21 is unaware of the mix-up. In this case, the SVCs are up and “green” on the SAM21 GUI, but inband messaging fails. WanBuilder Heartbeat Ping will correct the situation by swapping the SVCs.

The DCC takes its provisioning for the IP address to ping for each connection type from the LCI. It sends a message to each ITP or ABI telling it to start heartbeat. If heartbeat fails on one ITP or ABI, the DCC heartbeat controller requests a status update from all ITPs or ABIs. After collecting the status updates, the controller decides upon a course of action.

If all heartbeats for a given connection type (OAM, Call Control or DS512) are failing, there are two actions that can be taken. The first step is to swap the SVCs, while the second, more drastic step is to raise an alarm which may result in a SWACT of the DCCs. The SWACT decision is left to node maintenance's service evaluation.

If heartbeat is failing for one or more VMGs within a connection type, but not for all of them, an alarm can be raised on ITPs/ABIs that are failing heartbeat. Again, this may result in a SWACT of the ITP or ABI.

168.4 Provisioning

The heartbeat address is an newly added field on each Connection page. It is an optional field and if not provisioned, heartbeat is not enabled.

169: Functional Description (FN): A00005322

169.1 Feature name

Spectrum Common Equipment Module (CEM) Overload Enhancement: Asynchronous Transfer Mode Resource Module (ATMRM) Status

169.2 Description

This feature introduces several changes into the reporting of ATMRM resource exhaustion and CEM overload conditions. Since the ATMRM resources are integral to call processing on the MG4K/IW variants of the SPM peripheral node, attempts are made to make ATMRM resource exhaustion conditions very visible. To this end, depending upon the severity of the ATMRM resource exhaustion:

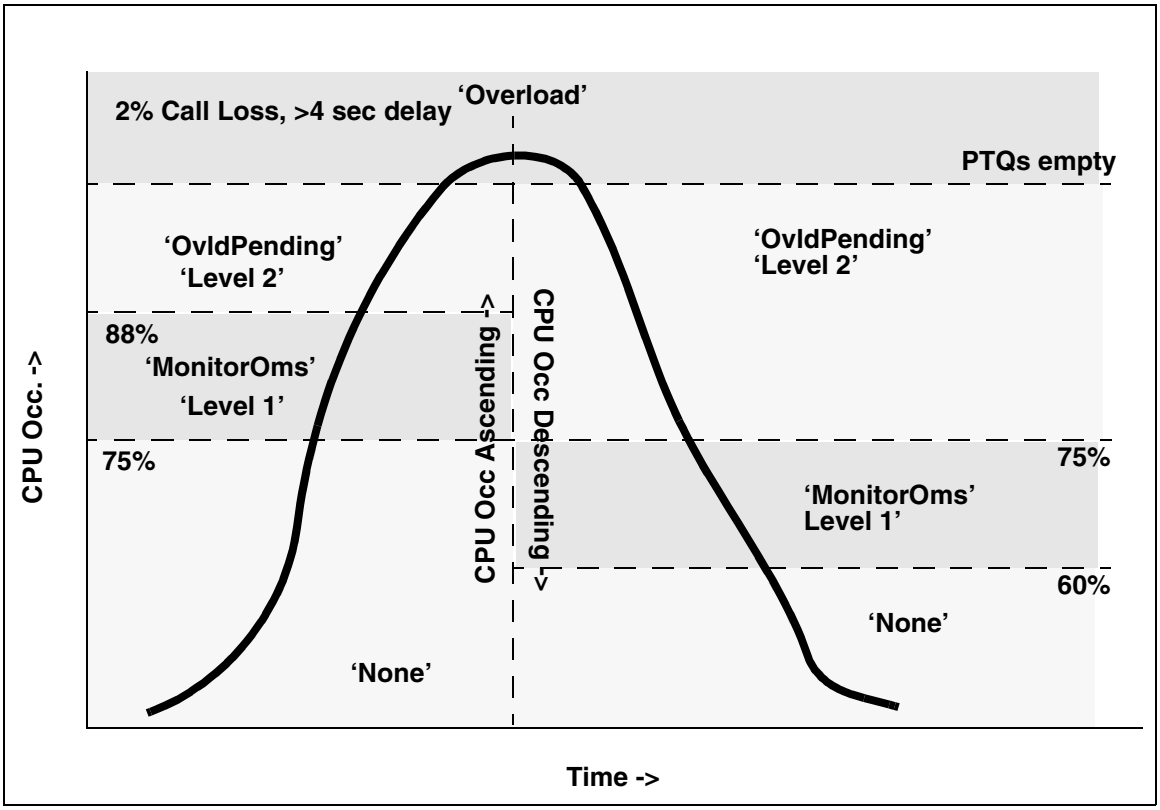
- CEM CALLP can go into Overload which results in SPM399 Overload logs, Minor alarm, CEM state change to ISTb, Node state change to Istb (NODE500, NODE602), MAPCI MIP strings indicating Overload and "querypm flt reason" indicating an overload condition being generated.
- On the ATMRM, a minor alarm will be raised, RM state change to ISTb (SPM500 state change and SPM300 fault reason logs), MAPCI MIP strings indicating Overload and "querypm flt reason" indicating an overload condition will be generated.

The severity of ATMRM resource exhaustion is reported via predefined utilization levels. Each level has a different onset and abatement value to prevent quick entry/exit (jitter) from a single level at a boundary value. The ATMRM resource utilization levels (NONE, LEVEL1 and LEVEL2) are transferred to the CEM and are applied to CEM resources. As a result, the ATMRM and CEM share resource utilization levels. For the case of CPU occupancy/CALLP flow control, these levels are as follows:

- None: Exit: 75 % (Level 1 Onset), Onset: 0% (system initialization) or 60% (Level 1 abatement) - The monitored resource is below 75% utilization since last being in "Level 1" or since system initialization.
- Level 1: Onset: 75%, Exit: 88% (Level 2 onset), Abatement: 60% (Level 1 onset) - The CPU resource utilization was initially above its engineering level of 75% and has not dropped below 60% utilization since the initial 75% level was encountered.
- Level 2: Onset: 88%, Exit: Overload triggered, Abatement: 75% - The CPU resource is dangerously overused. CALLP flow control has been triggered to delay call originations in order to lessen CPU occupancy.

- Overload: Onset: Any call delayed by flowcontrol for more than 4 seconds or more than 2% of the calls have been discarded. Abatement: No calls are being delayed. Overload determination is not resource based, it is determined by the characteristics of the states of the calls in flow control.

Figure 1 CPU Occupancy and Resource Utilization Level



The following table shows the maintenance interaction mapped to CPU resource levels. The shaded entries are the new interactions introduced by this feature. Please note, with introduction of this feature, the ATMRM CPU resource level will effect existing maintenance interactions for the CEM.

.

Table 1 Maintenance Interactions for each ATMRM Resource Utilization Level

Mtc Interaction	No Overload	Level 1 Resource Utilization	Level 2 Resource Utilization	CALLP Overload (call state based)
CEM Flowcontrol	Off	Off	On	On
CEM Alarms	None	None	Minor	Minor
ATMRM Alarms	None	Minor	Minor	Minor

Changing Existing Interaction

New Interaction

Table 1 Maintenance Interactions for each ATMRM Resource Utilization Level

Mtc Interaction	No Overload	Level 1 Resource Utilization	Level 2 Resource Utilization	CALLP Overload (call state based)
CEM State	InSv	InSv	ISTb	ISTb
ATMRM State	InSv	ISTb	ISTb	ISTb
Node State	InSv	InSv	ISTb	ISTb
CEM MIP	None	“Monitor OMs”	“Overload Pending”	“Overload”
ATMRM MIP	None	“Monitor OMs”	“Overload Pending”	“Overload Pending”
CEM Logs				
SPM399	None	“Monitor OMs”	“Overload Pending”	“Overload”
NODE500	None	None	ISTb State Change	None
NODE602	None	None	“Reached or Nearing Overload”	None
ATMRM Logs				
SPM300	None	“Monitor OMs”	“Overload Pending”	None
SPM500	None	ISTb State Change	None	None

Please note, the above table indicates the interactions visible when entering or being in high resource utilization levels. When abating the “Level 1” state and returning to the “No Overload” state, alarms are extinguished, MIP strings are cleared, module states are returned to InSv and the logs indicate overload states have cleared, resources utilization levels have returned to normal, and module states are back to InSv.

169.3 Hardware Requirements or Dependencies

None.

169.4 Software Requirements or Dependencies

- A00002431 - SP20 “LX82BA Capacity Delivery” required for the new CALLP overflow infrastructure.
- A00002432 - SP20 “SPM Enhanced Overload OMs and Logs” needed for the overload reporting infrastructure.

169.5 Limitations and restrictions

SP20 CORE load required for full reporting infrastructure to function.

169.6 Interactions

This feature depends upon the reporting infrastructure introduced into the Spectrum by A00002432 - SP20 “SPM Enhanced Overload OMs and Logs” for overload reporting.

The feature also uses the new CALLP flow control infrastructure introduced by A00002431 - SP20 “LX82BA Capacity Delivery”.

169.7 Applicable customer facing sections

Fault Management

- Logs __X__
- Alarms __X__

Configuration

- Data Schema __N/A_
- User Interface __N/A_
- Element Management __N/A_
- Security __N/A_
- Service Order __N/A_
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

169.8 Glossary

Term	Description
New term	Definition

170: Functional Description (FN): A00005337

170.1 Feature name

CBM 800 OC3 BRISC Connectivity

BRISC - BNR Reduced Instruction Set Computer (DMS Core)

CBM - Core Billing Manager

OC3 - Optical Carrier- Level 3 (transmission interface)

170.2 Description

170.2.1 General Description

The purpose of this feature is to allow the usage of OC3 paddleboards on the MS for communication between the CBM (running on a SUN Netra server) and the message switch (MS), connected to the computing module (CM) or core.

The changes introduced in the software can be broken up into two separate components, where one portion resides on the message switch (MS) and the other on the computing module (CM). The CM portion will basically allow the datafill of table MSCDINV (Message Switch CarD INVentory) so that the NT9X63AB OC3 paddleboard can be shown on the user MAP. From this, maintenance (mtc) actions can be issued on it (eg - bsy/tst/rts). The local MS software component is what allows the OC3 paddleboard to be recognized and allow the actual mtc actions to be performed on it.

170.2.2 System Behaviour/Feature Operation

To allow the NT9X63AB OC3 paddleboard to be used for communication between the MS and a CBM server, the following steps should be used as a guideline to get the paddleboard into service.

a. ensure that both the CM and MS images have the software code changes introduced in this feature

   - If only one portion is present the user will either not be able to datafill the MSCDINV table or not be able to bring the card into service

b. make sure that there are two NT9X63AB OC3 paddleboards and two NT9X17AD circuit packs available for insertion

   - one set will be inserted into each MS

The next set of instructions are from the Nortel Networks MS card replacement procedure. Please refer to DMS-100 Card Replacement Procedures document (297-9051-547).

c. go to the MS level of the MAP, bsy out MS1 (change it to the slave MS if it is not)

   >mapci;mtc;ms

   >swmast % if MS1 is not the slave MS

   >bsy 1

d. power down the busied MS

e. insert the NT9X63AB paddleboard as well as the corresponding NT9X17AD into the MS for the chosen slot location[1]

f. powerup the busied MS

g. load the MS software image onto the busied MS

   >loadms <ms_number>

   Note that if the MS software image does not contain the changes introduced in this feature, the paddleboard rts may fail.

h. issue an out of service test on the MS

   >tst <ms_number>

i. rts the busied MS, this will trigger a restart of the local MS code, which enables the software to find the OC3 paddleboard[2]

   >rts <ms_number>

j. add the datafill into the MS card inventory table, MSCDINV

   >table mscdinv

   >ove

   >format pack

   >add <ms_#> <shelf_#> <card_#> DS512 NT9X17AD NT9X63AB

   >yes

k. bring the OC3 paddleboard into service

   >mapci;mtc;ms;shelf

   >bsy <ms_#> <card_#>

   >rts <ms_#> <card_#>

l. repeat steps (c) to (k) for MS0

[1]Refer to “170.5 Limitations and restrictions” on page 1917

[2]If not seen or the PEC read fails, the user will be unable to rts with a pec mismatch error given.

170.3 Hardware Requirements or Dependencies

The OC3 paddleboard inserted on the MS to be used for the CBM communication is identified with the PEC (Product Equipment Code) of NT9X63AB. The front circuit pack card on the MS should be the NT9X17AD card.

170.4 Software Requirements or Dependencies

n/a

170.5 Limitations and restrictions

A restriction for using the NT9X63AB OC3 paddleboards is the card location on the MS shelf that the paddleboard may be inserted into. Allowable card locations are listed in Table 1 : Provisionable paddleboard locations.

Table 1 Provisionable paddleboard locations

MS Configuration	Provisionable Slots	Card Location Equivalent
SuperNode (SN)	12R up to 27R	cards #6 up to #21
Super Node System Enhanced (SNSE) MS0	11R up to 15 R	cards #5 up to #9
Super Node System Enhanced (SNSE) MS1	24R up to 28R	cards #5 up to #9

There is no particular card/slot location that is recommended by Nortel. The easiest method for choosing a slot to use is to start from the lowest card number[1] and use the first available location. The OC3 inserted in each MS shelf should have matching card locations (eg - if inserted in card 5 for MS0, it should also be in card 5 of MS1).

170.5.1 Examples

The following shows table MSCDINV before and after the datafill is added for a NT9X63AB OC3 paddleboard in card #8.

```
-> MSCDINV before datafilling the OC3 paddleboards:

>table mscdinv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MSCDINV
```

[1]Please refer to Table 1 : Provisionable paddleboard location for the card numbers to use.

```
>list all
TOP
   MSCDKEY                                                          SLOTINFO
-------------------------------------------------------------------------------
   0  0  1                                                  TBUSACC NT9X52AA NIL
   0  0  2                                                CLOCK NT9X53AC NT9X54AC
   0  0  3                                                  MSP NT9X13DD NT9X26AA
   0  0  5                                                       MAPPER NT9X15AA
   0  0  6                                CHAIN DS512 NT9X17DA NT9X20BB $
   0  0 10                                CHAIN DS512 NT9X17DA NT9X20BB $
   0  0 16                                            DS512 NT9X17AD NT9X62BA 4
   0  0 22                                               DS30 NT9X17AA NT9X23AA
   0  0 23                                               DS30 NT9X17AA NT9X23AA
   0  0 24                                               CMIC NT9X17AA NT9X20AA
   0  0 25                                               CMIC NT9X17AA NT9X20AA
   0  0 26                                                    PBUS NT9X49CB NIL
   1  0  1                                                  TBUSACC NT9X52AA NIL
   1  0  2                                                CLOCK NT9X53AC NT9X54AC
   1  0  3                                                  MSP NT9X13DD NT9X26AA
   1  0  5                                                       MAPPER NT9X15AA
   1  0  6                                CHAIN DS512 NT9X17DA NT9X20BB $
   1  0 10                                CHAIN DS512 NT9X17DA NT9X20BB $
   1  0 16                                            DS512 NT9X17AD NT9X62BA 4
   1  0 22                                               DS30 NT9X17AA NT9X23AA
   1  0 23                                               DS30 NT9X17AA NT9X23AA
   1  0 24                                               CMIC NT9X17AA NT9X20AA
   1  0 25                                               CMIC NT9X17AA NT9X20AA
   1  0 26                                                    PBUS NT9X49CB NIL
BOTTOM
>
```

-> MSCDINV after datafilling the OC3 paddleboards into card #8:

```
>table mscdinv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MSCDINV
>list all
TOP
   MSCDKEY                                                          SLOTINFO
-------------------------------------------------------------------------------
   0  0  1                                                  TBUSACC NT9X52AA NIL
   0  0  2                                                CLOCK NT9X53AC NT9X54AC
   0  0  3                                                  MSP NT9X13DD NT9X26AA
   0  0  5                                                       MAPPER NT9X15AA
   0  0  6                                CHAIN DS512 NT9X17DA NT9X20BB $
   0  0  8                                             DS512 NT9X17AD NT9X63AB
   0  0 10                                CHAIN DS512 NT9X17DA NT9X20BB $
   0  0 16                                            DS512 NT9X17AD NT9X62BA 4
   0  0 22                                               DS30 NT9X17AA NT9X23AA
   0  0 23                                               DS30 NT9X17AA NT9X23AA
   0  0 24                                               CMIC NT9X17AA NT9X20AA
   0  0 25                                               CMIC NT9X17AA NT9X20AA
   0  0 26                                                    PBUS NT9X49CB NIL
   1  0  1                                                  TBUSACC NT9X52AA NIL
   1  0  2                                                CLOCK NT9X53AC NT9X54AC
   1  0  3                                                  MSP NT9X13DD NT9X26AA
   1  0  5                                                       MAPPER NT9X15AA
   1  0  6                                CHAIN DS512 NT9X17DA NT9X20BB $
   1  0  8                                             DS512 NT9X17AD NT9X63AB
   1  0 10                                CHAIN DS512 NT9X17DA NT9X20BB $
   1  0 16                                            DS512 NT9X17AD NT9X62BA 4
   1  0 22                                               DS30 NT9X17AA NT9X23AA
```

```
   1  0 23                                                DS30 NT9X17AA NT9X23AA
   1  0 24                                                CMIC NT9X17AA NT9X20AA
   1  0 25                                                CMIC NT9X17AA NT9X20AA
   1  0 26                                                     PBUS NT9X49CB NIL
BOTTOM
>
```

After datafilling table MSCDINV for the OC3 paddleboards, they will automatically show up on the map. No extra action is required by the operator. By following the guidelines for getting the OC3 paddleboards into service (See “System Behaviour/Feature Operation” on page 1915.), card 8 for our example, will look like the following:

```
CM      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 CM Flt  Clock   OM   B   1Shlv   1EIU   2   RS    .      74C..   1Crit   SDM
   M       M             *C*     *C*     *C*             *C*     *C*     *C*
 CARD              Message Switch   Clock   Shelf  0       Inter-MS Link 0 1
  0 Quit       MS 0       .          M Free          .                     - -
  2            MS 1       .          Slave           .                     - -
  3
  4            Shelf 0                  1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
  5            Card  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
  6 Tst_       Chain           |       |
  7 Bsy_       MS 0  . . . - . . - . - . - - - - - - . - - - - - - . . . . .
  8 RTS_       MS 1  . . . - . . - . - . - - - - - - . - - - - - - . . . . .
  9 Offl_
 10            Card 08 Protocol Port  0
 11 LoadCd_    MS 0  .   DS512    1   -
 12 QueryCd_   MS 1  .   DS512    1   -
 13 Card_
 14 QueryMS   CARD:
 15 Trnsl_
 16
 17 Next
 18 Port_
   TAK3
 Time  10:00  >
```

170.6 Interactions

There should be no interaction between this feature and any existing feature as seen by the end user. That is, there would be no effect on existing call functionalities, etc.

170.7 Applicable customer facing sections

Fault Management

Logs	__NA__
Alarms	__NA__

Configuration

Data Schema	__NA__
User Interface	__NA__
Element Management	__NA__
Security	__NA__
Service Order	__NA__
Office Parameters	__NA__
Accounting (includes AMA billing)	__NA__
Performance (includes operational measurements)	__NA__

170.8 Glossary

Term	Description
BRISC	BNR Reduced Instruction Set Computer (DMS Core)
CBM	Core and Billing Manager
CBM 800	OC3 connected simplex CBM
MAP	Maintenance and Administration Position (core I/O terminal)
MS	Message Switch
MSCDINV	Message Switch Card Inventory
OC3	Optical Carrier- Level 3 (transmission interface)
PEC	Product Equipment Code
SN	SuperNode
SNSE	SuperNode System Enhanced

i. **Recommended Reading/References**DMS-100 Card Replacement Procedures document (297-9051-547),

ii. DMS SN and SNSE Message Switch Maintenance Guide (297-5001-549)

171: Functional Description (FN): A00005363

171.1 Feature name

A00005363 - CAIN FlexCDR Enhancements

171.2 Description

Additional information is needed that is not currently collected and presented in CDR records. This information will be made available in new CDR fields, that are used by the Flexible CDR capability. Some of this information comes from new CAIN message processing. The Flexible CDR capability is controlled by the existing SOC UBFR0001.

The processing of this new information is controlled by a new SOC CAIN0202 - CAIN FlexCDR Enhancements.

The new processing consists of:

1. Support for a new CAIN parameter, AMABusinessCustomerId in some incoming messages.
2. Support for a new digits id (300) for an existing CAIN parameter, AMADigitsDialedWC.
3. Support for recording all the digits for a currently supported digits id (301) for the existing CAIN parameter AMADigitsDialedWC.
4. Support for retaining the first occurrence of an existing CAIN parameter, AMASlpID. Currently, only the last occurrence of this parameter is retained.
5. Support for 4 new parameters in the CDRTMPLT table: SLPID1ST, BUSCSTID, DGI300 and DGI301. This feature does not create a new predefined template. The customer must either modify their existing template or create a new template which includes the 4 new parameters.

171.3 Functional Overview

171.3.1 CAIN: AMABusinessCustomerId

Prior to this feature, the AMABusinessCustomerId parameter was not supported by the DMS-250. This feature provides support for this parameter, including enhancements to the CAIN simulator to generate this parameter in the messages listed below. The size of this parameter is 11 digits.

The call processing support consists of parsing the incoming parameter, and making the data available for use by the billing component - it will not affect call processing (either by its value, presence or absence) in any other way. Only the last occurrence of this parameter will be retained for use by the billing component. This parameter will be supported in the DMS-250 being received in the following messages from an SCP:

- Analyze_Route
- Disconnect
- Send_To_Resource

This includes display of this parameter in the VAMP log.

171.3.2 CAIN: AMADigitsDialedWC - 300

Prior to this feature, the AMADigitsDialedWC was not supported for a digits id of 300. This feature adds this support, which consists of parsing the incoming parameter for this digits id, and making the data available for use by the billing component. Only the last occurrence of a AMADigitsDialedWC with a digits id of 300 will be retained for use by the billing component (as is the case today with other such AMADigitsDialedWC digits id). The maximum supported length for the value of this digits id is 24 digits (with the three digits of the digits id makes a maximum total length of 27 digits).

The AMADigitsDialedWC parameter is currently supported by the DMS-250 for various incoming messages from the SCP, and this activity does not alter that support - that is to say that the DMS-250 will support receiving a AMADigitsDialedWC parameter with a digits id of 300 in all cases that reception of a AMADigitsDialedWC parameter is valid. However, the functionality added by this feature (recording the value received in a AMADigitsDialedWC parameter with digits id = 300) will only be supported for the following messages:

- Analyze_Route
- Disconnect
- Send_To_Resource

This includes display of this new digits id in the VAMP log.

171.3.3 CAIN: AMADigitsDialedWC - 301

Prior to this feature, only the first four digits in the AMADigitsDialedWC parameter with digits id = 301 were recorded (in field PINDIGS). This feature records the entire parameter (the 3 digits of the digits id plus 24 digits) in the new field DGI301. When this feature is active, the AMADigitsDialedWC parameter with digits id = 301 is no longer recorded in field PINDIGS, but only in field DGI301.

171.3.4 CAIN: AMASlpId

Prior to this feature, only the last AMASlpId parameter for a call received in a message from the SCP was retained for use by the billing component. This feature adds support for also retaining the first AMASlpId parameter for a call received in a message. This support applies to all messages from the SCP that contain an AMASlpId parameter. Note that in the case that there is only one such AMASlpId parameter received during a call, the first and last AMASlpId values will be the same. The AMASlpId parameter is currently supported by the DMS-250 for various incoming messages from the SCP, and this activity does not alter that support. The functionality added by this feature (retaining the first AMASlpId) will however only be supported for the following messages:

- Analyze_Route
- Disconnect
- Send_To_Resource

171.3.5 CAIN: Simulator changes

To support the changes to the CAIN simulator for the new parameter and AMADigitsDialedWC digits, the following CAIN simulator tables are changed. Table Control Changes

Table	Desc
CAINRESP	A new parameter, AMABusinessCustomerId, with a value of 11 digits, is supported in the following operation types: • Analyze_Route • Disconnect • Send_To_Resource This new parameter is also supported in the “non-restricted” message (as are all parameters). For the existing parameter AMADIGS, a new digits type, 300, is supported.
CAINREXT	For the existing parameter AMADIGS, a new digits type, 300, is supported.

171.3.6 CDR: Table changes

To allow the recording of Dialed digits, Customerid and the first received Amaslpid, the following changes are made to the CDRTMPLT table.

Table	Desc
CDRTMPLT	4 new parameters for the FIELDS and REORIGCP subfields of table CDRTMPLT are added to record the data collected for the AMADigitsDialedWC, AMABusinessCustomerId, and AMASlpID CAIN parameters.

Sample datafill for table **CDRTMPLT** (new fields in bold):

NAME ACTIVE PRIMARY FIELDS REORIGCP

VZN_FLXCDR Y N (SEQNUM) (CIC) (ORIGTIME) (ORIGDATE) (ANSTYPE) (TIMECHNG) (ORIGAMPM) (INCINTL) (DISCTIME) (DISCDATE) (ANISUFF) (DISCAMPM) (INCBILL) (FILL1) (CALLDUR) (PINDIGS) (ANISP) (INFODIG) (BILLNUM) (ACCTCD) (CLGPTYNO) (RLTCDR) (ACCTV) (UNIVACC) (DIALEDNO) (CALLEDNO) (OUTPULNO) (FILL4) (ORIGOPRT) (PREDIG) (CNPREDIG) (OPART) (TPART) (QUEUED) (FILL3) (FILL3) (FILL4) (RTENO) (NETSEC) (OPCHOICE) (COLLTIME) (ADIN) (LNPCHECK) (NUMWBCKT) (WBCKTS) (FINSID) (BILLTYPE) (ORIGGRP) (DISCTYPE) (ORIGMEM) (PASSTHRU) (TERMGRP) (PRESIND) (TERMMEM) (OSRASSOC) (DIGDATA) (FINTKGRP) (TRAP) (COSOVE) (FINTKMEM) (SCPBILL) (FILL3) (FILL3) (FILL3) (FILL2) (FILL3) (FILL2) (TRTMTCD) (COMPCODE) (CRID) (DNIS) (ORIGPVN) (TERMPVN) (ORIGLRN) (PORTEDNO) (CAINCT) (ACG) (DNISNOA) (FILL1) (MLTCOSID) (FILL4) (FILL1) (COSINDEX) (FILL2) (CARRSEL) **(SLPID1ST) (BUSCSTID) (DGI300) (DGI301)** (FILL8) $ $

171.3.7 CDR: New Field Description

The new data captured by this activity will be formatted into the CDR record using the following layout:

Field Name	Chars	CDR Field Description
DGI300	27	Contains the Digit ID “300” followed by the dialed digits which are contained in the SCP message whenever the digits id = 300. This will be performed as described in section 2.3.2.
DGI301	27	Contains the Digit ID “301” followed by the dialed digits which are contained in the SCP message whenever the digits id = 301. This will be performed as described in section 2.3.3.
BUSCSTID	11	Contains the customer id which is received in the SCP message. This field is populated based on the description in section 2.3.1.
SLPID1ST	9	Contains the first AMASLPID received. This field is populated as described in section 2.3.4.

Sample CDR Log (new fields in bold):

```
          RTPE_B115BH     CDR273 FEB04 21:44:14 4200 INFO CDR_CALL_ENTRY
250X15AY       CDR273 FEB09 13:44:20 0800 INFO CDR_CALL_ENTRY

RECCD     F0                          TEMPLID   016
ACTIDX    6                           TOOLGEN   Y
USEEDIT   N                           VARLNGTH  N
SEQNUM    00001                       CIC       5676
ORIGTIME  34992                       ORIGDATE  035
ANSTYPE   03                          TIMECHNG  N
ORIGAMPM  1                           INCINTL   N
DISCTIME  35052                       DISCDATE  035
ANISUFF   1                           DISCAMPM  1
INCBILL   1                           CALLDUR   00013107
PINDIGS   6987                        ANISP     5124599628
INFODIG   1                           BILLNUM   508543214997790000001234
ACCTCD    802000012345                CLGPTYNO  214684552900000
RLTCDR    Y                           ACCTV     3
UNIVACC   8007654321                  DIALEDNO  508345214997799
CALLEDNO  508543214997790             OUTPULNO  508345129479970
ORIGOPRT  501                         PREDIG    1
CNPREDIG  1                           OPART     511
TPART     31                          QUEUED    Y
OPCHOICE  232                         COLLTIME  060
```

```
ADIN      12                          LNPCHECK  7
NUMWBCKT  16                          WBCKTS    10000000 10000000 00000000
FINSID    111                         BILLTYPE  35
ORIGGRP   0353                        DISCTYPE  1
ORIGMEM   0101                        PASSTHRU  2
TERMGRP   0355                        PRESIND   1
TERMMEM   0101                        OSRASSOC  N
DIGDATA   Y                           FINTKGRP  09999
TRAP      N                           COSOVE    Y
FINTKMEM  62843                       SCPBILL   FE17700B
TRTMTCD   010                         COMPCODE  3
CRID      684149400                   DNIS      214684149400000
ORIGPVN   214684149400000             TERMPVN   214684466200000
ORIGLRN   2146841494                  PORTEDNO  2146844662
CAINCT    1                           ACG       Y
DNISNOA   103                         MLTCOSID  0001
COSINDEX  0001                        CARRSEL   02
SLPID1ST  032401234                   BUSCSTID  02532401234
DGI300    300997799912345678901234567DGI301    301997799912345678901234567
```

171.3.8 Software Optionality Control

The actual recording of the four items, DGI300,DGI301, BUSCSTID, and SLPID1ST is controlled by a new SOC, CAIN0202 - CAIN FlexCDR Enhancements.

171.4 Hardware Requirements or Dependencies

No new hardware dependencies are introduced by these features.

171.5 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced by these features.

171.6 Limitations and restrictions

None

171.7 Interactions

None.

171.8 Applicable customer facing sections

Fault Management

Logs	___X__
Alarms	__na__

Configuration

Data Schema	___X__

User Interface	__na__
Element Management	__na__
Security	__na__
Service Order	__na__
Office Parameters	__na__
Accounting (includes AMA billing)	__X___
Performance (includes operational measurements)	__na__

171.9 Glossary

Term	Description
AMA	Automatic Message Accounting
CAIN	Carrier AIN
CDR	Call Detail Recording
SCP	Service Control Point
SOC	Software Optionality Control

172: Functional Description (FN): A00005375

172.1 Feature name

A00005375: New Shelf Discovery Alarms.

172.2 Description

Note: This feature does not add any extra functionality. The only addition is the extra faults to indicate shelf discovery failure due to a particular card or card incompatibility. Refer to the Fault Management (FM) A00005375 for further details.

173: Functional Description (FN): A00005391

173.1 Feature name

SBA: Support for Verizon GNS personal Toll Free Service : A00005391.

173.2 Description

New CDR fields are required by Verizon to support introduction of their Personal Toll Free Service. This activity will ensure that new records can be handled by SBA and recognized by SDM AMADUMP. There is corrresponding activity on the core side also with the activity id A00005363.

173.3 Hardware Requirements or Dependencies

Requires no additional hardware resources to implement the activities in this feature.

173.4 Software Requirements or Dependencies

Requires no additional software resources to implement the activities in this feature.

173.5 Limitations and restrictions

No new limitations/restrictions as a result of this feature. The only limitation relates to the time-lag in the interpretation of changed templates on the core. During this time-lag, the new templates are downloaded from the core to SDM side.

173.6 Applicable customer facing sections

The customer will be able to see the the new records in the correct format at the amadump display output.

173.7 Glossary

Term	Description
SBA	SuperNode Billing Application is a distributed, high capacity, scalable billing system that enhances the functionality of the DMS family switch. The primary purpose of the SBA is to receive records from the Computing Module (CM), perform processing, and route the records to files. The SBA can also be configured to send billing files to the operating company's downstream processor(s).
SDM	The term Supernode Data Manager (SDM) refers to the SDM peripheral as a whole. In other words, it includes SDM hardware, AIX operating system, SDM software, SBA base software and other applications.
AMADUMP	Amadump is a tool that allows you to view billing records from the standard billing files. You can display all the records using amadump or you can create filters that allow you to display only records matching a specific search criteria. Amadump can be used to view records in multiple files by specifying a time period or by entering the filename(s).

174: Functional Description (FN): A00005485

174.1 Feature name

SAM21 Platform Installation on SSPFS

174.2 Purpose

To allow the installation of the SAM21 Platform Package from CDROM on to the SSPFS box.

In SN07, the new SSPFS box does not contain a DAT Tape Drive but only a CD/DVD ROM drive. Therefore, the Platform Installation tool will be further enhanced to allow the user to extract the SAM21 Platform Package from CD where it is stored in a “RPM” format.

What this means is that this tool will now be used in ALL Solutions to allow the user to install the SAM21 Platform Loads using a DAT tape, to be backward compatible, and CDROM moving forward. The CDROM will be of ISO format containing the following files:

- SAM21 Platform Fileset (This is used for installation on the AIX SDM)
- SAM21 Platform TAR file
- SAM21 Platform RPM file

If the solution contains an AIX SDM, the user will be prompted for a roo passwd for the SDM so that the fileset will be Secure Copied onto the SDM.

Note: The implementation of this activity will also satisfy the problem described by CR.Q00808578 -

This tool will be further expanded to allow the user to install the Call Agent and Message Controller Linux loads from CDROM. It must be noted that the SOS images will not be extracted from CD using this tool.

175: Functional Description (FN): A00005538

175.1 Feature name

Preset Conference on Succession

175.2 Description

This feature addresses the functionality of Preset Conference in Succession..

For a detailed description of the Preset Conference please refer to the NTP 297-8001-350 DMS 100 Family NA100 Translations Guide Volume 13 of 20. However, in the Succession domain, there are further limitations to the Preset Conference functionality which are described in this document.

This activity provides support for the following types of lines on both North American and International markets.

- CICM lines - i2002, i2004 and m6350 softclients
- MG9K Pphones and IBN lines

175.3 Hardware Requirements or Dependencies

There is no special hardware dependency for this service. It is assumed that the lines types as described in Section 175.2 are available. UAS is also needed in order to provide this functionality. Please refer to the configuration section of activity A59036149 in FMDOC for provisioning details of the AudioServer.

175.4 Software Requirements or Dependencies

The SN07 software loads (both North American and International) are required of the Succession elements.

175.5 Limitations and restrictions

175.5.1 Maximum conferees in Preset Conference

The maximum supported conferees for Preset conference is 25. Larger conference sizes are not supported.

175.5.2 Hybrid Solution Limitation

This activity seeks to implement Preset conference in non-hybrid scenarios only. On Hybrid environment, the support remains unchanged.

175.5.3 Add ON

The ADDON functionality for Preset Conference is not supported on Succession. The subfield ADDON in Table PRECONF should be set to N.

Figure 1 Table PRECONF, ADDON subfield

```
0 0 9192461888 D IBN POTSDATA 0 N N N N Y $
```

175.5.4 Audio Tone Detector

The Audio Tone Detector is a MTM component and the functionality is not available through UAS. Hence, this activity does not support the ATD functionality of the Preset Conference. The ATD subfield in Table PRECONF should be set to N.

Figure 2 Table PRECONF, ATD subfield

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

175.5.5 Immediate Start

Support of Tones or Announcements for Preset Conference on Succession is not implemented through this activity. This would imply that the IMMSTART subfield in Table PRECONF should be set to Y.

Figure 3 Table PRECONF, IMMSTART subfield

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

175.5.6 Conferee Class

The Conferee class ‘P’ and ‘D’ are supported. The other conferee classes (ie., ‘A’ and ‘C’) are not supported in this activity.

175.5.7 Preset Conference Options

The Preset Conference options MADNOPT and NARS is not supported through this activity and should not be datafilled.

Figure 4 Table PRECONF, Options

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

175.5.8 Tones

This feature will make use of conference tones like conference entry tone, and conference exit tone. The Preconference tones PCNOR (Preset Conference Notification Tone) and PCALR (Preset Conference Precedence Notification Tone) is not supported through this activity.

175.5.9 Preset Conference on warm swact of Audio GWC

An alerting preset call will not be torn immediately after a warm swact of the audio controller GWC. It will continue ringing until expiration of Preset Conference timer, which is datafilled in table PRECONF. However, it is not possible to answer the call. (Note that the timer runs for two cycles).

175.6 Interactions

The existing feature interactions are described below:

If any of the conferees are connected to the CS2000 switch where the preset conference is being originated and has any of the following features,

- Call forwarding don’t answer
- Call forwarding busy
- Call forwarding intragroup

These features will remain active for the incoming preset conference call (if the primary address does not answer call forwarding will be attempted if it is activated).

Interaction of Preset Conference with any other feature other than the above listed ones is not supported and may result in undefined behaviour.

Note: *The fields described in Section 175.5.3 through 175.5.8 must be datafilled as described. It is to be noted that there exists no interface to restrict the office from provisioning the above mentioned ones , the*

maximum conferees in a Preset Conference and the feature interactions (described in Section 2.6). Any inconsistencies or failures that may result from such a provisioning violation should be considered beyond Nortel Networks CallServer2000's control and corresponding problems reported will be subject to immediate closure without further investigation.

175.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

175.8 Glossary

Term	Description
CICM	Centrex IP Client Manager
CS2000	Communication Server 2000
DMS	Digital Multiplex System
DN	Directory Number
GW	Gateway
GWC	Gateway Controller
MTM	Maintenance Trunk Module

Term	Description
UAS	Universal Audio Server

176: Functional Description (FN): A00005734

176.1 Feature name

Multiple Time Zone (MTZ) support for CICM lines.

176.2 Description

CICM lines can exist in multiple time zones as there is no geographical limitation that the call server and the agents should co-exist in the same time zone.

With the existing implementation line features, billing, logs etc. work on the switch time for all users irrespective of their local times.

This activty provides Multiple Time Zone (will be called by abbreviation MTZ henceforth) by providing the ability to store the local time of the user on the switch so that the features can be activated in terms of the local time of the user.

Activity A59038784 provided the same functionality for subscriber visible services for IBN and RES sets.

This activity extends the support to CICM KSET lines.

The services addressed by this feature are

a. WUCR (Wakeup Call Request)

b. ARDDN (Automatic Recall Directory Number)

c. QTD (Query Time and Date)

No changes are made to Logs and Billing records.

This new functionality reuses existing table MULTITM which can be datafilled with different time zones along with Day Light Savings if any. The items that can be entered in table MULTITM are shown in Figure 1.

Figure 1 : Items in table MULTITM (Range of MULTITM)

ENTRY NAME	ENTRY TYPE
MTZNAME	MULTITM_KEY
TMSENSE	MODIFY
MINUTES	MTZMINSTYPE
DST	YES_NO
DSTSENSE	MODIFY
DSTMINS	DSTMINSTYPE
STRTYEAR	MTZYEARTYPE
STRTMON	MONTHS
STRTDAY	DAYS
STRTHOUR	HOURS
STRTMIN	MINUTES
ENDYEAR	MTZYEARTYPE
ENDMON	MONTHS
ENDDAY	DAYS
ENDHOUR	HOURS
ENDMIN	MINUTES

Figure 2 shows a sample entry for table MULTITM. It shows that the timezone BERL is offset from the standard by 60 minutes, and that DST of plus 60 minutes begins on March 31st at 0200, and ends on October 27th at 0300.Similarly AZOR is offset with a nagative 60 (behind by 60 mins).

There is one pre-registered key in table MULTITM: 'LOC'. This key is used to show when the time local to the CM is applying DST. This is to cover situations such as the USA and the UK, whose DST start times are often one week apart.

Figure 2: Sample entries in Table MULTITM

```
MTZName TMSense Minutes DST DSTSense DSTmins STRTYear STRTMon STRTDay
STRTHour STRTMin ENDYear ENDMon ENDDay ENDHour ENDMin

LOC POS 0 N POS 0 2002 JAN 1 0 0 2002 JAN 1 0 0

BERL POS 60 Y POS 60 2002 MAR 31 2 0 2002 OCT 27 3 0

AZOR NEG 60 N POS 0 2002 JAN 1 0 0 2002 JAN 1 0 0
```

This activty introduces a new option ‘MTZ’ for KSET lines ,details about this option are:

- This option is a Set option ,can be assigned to any key .(DN key(key 1)or any other vacant key) .

- It is ‘data feature’ option , has one parameter, which is any key in table MULTITM.Table MULTITM is datafilled with different possible timezones.A KSET agent ‘s timezone if different from the switch timezone is configured by associating the corresponding entry in MULTITM through MTZ option

- MTZ option if applied to a Set affects the specified features(QTD.WUCR and ARDDN) on all DN appearances of the set.

- It is ‘Code access ‘ feature , does not require a key press to activate the feature.Also there is no explicit activation required,effective once assigned .

-No Lamp be lit by this option

-MTZ option is applicable to only M5216 LCC (It is the only supported KSET LCC on CICM currently)

Figure 3 shows how to datafill a line with the MTZ option. Figure 4 shows the qdn and qlen output .

Figure 3 : Assigning MTZ option

```
SO:
>ado
SONUMBER:    NOW   2  2 19 PM
>
DN_OR_LEN
>9915022
OPTkey:
>1
OPTION:
>MTZ
SO_MTZ_NAME:
>berl
OPTKEY:
>$
COMMAND AS ENTERED
ADO NOW 2 2 19 PM 9915022 (1 MTZ LOC)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO eDIT
>Y
```

Figure 4: QDN and QLEN output

```
-----------------------------------------------------
>qdn 9915022

DN: 9915022
TYPE: SINGLE PARTY LINE
SNPA: 919 SIG: N/A LNATTIDX: N/A
LINE EQUIPMENT NUMBER: HOST 00 0 15 17
LINE CLASS CODE: M5216 SET
KEY: 1
CUSTGRP: POTSDATA SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: 6X21AC GND: N PADGRP: PPHON BNV: NL MNO: Y
PM NODE NUMBER : 38
PM TERMINAL NUMBER : 498
DNGRPS OPTIONS:
NETNAME:PUBLIC
NAME: RTPH CO
OPTIONS:
MTZ BERL

>qlen 9915022
LEN: HOST 00 0 15 17
TYPE: SINGLE PARTY LINE
SNPA: 919
DIRECTORY NUMBER: 9915022
LINE CLASS CODE: M5216 SET
CUSTGRP: POTSDATA SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: 6X21AC GND: N PADGRP: PPHON BNV: NL MNO: Y
PM NODE NUMBER : 38
PM TERMINAL NUMBER : 498
DNGRPS OPTIONS:
NETNAME:PUBLIC
NAME: RTPH CO
OPTIONS:
MTZ BERL
 KEY DN
 --- --
 1 DN 9199915022
KEY FEATURE
 --- -------
1    MTZ
```

In this example the Set is configured to belong to BERL timezone .This timezone is 60 mins ahead of the switch time (see figure 2 - BERL tuple).

With above datafills if the CM clock is as below,

Date is THU. 26/FEB/2004 16:45:58 ,

Invoking QTD(Query Time and Date) on the KSET set will display

“Date is THU. 26/FEB/2004 **17:45:58**”

176.3 Hardware Requirements or Dependencies

N/A

176.4 Software Requirements or Dependencies

SN07 or equivalent CM load.

176.5 Limitations and restrictions

The information in table MULTITM, including time offsets and start and end points for daylight savings time, will have to be entered manually each year. Since it is up to each country or region to set their own DST dates, any routine to automatically generate these dates is in danger of becoming obsolete very quickly. An effort has been made to make the table as human readable as possible, to make the task of entering the data as easy as it can be.

When adding a tuple to table MULTITM, the starting and ending dates of the DST entries can be at most switch year+1. Any entry with a year greater than that value are rejected.

This activty tests MTZ feature only on CICM KSET line though the implementation is in the switch which does not differentiate a CICM line from other lines like MG9K etc...The feature is not restricted to other lines but as a part of this activity the functionality is tested only on CICM and testing on other lines like lines on MG9K are out of scope.

M5216 is the only LCC supported on CICM currently and is the only affected LCC by this activity.

MTZ assigned on a CICM line affects the date and time on the 3 specified features only viz. ARDDN,QTD and WUCR and does not affect the time provided by the CICM gateway for the Inbox,Outbox etc... on the CICM line.

No changes to billing records or logs for the affected features are included in this activty.

There is no restriction on the number of lines that can have this feature.

176.6 Interactions

This feature alters any customer activated feature where the time of day is a factor. Wake Up Call Request is an obvious example, where the user enters the time at which they wish to receive a call to wake them.The full list is:

1. WUCR (Wake Up Call Request)

2.ARDDN (Automatic Recall Dialable Directory Number)

3.QTD (Query Time and date) - pphone only

176.7 Applicable customer facing sections

Fault Management	
Logs	n/a
Alarms	n/a
Configuration	
Data Schema	n/a
User Interface	n/a
Element Management	n/a
Security	n/a
Service Order	x
Office Parameters	n/a
Accounting (includes AMA billing)	n/a
Performance (includes operational measurements)	n/a

176.8 Glossary

Term	Description
ARDDN	Automatic Recall Directory Number
CICM	Centrex IP Client Manager
DST	Daylight Savings Time
MTZ	Multiple Time Zone
QTD	Query Time and Date
WUCR	Wake Up Call Request

177: Functional Description (FN): A00005758

177.1 Feature name

ESUP OVER TELNET SUPPORT

177.2 Description

ESUP, Enhanced SDM Upgrade Procedure, is the recommended upgrade procedure for the SuperNode Data Manager from/to SDM20/CS2E00070.

The Major limitation of ESUP was its restriction on the usage of the Active System console to perform the upgrade. This feature provides the support for performing the ESUP upgrade over remote login sessions (telnet) as well.

This is achieved by the usage of the Open Source third party software 'SCREEN', a full-screen window manager that multiplexes a physical terminal between several processes.

ESUP process is launched with 'SCREEN' support. The usage of 'SCREEN' is transparent to the user.

The framework for a semi-automatic recovery in case of an ESUP failure is also introduced as part of this feature. Semi-automatic recovery here refers to the user initiated recovery procedure to recover the system from upgrade failures.

177.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

177.4 Software Requirements or Dependencies

177.4.1 Software requirements for downstream system

No new hardware requirements or dependencies are introduced by this feature.

177.4.2 Software requirements for SDM.

Open Source software 'SCREEN' is to be installed on the system.

177.5 Limitations and restrictions

- 'Telnet' is the only remote login supported.

177.6 Interactions

No

177.7 Applicable customer facing sections

Fault Management

- Logs ___N/A__
- Alarms ___N/A___

Configuration

- Data Schema __N/A_
- User Interface __X__
- Element Management _N/A_
- Security _N/A_
- Service Order _N/A_
- Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) __N/A__

177.8 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
OSS	Operations Support System
ESUP	Enhanced SDM Upgrade Procedure

178: Functional Description (FN): A00005986

178.1 Feature name

EM integration with PAM+ proxy

178.2 Description

Succession user authentication services are migrating to a single centralized 3rd party server, which provide authentication services to succession management systems via a Pluggable Authentication Module (PAM) on the SSPSFS platform. By using PAM, Succession management systems can interact with any pluggable authentication technology of a customers choosing, without having to make any changes to succession management applications. The use of a centralized authorization database via PAM also provides the advantage of having a single account management interface for use by all succession management tools.

This feature integrates the CICM-EM into this wider strategy for user authentication on Succession.

The CICM-EM now interfaces to PAM via the HTTPS PAM+ proxy on SSPFS.

The CICM-EM User Interface requires a username/password login. Prior to this feature, only a single user level was supported – which provided full access to all the provisioning, maintenance and admin functions of the CICM-EM. With the introduction of this feature, the CICM-EM can be configured to access the HTTPS PAM+ proxy, passing it the username and password, and the SSPFS then returns a user authentication level to the CICM-EM, or rejects the username and password if they are not a valid combination. This user authentication level is then used by the CICM-EM to restrict access to functions that are not appropriate for particular user groups.

178.2.1 Detail

Prior to this feature, the username and password supplied when logging into the element manager corresponded to local user accounts on the CICM-EM. For SN07 Succession deployments, username and password can be configured to be a global Succession account managed on a centralized authentication database, which interfaces to Succession management tools via the PAM+ proxy located on the SSPFS.

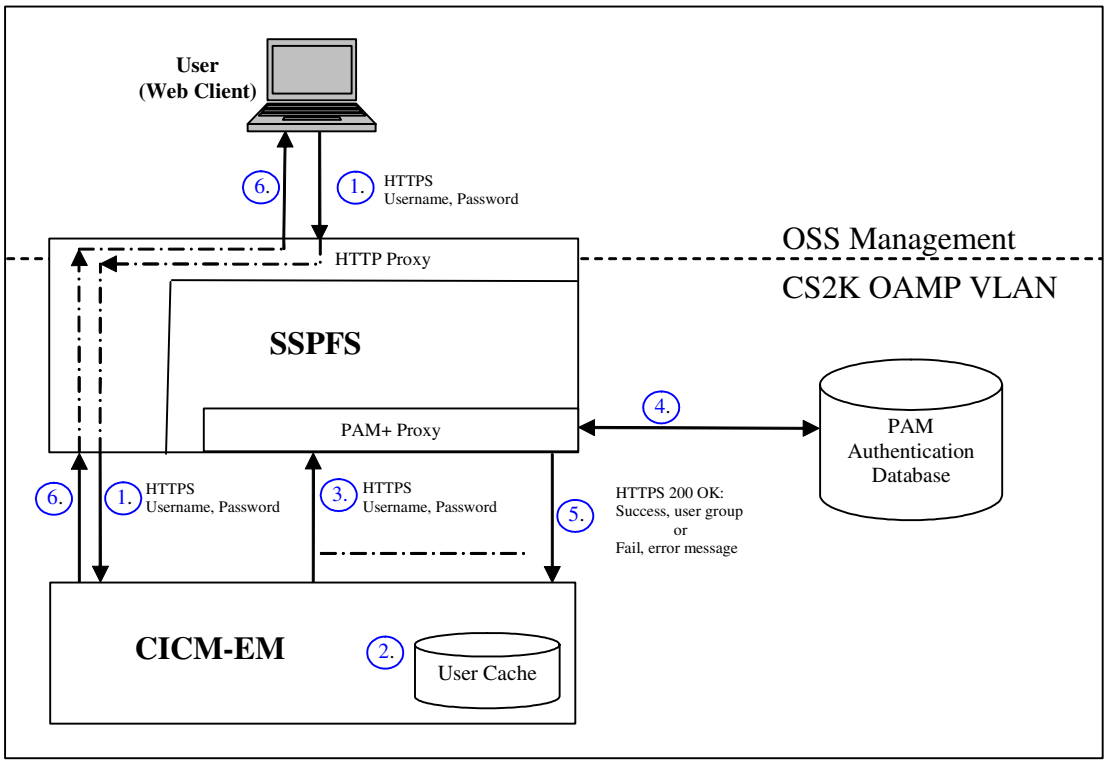
Local user account management and user authentication on the CICM-EM is preserved for TDM deployments, where the SSPFS platform is not used. For

Succession deployments, a method of local user authentication is also provided for use when connectivity is lost to the SSPFS platform.

178.2.2 User authentication via SSPFS PAM Proxy

The behavior provided by CICM-EM user authentication via the PAM proxy running on the SSPFS, is outlined in the functional behavior diagram below.

Functional Behaviour Diagram: HTTPS PAM+ proxy and CICM-EM integration



1 Using a web client, the user attempts to log into the CICM-EM through the HTTP proxy located on the SSPFS. The supplied username and password are for a global Succession user account which is managed on a centralised authentication database. The Web Client sends an HTTPS request to the CICM-EM with the username and password built into the HTTP authentication header.

2 The CICM-EM uses the supplied username and password as a key to search a cache of recently authenticated users. Each user entry in the cache contains a corresponding username and password for a temporary local user account assigned to that user. If the user is present in the cache, the mapped local username and password is passed back to the PAM authenticator and we go directly to step 5 (with successful authentication).

3 The CICM-EM sends an authentication request to the HTTPS PAM+ proxy located on the SSPFS.

4 The PAM+ proxy authenticates the user on a centralised authentication database via PAM.

5 If the authentication is successful, the PAM+ proxy responds with a list of succession user groups to which the user belongs. The CICM-EM has a list of pre-defined local user groups that are equivalent to the user groups returned by the PAM proxy. The CICM-EM creates a temporary local user account on the CICM-EM when a response to a user authentication request is successful. The temporary local user account is added to the pre-defined local user groups that are equivalent to the Succession user groups returned by the PAM proxy.

   Additionally, the CICM-EM adds the authenticated username/password and the corresponding temporary local username/password to the user cache. This entry is held in the local cache for a pre-determined amount of time. Whilst this entry is present in the cache, subsequent authorisation requests for this user do not need to be processed through the PAM proxy. This reduces the processing load on both the CICM-EM and PAM proxy.

   The CICM-EM also replaces the global Succession username/password in the HTTPS authentication request with the username/password of the temporary local user account. The temporary local username and password combination is then authenticated locally by standard user authentication. If the authentication is unsuccessful, then the CICM-EM rejects the user's attempt to log in.

6 If the authentication is successful, then the CICM-EM provides the user with the required webpage. If the authentication is unsuccessful, then the CICM-EM denies access to the requested webpage.

Succession User authentication levels on the PAM+ proxy are organised into five separate domains, with each domain containing 5 separate levels of user authentication. This provides a total of 25 user authentication levels, as shown below:

Access level	**User Domain**				
	Trunks	**Lines**	**MGC**	**MG**	**EMS**
Administrator	trkadm	lnadm	mgcadm	mgadm	emsadm
Read-Write	trkrw	lnrw	mgcrw	mgrw	emsrw
Provisioning	trkprov	lnsprov	mgcprov	mgprov	emsprov
Maintenance	trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
Read-Only	trkro	lnro	mgcro	mgro	emsro

The PAM proxy returns a list of groups against which the user has been successfully authentication. The user domains relevant to the CICM Element Manager are Lines, MG and EMS.

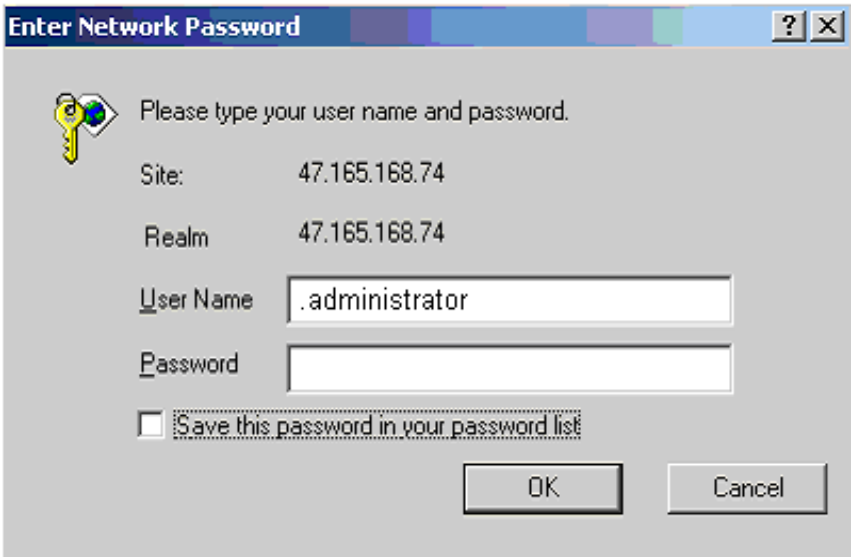
All CICM-EM web pages are configured with access control levels that are appropriate to their functionality.

178.2.3 Local User authentication

Centralised user authentication via the SSPFS PAM proxy is not available to TDM deployments of CICM. In addition, if connectivity is lost between the CICM EM and the SSPFS, it is important to provide the ability to access the CICM-EM to provide continued access to the functionality that it offers.

The CICM-EM will check if it is running in a TDM or Succession CICM deployment before it attempts to process the authentication via the PAM proxy. For TDM deployments, the authentication functionality will immediately pass control of the authentication back to the standard mechanism used for CICM.

For Succession deployments, users will be able to select local authentication by prefixing their username with a period (“.”). This will allow users to access the CICM-EM when the PAM proxy is out of service (provided they have a local user account on the CICM-EM). Therefore, to access the CICM-EM when the SSPFS is not accessible, the user can log in as shown below:



178.3 Configuration

The configuration of the IP address to use for the SSPFS PAM+ proxy is configured during p the EM preboot stage as follows:

Screen capture of initial configuration of the EM

```
+----------------------------------------------------------------
| STEP n  : Configure the SSPFS PAM Proxy
+----------------------------------------------------------------


This CICM Element Manager can use Pluggable Authentication Module (PAM)
on the Succession Server Platform Foundation Software (SSPFS) platform
(if available).

Will this Element Manager use the PAM on the SSPFS to authenticate users?
[Y|N, default=N]:
Y

Will this EM connect to the PAM server using HTTPS [Y|N, default = N]
N

Please enter the IP address of the SSPFS PAM proxy:
1.2.3.4

You have entered the IP address of the SSPFS PAM proxy as 1.2.3.4
Is this correct [Y|N, default=N]
Y
```

The user can select to use HTTP or HTTPS (secure HTTP) to communicate with the PAM proxy. If HTTPS is selected, the user will be prompted to enter the Fully Qualified Domain Name (FQDN) of the PAM server. HTTPS requires that a certificate from a valid signing authority is installed on the SSPFS.

178.4 Hardware Requirements or Dependencies

N/A

178.5 Software Requirements or Dependencies

N/A

178.6 Limitations and restrictions

Authentication using the SSPFS will only occur when the user is accessing the CICM-EM via the web interface. This feature will not change the method used for authenticating users who are logging in using a Telnet session.

178.7 Logs (LG)

This feature interacts with A00003718 “CICM Osmine readiness – Faults, alarms and performance monitoring”, to log the following events on the IEMS:

- User successfully authenticated through PAM.
- User authentication through PAM failed.
- Request Timeout on PAM proxy.

The CICM-EM will also raise an alarm on the IEMS when a request to the PAM proxy times out. This alarm is cleared the next time an authentication request is successfully processed through the PAM server.

178.8 Glossary

Term	Description
CICM	Centrex IP Client Manager
CICM-EM	CICM Element Manager
HTTP(S)	Hypertext Transfer Protocol (Secure)
IP	Internet Protocol
PAM	Pluggable Authentication Module
SSPFS	Succession Server Platform Foundation Software
TDM	Time Division Multiplexed
VLAN	Virtual Local Area Network

178.9 References

- A00005985 “CICM Security”
- A00001912 “Centralised Security Administration”
- A00003718 “CICM Osmine readiness – Faults, alarms and performance monitoring”

179: Functional Description (FN): A00006032

179.1 Feature name

Loop Reversal On Answer (LROA), Loop Reversal on Seizure (LRS) and Insert Tone on Coin Phone Termination (NOCOLL) SN07 Support for Cable & Wireless Caribbean

179.2 Description

This feature will allow the use of the following features in ISN07 (International Call Server) with a North American Toneset on the Passport Packet Voice Gateway (PVG) and on the MG9K:

- Loop Reversal On Answer (LROA)
- Loop Reversal on Seizure (LRS)
- Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with trunks on a PVG

179.2.1 Loop Reversal On Answer (LROA)

Loop Reversal On Answer as detailed in AR0502 “Line option for Line Reversal On Answer” will be supported on IBN line types on the MG9K 32 port Global Line Card (GLC-32).

179.2.2 Loop Reversal on Seizure (LRS)

Loop Reversal on Seizure as detailed in A59008303 “Line option for Line Reversal on Seizure” will be supported on IBN line types on the MG9K GLC-32.

179.2.3 Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with PVG trunks

NOCOLL functionality as detailed in A59008313 “Insert Tone on Coin Telephone Termination” will be supported on interworkings with the following PVG trunks types:

- ETSI ISUP
- ANSI ISUP

The pay phone recognition tone will be played on the trunk when terminating to a IBN line with the NOCOLL option. The characteristics of the tone such as frequency, cadence, level, and repetition are defined by the toneset of the PVG.

179.3 Hardware Requirements or Dependencies

179.3.1 Loop Reversal On Answer (LROA)

The MG9K 32 port Global Line Card is required.

179.3.2 Loop Reversal on Seizure (LRS)

The MG9K 32 port Global Line Card is required.

179.3.3 Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with PVG trunks

A VSP3 or VSP3-o card is required on the PVG.

179.4 Software Requirements or Dependencies

None.

179.5 Limitations and restrictions

All limitations and restrictions for the original LROA, LRS, and NOCOLL are still applicable with the exception of the supported hardware configurations as stated in this FN.

LRS and LROA are only supported on the MG9K GLC-32 card for IBN line types.

Playback of the pay phone recognition tone is only supported on the PVG for ANSI ISUP and ETSI ISUP trunk types. Originations from other trunk types on a PVG terminating to IBN lines with the NOCOLL option will not result in the playback of the pay phone recognition tone.

A VSP3 or VSP3-o card is required on the PVG in order for speech to be heard during the playback of the pay phone recognition tone. The use of VSP2 or older card will cause the calling party to only hear the tone playback for the first 13 seconds of the call. During this time, voice from the called party will not be transmitted.

The use of features such as call waiting, call hold, conference calling are not supported on lines with the LROA option. The use of these features may result in the normalization of the polarity reversal.

LRS and LROA are not supported on lines with the CEPT option.

179.6 Interactions

A line with a service which uses flash can also have the NOCOLL option provisioned. If the line flashes while the tone is being applied, the playback of the tone will be halted.

179.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

179.8 Glossary

Term	Description
ANSI	American National Standards Institute
ETSI	European Telecommunications Standards Institute
IBN	Integrated Business Network
ISUP	ISDN User Part
LROA	Loop Reversal On Answer
LRS	Loop Reversal on Seizure
NOCOLL	NO COLLect - a servord option associated with the Insert Tone on Coin Phone Termination feature
PVG	Passport Packet Voice Gateway
VSP	Voice Services Processor

180: Functional Description (FN): A00006483

180.1 Feature name

Audio Server Node Announcement Capacity Increase to 1280

180.2 Description

This activity provides the capability to increase the number of simultaneous announcement calls which can be supported in the CS2K for an Audio Server Node from 300 to 1280.

180.3 Hardware Requirements or Dependencies

The audio server gateways subtending the Gateway Controller (GWC) that is datafilled as an Audio Server node must have the apppropriate configuration to support 1280 ports.

180.4 Software Requirements or Dependencies

This functionality requires both the Core and GWC to be at the SN07 releases or later.

180.5 Limitations and restrictions

With the ANNC option set to 1280, this reduces the number of conference resources available on for the Audio Server node. Please refer to A89009843 "UAS Announcement Traffic Distribution" for how to calculate conference and announcement availabilty.

Prior to SN06, the ANNC option did not exist. When the Core is upgraded to SN06, the reformat procedure for table SERVSINV assigns by default the ANNC option. The default value specified for the ANNTERMS field is 300 if no other options (i.e. 3PORT or 6PORT) are datafilled. The default value will not change in SN07. If 3PORT or 6PORT is datafilled, the ANNC ANNTERMS value is adjusted accordingly against the value in NUMTERMS. For upgrades from SN06 to SN07, the ANNC option ANNTERMS value is simply transferred.

180.6 Interactions

Not applicable.

180.7 Applicable customer facing sections

Fault Management

Logs _____N/A

Alarms	_____N/A
Configuration	
Data Schema	_____X
User Interface	_____N/A
Element Management	_____N/A
Security	_____N/A
Service Order	_____N/A
Office Parameters	_____N/A
Accounting (includes AMA billing)	_____N/A
Performance (includes operational measurements)	_____N/A

180.8 Glossary

Term	Description
GWC	Gateway Controller

181: Design Description excerpts: A00006495

181.1 Feature name

H.323 Flexible Carriers

181.2 Purpose

This SN07 activity enables the addition of H.323 virtual carriers with a size within the range of 4 to 672. The current implementation allocates H.323 virtual carriers in blocks of 24 or 32, based on the market. The new capability will only affect carriers that are defined as the type H.323.

The H.323 Flexible Carrier feature enables customers to allocate small and large groups of endpoints for H.323 gateways. By allowing variable size blocks of endpoints/TIDs (Terminal Identifiers), customers can manage the TID range of a H.323 GWC (Gateway Controller) more efficiently.

The new capability is targeted to customers who don't have OSS (Operations Support System) requirements to provision blocks of endpoints in (24 or 32) increments and support small H.323 systems.

> ***Note:*** If a craftperson adds a H.323 virtual carrier and does not specify a size, the default number of endpoints/TIDs will be allocated (24 North American/32 International).

181.3 H.323 Capacities

The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. The PRI data structures on the GWC currently support 168 D channels. Thus, the current maximum number of H.323 gateways is 168. This feature changes the PRI data structures on the GWC to support 254 D channels.

A craftperson can allocate (provision via SESM) 258 H.323 gateways (in the North American market) and virtual carriers with a minimum size of 4. A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs. Regardless of the number of gateways provisioned on a GWC, only 254 D channels can be defined on a H.323 GWC after this feature is delivered. D channel provisioning is executed on the core. If an attempt is made to provision a 255th D channel on a H.323 GWC, an error is generated stating that the maximum number of D channels has been exceeded.

The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs. The maximum size of a H.323 virtual carrier was based on the number of B channels that can be mapped to a PRI trunk group on the core in table TRKMEM (671 B channels maximum for a PRI trunk group). A H.323 virtual carrier can be any size within the range of 4 - 672.

H.323 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of endpoints/TIDs per GWC)	Gateway Capacity (maximum number of gateways per GWC)
H.323_INTL	1024	1024/4 = 256
H.323_NA	1032	1032/4 = 258

181.4 H.323 Gateway Profile Changes

This feature delivers changes to the H.323 gateway profiles:

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	consult the vendor documentation
SUCCESSION_1000	480	consult the vendor documentation
CISCO_2600	96	consult the vendor documentation
CISCO_3600	384	consult the vendor documentation
CISCO_AS5300	384	consult the vendor documentation
WESTELL	64	consult the vendor documentation
CISCO_H323_IOS	N/A	consult the vendor documentation
H323_PROXY	N/A	consult the vendor documentation

181.5 Limitations and restrictions

The limitations of this activity include the following:

- The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. A craftperson can allocate 258 H.323 gateways and virtual carriers with a minimum size of 4 but only 254 D channels can be defined on a H.323 GWC after this feature is delivered.
- The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs.
- If H.323 virtual carriers are attempted to be provisioned on a pre-SN07 GWC load, an error is generated detailing that this functionality is not supported in previous releases.

182: Functional Description (FN): A00006496

182.1 Feature name

H.323 Multiple D Channels

182.2 Purpose

This SN07 activity will enable the support of mapping multiple D channels to a single H.323 gateway. The current H.323 implementation on the GWC makes the assumption that there is only ***one*** D channel mapped to a single H.323 gateway. The new capability will only affect H.323 gateways.

The multiple D channel feature provides the support to map more than one trunk group on the core to the allocated TIDs on the GWC. The current maximum number of endpoints supported on a single H.323 gateway by the CS2K is 672.

The new capability enables support of large H.323 systems such as the Succession 1000 H.323 gateway. Once this feature is delivered, a single H.323 gateway can be mapped to the full capacity of a SN07 H.323 GWC (1024 for International/1032 for North American).

182.3 H.323 Capacities

The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. The PRI data structures on the GWC currently support 168 D channels. Thus, the current maximum number of H.323 gateways is 168. This feature changes the PRI data structures on the GWC to support 254 D channels.

A craftperson can allocate (provision via SESM) 258 H.323 gateways (in the North American market) and virtual carriers with a minimum size of 4. A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs. Regardless of the number of gateways provisioned on a GWC, only 254 D channels can be defined on a H.323 GWC after this feature is delivered. Thus the maximum number of H.323 gateways that can provide call processing is 254**.** D channel provisioning is executed on the core. If an attempt is made to provision a 255th D channel on a H.323 GWC, an error is generated stating that the maximum number of D channels has been exceeded.

The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs. The maximum size of a H.323 virtual carrier was based on the number of B

channels that can be mapped to a PRI trunk group on the core in table TRKMEM (671 B channels maximum for a PRI trunk group). A H.323 virtual carrier can be any size within the range of 4 - 672.

H.323 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of endpoints/TIDs per GWC)	Gateway Capacity (maximum number of gateways per GWC)
H.323_INTL	1024	1024/4 = 256
H.323_NA	1032	1032/4 = 258

182.4 H.323 Gateway Profiles

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	consult the vendor documentation
SUCCESSION_1000	480	consult the vendor documentation
CISCO_2600	96	consult the vendor documentation
CISCO_3600	384	consult the vendor documentation
CISCO_AS5300	384	consult the vendor documentation
WESTELL	64	consult the vendor documentation
CISCO_H323_IOS	N/A	consult the vendor documentation
H323_PROXY	N/A	consult the vendor documentation

182.4.1 H.323. Maintenance Model

The H.323 maintenance model will be changed by this feature. A H.323 D channel will come into service once a H.323 gateway successfully registers

with a H.323 GWC. If a H.323 gateway has multiple D channels, all the D channels will be brought into service once a H.323 gateway successfully registers. If at least one D channel comes into service the registration process will be successful.

A craftperson must take all the D channels out of service to successfully "de-register" the H.323 gateway. If at least one D channel remains in service the gateway will not be "de-registered".

182.5 Trunk Group Configuration

To support the mapping of multiple D channels or trunk groups to a single H.323 the configuration of the trunk groups must be identical. The translations, customer group, services, etc. must be provisioned on the core to be the same so there isn't any difference in services or terminations. Services and call routing via one trunk group or a different one mapped to the same H.323 gateway must be transparent to a user.

A H.323 gateway and the associated trunk group(s) must be mapped to only one GWC. A H.323 gateway can't be associated with two GWCs.

182.6 GWC Changes

The GWC software must be updated to support the Multiple D Channel feature. The changes focus on changing the D channel TID selection algorithm within the H.323 GWC application and the H.323 maintenance code on the GWC.

- Update the H.323 GWC maintenance application. The current H.323 GWC maintenance implementation assumes that there is only ***one*** D channel per H.323 gateway. The assigned TID range of the H.323 gateway must be traversed to capture all the mapped D channels.

The support of mapping multiple D channels to a single H.323 gateway changes the maintenance model. The changes include:

- Only ***one*** D channel is required to come into service for a H.323 gateway to successfully register.
- A H.323 gateway will be "unregistered" if ***all*** D channels are manually taken out of service. If a craftperson successfully executes the maintenance commands "BSY; BSY INB;" for all of the mapped D channels, the gateway will be unregistered. If any of mapped D channels do not reach an "INB" state, the gateway will not be unregistered.

182.7 Limitations and restrictions

The limitations of this activity include the following:

- The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. A craftperson can allocate 258 H.323 gateways and virtual carriers with a minimum size of 4 but only 254 D channels can be defined on a H.323 GWC after this feature is delivered.
- A craftperson must post **all** the D channels when manually “unregistering” H.323 gateways with multiple D channels.
- Multiple commands must be executed to manually “unregister” a H.323 gateway with multiple D channels. A utility does not exist to BSY INB all D channels mapped to a single H.323 gateway.
- A craftperson must “keep track” or capture all the mapped D channels of a H.323 gateway to manually “unregister” the respective gateway. A craftperson can capture the D channel mappings by traversing table TRKSGRP on the core to determine the D channel(s) of a H.323 gateway. The TMM (Trunk Maintenance Manager) application can be used to provide the D channel mappings of a H.323 gateway and to “unregister” the gateway by executing the proper maintenance commands. The D channels are not explicitly listed when querying the endpoint data via TMM but the information is listed.

183: Functional Description (FN): A00006639

183.1 Feature name

MG9K Overload OM pegs

183.2 Description

When a Media Gateway 9000 (MG9K) begins to reach an overload threshold call connections request are denied. This condition can occur on an ITP, ABI or at the nodal level (DCC). A llog is currently generated corresponding to the line or trunk which requested the connection.

Overload condition occurs when the MG9K has reached a threshold where subsequent calls with the exception of calls marked ‘essential or emergency’ must be denied to prevent further catastrophic degration of the MG9K node.

In SN07 an Operational Measurement (OM) register will be incremented for every connection which is denied. A new OM group GWOVLOM will be defined and the register OVERLOAD will be incremented upon connection denial.

In SN07 feature ‘A00004430 - SVC Failure OMs’ introduced the ability to peg OMs for ATM switched virtual circuits call failures. It pegs the logical group of the MG9K for calls which involve lines hosted off the ITP boards and it pegs the hosting legacy XPM peripherals directly connected to the ABI DS512 pack for calls involving lines subtending the ABI board.

To be consistent in pegging OMs this feature will follow the same model.

When a connection is denied for a call originated or terminated on an ITP board, i.e. a native MG9K call, the register associated with the logical group will be pegged. MG9Ks are indentified as ‘logical groups’ because the CS2K is not aware on the MG9Ks on a nodal basis. In SN06.2 the feature ‘A00002607 ABI XPMSITE and MG9K Location support on the Core’ provided the first step towards recognizing ABI XPM and MG9K on a nodal basis. However currently only ABI ‘nodes’ are recognized in the CS2K.

If the connection is denied for a call which originates or terminates on an agent which is subtending an ABI board, the OM peg will occurr on the hosting XPM which is directly connected to the DS512 pack on the ABI board. Currently the hosting XPMs which can be pegged are LTCs, SMA2s, LGCs.

For ABI connection failures line or RCC trunk could be rejected and pegging will be done for either one on the hosting XPM node.

Figure-1 shows how the level where the OM register will be pegged.

Figure 1 CS2K Identification of MG9k and ABI lines Pegs

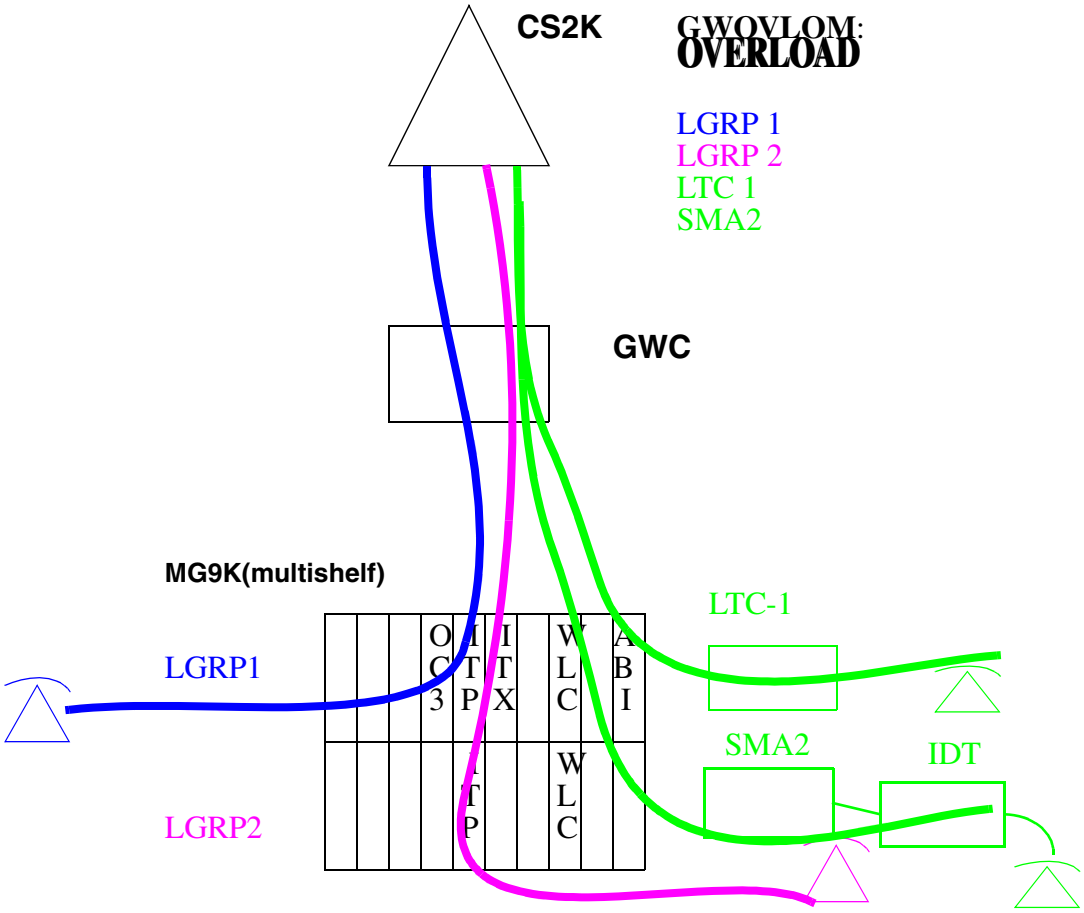


Figure 1 OM group GWOVLOM with OVERLOAD register

```
omshow gwovlom active
GWOVLOM

CLASS: ACTIVE
START:2004/03/05 13:30:00 FRI; STOP: 2004/03/05 13:56:48 FRI;
SLOWSAMPLES:        17 ; FASTSAMPLES:        161 ;

      KEY (GWOVL_OM_PM_INFO1)
      INFO (GWOVL_OM_TUPLE_DATA1)
        OVERLOAD


   68
   MG9K ABI SMA2   1
            0
   73
   MG9K ABI SMA2   0
            0
   87
   MG9K ABI SMA2   2
            0
   89
   MG9K ABI LTC 2
            0
114
      MG9K HOST 04 0
            0
   116
      MG9K HOST 01 2
            0
   117
      MG9K SLOA 31 3
              0
```

183.3 Hardware Requirements or Dependencies

This feature has no hardware requirements or dependencies.

183.4 Software Requirements or Dependencies

This feature is no additional software dependencies.

183.5 Limitations and restrictions

There are no new limitations or restrictions introduced by this feature.

183.6 Interactions

No new interactions are introduced by this feature.

183.7 Applicable customer facing sections

Fault Management

Logs	_N/A_
Alarms	_N/A_

Configuration

Data Schema	_N/A_
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_

Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	__X__

183.8 Glossary

Term	Description
MG9K	Media Gateway 9000
ITP	Integrated Telephony Processor
DCC	Data Communication Card
OM	Operational Measurement
ATM	Asynchronous Transfer Mode

184: Functional Description (FN): A00006693

184.1 Feature name

XA-Core IO Capacity Monitoring Toolset

184.2 Description

The IO Capacity monitoring toolset (IOCAP) provide the customer telemetry for messaging over HIOP and HCMIC.

XA-Core counts messages and bytes for each service. Software on the XA-Core accesses the measurements, calculates the messaging occupancy level, and displays the results on the IOCAP MAPCI level and the IOCAP OM group.

This feature will cause no more than 3% capacity degradation to IO capacity.

184.2.1 IOCAP MAPCI display

Following is a prototype of the IOCAP MAPCI display, which will subtend from the CAPACITY level. The display will be updated once per minute.

```
CATMP/HR   SMS/HR VLR_UPD/HR  CAP ENGBHCA CCOVRLD CMICOVRLD PESC
  303001      180     398700  128  233643    OFF       OFF    NO


Service IOUTIL%  TxMsg/s  TxSize RxMsg/s  RxSize
   ETHR      64    15324     107   13234      91
   CMIC      17     4102     202    1254     102
   AMDI       0        0       0       0       0
```

The Service column identifies the type of IO service (Ethernet, CMIC, or AMDI). IOUTIL is the calculated percentage utilization of the available system messaging capacity, based on the known IO system capacity, the average rate through other services on the same card, and the throughput on other cards. TxMsg/s, TxSize, RxMsg/s and RxSize report average transmit and receive message rates and sizes through that service. Because the MAPCI display is updated once per minute, high water mark information will not be displayed.

184.2.2 IOCAPCI tool

The information in the MAP display is also available through the IOCAPCI tool, in addition to the following tools:

- one month's history of hourly high water mark percent utilization for each service (Ethernet, CMIC, and AMDI), similar to DMSMON HIGHCAP.
- one month's history of hourly average percent utilization for each service.
- current hour and last hour utilization and throughput for each service

An example of the CMIC high water mark data follows. A similar output will be available for each service.

```
> iomax cmic
Maximum CMIC Utilization
                                                    Hour
Date    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  21  22  23
-------------------------------------------------------------------------------------------------------
-------
2/1     9   7   8   6   5   7   8  11  17  22  28  30  40  55  50  47  61  57  59  62  59  39  31  21
2/2     8   7   9  10   4   5   9  12  16  21  27  29  39  49  53  43  51  56  57  61  57  41  29  18
2/3     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/4     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/5     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/6     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/7     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/8     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/9     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/10    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/11    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
```

1970

2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

184.2.3 IO capacity OM

The information displayed in the IOCAP MAP command is also recorded in the IOCAP operational measurement, as shown below.

```
IOCAP

CLASS:  HOLDING
START:2003/12/03 09:30:00 WED; STOP: 2003/12/03 09:45:00 WED;
SLOWSAMPLES:         9 ; FASTSAMPLES:         90 ;

INFO (IO_SERVICE_TYPE)
           IOUTIL      IOHWM    TXMSG/S  TXSIZE
          RXMSG/S     RXSIZE   IOTHRESH
    1 ETHR
              64         72       15204     105
           13234         84           0
    2 CMIC
              17         18        1254     102
            1254         63           0
    3 AMDI
               0          0           0       0
               0          0           0
```

The IOCAP OM provides measurements of messaging rates and sizes for each service. The IO_SERVICE_TYPE indicates the service provided. IOUTIL refers to percentage utilization of the services on the switch. IOHWM refers to the highest level that the corresponding utilization has reached in the sample period. TxMSG/S, TxSIZE, RxMSG/S and RxSIZE report the average transmit and receive message rates and sizes through the service. The IOTHRESH register is pegged every time the service average utilization for one minute exceeds the value of new OFCENG office parameter IO_WARNING_THRESHOLD. This register is intended to give the customer a flexible warning that they are approaching the need to upgrade their IO system.

184.2.4 Office parameter

A new office parameter in table OFCENG, IO_WARNING_THRESHOLD, indicates the minimum IO service utilization at which the IOTHRESH register in the IOCAP OM will be pegged.

184.3 Hardware Requirements or Dependencies

This feature is unavailable for CMIC, Ethernet and AMDI packlets (NTLX05AB, NTLX09AA, NTLX05BA respectively).

This feature is supported on all versions of NTLX04 HIOP cards and NTLX17 HCMIC cards.

184.4 Software Requirements or Dependencies

None.

184.5 Limitations and restrictions

This feature will be submitted into CSP21 and patched back to CSP20.

When the system is in transition from IOP to HIOP, the utilization of all IO services are not be available.

184.6 Interactions

The MAPCI level display will subtend from the CAPACITY MAP level. It will be shown as an option from that level.

184.7 Applicable customer facing sections

Fault Management

Logs	__NA__
Alarms	__NA__

Configuration

Data Schema	__NA__
User Interface	__X___
Element Management	__NA__
Security	__NA__
Service Order	__NA__
Office Parameters	__X___

Accounting (includes AMA billing)	__NA__
Performance (includes operational measurements)	__X___

184.8 Glossary

Term	Description
New term	Definition

185: Functional Description (FN): A00006741

185.1 Feature name and Feature ID

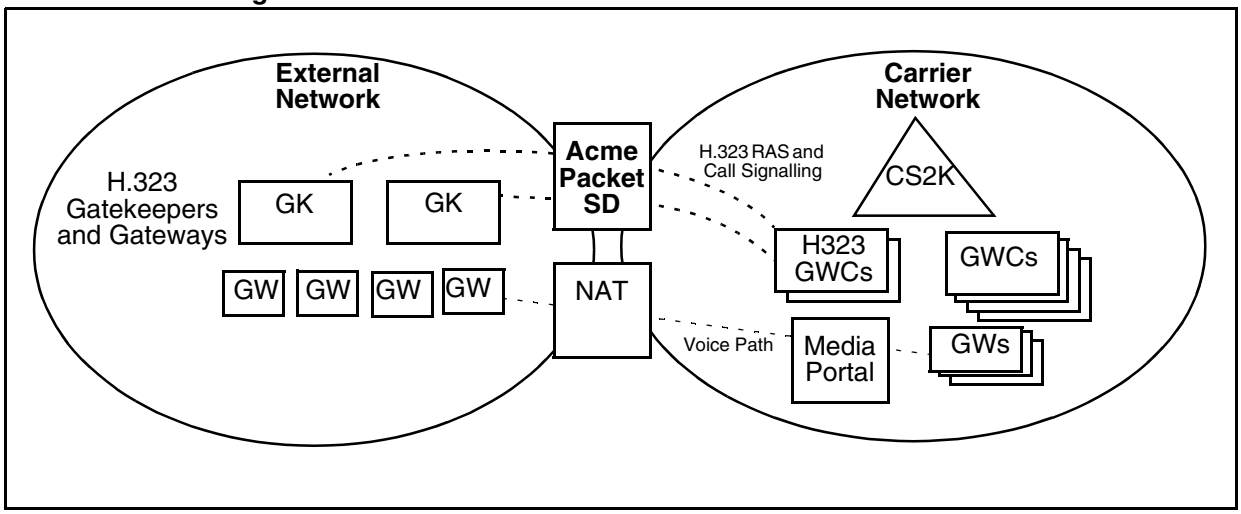
A00006741: H.323 Gatekeeper to CS2K Gatekeeper Interworking

185.2 Description

This feature supports interworking (call routing) between H.323 Gatekeepers in an external network and a CS2K H.323 Gatekeeper (GWC) on a carrier network. The external network could be an enterprise network, another carrier's network, or any other private or public network.

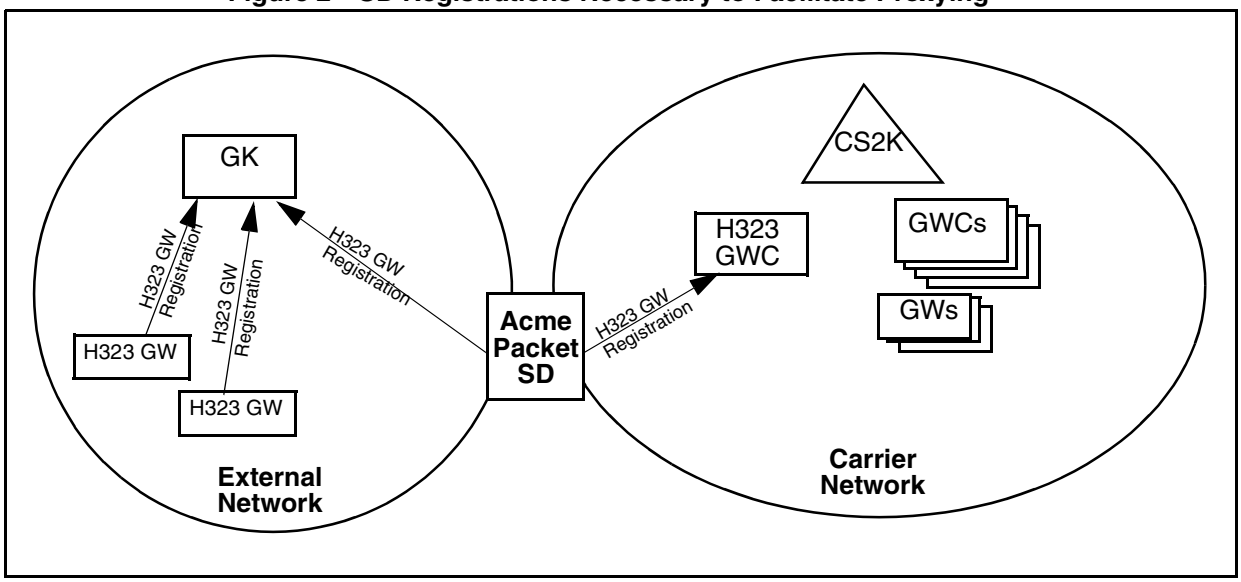
The solution uses an Acme Packet Session Director (**SD**) to proxy H.323 messaging between Gatekeepers in an external network and an H.323 GWC on the Carrier network. Voice is not routed through the SD as part of this solution, therefore, a NAT (middlebox) is required to route voice between the two networks. Figure 1 shows a very high level overview what is supported.

Figure 1 Feature Overview



As shown in Figure 1, this activity allows calls from Gateways (GWs) that are registered with External Gatekeepers (GKs) to route calls via the Gatekeeper and Acme Packet SD to the CS2K using H.323. To facilitate this, the Acme SD registers as an H.323 Gateway with both an external Gatekeeper and with the CS2K H.323 GWC as shown in Figure 2. In this way, the SD acts as a back-to-back H.323 gateway, routing calls from one gatekeeper to the other. Both gatekeepers (external and H.323 GWC) view the SD as a registered H.323 gateway that can originate and terminate calls.

Figure 2 SD Registrations Necessary to Facilitate Proxying



185.2.1 Example Call Flows

With the SD registered as an H.323 Gateway with both gatekeepers, a call would be routed from an external gateway to the CS2K as follows:

- An external H.323 gateway (H323 GW) originates a call, sends H.323 signalling to the external Gatekeeper (GK).
- The GK routes the call to the SD, basically treating the SD as a terminating H.323 gateway. Neither the GK, nor the originating H323 GW, is aware that the SD actually proxies the call to a CS2K on the carrier network.
- When the SD receives the incoming H.323 call from the originating H323 GW (or GK), it immediately originates a call on the carrier network by sending H.323 signalling to the H.323 GWC. From the H.323 GWC's perspective, this appears as a new call originating from an H.323 gateway (the SD). The fact that the call actually originated on the external network from another H.323 gateway, via an external GK, is transparent to the CS2K.
- The call is translated through the CS2K to a terminating GWC/GW and the call is set up end to end from the external H.323 GW (originator) to the terminating agent on the CS2K (with voice routing through a NAT and media portal, not the SD). A list of supported terminating agents (gateways) off the CS2K is in Section 2.6.3.

A call from the CS2K to an external H.323 gateway registered with an external gatekeeper would be the opposite:

- A CS2K-hosted gateway makes a call and CS2K routes the call to the SD H.323 PRI trunk via call translations which results in H.323

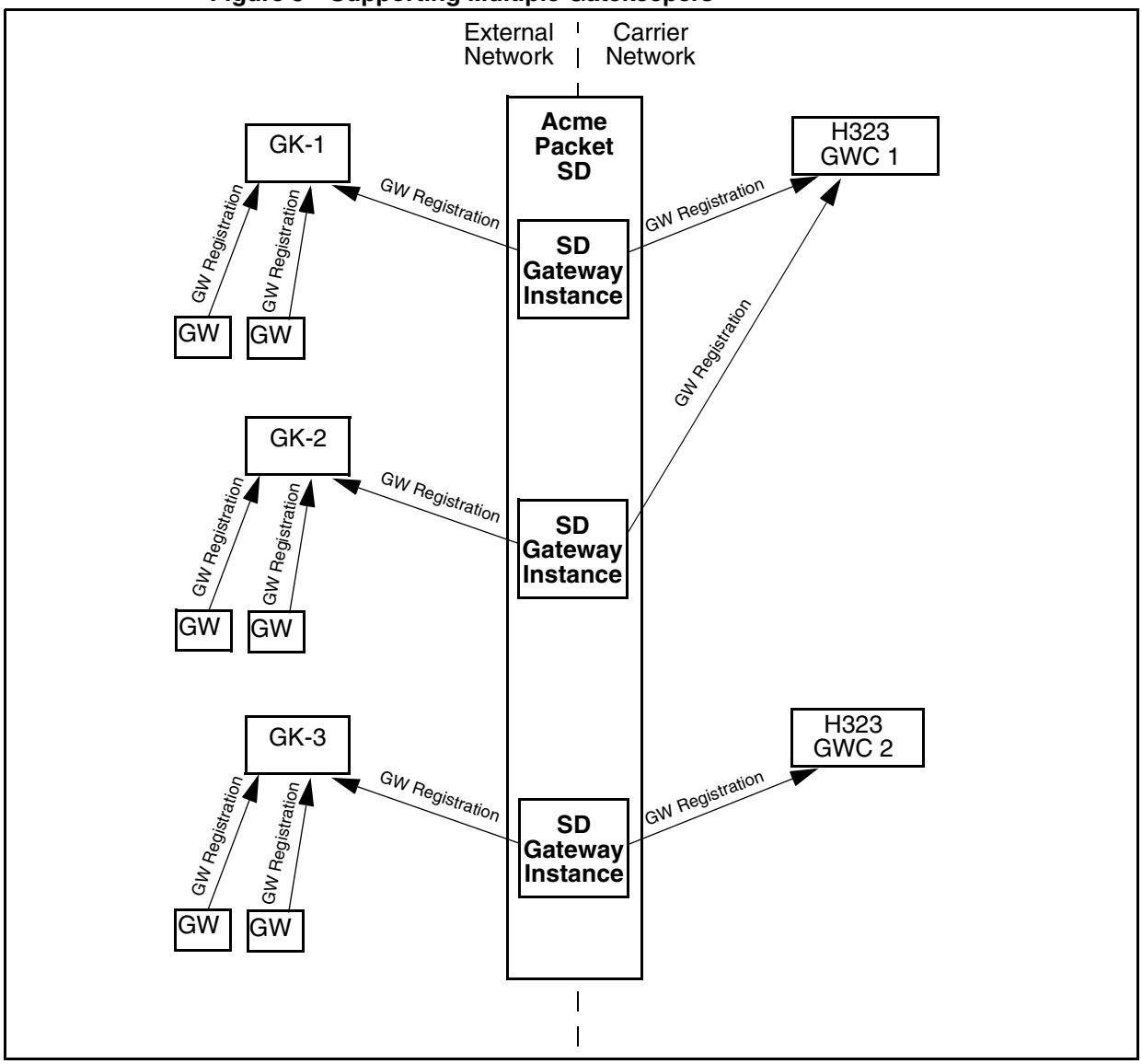
messaging sent to the SD. Again, the CS2K views the SD as a terminating H.323 gateway.

- The SD initiates a call on the external network by sending H.323 signalling to the external gatekeeper (GK). From the GK's perspective, this is a new call originating from an H.323 gateway (the SD).
- The GK routes the call to the appropriate registered H323 GW and the call is set up end to end from the CS2K originating gateway to the external H.323 gateway.

185.2.2 Interworking with Multiple External Gatekeepers

The SD supports interworking between multiple external gatekeepers and GWCs. This is done by configuring multiple back-to-back gateway instances in the SD as shown in Figure 3.

Figure 3 Supporting Multiple Gatekeepers



This is a logical view only, intended to show how the SD can support multiple gatekeepers - it does not show all the nodes that must be provisioned in the SD in order to support this (provisioning is discussed in Section 2.5).

Each external gatekeeper (GK-1, GK-2, and GK-3) is represented to the CS2K by a unique SD Gateway Instance. Each of these will register with one external gatekeeper, and one GWC. Multiple SD Gateway instances can register with a single GWC, as indicated in the figure - two are registered with GWC 1.

The key concept here is that each SD Gateway Instance that registers with an H.323 GWC is basically a gateway that represents an external gatekeeper and

all gateways that are registered with that external gatekeeper. The GWC has no direct knowledge of the external gatekeeper or any of its subtending gateways. Instead it views each SD Gateway Instance simply as an H.323 Gateway that can originate and terminate calls. Also of importance is that multiple SD gateway instances can be registered with a single GWC.

185.3 Hardware Requirements or Dependencies

- Acme Packet Session Director (SD)
- NAT Router (for media between external network and Carrier Network or DMZ)
- Media Portal
- Succession Call Server

185.4 Summary of Customer Impacting Changes

185.4.1 CS2K Provisioning Changes

The CS2K has no knowledge of the gatekeepers or gateways on the external networks. Therefore, provisioning on the CS2K is limited to simply provisioning the Acme Packet SD Gateway Instances as H.323 gateways, both in SESM and core trunk datafill. Because of specific behaviors of the SD, there are two customer facing changes when provisioning a SD in SESM:

1. A new gateway profile has been added
2. Multiple gateways can be provisioned, all sharing a single IP address

185.4.1.1 New Gateway Profile: H323_PROXY

All SD gateway instances are provisioned in SESM with the new profile `H323_PROXY`.

185.4.1.2 Multiple Gateways with Single IP Address

The SD can register multiple gateway instances with one GWC, all using a single IP address. This requires new functionality in SESM, although from a customer perspective, it is functionality provided by removing some existing error checking. Specifically, prior to SN07, a gateway could not be associated in SESM if its IP address was already in use by another provisioned gateway. This restriction is removed in SN07 to support GK-GK Interworking. Two conditions must be met, however, in order to add multiple gateways with a single IP address:

- Each gateway must be provisioned with **Protocol type** H.323 (6)
- Each gateway must be provisioned with **Protocol port** 0.

There are some configuration related considerations for various fields when adding SD gateway instances in SESM (detailed discussed in Section “185.5 Configuration and Provisioning” on page 1979), but the new profile and ability

to provision multiple gateways with a single address are the only actual SESM changes in terms of customer visibility.

185.4.1.3 Implications of Provisioning an H.323 Gateway with Port 0

Provisioning a gateway with **Protocol port** 0 in SESM has three effects:

1. It indicates that the gateway requires **automatic port discovery**. This means the gateway's protocol port is not known at provisioning time, so the port must be discovered (by the GWC) when the gateway registers (the initial registration message from the gateway to the GWC contains the port). All Acme SD and Cisco IOS gateways require auto port discovery. Other gateways can be provisioned as auto port discovery as well.

   Prior to SN07, we only supported Cisco gateways as auto port discovery gateways, and this was done based on the gateway profile name. Although port 1719 was the supported (and default) port to use when provisioning Cisco gateways, in reality it didn't matter what port was provisioned since Cisco gateways were always treated as auto port discovery gateways. No other gateway types could be provisioned as auto port discovery.

   Beginning in SN07, any gateway, regardless of its profile, can be treated as auto port discovery by setting the Protocol port as 0. This means that all Cisco and Acme SD gateways must be provisioned with port 0, since they are all auto port discovery gateways.

2. For gateways behind a NAT, it indicates that the gateway has a 1:1 NAT mapping, as opposed to N:1 NAT mapping. The GWC assigns the gateway's H.323 signalling port based on whether the gateway is mapped 1:1 or N:1 by the NAT. Gateways provisioned as 1:1 (port = 0) will be assigned call signalling port of 1720. Gateways provisioned as N:1 (port = anything other than 0) will be assigned a call signalling port of provisioned port + 1.

3. It is a necessary condition in order to add a gateway with the same IP address as another provisioned gateway.

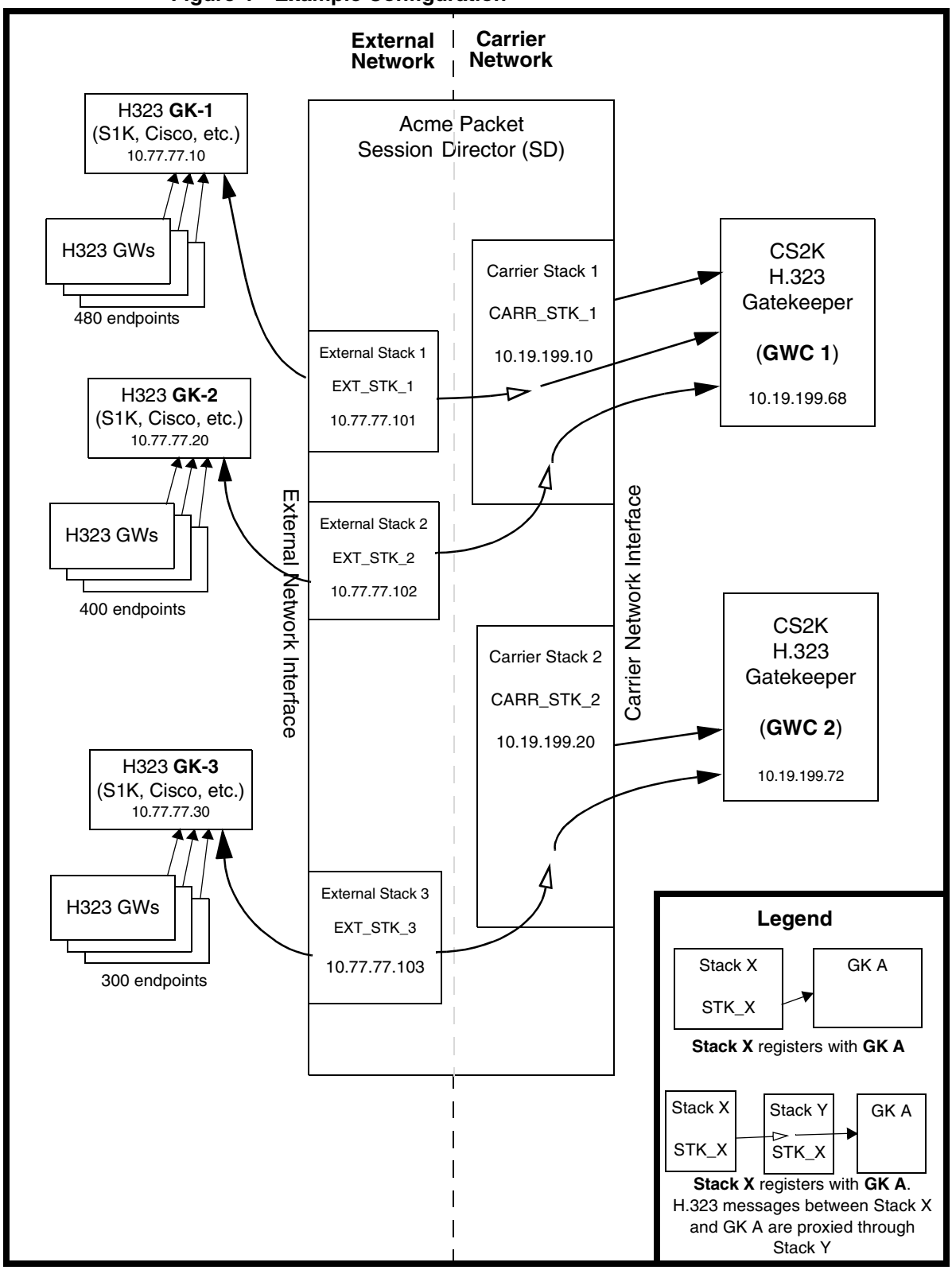
185.4.2 Acme Packet Session Director (SD) Configuration and Provisioning

The Acme SD is a required node in this solution. As such, it requires installation and "ground-up" provisioning which will likely be new to the customer. This document provides detailed SD configuration and provisioning requirements that are pertinent to supporting Gatekeeper to Gatekeeper Interworking. It does not, however, cover basic SD provisioning and configuration. It is expected that the customer will have access to documentation and/or other product support mechanisms provided by Acme Packet.

185.5 Configuration and Provisioning

This section discusses GK-GK Interworking configuration and provisioning, referring to the example configuration shown in Figure 4.

Figure 4 Example Configuration



185.5.1 Configuration Overview

The example in Figure 4 shows how one might configure interworking between three Gatekeepers (GK-1, GK-2, and GK-3) on an *external network* (or networks) and two GWCs subtended off a CS2K on the *carrier network*. The external gatekeepers may be on the same external network, or on different external networks.

185.5.1.1 Session Director Properties

To configure an SD to support Gatekeeper to Gatekeeper Interworking, there are some important SD characteristics to understand:

1. **The SD has two physical network interfaces that route all media including H.323 messaging.** These can be ethernet or optical ports depending on the hardware. The SD is capable of routing voice and other real-time media on these two physical interfaces; but in this solution, voice will not be routed through the SD (it will route through a NAT and media portal). So in general, these two physical interfaces will handle all H.323 signalling into and out of the SD.

   - One of these two physical interfaces should be connected to the Carrier Network.
   - The other should be connected to one or more External Networks. Connecting a SD physical interface to multiple External Networks is done through advanced IP network configuration and is beyond the scope of this FN, but it is supported by the SD.

   In Figure 4, the carrier network interface is logically shown as the right edge of the SD. The external network interface is logically shown as the left edge of the SD.

   The SD has additional physical interfaces including a serial console port, and three ethernet (wancom) ports that can be configured for maintenance access, including telnet and ftp, or as direct links to a redundant SD to support data sync. These are not shown in the example and provisioning these is beyond the scope of this FN - refer to Acme Packet documentation and/or product support.

2. **Multiple H.323 *Gateway instances* (stacks) can be configured on a single SD device.** The objects we have been referring to as “gateway instances” or “back-to-back gateway instances” up until now are provisioned as **stacks** in the Acme SD. In Figure 3, we have five stacks configured - each basically has properties of a unique H.323 gateway.

3. **Each SD stack can be associated to one, and only one, network interface.** When a stack is configured on the SD, it can be mapped to use either one of the two physical interfaces described in (1) above, but not both. For example, in Figure 3, *External Stack 1* is associated with the external network interface, and the IP address assigned to it must be an external network address. As such, it will be unable to directly send messages out to, or receive messages from, the carrier network.
4. **Each SD stack must have one unique IP address.** This is a requirement on the SD and ports are not considered part of the IP address for this rule - when provisioning the SD, each stack must be assigned a unique IP address. Again, this must be a reachable address on the network this stack is associated with.

185.5.1.2 SD Stack Proxying

The last two characteristics above (3 and 4) present obstacles when configuring the SD to register a stack with GKs on both networks. Specifically, we cannot simply provision a single stack to register directly with both an external gatekeeper and a GWC because each stack can have only one IP address, and can be mapped to only one physical network interface.

To get around this, the SD allows a stack to access a physical network, other than the one it is directly associated with, by proxying messages through another stack. For example: External Stack 1, being associated with the external network interface, is unable to send/receive messages on the physical interface. So we will provision Carrier Stack 1 as an associated stack (**assoc-stack**) against External Stack 1. When External Stack 1 needs to send a message to the carrier network, for example a registration request to the GWC, it will send the message to Carrier Stack 1. Carrier Stack 1 will proxy the message to the GWC on the carrier network.

One side effect of this proxying is that the IP address in messages being proxied through the carrier stack will be changed from External Gateway 1's address (10.77.77.101) to Carrier Stack 1's address (10.19.199.10). This is important because it means that when provisioning External Stack 1 in SESM, we will assign it Carrier Stack 1's IP address. In fact, all of the external stacks registering with a GWC via a carrier stack will be provisioned in SESM with the carrier stack's address. When they register with the GWC, they will each have a unique RAS port, and they have unique H323_IDs. Since we won't know at provisioning time what RAS port each stack will have, the port should be provisioned as 0. Provisioning an H.323 gateway in SESM with port 0 can be considered a flag that indicates that the port will be auto-discovered at registration time (see xxx).

When the GWC sends messages to External Stack 1, for example, it sends them to Carrier Stack 1's IP address. Carrier Stack 1 will proxy the message to the appropriate external stack based on the RAS port, H323_ID, or both.

185.5.1.3 Determining the number of stacks provisioned against a GWC

To support the proxying described in the previous section, it is clear that exactly one *carrier stack* must be provisioned against, and registered with, each H.323 GWC.

The number of *external stacks* provisioned against a GWC will be determined based on the number of endpoints required by each external GK.

So, the total number of provisioned stacks on each GWC will be:

Number of external stacks + 1 carrier stack

Again, all of the stacks provisioned in SESM against a single GWC, carrier and external, will have the same IP address - the carrier stack's local IP address.

The example in Figure 4 shows that External GK-1 has four H.323 gateways registered with it in the external network, and a total of 480 endpoints off those gateways. We can assume, perhaps, that there are 4 gateways with 120 endpoints each. So the maximum number of simultaneous calls between External GK 1 and the GWC is:

4 GWs **x** 120 endpoints = **480**

This means External Stack 1 will need 480 reserved terminations (endpoints) provisioned against it in both the CS2K and the SD.

Similarly, External Stack 2 requires an additional 400 terminations to support the gateways registered with External GK 2, and External Stack 3 requires 300 reserved terminations to support External GK 3. These are just arbitrary numbers used in the example.

Thus, the total number of reserved endpoints required by all three external gatekeepers is:

480 (GK 1) + 400 (GK 2) + 300 (GK 3) = **1180**

This exceeds the capability of a single GWC, which can only support 1032 (North American) or 1024 (International) H.323 endpoints. Thus two GWCs are required, as shown in the example.

185.5.1.4 Provisioning Sequence

This section provides the sequence for provisioning the example shown in Figure 4. Detailed provisioning instructions are provided in Sections 2.5.3 (carrier stacks) and 2.5.4 (external stacks).

The general sequence for configuring the example shown is:

1. Provision both carrier stacks in SESM (See Section "185.5.3.1 Carrier Gateway SESM Provisioning" on page 1986)
   a. Add the stacks in SESM by associating each one as a gateway against an H.323 GWC. Exactly one carrier stack per GWC is required. CARR_STK_1 should be associated with GWC 1 and CARR_STK_2 should be associated with GWC 2.
   b. Add four carrier ports for each stack in SESM. Although only one is actually needed, for the d-channel, 4 is the minimum number that can be added in SESM. B-channels are not needed for the carrier stacks, since these stacks are only used to proxy messages to/from the external stacks. It is the external stacks that actually originate and terminate calls, so they will require b-channels.
2. Add trunk datafill in the core for each carrier stack. No trunk members are required for carrier stacks. (See Section "185.5.3.2 Carrier Gateway Core Provisioning" on page 1988)
3. Add each carrier stack in the SD with the following properties (see Section "185.5.3.3 Carrier Gateway Session Director Provisioning" on page 1988). SD provisioning is done via a command line interface in the SD itself (that is, there is no element manager). How to access and use this interface is beyond the scope of this FN - refer to Acme documentation and/or product support.
   a. Associate both stacks with the carrier network interface. This is a multi-layer association: A **stack** is associated with a **realm**; a realm is associated with a **network-interface**, a network interface is associated with a **physical interface**.
   b. Assign each stack carrier network local IP (**local-ip**) addresses (10.19.199.10 and 10.19.199.20 in the example).
   c. Add the IP address of each stack to the **hip-ip-list** in each stack's associated **network interface**. This step is critical and often overlooked since the hip-ip-list field is not part of the stack provisioning tuple, but rather is under network-interface provisioning. Without this step, the stacks will not be able to send messages via the carrier network.
   d. Assign each stack a **gatekeeper** address - this will be the stack's respective GWC address (10.19.199.68 and 10.19.199.72 in the example).
   e. Assign the **maintenanceProxy** option to each stack

After completing these three steps, the carrier stacks will begin sending registration attempts to the GWCs, the GWCs will confirm these requests, and the stacks will be successfully registered with the GWCs.

4. Provision each of the three external stacks in SESM (see Section "185.5.4.1 External Gateway SESM Provisioning" on page 1990).
    a. Add the stacks in SESM by associating each it as a gateway against an H.323 GWC. It must be the same GWC that carrier stack that will proxy H323 messages is provisioned against. Assign the gateway the same IP address as its associated carrier stack's local IP address.
    b. Add sufficient carrier ports in SESM to support the maximum number of endpoints each stack will need, based on the number of endpoints registered with the external GK the stack represents. (See Section "185.5.3.1 Carrier Gateway SESM Provisioning" on page 1986)
5. Add trunk datafill in the core for the stack, including one TRKMEM per carrier port provisioned in SESM in step 4b (see Section "185.5.4.2 External Gateway Core Provisioning" on page 1991).
6. Add the stacks in the SD (see Section "185.5.4.3 External Gateway Session Director Provisioning" on page 1992) with the following properties:
    a. All three stacks are associated with the *external network interface*
    b. All three stacks are assigned external network addresses (10.77.77.101, 10.77.77.102, 10.77.77.103)
    c. Each stack is provisioned with its respective external GK address (10.77.77.10, 10.77.77.20, and 10.77.77.30)
    d. Stacks External Stack 1 and External Stack 2 are associated with Carrier Stack 1.
    e. Stack External Stack 3 is associated with Carrier Stack 2
7. Provision each stack in its respective external GK, if necessary. This step is optional on Cisco GKs but required on S1000 GKs.

After completing steps 4 through 7, the external stacks will begin sending registration attempts to their respective external GKs; the GKs will confirm these requests; and the stacks will be successfully registered.

Next, the stacks will begin sending registration attempts to their respective GWCs on the carrier network, *proxying these requests through the carrier stacks*. The GWCs will confirm these requests (*also proxied through the carrier stacks*), and the stacks will be successfully registered with the GWCs, as well as with the external GKs.

At this point, calls can be routed between the external GKs and the GWCs based on routing in the GKs and core translations (neither of which is addressed in this FN).

Note: External stacks will not be able to proxy messages to the carrier network if its associated carrier stack is not successfully registered. This is important to consider when debugging configuration/provisioning/registration issues.

185.5.2 Maintenance Proxying

Maintenance proxying is a functionality on the SD that is specific to gatekeeper to gatekeeper interworking. Understanding the role of maintenance proxying will be useful in debugging configuration/provisioning/registration issues.

Some brief background: when an H.323 Gateway (any profile) successfully registers with a GWC, the gateway's PRI trunk d-channels and b-channels transition to "in service" state (INS) in the core. The trunk being in service should imply that we should be able to now terminate calls to this trunk and the call should complete, at least to the far end of the trunk. In the case of H.323 Gateways, the implication is that the gateway is in service and is capable of originating/terminating calls - otherwise it would not be registered.

This model breaks down somewhat when external stacks on a SD are registering with the GWC. The reason is that, an external stack could successfully register with a GWC, even if it is not successfully registered with an enterprise GK. The result in this case would be that the stack's trunk in the core would go INS, when in reality, there are no agents on the external side of the SD to terminate a call to, since the stack is not even registered with an external GK.

To solve this, the SD practices maintenance proxying. Basically, an external stack will attempt to register with a GK on the carrier network (GWC) **only** if it is successfully registered with an external gatekeeper. Similarly, once it is successfully registered with both a GK and GWC; if the stack, for any reason, unregisters with the external GK, then it will immediately unregister from the GWC. This behavior results in a trunk state on the core that is more reflective of the stack's readiness to process calls. When a stack's trunk is INS, this always implies that the stack is registered with an external GK and, in theory, is able to process calls.

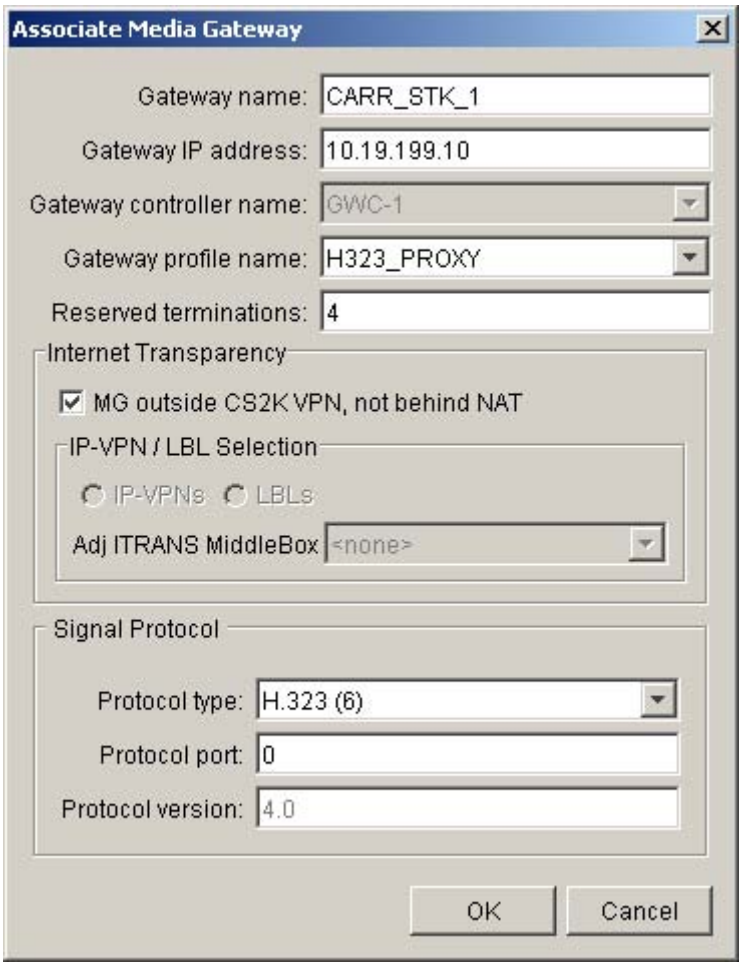
185.5.3 Configuring Acme SD *Carrier Stacks*

This section discusses details on provisioning carrier stacks.

185.5.3.1 Carrier Gateway SESM Provisioning

Figure 5 shows example SESM provisioning for Carrier Stack 1. (CARR_STK_1). The gateway will be associated against GWC 1. Carrier Stack 2 would be similarly provisioned against GWC 2.

Figure 5 Example SESM Provisioning - Carrier Stack 1

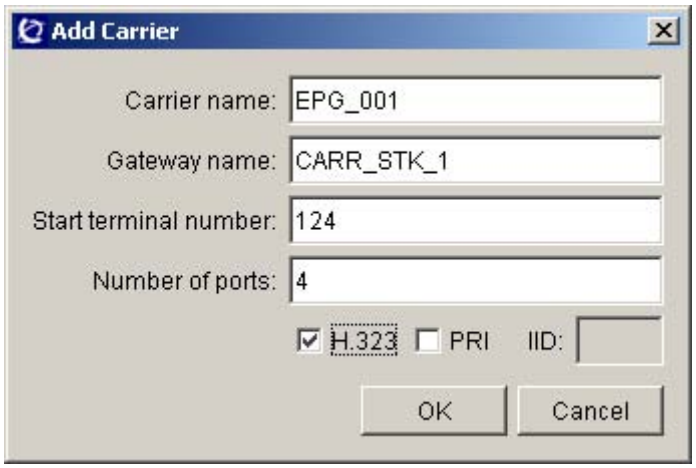


Fields that are significant to GK-GK interworking include:

- **Gateway Profile name: H323_PROXY**
  This **new profile** should be used for all Acme Packet SD Gateways (stacks).
- **Reserved terminations: 4**
  This gateway (stack) should be provisioned with the minimum reserved terminations (4). We actually only need one, for the d-channel, but four is the minimum number that can be added.
- **MG outside CS2K VPN, not behind NAT**
  It is not necessary to associate a NAT for this gateway (stack). This field can be checked or left blank. An **Adj ITRANS MiddleBox** should not be selected in either case.
- **Protocol port: 0**
  H323_PROXY gateways should always be provisioned with a signalling protocol port of 0.

After the gateway is associated, a carrier must be added for this gateway in SESM. Provision the carrier just like any other H323 gateway - there are no carrier group changes specific to GK-GK interworking.

Figure 6 Example SESM Provisioning - Add Carrier for Carrier Stack 1



Fields that are significant to GK-GK interworking:

- **Reserved terminations: 4**
  Only one port is required for this gateway (the d-channel). However, 4 is the minimum number SESM currently allows.

185.5.3.2 Carrier Gateway Core Provisioning

An H323 trunk group should be added to core datafill that maps to the gateway provisioned in SESM in section "185.5.3.1 Carrier Gateway SESM Provisioning" on page 1986. There are no core datafill changes specific to this feature - the trunk should be datafilled just like any H323 trunk group. It is not necessary to provision any b-channels for carrier stacks.

185.5.3.3 Carrier Gateway Session Director Provisioning

Example configuration for Carrier Stack 1 on the Acme SD is shown below:

```
h323-stack
        name                            CARR_STK_1
        state                           enabled
        isgateway                       enabled
        realm-id                        carrier_ntwk
        assoc-stack
        local-ip                        10.19.199.10
        max-calls                       1
        max-channels                    2
        registration-ttl                50
        terminal-alias
                                        h323-ID=CARR_STK_1
        prefixes
        ras-port                        1719
```

```
 auto-gk-discovery             disabled
 multicast                     0.0.0.0:0
 gatekeeper                    10.19.199.68:1719
gk-identifier
 q931-port                     1720
 alternate-transport
 q931-max-calls                880
 h245-tunneling                enabled
 fs-in-first-msg               disabled
 call-start-fast               disabled
 call-start-slow               disabled
 media-profiles
 process-registration          disabled
 options                       maintenanceProxy
 anonymous-connection          enabled
 proxy-mode                    H245
 filename
 last-modified-date            2004-05-06 09:38:59
```

The **name** field has been assigned the value **CARR_STK_1** in the example, although this could be named anything and is only used as an identifier for this stack. The field in which the name is important is **terminal-alias** which needs to include the h323-ID that was provisioned in SESM. In this case, **h323-ID=CARR_STK_1**.

The **realm-id** field points to a provisioned realm on the SD that is associated with the carrier network interface. Provisioning realms, network interfaces, and physical interfaces on the SD is beyond the scope of this FN - refer to Acme Packet documentation or product support.

The **assoc-stack** (associated stack) field should be left blank for this stack.

The **local-ip** (local IP address) is assigned an available address on the carrier network (10.19.199.10).

The **q931-max-calls** field indicates the maximum number of calls supported by this stack. It should be assigned the number of resources necessary to support all endpoints off the external stacks that will use this carrier stack to proxy messages to a GWC. In our example, we have determined that External Stack 1 requires 480 max calls, and External Stack 2 requires 400. Therefore, Carrier Stack 1 must support **880** calls.

The **gatekeeper** field is assigned the GWC address and port 1719 (standard RAS port).

The **maintenanceProxy** option indicates that these stacks will be used to proxy H.323 maintenance and call processing messaging to the GWCs from other SD stacks.

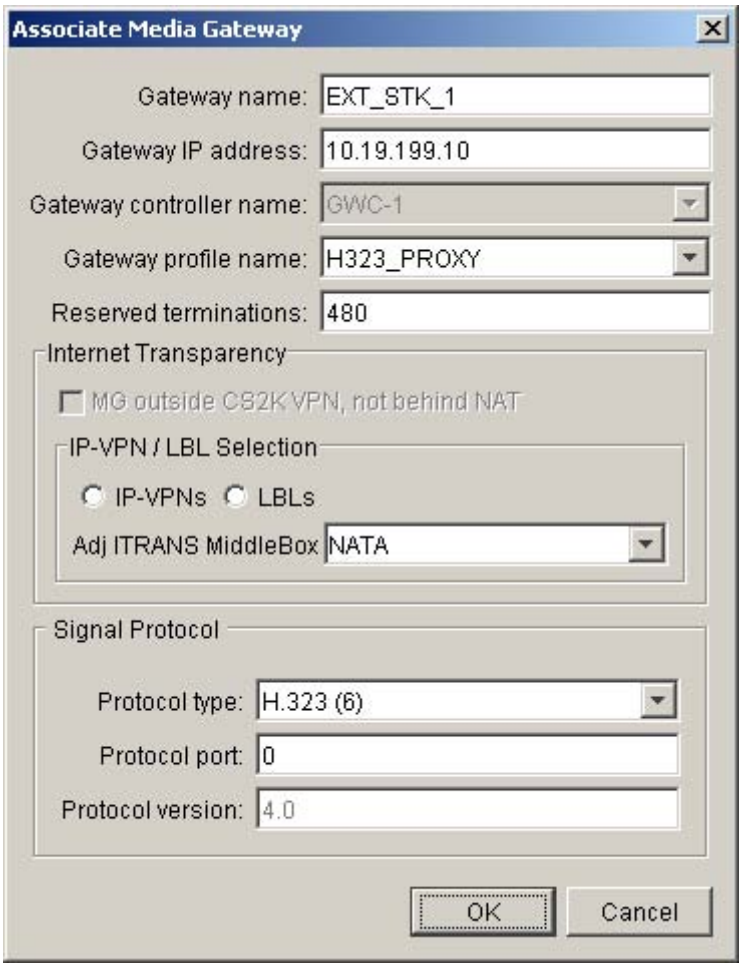
185.5.4 Configuring Acme SD *External Stacks*

External Stacks 1, 2, and 3 (EXT_STK_1, EXT_STK_2, and EXT_STK_2) will register with GK-1, GK-2, and GK-3, respectively, on the external network(s), as well as with GWC-1 and GWC-2 on the carrier network. These gateways will proxy H.323 calls through the SD. This section walks through provisioning for External Stack 1.

185.5.4.1 External Gateway SESM Provisioning

Figure 7 shows example SESM provisioning for External Stack 1. The gateway will be associated against GWC 1. External Stack 2 would also be provisioned against GWC 1, and External Stack 3 would be provisioned against GWC 2.

Figure 7 Example SESM Provisioning - External Stack 1



Fields that are significant to GK-GK interworking include:

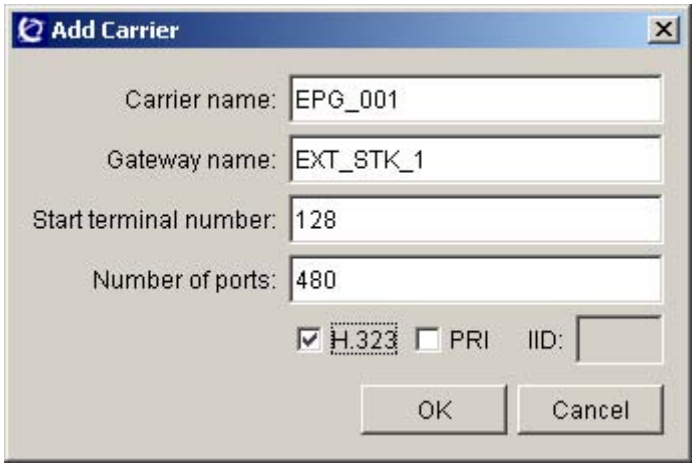
- **Gateway IP address: 10.19.199.10**

Messaging from the External Gateway to the GWC will be proxied via the Carrier Stack - thus we provision Carrier Stack 1's IP address here.

- **Gateway Profile name: H323_PROXY**
  This **new profile** should be used for all Acme Packet SD Gateways (stacks).
- **Reserved terminations: 480**
  Reserved terminations should be populated with the total number of calls supported between the CS2K and the external GK represented by this stack (480 in our example).
- **Adj ITRANS MiddleBox: NATA**
  A NAT should be added for the external network that GK-1 resides in.
- **Protocol port: 0**
  H323_PROXY gateways should always be provisioned with a signalling protocol port of 0.

After the gateway is associated, a carrier must be added for this gateway in SESM. Provision the carrier just like any other H323 gateway. Refer to Figure 8.

Figure 8 Example SESM Provisioning - Add Carrier for External Stack 1



The **number of ports** represents the supported calls between the CS2K and the gatekeeper represented by the external stack (480 in our example).

185.5.4.2 External Gateway Core Provisioning

An H323 trunk group should be added to core datafill that maps to the gateway provisioned in SESM in section "185.5.4.1 External Gateway SESM Provisioning" on page 1990. There are no core datafill changes specific to GK-GK Interworking - the trunk should be datafilled just like any H323 trunk group. In this example, 480 trunk members (b-channels) should be added for EXT_STK_1.

185.5.4.3 External Gateway Session Director Provisioning

Example configuration for External Stack 1 on the Acme SD is shown below:

```
h323-stack
        name                            EXT_STK_1
        state                           enabled
        isgateway                       enabled
        realm-id                        enterprise_z
        assoc-stack                     CARR_STK_1
        local-ip                        10.77.77.30
        max-calls                       480
        max-channels                    4
        registration-ttl                50
        terminal-alias
                                        h323-ID=EXT_STK_1
        prefixes
        ras-port
        auto-gk-discovery               disabled
        multicast                       0.0.0.0:0
        gatekeeper                      10.77.77.10:1719
        gk-identifier
        q931-port                       1720
        alternate-transport
        q931-max-calls                  480
        h245-tunneling                  enabled
        fs-in-first-msg                 disabled
        call-start-fast                 disabled
        call-start-slow                 disabled
        media-profiles
        process-registration            disabled
        anonymous-connection            enabled
        proxy-mode                      H245
        filename
        last-modified-date              2004-05-06 09:38:59
```

The **realm-id** field points to a provisioned realm on the SD that is associated with the external network interface. Provisioning realms, network interfaces, and physical interfaces on the SD is beyond the scope of this FN - refer to Acme Packet documentation or product support.

The **assoc-stack** (associated stack) field points to the carrier stack that will proxy messaging for this stack to/from the GWC. EXT_STK_1's associated stack is CARR_STK_1.

The **local-ip** (local IP address) is assigned an available address on the external network.

The **q931-max-calls** field indicates the maximum number of calls supported by this stack. It should be assigned the number of resources necessary to support all endpoints off the external GK (480 in our example).

The **maintenanceProxy** option is *not* added to this gateway.

185.6 Hardware Requirements or Dependencies

185.7 Software Requirements or Dependencies

185.8 Limitations and restrictions

185.8.1 Supported GK Devices

GK-GK interworking is supported between the CS2K GK and the following GKs

- Cisco 36xx (IOS 12.2.24)
- Cisco 72xx (IOS 12.2.24)
- Nortel S1000 (Succession Rls 3)

185.8.2 Supported H323 Gateways

GK-GK interworking is supported between the CS2K GK and the following GWs. That is, these Gateways can be registered with the Gatekeepers listed in section 2.6.1.

- Cisco 26xx (IOS 12.2.24)
- Cisco 36xx (IOS 12.2.24)
- Cisco 37xx (IOS 12.2.TBD)
- Nortel S1000 (Succession Rls 3)
- Nortel S1000M (Succession Rls 3)
- Nortel BCM (Version 3.6)

185.8.3 Supported CS2K Interworking

Interworking is supported between any combination of gateway and gatekeeper pairs listed in sections 2.6.1 and 2.6.2, and the following:

- Cisco 26xx (IOS 12.2.24)
- Cisco 36xx (IOS 12.2.24)
- Cisco 37xx (IOS 12.2.TBD)
- Nortel S1000 (Succession Rls 3)
- Nortel S1000M (Succession Rls 3)
- Nortel BCM (Version 3.6)

Non-H323 Gateways

- PVG

- Mediatrix
- CICM
- UAS
- MG9000
- SIP-T (VRDN)
- SIP-T (NGSS)
- MCS

185.8.4 GWC Limitations

The same H.323 GWC capacity requirements apply to SD stacks as to any other H.323 gateways - specifically, only 1032 (NA) or 1024 (international) endpoints are supported off a single GWC. The engineering decision of how many external stacks can be provisioned against a single GWC should be based on how many endpoints are represented by each external stack. Each stack represents the combined number of endpoints on all the external gateways registered with the external gatekeeper the stack is registered with.

185.8.5 Acme Session Director Limitations

- Maximum BHCA: currently unknown/uncharacterized
- Maximum simultaneous calls: Tiered based on license
- Maximum number of provisionable stacks: approximately 100-200
- Maximum number of provisionable endpoints per stack: this is manually engineered based on the licensed number of simultaneous calls and the number of provisioned stacks. For example, if 100 stacks are configured and a license allows for 8,000 simultaneous calls, then the maximum number of endpoints per stack would be 8000/100 = 80 (on average).
- Failover speed: depends on the outage type but anywhere from 40 ms to 300 ms should be expected

185.9 Interactions

185.10 Glossary

Term	Description
New term	Definition

186: Functional Description (FN): A00007063

186.1 Feature name

A00007063 SN07 Corrective CAF H.323 Gateway Profile Changes

186.2 Description

The current design to limit the number of endpoints that can be assigned to a specific gateway via the CS2M (CS2K Management Tools) is to set a maximum reserved terminations value in the respective gateway profile. The maximum reserved terminations value is set in the GWC EM (Gateway Controller Element Manager) database during initial installation and upgrades. The values are set per release and cannot be changed dynamically by a craftperson.

A better solution has been adopted to manage the number of endpoints a single H.323 gateway can have allocated towards it.

A single gateway cannot be assigned more endpoints/TIDs than the maximum reserved terminations value of the assigned gateway profile.

H.323 gateways are different than most supported Succession gateways from a capacity perspective. A number of H.323 gateways do not have physical limitations. H.323 gateways have many variables that determine the maximum number of simultaneous calls:

- What is the hardware platform the H.323 gateway application is running on?
- How much memory does it have?
- Which hardware version?
- Which software version?

Determining the proper maximum capacity for a H.323 gateway from release to release is inaccurate. Nortel's H.323 gateways' maximum reserved termination values are difficult to properly set during a given release. H.323 third party gateways are even more difficult.

The solution is to set the maximum reserved termination values for all the H.323 gateway profiles to the maximum capacity of a H.323 GWC. The maximum reserved terminations value for a H.323 gateway is now restricted by the GWC not the gateway profile maximum reserved termination setting. Instead of the design team trying to manage the capacities of Nortel and third party H.323 gateways, our customers will configure the number of desired

endpoints against H.323 gateways. Nortel will no longer dictate the maximum capacity of a third party H.323 gateway supported by the CS2K.

Nortel documentation will direct our customers to the respective gateway vendor documentation for the maximum capacities of the supported H.323 gateways.

The maximum number of endpoints that can be assigned to a single H.323 gateway in SN07 will now be the capacity of a H.323 GWC. If an attempt is made to associate more endpoints/TIDs to a H.323 gateway than the capacity of a H.323 GWC, the request is rejected and an error message is generated.

186.2.1 H.323 Capacities

A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs.

Note: The SN07 H.323 GWC capacities have not changed from SN06.2.

A H.323 virtual carrier can be any size within the range of 4 - 672.

Table 1 H.323 SN07 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of endpoints/TIDs per GWC)
H.323_INTL	1024
H.323_NA	1032

The H.323 gateway profiles have been consolidated and updated by setting the maximum reserved terminations values to the capacity of the H.323 GWC.

The updated SN07 H.323 gateway profiles are listed in Table 2, “H.323 gateway maximum reserved terminations,” on page 1997.

Note: The H.323 gateway profiles that are being removed are designated by the “***~~strike through~~***”.

Table 2 H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
~~NORTEL_BCM_NA~~	~~48~~	~~48~~
SUCCESSION_1000	480	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_2600	96	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_3600	384	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_AS5300	384	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_H323_IOS	N/A	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
WESTELL	64	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)

Table 2 H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
H323_PROXY	N/A	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)

186.3 Hardware Requirements or Dependencies

N/A

186.4 Software Requirements or Dependencies

N/A

186.5 Limitations and restrictions

N/A

186.6 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface ___X___
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

186.7 Glossary

186.7.1 Definitions & Abbreviations

Acronym	Definition
ASPEN	Nortel proprietary GW control protocol (not an acronym).
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS2K	Call Server 2000
CS2M	Call Server 2000 Management Tools
DDMS	DMS Data Management System
DMS	Digital Multiplex System
DTC	Digital Trunk Controller
DTCI	ISDN Digital Trunk Controller
DTD	Document Type Definition
EPID	End Point Identifier
ETSI	European Telecommunications Standards Institute
GPS	Global Product Support
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
GWC EM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
HTML	HyperText Markup Language
IDL	Interface Definition Language

IP	Internet Protocol
ITA	Internet Transparency Agent
JAR	Java Archive
JDBC	Java Database Connectivity
JNLP	Java Network Launching Protocol
JWS	Java Web Start
LAN	Local Area Network
LTC	Line/Trunk Controller
MEGACO	H.248. Industry protocol for MG/MGC <->MG/MGC communication.
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Block
MOP	Method of Procedure
MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PLM	Product Line Management
PSTN	Public Switched Telephone Network
RMGC	Redirecting Media Gateway Controller

SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol
SQL	Structured Query Language (for DBs)
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number

187: Functional Description (FN): A00007211

187.1 Feature name

H.323 GWC600 Log Changes

187.2 Purpose

Log report GWC600 indicates an Info Log for a H.323 failure with a failure reason that indicates specifically what happened.

The current GWC600 log does not adhere to the log formatting standards as described in IEMPG.AF01. Not adhering to the requirements often makes the log in question unsupportable or difficult to support in the OSS.

This SN07 activity will modify the existing H.323 GWC600 log format to follow a generic OSS log framework. These changes will impact both the NA and international versions of H.323.

187.2.1 GWC Changes

The H323 application will generate formatted GWC600 logs to adhere to the OSS requirements. The formatted logs are sent to the syslog customer log interface. The fields in the log body are defined and populated in the H323 application.

The header is changed from "H323 LOG MESSAGE" to something not H323 specific, but more function-indicating, like "Protocol Event". So we won't have to define GWC601 as "SCTP Event" and GWC602 as "TCP event", and etc. The log body is modified as well.

After the changes, for H323 the GWC600 log will look like:

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=BCM_RTPG
Specific Problem: H323 keepAlive RRQ rejected
Description: D-Channel Out Of Service

Logs for other applications will follow the same framework, and will look something like:

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=ABI_1_2_3
Specific Problem: SCTP packet NACK
Description: SCTP association re-established

and

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=CS2M_IP_ADDR
Specific Problem: SNMP ASN.1 format error
Description: Message from 47.142.108.100 dropped

188: CR: Q00681924

188.1 Name

AIN Response Simplification

188.1.1 Problem

In some instances, the application of SOC code AIN00026 (Translation Simplification Phase II) creates a situation in which the CDP query and AR response repeat in a loop until the value of AIN_MAX_SERIAL_TRIGGERS is exceeded in table OFCENG.

188.1.2 Resolution

Every second time the PUB_NET_ACC code matches the CDP trigger code, the CDP trigger does not happen, so no loop occurs.

For example, the first match allows the CDP trigger to occur, and the second match prevents the CDP trigger.

If the call flow hit this scenario a third time, the CDP trigger would occur, then the fourth time the CDP trigger would not occur. However, it is highly unlikely that multiple hits would occur.

Fault Management (FM)

Introduction

This chapter describes impacts to fault management, such as logs and alarms, for the features planned for this release. Only those features with fault-management impacts are listed.

Featid	Title
A00001893	MG9K Imaging
A00002012.AA13	XA-Core CMIC/RTIF HIOP Maintenance Software
A00002013.AA06	Intelligent Network T1 Timer Expiry Message Suppression
A00002020.AB10	ESA Translation Download
A00002146.AA09	MAPCI ABI Link Test & Legacy Comparison
A00002380.AA21	MG9K ABI ESA
A00002433.AA07	XA-Core Baseline Control
A00002499.AA05	XA-Core Baseline Control
A00002510.AA08	LANCOMM IP over IRM
A00002549.AA04	CSP20 Callp Robustness
A00002607.AA11	ABI XPM SITE and MG9K Location support
A00002757.AA08	CBM Fault Management (HA)
A00002823.AA08	SDM Core HA Maintenance (HA OAMMTCE)
A00002858.AA26	Node ISTB for SPM Carrier Outage

A00002970.AA11	SMG4 Remote Site Provisioning
A00003371	Common Inventory and Data Consolidation
A00003487.AA27	SN07 Trimodal Call Server Feature
A00003567	MG9000 Element Manager support for ABI ESA
A00003591	MG9000 OC3 Channelization support from EM
A00003650.AA08	MG4K-IP Logs Core Component
A00003667	SESM NB Alarm Interface Changes required for OSS
A00003687.AA06	TOPS Wireless Intelligent Network Integration
A00003767.AA29	IP ABI PPVM Robustness & Msg Loss Alarms
A00003933.AA07	Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application
A00003947.AA16	Trimodal LOGs and Operational Measurements (OM)
A00003971.AA10	SPM Log Robustness
A00004045.AA06	Calling Line Identification Directory Number (CLIDN) for DMS-250
A00004260.AA24	XPKT301 Alarm Banner for MG4K/IW/DPT
A00004271.AA08	SIP App Server SOC
A00004391	ACD Agent Expansion from 9,999 to 30,000 Agents
A00004430.AA08	SVC Failure OMs
A00005016	VMG Out of Service Alarms
A00005073.AA18	SBA Outbound Connection Security
A00005074.AA07	OMDD: Outbound Connection Security
A00005160.AA10	OSSAIN XA-Core Data Messaging Capacity Enhancements
A00005192.AA24	CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance

A00005322.AA08	Spectrum Common Equipment Module (CEM) Overload Enhancement: Asynchronous Transfer Mode Resource Module (ATMRM) Status
A00005363.AA16	CAIN FlexCDR Enhancements
A00005375	New Shelf Discovery Alarms

2008

1: Fault Management (FM): A00001893

This feature, MG9K Imaging, introduces two new logs; a new node type customer log and a new MG9K Audit log. Both logs are new numbers in an existing series for each type.

Document Name:

MG9K_Image_FM.fm; A00001893/A00001894

Document Version:

/main/pnmdoc/3

1.1 Fault management strategy

No additional tools are implemented by this feature. Customer and Audit logs for this feature are generated via the existing log software in the MG9K Element Manager.

1.2 Fault management tools and utilities

This feature utilizes the fault management tools provided by the MG9K Element Manager application.

Customer logs are generated by the Element Manager application and are based on the processing of node logs received from the MG9K gateway.

Audit logs are generated by the Element Manager and are based on maintenance actions performed by the craft person only at the Element Manager console.

1.3 Logs

1.3.1 New MGEM 714 Audit Log

This log is generated whenever a user attempts to image an MG9K device.

1.3.1.1 Format

The following table is an example of the new MGEM 714:

Oct 2 14:37:14 wnc0s00v MGEM:joeuser 714 Software Image Requested MG9K: U16 [16]

Table 1 Field Description for the MGEM log

Field	Description	Example
Date/Time	Date and Time stamp of the log	Oct 2 14:37:14
Host Name	Host machine name	wnc0s00v
Application Name	Specifies the application producing the log	MGEM
User Name	User name attempting the action	joeuser
Log Number	The log number	714
Log Text	Specifies the action attempted and any associated details.	Software Image Requested MG9K: U16[16]

1.3.1.2 Action

No action is required.

1.3.1.3 Associated Operational Measurements or Performance Measurements

None.

1.3.1.4 Additional Information

None.

1.3.2 New NE609 Software Image Log

This new log is generated whenever a user executes an image request.

1.3.2.1 Format

The following is an example of what the new log might look like:

NE609 OCT6 11:06:14 0029 INFO MG9K Software Image Event

Imaging: NE Number: 7 NE Name: PL7 Card Type: DS1

Image Type: Card Type

Image Action: Image

Image Status: Image Completed

Time: Thu Oct 02 18:17:11 EDT 2003

1.3.2.2 Action

If the Image Status field indicates a failure, the user may want to attempt to image the device again.

1.3.2.3 Associated Operational Measurements or Performance Measurements

None.

1.3.2.4 Additional Information

None.

1.4 Related documentation

SN06.2 MG9K Logs

2: Fault Management (FM): A00002012

2.1 Fault management strategy

This feature does not change the fault management strategy of the XA-Core.

2.2 Fault management tools and utilities

This feature does not change the fault management tools and utilities of the XA-Core.

2.3 Logs

2.3.1 CMIC XAC log changes

Since this feature introduces port/link separation for the CMIC functionality on HIOP, the XAC information and action logs will now show the new CMIC port device, in addition to the CMIC packlets and CMIC links. The feature does not change the format of either the information or action logs.

- CMIC packlets and CMIC links on packlet are going to be shown the same way as before (no port/link separation for CMIC packlets),
- CMIC ports and links on HIOP will have the packlet field left blank.

The XAC610 log is chosen to show the difference.

Current XAC610 Log for CMIC packlet:

```
XA506AX     XAC610 JAN29 06:37:35 8000 RTS  Returned To Service
        DESCRIPTION: State has changed from SYSB to INSV by RECOVERY action
        CARD:   Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
                CMIC INSV  HOST 01 A00 DPCC:00 00 15R L  NTLX05AB/NNTM171VY7C0
```

Current XAC610 Log for CMIC link on packlet:

```
XA506AX     XAC610 JAN29 06:37:35 8000 RTS  Returned To Service
        DESCRIPTION: State has changed from SYSB to INSV by MS-MTCE action
        LINK:   Type State Site FL Row Bay    Shf/Slt/Pk/Lk    EqPEC/Serial
              CMIC INSV  HOST 01 A00 DPCC:00 00 15R L  1  NTLX05AB/NNTM171VY7C0
```

New XAC610 Log for CMIC port on HIOP (packlet field blank):

```
XA506ax XAC610 MAR05 17:54:47 1200 RTS  Returned To Service
        DESCRIPTION: State has changed from SYSB to INSV by RECOVERY action
        PORT: Type State Site FL Row Bay    Shf/Slt/Pk/Pt EqPEC/Serial
              CMIC INSV  HOST 01 A00 DPCC:00 00 15R    1 NTLX17AA/NNTM64422MWV
```

New XAC610 Log for CMIC link on HIOP (packlet field blank):

```
XA506ax XAC610 MAR05 17:54:47 1200 RTS  Returned To Service
        DESCRIPTION: State has changed from SYSB to INSV by MS-MTCE action
        LINK: Type State Site FL Row Bay    Shf/Slt/Pk/Lk EqPEC/Serial
              CMIC INSV  HOST 01 A00 DPCC:00 00 15R    1 NTLX17AA/NNTM64422MWV
```

2.3.2 RTIF XAC log changes

Since this feature introduces port/link separation for the RTIF functionality on HIOP, the XAC information and action logs will now show the new RTIF link device, in addition to the RTIF packlets and RTIF ports. This feature does not change the format of either the information or action logs.

- RTIF packlets are going to be shown the same way as before,
- RTIF port representation on packlets will be changed to RTIF links: Llink0 and Link1,
- RTIF ports and links on HIOP will have the packlet field left blank.

The XAC610 log is chosen to show the difference.

Current XAC610 Log for RTIF packlet:

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
        DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk   EqPEC/Serial
              RTIF INSV  HOST 01 A00 DPCC:00 00 04R U NTLX08AA/NNTM171P3G37
```

Current XAC610 Log for RTIF port on packlet (port will be obsoleted):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
        DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
        PORT: Type State Site FL Row Bay    Shf/Slt/Pk/Pt   EqPEC/Serial
              RTIF INSV  HOST 01 A00 DPCC:00 00 04R U  0 NTLX08AA/NNTM171P3G37
```

New XAC610 Log for RTIF link on packlet (no port field on packlet):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
        DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
        LINK: Type State Site FL Row Bay    Shf/Slt/Pk/Lk EqPEC/Serial
              RTIF INSV  HOST 01 A00 DPCC:00 00 04R U  0 NTLX08AA/NNTM171P3G37
```

New XAC610 Log for RTIF port on HIOP (packlet field blank):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
        DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
        PORT: Type State Site FL Row Bay    Shf/Slt/Pk/Pt EqPEC/Serial
              RTIF INSV  HOST 01 A00 DPCC:00 00 04R    0 NTLX17AA/  NNTM171P3G37
```

New XAC610 Log for RTIF link (packlet field blank):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
        DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
        LINK: Type State Site FL Row Bay    Shf/Slt/Pk/Lk    EqPEC/Serial
              RTIF INSV  HOST 01 A00 DPCC:00 00 04R    0  NTLX17AA/NNTM171P3G37
```

2.3.3 IO XAC log changes

Since this feature introduces the new CMIC/RTIF HIOP card, minor modifications are needed to the impact statement of the existing XAC logs for this new resource. There is no other change for any information or action logs.

Current XAC312 Log for AMDI/RTIF/ETHR HIOP:

```
S106BI   *  XAC312 MAR11 10:24:19 6700 FLT  IOP (Input Output Processor Fault)
        IMPACT: AMDI, Ethernet and RTIF services are unavailable on this IO
        DESCRIPTION: State has changed from INSV to MBSY by MANUAL action
        CARD: Type State Site FL Row Bay    Shf/Slt         EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 05R      NTLX04BA/  NNTM64422MWV
```

XAC312 Log for new CMIC/RTIF HIOP (different impact statement):

```
S106BI   *  XAC312 MAR11 10:24:19 6700 FLT  IOP (Input Output Processor Fault)
        IMPACT: CMIC, Ethernet and RTIF services are unavailable on this IO
        DESCRIPTION: State has changed from INSV to MBSY by MANUAL action
        CARD: Type State Site FL Row Bay    Shf/Slt         EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 05R      NTLX17AA/  NNTM64422MWV
```

2.4 Alarms

This feature does not add or remove any existing XA-Core system alarms which are displayed under the XAC title in the alarm banner. It only adds to the scenarios by which the MSComm XAC Alarm is raised.

2.4.1 MScomm alarm

The MScomm alarm is raised if there is a communication problem between the XA-Core and the Message Switch (MS).

2.4.1.1 Current MScomm alarm and CMIC link RTS behavior

Currently, the MScomm alarm is raised only if a hardware component used for the communication between the XA-Core and the Message Switch (MS) goes out of service, on either the XA-Core or MS side. The following severities can be observed:

- CRITICAL: no communication,
- MAJOR: no communication link redundancy,
- MINOR: communication link redundancy is partially lost.

Configuration problems with the CMIC links between the XA-Core and the Message Switch (MS) do *not* directly raise the MScomm alarm. The alarm is raised indirectly by the fact that the system will not bring the misconfigured CMIC link in-service.

Following steps show how the current system behavior handles CMIC link misconfiguration on a packlet:

- the CMIC link on the packlet gets misconfigured,
- the CMIC link will *not* come in-service,

- the XAC326 ‘MS link Configuration Mismatch’ log is generated,
- the XAC303 ‘MScomm’ log is generated, and
- as a consequence of the CMIC link will being out of service, the MScomm XAC alarm is raised.

Once the correct configuration is established, the following will occur:

- the CMIC link on the packlet will come in-service,
- the XAC626 ‘MS Link Configuration Restored’ log is generated,
- the XAC603 ‘MScomm Alarm Cleared’ log is generated,
- the MScomm XAC alarm is cleared.

Recommended XA-Core to MS configuration

Currently, the only supported configuration between the XA-Core and the Message Switch (MS) requires four CMIC links to be cross-connected between the XA-Core and the Message Switch (MS), with specific mappings between the MS CMIC paddle board ports and the XA-Core CMIC links. This setup provides the maximum CMIC link redundancy, and node and component isolation protection.

Note: This feature does *not* change the currently recommended XA-Core to MS configuration.

Please refer to “Figure 1 Recommended XA-Core - MS configuration (SuperNode)” on page 2017.

Please refer to “Figure 2 Recommended XA-Core - MS configuration (SuperNode SE)” on page 2017.

Figure 1 Recommended XA-Core - MS configuration (SuperNode)

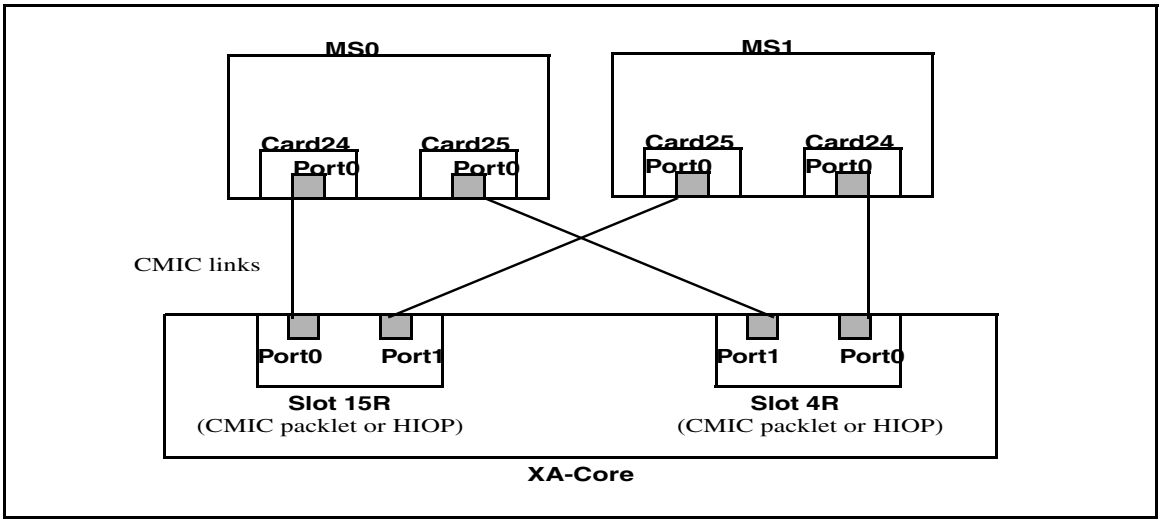
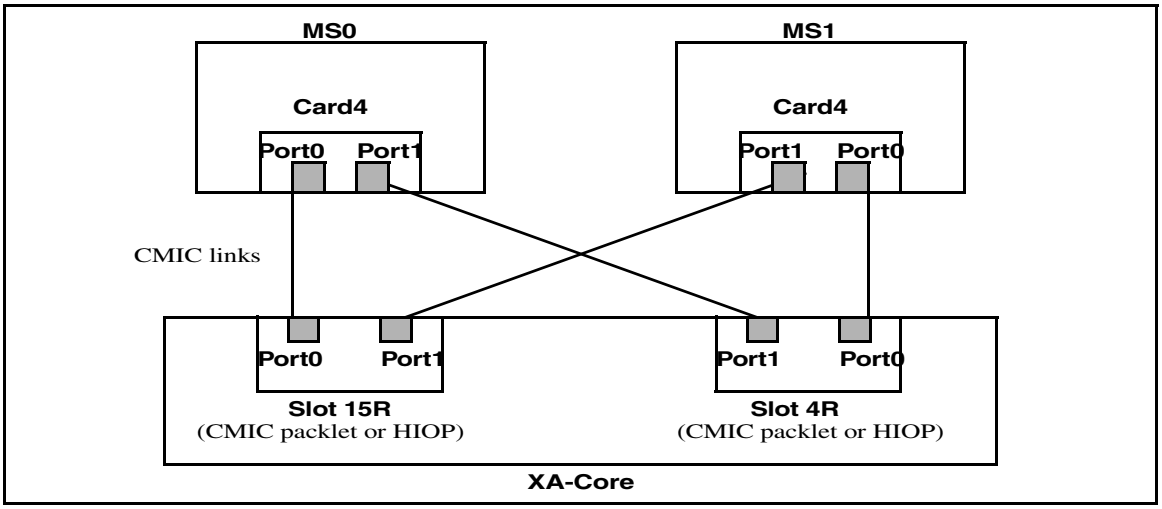


Figure 2 Recommended XA-Core - MS configuration (SuperNode SE)



2.4.1.2 New MScomm alarm and CMIC link RTS behavior

This feature adds to the scenarios that raise the MSComm XAC Alarm.

Presently, the MScomm alarm is raised only if a hardware component used for the communication between the XA-Core and the Message Switch (MS) goes out of service, on either the XA-Core or MS side.

In addition to these scenarios, from now on, an MScomm MAJOR alarm will also be raised if a CMIC link between the XA-Core and the Message Switch (MS) is in-service but not configured properly.

Support for new XA-Core to MS configuration

This feature does *not* change the currently recommended XA-Core to MS configuration.

Please refer to “Figure 1 Recommended XA-Core - MS configuration (SuperNode)” on page 2017.

Please refer to “Figure 2 Recommended XA-Core - MS configuration (SuperNode SE)” on page 2017.

However, with the introduction of flexible provisioning of CMIC components, the system will be able to support new XA-Core to MS configurations. CMIC packlets or CMIC/RTIF HIOPs can possibly be provisioned in any empty (unequipped) element slots. The same redundancy and isolation protection rules are going to be applied as before.

This new approach will help the system to adapt more gracefully to CMIC link misconfigurations. For example, this will avoid a possible boot loop during commissioning of a new XA-Core office when all CMIC links are misconfigured with respect to the recommended setup (still satisfying all redundancy and isolation protection rules). Instead of failing the boot, the system will successfully boot and bring the CMIC links in-service. Once the system is up and running, craft personnel can rectify the CMIC link misconfiguration.

The system behavior with respect to bringing a misconfigured CMIC link in-service is different depending on the following scenarios:

- a misconfigured CMIC link is being newly provisioned by the system (e.g. boot, restart, provisioning): the system will bring the misconfigured CMIC link in-service and raise the MScomm MAJOR alarm. Please refer to Section “2.4.1.2.1 Misconfigured CMIC link provisioning” on page 2018.

- an already provisioned CMIC link is improperly connected into a different port (e.g. card replacement): the system will *not* bring the misconfigured CMIC link in-service. Please refer to Section “2.4.1.2.2 Provisioned CMIC link is misconfigured” on page 2020.

2.4.1.2.1 Misconfigured CMIC link provisioning

This scenario can happen during boot, restart, and provisioning.

Please refer to “Figure 3 CMIC links not cross-connected (SuperNode)” on page 2019.

Please refer to “Figure 4 CMIC links not cross-connected (SuperNode SE)” on page 2019.

Figure 3 CMIC links not cross-connected (SuperNode)

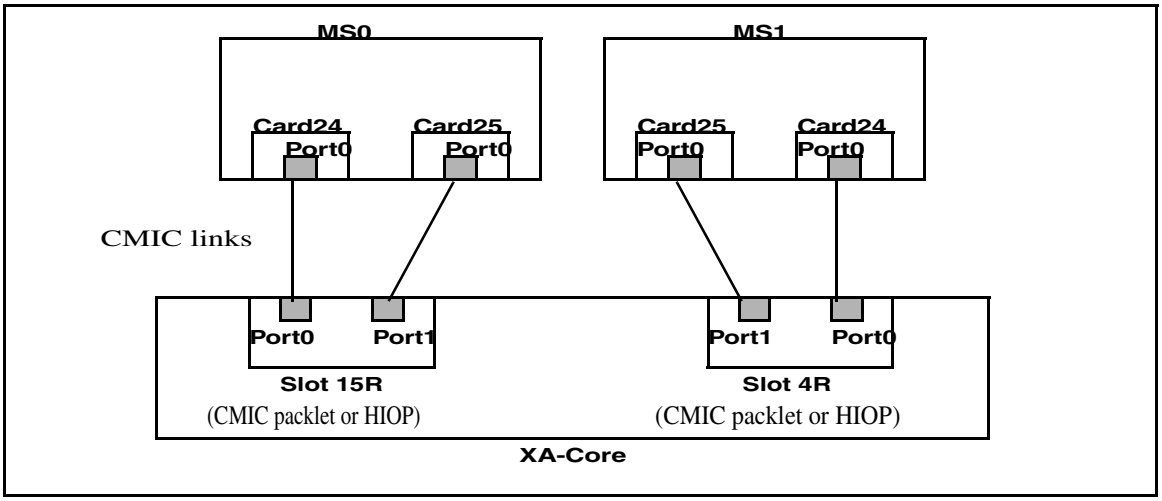
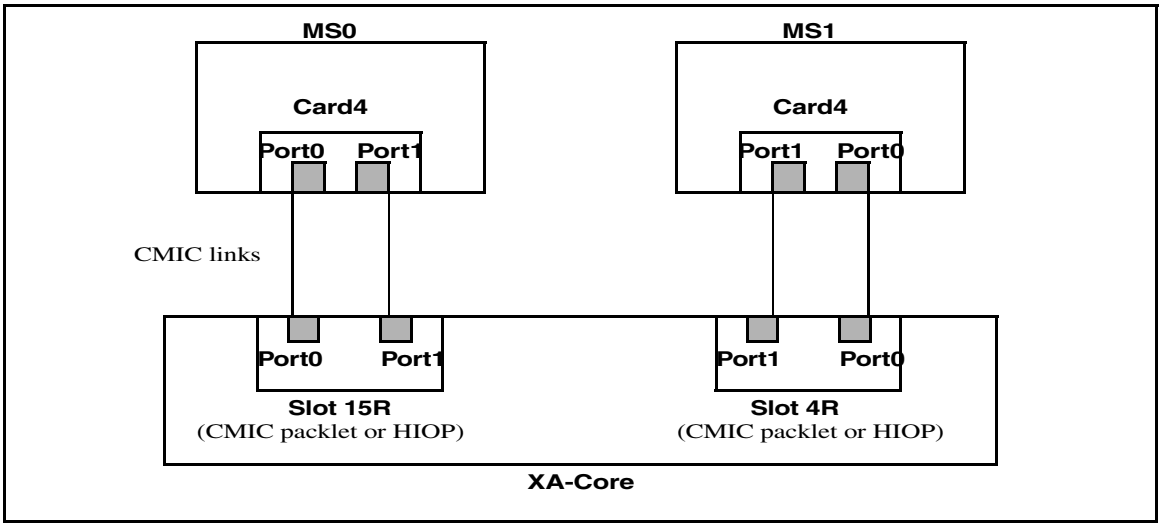


Figure 4 CMIC links not cross-connected (SuperNode SE)



Following steps show how the new system behavior handles CMIC link misconfiguration during boot, restart, and provisioning:

- the CMIC links get misconfigured (e.g. during commissioning of a new XA-Core office),
- the system will bring the CMIC links in-service,
- the XAC326 MS link Configuration Mismatch log is generated,
- although all CMIC components are in-service, the MScomm XAC MAJOR alarm is raised because of the configuration error.

Once the correct configuration is established, the following will occur:

- the XAC626 ‘MS Link Configuration Restored’ log is generated,
- the MScomm XAC alarm is cleared,

2.4.1.2.2 Provisioned CMIC link is misconfigured

This scenario can happen during a card replacement procedure. That is, two existing (provisioned) CMIC links on the same FRU are interchanged and incorrectly connected into the other port.

Please refer to “Figure 5 Interchanged CMIC links on same FRU (4R) (SuperNode)” on page 2020.

Please refer to “Figure 6 Interchanged CMIC links on same FRU (4R) (SuperNode SE)” on page 2021.

Figure 5 Interchanged CMIC links on same FRU (4R) (SuperNode)

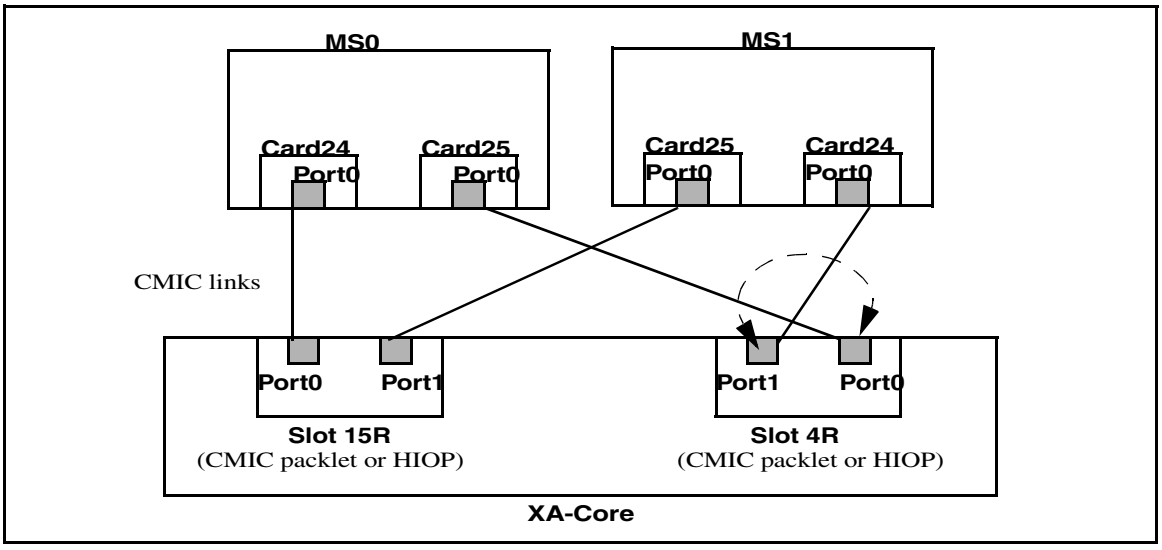
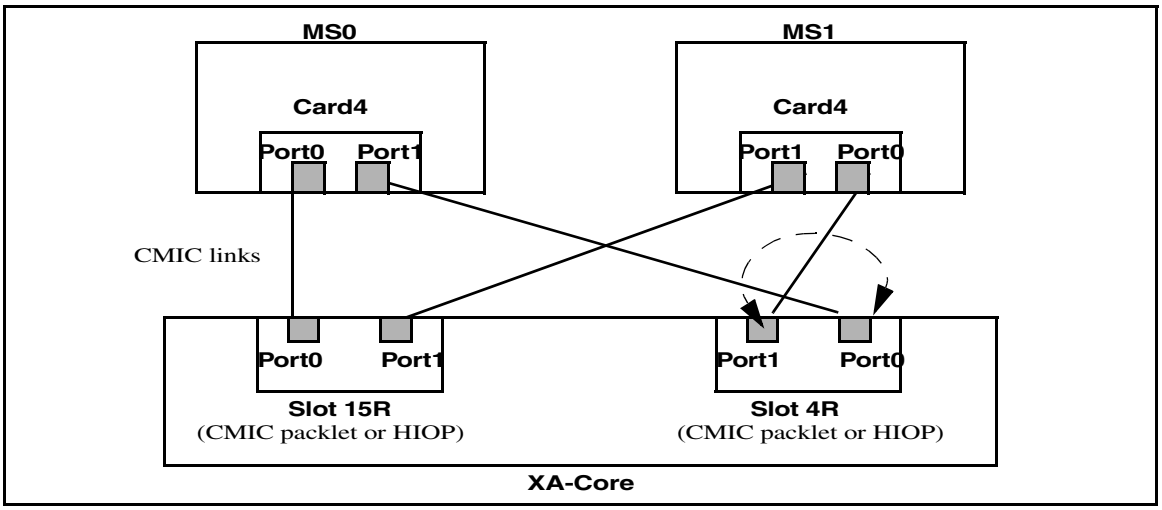


Figure 6 Interchanged CMIC links on same FRU (4R) (SuperNode SE)



Following steps show how the new system behavior handles CMIC link misconfiguration during card replacement:

- during a card replacement procedure, the CMIC links on a given FRU get misconfigured,
- the system will *not* bring the CMIC links in-service,
- the XAC326 MS link Configuration Mismatch log is generated,
- the MScomm XAC MAJOR alarm is raised because of the out of service CMIC links.

Once the correct configuration is established, the following will occur:

- the XAC626 ‘MS Link Configuration Restored’ log is generated,
- the MScomm XAC alarm is cleared,
- the system will attempt to bring the OOS CMIC links in-service.

3: Fault Management (FM): A00002013

3.1 Fault management strategy

None.

3.2 Fault management tools and utilities

None.

3.3 Logs

3.3.1 Log GAME101

3.3.1.1 Explanation

A GAME101 log will be created if the RSPTMOUT OM count is greater than zero. The log will be created during the RSPTMOUT OM transfer period and will record the RSPTMOUT OM count value.

3.3.1.2 Format

The log report format follows:

```
office * GAME101 mmmdd hh:mm:ss seqno INFO GAME_ERR_REPORT
REASON = reason_field
COUNT  = count_field
```

3.3.1.3 Example

An example of the log report follows:

```
S3_500_17BL CM GAME101 APR04 05:10:16 0504 INFO GAME_ERR_REPORT
REASON    = Suppressed T1 Timer Expiry Message
COUNT     = 25
```

3.3.1.4 Field descriptions

Table 1 Field descriptions

Field	Value	Description
reason_field	CONSTANT	A string describing the reason the log was created. In this case, it is due to suppressing a 'T1 Timer Expiry' message.
count_field	UNSIGNED INTEGER	A copy of the RSPTMOUT OM count value. It will be a number in the range from 1 to 32,767.

3.3.1.5 Action

If a high number of GAME101 logs are output it could be an indication that there is a problem with the SCP. The SCP should be checked to verify that it is operating normally.

If a low number of GAME101 logs show occasionally, it could be related to a network congestion.

Any number of GAME101 logs are highlighting a problem that needs to be addressed by your SCP first level support.

3.3.1.6 Associated Operational Measurements or Performance Measurements

This feature monitors the RSPTMOUT OM count, found in the AIN OM group, checking to see if it increments past zero. The count is incremented everytime the T1 timer expires and the SSP, as a consequence, attempts to generate a 'T1 Timer Expiry' message.

3.3.1.7 Additional information

N/A

3.3.2 Log GAME102

3.3.2.1 Explanation

A GAME102 log will be created if RSPTMOUT OM count becomes equal to the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value. The log will be created when this feature suppresses a 'T1 Timer Expiry' message.

When a GAME102 log is created it will raise an external minor alarm. The alarm will need to be cleared before another log entry will be created through

the situation described earlier. The alarm will be cleared either by an operator or by this feature. The feature will clear the alarm during the second transfer period to pass after initially creating the log entry. The reason for doing this, will be to expose the alarm for long enough to get noticed by an operator. If the problem persists after clearing the alarm, then a new log will be created, as described earlier and as a consequence, a new external minor alarm will be raised.

3.3.2.2 Format

The log report format follows:

```
office * GAME102 mmmdd hh:mm:ss seqno INFO GAME_ERR_REPORT
REASON = reason_field
COUNT  = count_field
```

3.3.2.3 Example

An example of the log report follows:

```
S3_500_17BL CM GAME102 APR04 05:10:16 0504 INFO GAME_ERR_REPORT
REASON = Threshold reached for suppressing T1 Timer Expiry Messages
COUNT  = 100
```

3.3.2.4 Field descriptions

Table 2 Field descriptions

Field	Value	Description
reason_field	CONSTANT	A string describing that the number of times a 'T1 Timer Expiry' message was suppressed has reached the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value.
count_field	UNSIGNED INTEGER	A copy of the RSPTMOUT OM count value. It will be a number in the range from 1 to 32,767.

3.3.2.5 Action

If you frequently find a high number of GAME102 logs, it could be that you have the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value set too low. If this is the case, the threshold value should be modified according to the configuration recommendations.

If the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value is not too low, it could be a problem with the SCP.

If the T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value has been set accordingly, it could be a problem with the application T1 Timer value being set too low.

You should have your SCP first level support look into any of these problems.

3.3.2.6 Associated Operational Measurements or Performance Measurements

This feature monitors the RSPTMOUT OM count, found in the AIN OM group, checking to see if it increments to value equal to the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold. The count is incremented everytime the T1 timer expires and the SSP, as a consequence, attempts to generate a 'T1 Timer Expiry' message.

3.3.2.7 Additional information

N/A

3.4 Alarms

3.4.1 Alarm GAME102

This is a minor external alarm, that is associated with GAME102 log ("3.3.2 Log GAME102" on page 2024). This alarm indicates that Service Control Point (SCP) is not responding to each query and the T1 timers associated with each query is expiring.

3.5 Related documentation

1. 297-5161-022, Vol 1-3, AIN Service Enablers: Service Implementation Guides.

4: Fault Management (FM): A00002020

4.1 Fault management strategy

New ESA logs are generated whenever an attempt to generate an ESA data file succeeds or fails.

Existing ESA logs are generated when internal ESA data structures overflow.

4.2 Fault management tools and utilities

LOGUTIL

4.3 Logs

4.3.1 ESA 120 - ESA Data Generation

4.3.1.1 Explanation

Log Title: ESA120

Name: ESA Data Generation

Description:

An ESA120 is generated if the CS2000 successfully generates an MG9000 ESA data file in SFDEV. The file generation is initiated every 24 hours or from a manual command.

Event type: informational

4.3.1.2 Format

```
ESA120 mmmdd hh:mm:ss ssdd INFO ESA DATA GENERATION

ESA120 MAY20 01:00:40 2400 INFO ESA DATA GENERATION
```

4.3.1.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
ESA DATA GENERATION	constant	Successfully generation of file with MG9000 ESA data.

4.3.1.4 Action

Informational log only. Note that the MG9000 EM must download the ESA data to the MG9000 for it to be used during an emergency stand alone event.

4.3.1.5 Associated Operational Measurements or Performance Measurements

None.

4.3.1.6 Additional information

None.

4.3.2 ESA 121 - ESA Data Generation Fail

4.3.2.1 Explanation

Log Title: ESA121

Name: ESA Data Generation Fail

Description:

An ESA121 is generated if the CS2000 fails to generate an MG9000 ESA data file in SFDEV. The file generation is initiated every 24 hours or from a manual command. If the MG9000 goes into emergency stand alone then the last ESA data file successfully downloaded will be used.

Event type: non-critical failure.

4.3.2.2 Format

```
ESA121 mmmdd hh:mm:ss ssdd INFO ESA DATA GENERATION FAIL
MG9000 ESA WILL USE PREVIOUS DATA FILE

ESA121 MAY20 01:00:48 3500 INFO ESA DATA GENERATION FAIL
MG9000 ESA WILL USE PREVIOUS DATA FILE
```

4.3.2.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
ESA DATA GENERATION FAIL	constant	Failed to generate file with MG9000 ESA data.

Table 2 Field descriptions

Field	Value	Description
MG9000 ESA WILL USE PREVIOUS DATA FILE	constant	Last file successfully downloaded to the MG9000 EM and MG9000 will be used if an ESA event occurs.

4.3.2.4 Action

The MG9000 ESA data file ESA_SYSTEM_SD$XML failed to generate on the device specified by OFCENG parameter ESA_GWDATA_DEVICE.

The craftsperson should ensure there is enough room on the device and consider using a disk device instead of SFDEV.

4.3.2.5 Associated Operational Measurements or Performance Measurements

None.

4.3.2.6 Additional information

The MG9000 EM will continue to use the last valid ESA data file successfully downloaded.

Table DSLIMIT specifies the maximum allowed size of SFDEV in the STOREFS entry. This entry can not be set above 5 million words (10 million bytes).

4.4 Related documentation

[1] A00001982 - ESA Enhancements [MG9000] - version AA01 - March 2003- PLS FMDOC

[2] A00002019 - ESA EM Enhancements [MG9000 EM] - version AA01 - March 2003 - PLS FMDOC

5: Fault Management (FM): A00002146

5.1 Fault management strategy

The cside links of an ABI-hosted XPM will be managed from the new ABILink map level after posting an LGC-type XPM. (See Configuration section for more details of the map level and commands.) When a fault occurs on the cside links of an ABI-hosted XPM, an alarm will be raised on the XPM and will be visible under the PM heading of the alarm banner. This behavior will be the same as for existing ENET-hosted XPMs. When a cside link of an ABI-hosted XPM goes into or out of service, a new PM log will be generated.

5.2 Fault management tools and utilities

The alarm system and LOGUTIL are used to trouble shoot problems on the ABI XPM just as for other types of XPMs. The logs to look for are PM logs. Also, the MG9000 Element Manager should be used to manage the ABI cards which host the XPM.

5.3 Logs

A new PM log is defined for state changes on the cside links of an ABI-hosted XPM.

5.3.1 PM 610

5.3.1.1 Explanation

Log Title: PM 610

Name: State change log for ABI-XPM cside links

Event type: INFO

Description: A cside link of an ABI-hosted XPM has changed state. The log has no alarm level.

5.3.1.2 Examples

```
PM610 APR14 15:25:52 8700 INFO ABI XPM C-side Link State Change
       Node: LGC 3   Link: 1   Plane: 1   Port: 0
       From: InSv   To: ManB
       Reason: Manual action by user
```

```
PM610 APR14 15:26:23 8800 INFO ABI XPM C-side Link State Change
       Node: LGC 3   Link: 1   Plane: 1   Port: 0
       From: ManB   To: InSv
       Reason: Manual action by user
```

```
PM610 APR14 15:27:04 8900 INFO ABI XPM C-side Link State Change
       Node: LGC 3   Link: 1   Plane: 1   Port: 0
       From: InSv   To: SysB
       Reason: Port error detected by XPM
```

```
PM610 APR14 15:28:44 9000 INFO ABI XPM C-side Link State Change
       Node: LGC 3   Link: 1   Plane: 1   Port: 0
       From: SysB   To: InSv
       Reason: Link opened by MG9K/ABI
```

5.3.1.3 Format

```
PM610 <date> <time> <log_no> INFO ABI XPM C-side Link State Change
  Node: <pm_type> <pm_no>  Link: <link_no>  Plane: <plane_no>  Port: <port_no>
   From: <state>   To: <state>
   Reason: <reason_text>
```

5.3.1.4 Field descriptions

Table 1 Field descriptions

Field	Value	Description
date	mmmdd	month and day
time	hh:mm:ss	hour:minute:second
log_no	dddd	standard log number
pm_type	LGC, LTC, etc.	the pm_type of the host XPM
pm_no	integer	the external pm number of the host XPM
link_no	integer {0 to 31}	the cside link number
plane_no	integer {0 to 1}	the plane of the link -- corresponds to ABI card

Table 1 Field descriptions

Field	Value	Description
port_no	integer {0 to 15}	the port of the link
state	{INSV, CBSY, PBSY, SYSB, MANB}	the state of the link just prior to or just after the state change
reason_text	string	some additional information about the state change

5.3.1.5 Action

Depends on the state of the link:

- If the To state is InSv, the indicated link has returned to service. No further action is necessary.
- If the To state is ManB, a craftsperson has manually busied a link. No further action is necessary.
- If the To state is SysB, investigate why the link went SysB.
- If the To state is CBsy, the cside node (i.e. the GWC) has gone OOS. No communication with the link is possible.
- If the To state is PBsy, the pside node (i.e. the XPM) has gone OOS.

5.3.1.6 Associated Operational Measurements or Performance Measurements

none

5.3.1.7 Additional information

none

5.4 Alarms

In the area of CSide link maintenance, an ABI-hosted XPM will exhibit the same alarm behavior as an ENET-based XPM.

5.5 Related documentation

6: Fault Management (FM): A00002380

6.1 Fault management strategy

Exiting ESA for the ABI board will be controlled by the CM. Whenever an attempt to exit ESA, a new MAP indicator will be displayed on the posted ABI-hosted XPM (See Configuration section for more details of the new map indicator). In addition, PM181 informational logs are output whenever an attempt to exit ESA occurs.

6.2 Fault management tools and utilities

LOGUTIL is used to inform the craftsperson of the ABI board exiting esa. The logs to look for when the ABI board is exiting ESA are PM181 logs.

6.3 Logs

Existing PM181 logs are generated with new strings.

An ESA120 or ESA121 is output when an attempt is made to generate MG9000 ESA data. This is an existing capability of Activity A00002020 - ESA Translation Download. The format of these logs has not changed.

6.3.1 Explanation

Log Title: PM181

Name: Informational log for PMs (peripheral modules)

Description: The PM181 logs are generated when the ABI of an ABI-hosted XPM is attempting to exit esa, cannot exit, or successfully exit(s) esa. The log has no alarm level.

Event type: INFO

6.3.2 Format

This format of the PM181 is not documented in the NTP 297-9051-840, “DMS-100 Family MMP Log Report Reference Manual Volume 6 of 7 MMP15 and up”.

```
PM181 mmmdd hh:mm:ss dddd INFO pmid
Node:statxt, Unit0 actxt:statxt1, Unit1 actxt:statxt1
<string1>
<string2>
```

6.3.3 Examples

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI discovered in ESA
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI board cannot exit ESA
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:ManBUnit1 Act:ManB
COLD ABI ESA attempt started by Username : John
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Query Failed - Reason : No reply from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Query Failed - Reason : Bad message received from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Exit Failed - Reason : No reply from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Exit Failed - Reason : Bad message received from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Exit Force Failed - Reason : No reply from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA Exit Force Failed - Reason : Bad message received from ABI board
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA enter reason: ABI Loop around failed
ABI ESA Warm Entry/Cold Exit/Enabled
```

```
PM181 APR14 15:25:52 8700 INFO LGC 2
Node:SysB,Unit0 Inact:SysB(PM entered ESA)Unit1 Act:SysB(PM entered ESA)
ABI ESA enter reason: ABI megaco failed
ABI ESA Warm Entry/Cold Exit/Enabled
```

Field descriptions

Table 1 Field descriptions

Field	Value	Description
date	mmmdd	month and day
time	hh:mm:ss	hour:minute:second
log_no	dddd	standard log number
pmid	LGC 0	pm name and external pm number
statxt	{InSv, SysB, ManB, Cbsy}	state of XPM node
actxt	Act, InAct	activity of the XPM unit
statxt1	{InSv, SysB, ManB, Cbsy}	state of XPM unit
string1	ABI discovered in ESA	ABI ESA information
string2	ABI ESA Warm Entry/ Cold Exit	ABI ESA information which is optional

6.3.3.1 Action

- ***ABI discovered in esa*** log does not require any action.
- ***Cold ABI esa attempt*** log does not require any action.
- ***ABI ESA Failed*** log requires the craftsperson to inform their first-level support that there was a communication failure between the CM and the ABI.
- ***ABI board cannot exit ESA*** log requires the craftsperson to inform their first-level support that the ABI board is having problems exitting esa - check the element manager.
- ***ABI ESA Cold Exit*** log does not require any action.

6.4 Alarms

No alarms are generated by PM 181 logs.

6.4.1 ESA Failed to Exit

Alarm Format		
	Fault Type	“Failed to exit ESA“

Associated Alarm Message	“Failed to exit ESA”
Severity	MAJOR. Call functional will not be establish if this card is brought out of ESA
Cause or Condition	The messaging is down on the card.
Duration	Alarm will remain set until card restarts.
Cause / Prevent a SWACT	This alarm does go through Node Maintenance; it will cause a SWACT of any card; it will prevent a SWACT of any card.
Action / Clearing Procedure	none.
Association	There are no related Core logs, other alarms, or performance measurements.

6.4.2 New fault type for the ESA alarm

New fault type, failed to enter ESA, will be added to the MG9000 ESA alarm for the ABI ESA. This alarm will be displayed at MG9000 Eelemet Manager and MG9000 LCI..

Alarm Format	**Log Id**	“ESA302”
	Fault Type	“Failed to enter ESA“
Associated Alarm Message	“Failed to enter ESA”	
Severity	Critical. ESA call processing will not function at all, and there is no dial tone provided.	
Cause or Condition	The links between MG9000 and XPM are down.	
Duration	Alarm will remain set until the links between MG9000 and XPM recover.	
Cause / Prevent a SWACT	This alarm does not go through Node Maintenance; it will not cause a SWACT of any card; it will not prevent a SWACT of any card.	
Action / Clearing Procedure	Establish the links between MG9000 and XPM by manually restart both active and inactive ABI cards by the craftperson..	
Association	There are no related Core logs, other alarms, or performance measurements.	
Interfaces	MG9000 Element Manager and MG9000 LCI	

6.5 Related documentation

[1] NTP 297-9051-840, “DMS-100 Family MMP Log Report Reference Manual Volume 6 of 7 MMP15 and up”.

[2] Activity A00002020 - ESA Translation Download

7: Fault Management (FM): A00002433

7.1 Fault management strategy

7.1.1 Baseln Alarm

System alarm “Baseln” is raised whenever any XA-Core Field Replaceable Unit (FRU) installed in the shelf is not at Hardware (HW) or Firmware (FW) baseline. Only the Major level is used.
“ALARM Baseln” command will list the non-baseline components from MAPCI;MTC;XAC level, or its sub-levels.

1. Baseln alarm is raised due to HW issue when:
   a. Product Equipment Code (PEC) is missing from table PECINV
   b. Actual PEC HW release is less than PECINV baseline release
   c. Actual PEC HW release equals one of the PECINV exception releases
2. Baseln alarm is raised due to FW issue when:
   a. PEC is missing from table FWINV, and associated FRU has FW
   b. Actual PEC FW version is less than FWINV baseline version
   c. Actual PEC FW version equals one of the FWINV exception releases

7.1.2 Logs

1. New XAC337 FLT log is produced when:
   a. Baseln alarm is first raised
   b. Baseln alarm still raised, and non-baseline component list changes. The log lists all of the non-baseline components known.
2. New XAC637 INFO log is produced when Baseln alarm is cleared, due to an empty list of non-baseline components.
3. Existing XAC415 log adds “not at baseline” reason for not running the SREx test.

7.2 Fault management tools and utilities

7.2.1 MAPCI;MTC;XAC; ALARM BASELN

Returns a list of field replaceable unit (FRU) which are not at HW or FW baseline.

7.2.2 MAPCI;MTC;XAC; QUERY SHELF

Returns a list of FRU installed in the XA-Core shelf. Those FRU which are not at HW or FW baseline are indicated with a "*" in the OK column[s] - see CN section for more info.

7.2.3 LOGUTIL; OPEN XAC 337/637/415

XAC337 - list of components not at baseline
XAC637 - all components now at baseline
XAC415 - system state at time SREx test was bypassed, due to HW or FW not being at baseline.

7.2.4 Update HW

BSY, remove, and replace with correct PEC/release.

7.2.5 Update FW

FW is updated from MAPCI;MTC;XAC; <level> as per MTC manual steps, summarized briefly here:

a. update table XAFWLOAD PEC/NEW tuple to baseline FW (and HIOP DLL) version found in table FWINV

b. BSY <pos>; LOADFW <pos> FILE NEW; RTS <pos>
(Note that RTS downloads HIOP DLL during OOS TST)

c. update table XAFWLOAD by changing current to old, new to current

7.3 Logs

3 logs are detailed below: XAC415, XAC337, XAC637.

7.3.1 Explanation

Log Title: XAC415

Name: INFO Routine Exercise (REx) Report

Description:
Generated when SREx is bypassed, due to:

1 or more non-baseline PE|SM card being found in the XA-Core shelf. SREx is not impacted by FW being BELOW baseline on the PE, since FW is updated AFTER the ONP; however, SREx is not run if the PE/SM's entry is absent from FWINV, or it uses an exception version.

Event type: Log severity = MAJOR

7.3.2 Format

Figure 1 XAC415 Format and Example

```
<switch>      XAC415 <mmmdd hh:mm:ss ssd> INFO Routine Exercise (REx) Report
        INITIATOR      CLASS      RESULT
          System       <class>    Not Run
        Reason:<reason>
```

```
     **  XAC415 JAN08 19:47:22 5201 INFO Routine Exercise (REx) Report
            INITIATOR      CLASS      RESULT
             System        Full       Not Run
            Reason: XA-Core HW (PECINV) or FW (FWINV) is not at baseline
```

7.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
<class>	Existing list: "BASE", "ALL", "FULL", "IO", "PE", "SM"	SREx class requested.
<reason>	"XA-Core HW (PECINV) or FW (FWINV) is not at baseline" <other existing reasons>	Self-explanatory

7.3.4 Action

Investigate non-baseline components using:

1. LOGUTIL; OPEN XAC337 or
2. MAPCI;MTC;XAC;ALARM BASELN.

Update HW or FW/DLL as required.

7.3.5 Associated Operational Measurements or Performance Measurements

None.

7.3.6 Explanation

Log Title: XAC337

Name: FLT Baseln Alarm Raised

Description:
Log is produced when:

a. Baseln alarm is first raised

b. Baseln alarm still raised, and non-baseline component list changes. The log lists the non-baseline components known at generation time.

Event type: Log severity = MAJOR

7.3.7 Format

Figure 2 XAC337 Format and Example

```
**  XAC337 <mmmdd hh:mm:ss ssd> FLT  Baseln Alarm Raised
      Card/packlets below have non-baseline HW and/or FW.
      Investigate items with "N*" or U* in OK column.
                   - HW vs. PECINV -  -- Firmware vs. FWINV --
      Type FRU     PEC+Release BL OK  Typ Version  Baseline OK
      ---- ------  ----------- -- --  --- -------- -------- --
     <fru> <pos>   <pec+rel><rel><ok><fw_dll><fwname><fwname><ok>
```

```
**  XAC337 JAN15 22:55:35 7176 FLT  Baseln Alarm Raised
      Card/packlets below have non-baseline HW and/or FW.
      Investigate items with "N*" or U* in OK column.
                   - HW vs. PECINV -  -- Firmware vs. FWINV --
      Type FRU     PEC+Release BL OK  Typ Version  Baseline OK
      ---- ------  ----------- -- --  --- -------- -------- --
  eg. HIOP 14 R    NTLX14CA 01 02 N*  FW  XHIO02AH XHIO02AH Y
                                      DLL XHIO02AI XHIO02AH N*
      CMIC  4 R L  NTLX05AB 01 01 Y   FW  PK12CE12 ??       N*
      PE    4 F    NTLX02DA 01 ?? N*  FW  XAPE02AB XAPE02AB Y
      PE    5 F    NTLX02AA 01 ?? U*  FW  XAPE02AB XAPE02AB Y
```

7.3.8 Field descriptions

Table 2 Field descriptions

Field	Value	Description
fru	Valid fru names: cards: pe, iop, hiop, **sm** pklts: cmic, amdi, ethr, **disk, tape, rtif**	FRU (field replaceable unit) names. **Bolded** FRU have no FW.
pos	Slot number: 1-30 front/rear: F or R upper/lower: U or L	Position of FRU in XA-Core shelf.
pec	8 character alphanumeric. NTLXnnaa: n=0-9, a=A-Z	Product Equipment Code (PEC)

Table 2 Field descriptions

Field	Value	Description
rel	2 character alphanumeric. "00" through "ZZ"	HW rel
OK	2 chars: "Y " = Yes - at baseline "N*" = Non-baseline	Indicates if HW and/or FW is baseline compatible.
fw_dll	FW or DLL	Indicates if following fw_name field is for FirmWare or DLL.
fw_name	8 character alphanumeric.	Firmware load name.

7.3.9 Action

See *"7.3.4 Action" on page 2043*

7.3.10 Associated Operational Measurements or Performance Measurements

None.

7.3.11 Explanation

Log Title: XAC637

Name: INFO Baseln Alarm Cleared

Description:
Log is produced when alarm was raised, but now lowered, since no longer any non-baseline components.

Event type: Log severity = NONE

7.3.12 Format

Figure 3 XAC637 Format and Example

```
<switch>      XAC637 <mmmdd hh:mm:ss ssd> INFO Baseln Alarm Cleared
                <string>
```

```
XAC637 JAN15 23:13:26 4432 INFO Baseln Alarm Cleared
  All XAC HW at PECINV baseline. All XAC FW/DLL at FWINV baseline.
```

7.3.13 Field descriptions

Table 3 Field descriptions

Field	Value	Description
string	`All XAC HW at PECINV baseline. All XAC FW/DLL at FWINV baseline.`	XA-Core now at baseline.

7.3.14 Action

See *"7.3.4 Action" on page 2043*

7.3.15 Associated Operational Measurements or Performance Measurements

None.

7.4 Alarms

System alarm Baseln is added.
See *"Fault management strategy" on page 2041*, for alarm behaviour, and associated logs. The components listed should be investigated, and likely replaced. ALARM Baseln output simply lists the problem FRU and locations. More useful information appears in XAC337 log/QUERY SHELF outputs.

The alarm is cleared when no XA-Core components are non-baseline.

The output format for MAPCI; MTC; XAC; ALARM BASELN lists those components which are non-baseline.

Figure 4 ALARM BASELN Format

```
Alarm       Severity       Status
SysBTh      <sev     >     <Enabled/Disabled>
Cause                             Resource      State Slot/Pk/Dev
<cause>                           <res>         <st>  <slot > <dev>
....
<cause>                           <res>         <st>  <slot > <dev>

Where:
<sev>   = Cleared, Minor, Major, Critical
<cause> = HW or FW is non-baseline.
<res>   = NIL, PE, SM, IOP, HIOP, Tape, Disk, RTIF, CMIC,
          AMDI, ETHR, RTIFp, RTIFp, AMDIp, CMICp,
          AMDIl, CMICl, ETHRp, ETHRl, TOD};
<st>    = '     ', INSV, ISTB, SYSB, CBSY, MBSY, SPLT, UNEQ
<slot>  = <slot number> +  <' ' | F | R> +  <' ' | L | U>
<dev>   = ' ' | 0 | 1
```

Figure 5 ALARM SysBTh Example - alarm OFF

```
Alarm       Severity       Status
Baseln      Cleared        <Enabled/Disabled>
```

Figure 6 ALARM SysBTh Example - alarm ON

```
Alarm      Severity      Status
Baseln     Major         Enabled
Cause                              Resource     State Slot/Pk/Dev
HW or FW is non-baseline.          RTIF         INSV  15R  U
HW or FW is non-baseline.          IOP          INSV  15R
```

7.5 Related documentation

XA-Core Maintenance Manual - 297-8991-510.
XA-Core Reference Manual - 297-8991-810.

8: Fault Management (FM): A00002499

8.1 Fault management strategy

Three new logs are introduced by this feature to flag the detection of faults by the XA-Core Store Audit. There are existing STOR logs already defined for use by the audit which the new logs will augment.

8.2 Fault management tools and utilities

N/A.

8.3 Logs - STOR605

8.3.1 Explanation

Log Title: STOR605

Name: Store Bstree Corruption

Description: This log is output when the Store Audit has detected a corruption in the Bstree structures containing the information about the data address space STOR is responsible for.

Event type: Critical.

8.3.2 Format

Figure 1 STOR605 Format

```
HHHHHHH STOR605 mmmdd hh:mm:ss ssdd INFO Store Bstree Corruption
      Bstree nodes corrupt= XXXX
      Check SOSB Footprint data - STORE FP EVENT generated.
```

8.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Bstree nodes corrupt	1 - 9999	Number of problems detected by a single pass of the audit.

8.3.4 Action

The log text indicates to the support personnel that footprints should be collected. This log is only notification that a problem was detected; the detailed fault information is dumped in the SOSB footprints (with the title text

"STORE FP EVENT"). Once the details of the corruption(s) is analyzed further recovery action may be required. The corruption may be an invalid pointer or a bad state in the data, and may affect any store type. If DSTEMP is affected the corruption may be cleared by a core restart. If DSPROT is affected the core image may no longer be viable and a reboot or system SWACT may be needed to recover.

8.3.5 Associated Operational Measurements or Performance Measurements

None.

8.3.6 Additional information

None.

8.4 Logs - STOR606

8.4.1 Explanation

Log Title: STOR606

Name: Dump Data Corruption

Description: This log indicates that the Store Audit has found a corruption in the allocation information for data store which is dumped (such as DSPROT) and it is very likely that a attempt to perform a dump while in this state would fail.

Event type: Critical.

8.4.2 Format

Figure 2 STOR606 Format

```
HHHHHHH STOR606 mmmdd hh:mm:ss ssdd INFO Store Dump Data Corruption
      ADDR= XXXXXXXX STORTYPE= YYYYYYYY BLOCKSIZE= ZZZZZZZZ
```

8.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
ADDR	00000000 - FFFFFFFF (hexidecimal)	Address of the block of store flagged as corrupt.
STORTYPE	STORTYPE2 (module STOR)	Storetype of the corrupted block.

Table 2 Field descriptions

Field	Value	Description
BLOCKSIZE	00000000 - FFFFFFFF (hexidecimal)	Size in bytes of the corrupted block.

8.4.4 Action

Should these logs be generated the state of the system's allocation information for protected store is such that a valid image dump cannot be performed. Nortel Networks support personnel should be contacted immediately to further investigate the problem. If a valid image file exists then the system may need to be rebooted or otherwise restored to the valid image using a SWACT.

8.4.5 Associated Operational Measurements or Performance Measurements

None.

8.4.6 Additional information

None.

8.5 Logs - STOR607

8.5.1 Explanation

Log Title: STOR607

Name: Store Attribute Corruption

Description: This log is generated when the Store Audit detects a mismatch between the Store Allocator's internal setting of an address' blocking attribute and the actual setting of the attribute in memory hardware. The attribute is either blocking or write-blocking. An incorrect value could mislead the Store Allocator's initialization routines and cause traps.

Event type: Major.

8.5.2 Format

Figure 3 STOR607 Format

```
HHHHHHH STOR607 mmmdd hh:mm:ss ssdd INFO Store Attribute Corruption
      ADDR= XXXXXXXX ST2ATTR= YYYY HW_ATTR= ZZZZ
```

8.5.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
ADDR	00000000 - FFFFFFFF (hexidecimal)	Address of the block of store flagged as having mismatching attributes.
ST2ATTR	0 - blocking memory 1 - write-blocking memory 2 - attribute read error	Blocking attribute of the memory recorded internally by the Store Allocator.
HW_ATTR	0 - blocking memory 1 - write-blocking memory 2 - attribute read error	Blocking attribute of the memory as reported by hardware.

8.5.4 Action

In the event of blocking attribute mismatches being detected support personnel will have to investigate further. Footprints and logs should be collected, as well as FQT (Fault Query Tool) data to determine if any memory hardware failures have occurred.

If blocking attribute mismatches exist in the system, it is possible that there will be no other immediate symptoms as long as there is no Store Allocator activity related to the affected memory. However if a restart occurs the Store Allocator may be unable to correctly access this memory, and in the worst case a restart progression may lead to a system reboot. Thus, manual restarts should be avoided until technical support can determine exactly what memory is affected.

8.5.5 Associated Operational Measurements or Performance Measurements

None.

8.5.6 Additional information

None.

8.6 Related documentation

None at this time.

9: Fault Management (FM): A00002510

9.1 Fault management strategy

9.2 Fault management tools and utilities

9.3 Logs

9.3.1 Explanation

Log Title: ITN307

Name:

Descriptio

XASKY07BD ITN313 SEP30 11:09:34 8200 INFO IP TRANSMIT FAILED

NODE:CM

Route to Destination Known but Unavailable

SRC IP: 47.129.216.60

DST IP: 47.80.0.209

Event type:

9.3.2 Format

9.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description

9.3.4 Action

9.3.5 Associated Operational Measurements or Performance Measurements

9.3.6 Additional information

9.4 Related documentation

10: Fault Management (FM): A00002549

10.1 Fault management strategy

N/A

10.2 Fault management tools and utilities

N/A

10.3 Logs

10.3.1 Explanation

Log Title: AUDmmm & XAUDnnn (where mmm & nnn are numeric values)

Name: Call Processing Resource Dump

Description: XAUD logs are generated whenever a call processing resource is recovered by the audit process running on the XA-Core platform. AUD logs are generated/used by all other non-audit processes.

The numeric values for the XAUD logs used to cover the range from 600 to 610 for standard resources (ie. XAUD600, XAUD601, XAUD602, and XAUD609) and 700 to 955 for extension block resources. The numeric values for the XAUD logs are being extended and changed to match those for the AUD logs for simplicity. The new numeric values for the XAUD logs will now be 395, 397, 432, 434 and ranges from 400 to 431 and 500 to 982. A table is being included below (in the 'Additional Information' section 12.3.6) to illustrate the new numbering system for the XAUD logs.

Please note, the total number of AUD and XAUD logs will vary from load to load. This feature is not adding more AUD or XAUD logs to the load, it is only setting the framework so that applications will be able to add more in the future.

The size, format and contents for the AUD and XAUD logs of standard resources is not being changed. However, the location and number of bits used to represent the extension block's format code in the header (within the hex dump of the log) has changed for all extension block logs. **The only noticeable difference to the cutomer will be the number following the XAUD string in the log title**.

Event type: INFO

10.3.2 Format

No change to the format of the AUD or XAUD log (originally defined by feature ACT.A19011742). A sample format is being included for reference.

General format of all XAUD logs:

```
XAUD<nnn> <date> <time> <sequence> INFO <resource> Recovery
  REMARK: <remark>
  PTR: <item> INDEX: <prim> <sec> CURRENT AUDIT GENERATION: <gen>
  STATE: <state> PROBLEM: <problem>
  <hex dump>
```

Sample of an encapsulator recovery log (standard resource):

```
XAUD397 APR29 10:34:37 2900 INFO Encapsulator Recovery
  REMARK: Associated CCB queue is empty
  PTR: 4B1EF920  INDEX: 0001 000F  CURRENT AUDIT GENERATION: 00BD
  STATE: UNAVAILABLE_ENC  PROBLEM:   ERROR_LINKS
  444B B9D4 0000 0001 0001 FDCF 7BCD FDFD FDFD FDFD
  FDFD FDFD FDFD FDFD FDFD FDFD FD72 0001 0000 FDFD
  FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD
  FDFD FDFD FFFF 0000 FD02 FFFF 0000 FFFF 0000 0000
  FDFC FFFF 0000 FDFD FDFD FDFD FDFD FDFD
```

The total size of the extension block header has not been increased and hence the total size of the hex dump has not been increased. However, the location and number of bits used to represent the extension block format code in the header portion of the hex dump has changed for all extension block logs.

Sample hex dump portion of an extension block recovery log:

```
<XAUD or AUD log title>
<hex_dump>:
   FFFF 0000 7340 FCF5 FDFD FDFD FDFD FDFD FDFD FDFD
   FDFD FDFD FDFD FDFD FDFD FDFD
```

The extension format code will now be 9-bits starting at offset 6 (ie. 14th hex digit) in the hex dump. As illustrated in the above, the format code will be 9-bits of CF5.

```
ie. CF5 hex = 1100 1111 0101 bin ==> FORMAT CODE = 245
only the right most 9-bits of the 14th, 15th and 16th hex digits in
the hex dump will be used to represent the format code. In this case
the format code is 245. The remaining three bits of the 14th hex
digit are unused at present.
```

10.3.3 Field descriptions

No change. The field descriptions are being provided here for reference.

Table 1 Field descriptions

Field	Value	Description
nnn	numeric	Value from ranges outlined in description above
date	date	System supplied, when the recovery happened
time	time	System supplied, when the recovery happened
sequence	numeric	System supplied, sequence within log system
resource	text	Name of the resource recovered

Table 1 Field descriptions

Field	Value	Description
remark	text	Further clarification as to why it was recovered
item	hex numeric	Memory address of item
prim	hex numeric	Primary index into item's resource pool
sec	hex numeric	Secondary index into item's resource pool
gen	hex numeric	Audit generation when recovered
state	text	State of item at the time of recovery
problem	text	Description of problem that resulted in the log
hex dump	hex numeric	Multi line dump of the contents of the resource

10.3.4 Action

No immediate action required.

10.3.5 Associated Operational Measurements or Performance Measurements

N/A

10.3.6 Additional information

New mapping of XAUD log numbers being introduced by this feature.:

Table 2 *New mapping for Standard resources*:

AUDnnn	Old XAUDxxx	New XAUDnnn
AUD397	XAUD600	XAUD397
AUD395	XAUD601	XAUD395
AUD432	XAUD602	XAUD432
AUD434	XUAD609	XAUD434

Table 3 *New mapping for extension block resources*

AUDnnn	Old XAUDxxx	New XAUDnnn
AUD400	XAUD700	XAUD400
AUD401	XAUD701	XAUD401
...	...	...
AUD430	XAUD730	XAUD430
AUD431	XAUD731	XAUD431

Table 3 *New mapping for extension block resources*

AUDnnn	Old XAUDxxx	New XAUDnnn
AUD500	XAUD732	XAUD500
AUD501	XAUD733	XAUD501
...	...	...
AUD708	XAUD940	XAUD708
AUD709	XAUD941	XAUD709
AUD979	XAUD942	XAUD979
AUD980	XAUD943	XAUD980
AUD981	XAUD944	XAUD981
AUD982	XAUD945	XAUD982
AUD714	XAUD946	XAUD714
AUD715	XAUD947	XAUD715
...	...	...
AUD723	XAUD955	XAUD723
AUD724	N/A	XAUD724
AUD725	N/A	XAUD725
...	...	...
AUD977	N/A	XAUD977
AUD978	N/A	XAUD978

10.4 Related documentation

XAUD logs were originally introduced by the Call Processing Resource Audit Robustness Feature (ACT.A19011742). Additional information can be found in the PLS FMDOC library if required.

11: Fault Management (FM): A00002607

11.1 Fault management strategy

This feature does not expect to modify existing logs or create new logs. This feature will, as a positive side effect, correct existing logs SITE data for XPMs involved in ABI Configurations.

The ABI XPM Location component of this feature, which allows for the provisioning of ABI XPMs Site and hosting MG9K information, will have a beneficial impact on some existing logs. These logs are the ones mainly associated with XPM peripherals, PM logs. The impact will take the form of the log containing the correct SITE name for these ABI XPMs. As mentioned in the DID, XPMs generally had “HOST” as their Site name.

11.2 Fault management tools and utilities

N/A

11.3 Related documentation

12: Fault Management (FM): A00002757

12.1 Fault management strategy

This feature provides functionality to a SSPFS Platform for the aggregation of Alarms into one database. Logs will be generated by the reporting entity when using the *Reporting API* to enter/update/clear alarms in the database.

12.2 Fault management tools and utilities

Two command line tools will be available to report and query faults contained in the *Alarm Database*.

The tools are called *queryflt*, and *reportflt*.

12.3 Logs

12.3.1 Explanation

Log Title: Report Alarm

Name: Report Alarm Log

Description:

This log is sent when requested by the entity that is reporting an alarm.

Event type: Customer Log

12.3.2 Format

```
_V2_~I=CBM~H=<hostname>~A=<application>~S=<seqNum>~~
<reportName><reportNum> <alarmLevel> <eventType> <description>
      TimeStamp: <timeStamp>
      ComponentID: <componentID>
      Category: <categoryString>
      Probable Cause: <probableCauseStr>
      Specific Problem: <specificProblemStr>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

12.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
hostname	variable	Hostname of the cluster on which the log is being generated.

Table 1 Field descriptions

Field	Value	Description
application	variable	Name of the application for which the alarm is raised.
seqNum	variable	Sequence number of the log being generated.
reportName	variable	The Customer Log report name (e.g.: CBM)
reportNum	variable	The Customer Log report number (e.g.: 300).
alarmLevel	variable	The alarm level for this alarm, one of: Cleared, Warning, Minor, Major, Critical, or Indeterminate.
eventType	variable	The Customer Log event type. This is eAlarmEventType.
description	variable	Description for this particular alarm. Not describing the problem that happened, but describing what the alarm relates to or represents.
timeStamp	variable	This is the time at which the alarm was raised.
componentID	variable	This field is specified by the application to include the name of the component being alarmed (see definitions in section “1.7.4 Use of component name” on page 33 for details of how to specify this field).

Table 1 Field descriptions

Field	Value	Description
categoryString	variable	The alarm category for this alarm. This is eAlarmProblemCategory.
probableCauseStr	variable	This is eAlarmProbableCause
specificProblemStr	variable	Further qualifies the probable cause for this alarm.

12.3.4 Action

The action required is dependent on what the particular alarm report is. Any specific action will be described in the *description* field above.

12.3.5 Associated Operational Measurements or Performance Measurements

N/A

12.3.6 Additional information

12.3.7 Explanation

Log Title: Clear Alarm

Name: Clear Alarm Log

Description:

This log will be generated when a client clears an existing alarm in the alarms database managed by Alarmd.

Event type: Customer Log

12.3.8 Format

```
_V2_~I=CBM~H=<hostname>~A=<application>~S=<seqNum>~~
<reportName><reportNum> NONE <eventType> <description>
      ComponentID: <componentID>
      Category: <categoryString>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

12.3.9 Field descriptions

Table 2 Field descriptions

Field	Value	Description
hostname	variable	Hostname of the cluster on which the log is being generated.
application	variable	Name of the application for which the alarm is raised.
seqNum		Sequence number of the log being generated.
reportName	variable	The Customer Log report name (e.g.: CBM)
reportNum	variable	The Customer Log report number (e.g.: 300).
eventType	variable	The Customer Log event type. . This is eAlarmEventType.
description	variable	Description for this particular alarm. Not describing the problem that happened, but describing what the alarm relates to or represents.
componentID	variable	This field is specified by the application to include the name of the component being alarmed (see definitions in section “1.7.4 Use of component name” on page 33 for details of how to specify this field).

Table 2 Field descriptions

Field	Value	Description
categoryString	variable	The alarm category for this alarm. This is eAlarmProblemCategory.

12.3.10 Action

No action required.

12.3.11 Associated Operational Measurements or Performance Measurements

N/A

12.3.12 Additional information

N/A

12.3.13 Explanation

Log Title: Alarm Summary

Name: Alarm Summary Log

Description:

This log is sent periodically by Alarmd, to summarize the Alarms in the database managed by Alarmd.

Event type: Customer Log

12.3.14 Format

```
_V2_~I=CBM~H=<hostname>
       TimeStamp: <timeStamp>
       Minor: <minorCount>
       Major: <majorCount>
       Critcal: <criticalCount>
       Most Recent Minor: <MRMinorComponentID>
       Most Recent Major: <MRMajorComponentID>
       Most Recent Critical: <MRCriticalComponentID>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

12.3.15 Field descriptions

Table 3 Field descriptions

Field	Value	Description
hostname		
timeStamp		
minorCount		
majorCount		
criticalCount		
MRMinorComponentID		
MRMajorComponentID		
MRCriticalComponentID		

12.3.16 Action

12.3.17 Associated Operational Measurements or Performance Measurements

N/A

12.3.18 Additional information

N/A

12.3.19 Explanation

Log Title: Alarmd (Data Collection service) generated alarm

Name: SDM 330

Description: This log is a special case of the “Report Alarm” log described in section “12.3.1 Explanation” on page 2060.

The distinction is that this log is generated directly by the data collection thread alarmd process when it detects a problem situation; rather than by a “client” process using alarmd. The format is the same as the “Report Alarm” log, but it’s log name and number are fixed.

Event type: Customer Log

12.3.20 Format

```
<log office id> <ECORE> *  SDM330 APR28 13:39:17 4668 FLT  Alarm raised or updated.
        <description>
```

```
<log office id> <ECORE> *  SDM330 APR28 13:39:17 4668 FLT   Alarm raised or
updated.
         <description>
         TimeStamp: <imeStamp>
         ComponentID: <componentID>
         Category: <categoryString>
         Probable Cause: <probableCauseStr>
         Specific Problem: <specificProblemStr>
```

12.3.21 Field descriptions

Table 4 Field descriptions

Field	Value	Description
description	Alarmd Data Collection from mate node timed out or Incompatible Payload version from mate node Alarmd	The alarmd processes on both system of a HA cluster cannot exchange data because of inter-system communication error The two nodes in a HA cluster are running different software versions, and the alarmd is unable to understand the messages from its peer because of a protocol change
timeStamp	variable	This is the time at which the alarm was raised.
componentID	<profile>=<clusterName>;NODE=<clusterName>-unit<no>	Identifies the remote node
categoryString	variable	The alarm category for this alarm.
probableCauseStr	variable	
specificProblemStr	variable	Further qualifies the probable cause for this alarm.

12.3.22 Action

12.3.23 Associated Operational Measurements or Performance Measurements

N/A

12.3.24 Additional information

N/A

12.4 Related documentation

13: Fault Management (FM): A00002823

13.1 Fault management strategy

An Ethernet connected SDM or CBM will report it's alarms independantly of the core. However, logs will be generated on the core to indicate connection status as seen by the core to assist in correlation of application alarms.

While a loss of connectivity log will contain an alarm level, no alarms are raised on the MAPCI alarm banner by this activity.

13.2 Fault management tools and utilities

Current connectivity status is available with the CI tool OAMPPCI.

Core connectivity logs are available via LOGUTIL.

13.3 Logs

13.3.1 Explanation

Log ID: OAMN600

Description: Generated when heartbeats are established between the SDM or CBM process oammtce and the Core process oampnmpp.

Event type: INFO

Event label: OAMP Node Status

13.3.2 Format

```
header
        Cluster number: 1 Node: <A or B>
        Core address:               <IRM IP address>
        Cluster address:            <CBM floating address>
        Cluster Heartbeat Status:   <heartbeat status>
        Cluster Application Status: <application started or stopped>
        Node A address:             <CBM/SDM fixed address>
        Node A heartbeat Status:    <heartbeat status>
        Node A Application Status:  <application started or stopped>
        Node B address:             <CBM/SDM fixed address>
        Node B heartbeat Status:    <heartbeat status>
        Node B Application Status:  <application started or stopped>
```

13.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Cluster number:	1	The number of the cluster connected to the Core. Only 1 is currently supported.
Node:	A or B	The node, within a cluster, which is reporting a change. For CBM HA this can be either A or B. For CBM simplex and SDM this will always be A. Note that there is no relationship between A and B and CBM units 0 and 1. A corresponds to the first node to connect to the core.
Core address:	nnn.nnn.nnn.nnn	The Core side IP address which is being used by the SDM or CBM.
Cluster address:	nnn.nnn.nnn.nnn	The floating address of the CBM cluster or the node address of an SDM.
Cluster Heartbeat Status:	Unequipped	Resetipaddress command has been executed from oamppci to delete a non-heartbeating ip address.
	No heartbeat	The SDM or CBM has stopped heartbeating to the Core from this Node.
	heartbeat received	This SDM or CBM node is currently heartbeating with the Core
Cluster Application Status:	unknown	The SDM or CBM has not supplied an application status on any connected nodes.
	applications stopped	All the SDM or CBM applications have been stopped on all connected nodes.
	Applications started	The SDM or CBM applications have been started with the exception of those which have been individually selected and stopped on one of the connected nodes.
	Switch Activity	Both Nodes are currently reporting applications started. This can happen on some CBM failure scenarios.

Table 1 Field descriptions

Field	Value	Description
Node A address:	nnn.nnn.nnn.nnn	The node address of an CBM or SDM
Node A Heartbeat Status:	Unequipped	Resetipaddress command has been executed from oamppci to delete a non-heartbeating ip address.
	No heartbeat	The SDM or CBM has stopped heartbeating to the Core from this Node.
	heartbeat received	This SDM or CBM node is currently heartbeating with the Core
Node A Application Status:	unknown	Either the SDM or CBM node has not supplied an application status or it has stopped heartbeating.
	applications stopped	All the SDM or CBM applications have been stopped on this node.
	Applications started	The SDM or CBM applications have been started with the exception of those which have been individually selected and stopped on this node.
Node B address:	nnn.nnn.nnn.nnn	The node address of an CBM or SDM
Node B Heartbeat Status:	Unequipped	Either Node B has never contacted the Core OR the resetipaddress command has been executed from oamppci to delete a non-heartbeating ip address.
	No heartbeat	The SDM or CBM has stopped heartbeating to the Core from this Node.
	heartbeat received	This SDM or CBM node is currently heartbeating with the Core
Node B Application Status:	unknown	Either the SDM or CBM node has not supplied an application status or it has stopped heartbeating
	applications stopped	All the SDM or CBM applications have been stopped on this node.
	Applications started	The SDM or CBM applications have been started with the exception of those which have been individually selected and stopped on this node.

13.3.4 Action

This is an information log which may not require action. The SDM or CBM generates its own alarms and logs.

13.3.5 Associated Operational Measurements or Performance Measurements

None

13.3.6 Additional information

Example:

```
XA1_PPC07BR     OAMN600 JAN15 02:28:32 5000 INFO OAMP Node Status
        Cluster number: 1 Node: A
        Core address:               10.40.14.200
        Cluster address:            10.40.14.241
        Cluster Heartbeat Status:   Heartbeat Active
        Cluster Application Status: Applications started
        Node A address:             10.40.14.242
        Node A Heartbeat Status:    Heartbeat Active
        Node A Application Status:  Applications stopped
        Node B address:             10.40.14.243
        Node B Heartbeat Status:    Heartbeat Active
        Node B Application Status:  Applications started
```

13.4 Related documentation

None

14: Fault Management (FM): A00002858

14.1 Fault management strategy

The purpose of the “SPM Node ISTb for Carrier Outage” feature is to mark an SPM as ISTb so an indicator appears under the PM Map banner whenever one of these carrier faults appear:

1. Any of the SPMs carriers goes SysB.
2. Any of the SPM’s line carriers (STS3L or STM1M) has an RFI (Remote Failure Indicator) alarm.

The new steps for resolving these faults will be integrated into the existing Succesion fault management documentation for troubleshooting SPM ISTb faults.

Note that the OPTFN section of this A00002858 feature document provides an easier to follow format for troubleshooting these faults. The OPTCN section documents the changes to the QUERYPM FLT REASON command. This OPTFM section documents changes to the impacted logs.

14.2 Fault management tools and utilities

No new tools. Existing tools used are MAPCI and LOGUTIL.

14.3 Logs

There are no new logs introduced by this feature, but some existing logs will act as triggers to cause the SPM node to go ISTb on the MAP, and there will be some modifications to existing logs.

14.3.1 CARR511 for SPM carrier going SysB

The CARR511 log is the first of the two new triggers than can cause the SPM node to get ISTb under the PM banner of the MAP display.

14.3.1.1 Explanation

Log Title: CARR511

Name: SYSB CARRIER SPM

Description: Generated when an SPM carrier changes state to SysB.

Event type: minor

14.3.1.2 Format

Existing log with no changes, so just showing an example:

```
MSH706BM   * CARR511 JUN04 05:46:03 6200 SYSB CARRIER SPM  34
                CKT: 13  CarrName: SPM34_STS1P_1_VT15P_3_DS1P_3
                Carrier: STS1P  1 VT15P 15 DS1P   1
                Previous State: INSV
```

14.3.1.3 Action

Follow the standard procedures for maintenance of a SysB SPM carrier.

14.3.1.4 Associated Operational Measurements or Performance Measurements

None

14.3.1.5 Additional information

CARR511 is generated when one of the OC3's carriers goes SysB, which corresponds to a Bellcore state of OOS-AU-FAF (which is same as OC3 carrier state of IS-UPS-FAF). FAF is FAcility Failure. While the carrier is SysB, any of its trunks will be in the CFL condition and not able to bear traffic.

For STM-1 international product, this log will occur when a STM-1 carrier goes SysB.

14.3.2 CARR310 for SPM line carrier raising RFI alarm

The CARR310 log is the second of the two new triggers than can cause the SPM node to get ISTb under the PM banner of the MAP display.

14.3.2.1 Explanation

Log Title: CARR310

Name: FLT CARRIER SPM

Description: Generated when an SPM line carrier (STS3L or STM1M) raises an RFI (Remote Fault Indicator) alarm.

Event type: minor

14.3.2.2 Format

Existing log with no changes, so just showing an example:

```
MSH8_03BM   * CARR310 APR18 10:27:41 3204 FLT  CARRIER SPM  41
                CKT: 178  CarrName: ATM_STS3L_SPM_41_CKT_178
                Carrier: RM     2 OC3S   0 STS3L  0
                Failure: RFI     Set
```

14.3.2.3 Action

Follow the standard procedures for maintenance of a SPM carrier fault.

14.3.2.4 Associated Operational Measurements or Performance Measurements

None

14.3.2.5 Additional information

The CARR310 log above is generated when one of the OC3'sInSv STS3L carriers has a RFI (Remote Failure Indication) alarm. Such an alarm can be caused by cutting the TX fiber on the OC3. Note that this trigger corresponds to "R" (for Remote alarm) in the A59036987 feature. Since OC3 sparing will not be allowed while the remote alarm condition is present on the line carrier, the OC3 is effectively in an E2 outage condition due to the loss of redundancy.

If the RFI alarm is set as NRPT (non-reportable) for the carrier in Table MNHSCARR, then the log will not be seen but the trigger will still occur. Note that the CI command:

MAPCI;MTC;TRKS;CARRIER;POST {carrier};LISTALM

will always show the presence of the alarm, independent of whether MNHSCARR sets the alarm as RPT or NRPT for the carrier.

This trigger/log clears when the RFI alarm clears (as reported by a CARR310 "RFI Clear" log).

For STM-1 international product, trigger will occur when a InSv STM1M carrier has a RFI alarm.

14.3.3 SPM300 for SPM carrier going SysB

The existing SPM300 log will occur for a new reason: a OC3 carrier going SysB. The SPM300 log shows why a OC3 RM went ISTb.

14.3.3.1 Explanation

Log Title: SPM300

Name: Device Fault Report / Check SysB Carrier

Description: generated when an OC3 has no SysB carriers and one of its carriers goes SysB.

Event type: minor

14.3.3.2 Format

Existing log that now has a new text reason beside the “7A” row:

```
STEC207AM   *  SPM300 MAY30 15:57:33 4093 TBL  Device Fault Report
      Location   : SPM : 26   OC3 : 0
      Status     : Alarm Raised
      Problem Description: Non Critical
       7A: Check SysB Carrier
      Action     : Refer to NTPs for Alarm Clearing Procedures.
      Cardlist   :
       No Cardlist Available.
```

14.3.3.3 Action

See troubleshooting chapter of OPTFN section for how to determine which carrier caused this log to occur.

14.3.3.4 Associated Operational Measurements or Performance Measurements

None

14.3.3.5 Additional information

None

14.3.4 SPM300 for RFI Alarm on STS3L Carrier

The existing SPM300 log will occur for a new reason: RFI alarm occuring on a STS3L carrier. The SPM300 log shows why a OC3 RM went ISTb.

14.3.4.1 Explanation

Log Title: SPM300

Name: Device Fault Report / Check RFI Alarm on STS3L Carrier

Description: generated when a STS3L carrier experiences an RFI alarm.

Event type: minor

14.3.4.2 Format

Existing log that now has a new text reason beside the “7A” row:

```
STEC207AM   *  SPM300 MAY30 15:57:33 4093 TBL  Device Fault Report
       Location   : SPM : 26   OC3 : 0
       Status     : Alarm Raised
       Problem Description: Non Critical
        7A: Check RFI Alarm on STS3L Carrier
       Action     : Refer to NTPs for Alarm Clearing Procedures.
       Cardlist   :
```

14.3.4.3 Action

See troubleshooting chapter of OPTFN section for how to determine which carrier caused this log to occur.

14.3.4.4 Associated Operational Measurements or Performance Measurements

None

14.3.4.5 Additional information

None

14.4 Alarms

There are no new or changed alarms for this feature.

14.5 Related documentation

None

15: Fault Management (FM): A00002970

15.1 Fault management strategy

This feature introduces a new field, ‘SITE’, in Table MNNODE for SMG4 variant of SPMs.

Hence the logs displaying site name will now show the site name data that is present in Table MNNODE and not ‘HOST’, as it showed prior to this feature.

15.2 Fault management tools and utilities

None.

15.3 SPM 300 Log

15.3.1 Explanation

Log Title: SPM300

Name : Device Fault Report

Description: This is an existing Log. The only changes occuring as a result of this feature are that the log will now show the ‘*site*’ name as the one that is datafilled in Table MNNODE.

Event type: IDM related logs that are transferred from the local.

15.3.2 Format

Not impacted.

Example 1

```
MG4K106BT   *  SPM300 JUN18 06:21:55 2700 TBL  Device Fault Report
          Location   : SPM : 62   SRM : 0
          Status     : Alarm Raised
          Problem Description: Non Critical
            Sync RM non critical fault(s) still present
          Action     : Refer to NTPs for Alarm Clearing Procedures.
          Cardlist   :
            Site    Flr  Row   FrPos    ShfPos    ShfPec       Slot

            REM1    1    B     13       40        NTLX72BA     1
```

Example 2

```
MG4K106BB   ***  SPM300   JAN28   22:58:01   6900  TBL  Device Fault Report
           Location   :     SPM  :  61    DLC : 0
           Status      : Alarm Raised
           Problem Description: Critical
           8I          : Cfg Failure, Intended Recovery Ac
           Action       : Replace the following cards in the order listed.
           Cardlist     :
           Site    Flr  Row   FrPos    ShfPos    ShfPec     Slot
           REM1    1     B      13        40       NTLX72BA     1
```

15.3.3 Field descriptions

Table 1 shows the fields in Log ‘SPM 300’ impacted as a result of this feature, ACT.A00002970.

Table 1 Field Descriptions

Field	Value	Description
SITE	This field will show the site name present in Table MNNODE, for that SPM.	In SN06 and previous releases, Log ‘SPM 300’ always showed the value, ‘HOST’ under field ‘site’. From Release SN07 onwards it will show the ‘site’ value present in Table MNNODE.

15.3.4 Action

None.

15.3.5 Associated Operational Measurements or Performance Measurements

None.

15.3.6 Additional information

None.
None.

15.4 Related documentation

1. A00002970 in PLS FMDOC.

16: Fault Management (FM): A00003371

16.1 Fault management strategy

The Common Inventory and Data Consolidation A00003371 feature is focused on the CMT network element data and database access. As such new customer logs will be generated to notify the system operators of note worthy database access events as per the Nortel standard document:

Log reporting Rules and guidelines

DIS Ref: IEMPG DIS No: AF01 Release: Standard

All Logs created apply the principles and comply with the formats specified in the standard. Also nomenclature or identifiers already in use will be used where possible.

Note that none of the logs created initiate operator actions. The event being logged are failures to obtain a database connection. These can occur when a resource limit has been exceeded, when a database password is changed or when the database server has stopped or restarted.

The following identifies the general format of the CS2M database access Logs created by this activity.

The general format for all logs is given in the next subsection. Specific Logs are defined further on in this document.

16.1.1 Log Header Formats

The SCC2 log header is organized as follows:

<severity> <minute> <LogName/Num> <sequence number> <logtype> <device type> <Event Label>

For Nortel Standard format, the header is organized as follows:

<CM CLLI> <severity> <logname/num> <mmmdd hh:mm:ss> <sequence number> <logtype> <device id> <Event Label>

Where:

Severity is NOA

Minute or mmmdd hh:mm:ss is minutes of the day or month, day, hour, minute

LogName/Num is CMTxxx where xxx is in the range 600 - 799

Sequence Number is number internally generated

LogType is INFO

Device Type is SESM

Event Label describes the event that occurred

16.1.2 Log Body Format

The body of logs will be the same for both Nortel and SSC2 formats:

Location: SSPFS=hostname
Information: <Detected problem>
Time: <MMM dd hh:mm:ss YYYY>
Component Id: Database
Specific Problem: <Specific problem>
Description: <short text description

16.2 Fault management tools and utilities

Not applicable

16.2.1 Faults, Alarms and Logs

16.3 Logs

16.3.1 Database Stopped Log

Log Title:DB600

16.3.1.1 Formats

NTSTD log format:

RTP2 DB600 SEP23 17:25:00 0401 INFO DB Connection Error

Location: SSPFS=wnc0s0jd
Information: I/O error, the database did not respond
Time: SEP23 17:25:00 2003
Component Id: Database, GWCEM User
Specific Problem: I/O error was detected when attempting to get a database connection.
Description: Transient error detected. The database maybe stopped for administrative actions. Investigate when this log occurs repeatedly.

Table 1 Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	600
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	I/O error, the database did not respond
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	I/O error was detected when attempting to get database connection.
Description	Transient error detected. The database maybe stopped for administrative actions. Investigate when this log occurs repeatedly.

16.3.1.2 Explanation

This Log is generated when an attempt to allocate a database connection encounters an I/O error. These errors can occur when the database has been stopped momentarily for administrative purposes. A few occurrances of this

log is informational. Continuous occurances within a 15 minutes or a half hour should be investigated to insure these errors are attributable to specific authorized administrative actions.

16.3.1.3 Action

Monitor for multiple occurances within a 15 minutes or a half hour for the same “Component Id”.(Note: It is expected that a Log will be generated for multiple different “Component Ids”.) If this is detected investigate to insure these errors are attributable to specific authorized administrative actions. If these are occurring and are not caused by administrative activity then verify the database on the SSPFS machine identified is functioning normally.

16.3.2 Database Connection Closed Log

Log Title:DB601

16.3.2.1 Formats

NTSTD log format:

RTP2 DB601 SEP23 17:25:00 0401 INFO DB Connection Error
Location: SSPFS=wnc0s0jd
Information: Database connection closed, stale connections will refresh.
Time: SEP23 17:25:00 2003
Component Id: Database, GWCEM User
Specific Problem: A closed or stale database connection was detected, all stale connections will be refreshed..
Description: Transient error detected. Investigate when a threshold is exceeded in a short time.

Table 2 Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	601
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error

Table 2 Log Field descriptions

Field	Value
Location	SSPFS=hostname
Information	Database started, stale connections were refreshed
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	A closed or stale database connection was detected, all stale connections were refreshed.
Description	Transient error detected. Investigate when a threshold is exceeded in a short time

16.3.2.2 Explanation

This Log is generated when an attempt to allocate a database connection encounters detects that the connection is already closed. These errors can occur when the database has been stopped momentarily and then again started. A single occurrance of this log is informational. Multiple occurances within a 15 minutes or a half hour for the same “Component Id” should be investigated to insure these errors are attributable to specific authorized administrative actions.

16.3.2.3 Action

Monitor for multiple occurances within a 15 minutes or a half hour for the same “Component Id”.(Note: It is expected that a Log will be generated for multiple different “Component Ids”.) If this is detected investigate to insure these errors are attributable to specific authorized administrative actions. If these are occurring and are not caused by administrative activity then verify the SSPFS machine identified is functioning normally.

16.3.3 Database Password Changed Log

Log Title:DB602

16.3.3.1 Formats

NTSTD log format:

RTP2 DB602 SEP23 18:25:00 0402 INFO DB Connection Error
Location: SSPFS=wnc0s0jd
Information: User password has changed
Time: SEP23 17:25:00 2003
Component Id: Database, GWCEM User
Specific Problem: Invalid password was detected on a database connection, the new password is now in use for this database user.
Description: Transient error detected. When a threshold is exceeded in a short time, investigate to insure security violations or unauthorized access are not the cause.

Table 3 Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	602
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	I/O error, stale connections were refreshed
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Invalid password was detected on a database connection, the new password is now in use for this database user.

Table 3 Log Field descriptions

Field	Value
Description	Transient error detected. When a threshold is exceeded in a short time, investigate to insure security violations or unauthorized access are not the cause.

16.3.3.2 Explanation

This Log is generated when an attempt to allocate a database connection encounters an invalid password error. These errors can occur when the database log in password for a database user is changed. A single occurrance of this log is informational. Multiple occurances within a 15 minutes or a half hour should be investigated..

16.3.3.3 Action

Monitor for multiple occurances within a 15 minutes or a half hour. If this is detected investigate to insure these errors are attributable to authorized security actions to change the database password and not due to security violations or unauthorized system access.

16.3.4 Database Maximum Sessions Log

Log Title:DB603

16.3.4.1 Formats

NTSTD log format:

RTP2 DB603 SEP23 18:45:00 0403 INFO DB Connection Error
Location: SSPFS=wnc0s0jd
Information: Maximum database sessions limit reached
Time: SEP23 17:25:00 2003
Component Id: Database, GWCEM User
Specific Problem: Maximum database sessions active was detected on an attempt to create a database connection.
Description: Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's limits maybe required.

Table 4 Log Field descriptions

Field	Value
Category	Information

Table 4 Log Field descriptions

Field	Value
Severity	NOA
LogName	DB
LogNumber	603
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	Maximum database sessions limit reached
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Maximum database sessions active was detected on an attempt to create a database connection.
Description	Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's limits maybe required.

16.3.4.2 Explanation

This Log is generated when an attempt to allocate a database connection encounters maximum database sessions exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity. A single occurrance of this log is informational indicating that database resources may need reconfiguration. Multiple occurances within a 15 minutes or a half hour should be investigated.

16.3.4.3 Action

Monitor for multiple occurances within a half hour or an hour. If this is detected notify the database or system administrator. A possible solution is increase the value of the SESSIONS initialization parameter.

16.3.5 Database Maximum Processes Log

Log Title:DB604

16.3.5.1 Formats

NTSTD log format:

RTP2 DB604 SEP23 18:45:00 0403 INFO DB Connection Error
Location: SSPFS=wnc0s0jd
Information: Maximum database processes limit reached
Time: SEP23 17:25:00 2003
Component Id: Database, GWCEM User
Specific Problem: Maximum database processes was detected on an attempt to create a database connection.
Description: Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's processes limit maybe required.

Table 5 Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	604
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	Maximum database processes limit reached
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Maximum database processes limit reached

Table 5 Log Field descriptions

Field	Value
Description	Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's processes limit maybe required.

16.3.5.2 Explanation

This Log is generated when an attempt to allocate a database connection encounters maximum database processes exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity. A single occurrance of this log is informational indicating that database resources may need reconfiguration. Multiple occurances within a 15 minutes or a half hour should be investigated.

16.3.5.3 Action

Monitor for multiple occurances within a half hour or an hour. If this is detected notify the database or system administrator. A possible solution is increase the value of the PROCESSES initialization parameter.

16.4 Related documentation

Log Reporting Rules and Guidelines DIS Ref: IEMPG DIS No: AF01 Release: Standard

17: Fault Management (FM): A00003487

17.1 Fault management strategy

17.2 Fault management tools and utilities

17.3 Logs IWBM 800

17.3.1 Explanation

Log Title: IWBM 800

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBM800 indicates that the number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

Event type: Unchanged

17.3.2 Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBM800 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Figure 1 Enhanced IWBM 800 Log

```
RTP7  **  IWBM800 SEP17  12:16:55  6600  1st Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 70 percent of all bridges in the pool.
           Total number of IW bridges:  2016
           Number of available IW bridges: <NN>
           Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

17.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLLI	Bridge pool name as datafilled in Tale NETBRDGE

17.3.4 Action

This log report requires no action.

17.3.5 Associated Operational Measurements or Performance Measurements

New OM group IWBMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

17.3.6 Additional information

This log report requires no additional information.

17.4 Logs IWBM 801

17.4.1 Explanation

Log Title: IWBM 801

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBM801 indicates that the number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWBM800.

Event type: Unchanged

17.4.2 Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBM801 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to ‘Y’. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Figure 2 Enhanced IWBM 801 Log

```
RTP7 ** IWBM801 SEP17 12:16:55 6600 1st Threshold Cleared
     The number of interworking bridges in use has
     fallen below 65 percent of all bridges in the pool.
          Total number of IW bridges: 2016
          Number of available IW bridges: <NN>
          Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

17.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLLI	Bridge pool name as datafilled in Tale NETBRDGE

17.4.4 Action

This log report requires no action.

17.4.5 Associated Operational Measurements or Performance Measurements

New OM group IWBMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

17.4.6 Additional information

This log report requires no additional information.

17.5 Logs IWBM 802

17.5.1 Explanation

Log Title: IWBM 802

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBM802 indicates that the number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

Event type: Unchanged

17.5.2 Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBM802 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Figure 3 Enhanced IWBM 802 Log

```
RTP7 ** IWBM802 SEP17 12:16:55 6600 2nd Threshold Exceeded
    The number of interworking bridges in use has
    exceeded 90percent of all bridges in the pool.
        Total number of IW bridges: 2016
        Number of available IW bridges: <NN>
        Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

17.5.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLLI	Bridge pool name as datafilled in Tale NETBRDGE

17.5.4 Action

This log report requires no action.

17.5.5 Associated Operational Measurements or Performance Measurements

New OM group IWBMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

17.5.6 Additional information

This log report requires no additional information.

17.6 Logs IWBM 803

17.6.1 Explanation

Log Title: IWBM 803

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBM803 indicates that the number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBM802.

Event type: Unchanged

17.6.2 Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBM803 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Figure 4 Enhanced IWBM 803 Log

```
RTP7  **  IWBM803 SEP17  12:16:55  6600 2nd Threshold Cleared
      The number of interworking bridges in use has
      fallen below 85 percent of all bridges in the pool.
            Total number of IW bridges:  2016
            Number of available IW bridges: <NN>
            Bridge Pool: <bridge pool CLLI from Table NETBRDGE>
```

17.6.3 Field descriptions

Table 4 Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLLI	Bridge pool name as datafilled in Tale NETBRDGE

17.6.4 Action

This log report requires no action.

17.6.5 Associated Operational Measurements or Performance Measurements

New OM group IWBMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

17.6.6 Additional information

This log report requires no additional information.

17.7 XNET 600 Series logs (new)

The XNET 600 series logs provide information on external packet network bearer connection problems. Three new logs are created:

17.7.1 XNET605

17.7.1.1 Explanation

Bearer Networks Cannot connect

This log indicates that the bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET.

- or an “Unavailable” indication when the conection source was an ENET hosted party, but that party can no longer be determined.

The ‘From Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the source party . The ‘To Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

17.7.1.2 Format

Figure 5 XNET605 Log Example

```
RTP7   XNET605  MAY17  12:16:55  9600 INFO Bearer Networks Cannot Connect
       From Agent              : VOIP 42 2 04 00      DN 6137204200
       From Bearer Network:  IP_PRIMARY
       To     Bearer Network: AAL1_SECONDARY
       Bearer Network Translations resulted in no interconnect
       Check Table NET2NET, NETPATH and NETBRDGE
```

17.7.1.3 Field descriptions

The ‘From Agent’ line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,
- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined

17.7.1.4 Action

The telco should determine whether the identified bearer networks are permitted to interconnect. If so, the appropriate datafill should be added to tables NET2NET, and if necessary NETPATH and NETBRDGE. If the bearer networks are not permitted to connect, the telco can:

a. if possible, change DN translations so that the originator can no longer dial the terminator, but will receive a treatment of some type,

b. use the EXTLOGCI command to disable the XNET605 log (see section 17.8)

c. use LOGUTIL to SUPPRESS the XNET 605 log

d. do nothing, the log will continue to print when two parties on the specified bearer networks attempt to dial one another.

17.7.1.5 Associated Operational Measurements or Performance Measurements

17.7.1.6 Additional Information

17.7.2 XNET606

17.7.2.1 Explanation

XNET606 - PKT Pathend Has NIL Bearer Net ID

This log indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt.

17.7.2.2 Format

Figure 6 XNET 606 Log Example

```
RTP7   XNET606  MAY17  12:16:55  9600 INFO PKT Pathend Has NIL Bearer Net ID
       Path   - Node: LGRP   07   Tid:  124
       Agent - VOIP 42 2 04 00     DN 6137204200
       Contact Product Support
```

17.7.2.3 Field descriptions

- The ‘Path’ line indicates the node at the network connection point, this can be in two forms:
- a PM name and number, and a channel or TID id,
- a node number, and a channel or TID id, when the PM name and number cannot be determined from the node number

The ‘Agent’ line identifies the suspect party, this can be in several forms:

- a LEN and DN,
- a Trunk Group name and member number
- or a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined

17.7.2.4 Action

The telco should report this log to appropriate Nortel Product Support.

17.7.2.5 Associated Operational Measurements or Performance Measurements

17.7.2.6 Additional Information

The telco can:

- use the EXTLOGCI command to disable the XNET606 log (see section 17.8)
- use LOGUTIL to SUPPRESS the XNET 605 log
- do nothing, the log will continue to print when the suspect party attempts to place calls

17.7.3 XNET607

17.7.3.1 Explanation

XNET607 - IW Bridge Not Available

This log indicates that an IW SPM interworking bridge was not available for the connection request, either because

- of a bridge exhaust condition on one of the bridge pools involved in the connection request,
- bridges are not inservice, or provisioned for one of the bridge pools involved with the connection request

17.7.3.2 Format

Figure 7 XNET 607 Log Example

```
RTP7    XNET607  MAY17  12:16:55  9600 INFO IW Bridge Not Available
        Bridge Pool       : ENET_TO_IP
        From Agent        : VOIP 42 2 04 00      DN 6137204200
        From Bearer Network:  IP_PRIMARY
        To      Bearer Network: AAL1_SECONDARY
```

17.7.3.3 Field descriptions

The ‘Bridge Pool’ line indicates the name of the bridge pool, as specified in table NETBRDGE, that has the ‘trouble’ condition. The ‘From Agent’ line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,
- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined
- or an “Unavailable” indication when the conection source was an ENET hosted party, but that party can no longer be determined.

The ‘From Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the source party. The ‘To Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

17.7.3.4 Action

The telco can:

- check for IWBM602 logs indicating a bridge exhaust condition,
- verify that the bridge pool identified in the log is provisioned on an SPM in table MNNODE,
- verify that the bridges in the bridge pool identified in the log are in-service.
- use the EXTLOGCI command to disable the XNET607 log (see section 17.8)
- use LOGUTIL to SUPPRESS the XNET 607 log

17.7.3.5 Associated Operational Measurements or Performance Measurements

17.7.3.6 Additional Information

17.8 EXTLOGCI Tool

The EXTLOGCI tool is an existing CI command that controls the XNET series of logs. By using the ENABLE and DISABLE commands, the user can control the production of XNET logs. The XNET 605, 606 and 607 logs are automatically enabled on all restarts.

17.9 Related documentation

18: Fault Management (FM): A00003567

18.1 Fault management strategy

This feature uses existing MG9KEM fault management structure.

18.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

18.3 Logs and Alarms

A new alarm (nnESADownloadFault) will be added to indicate a failure to download ESA data to given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in previous releases. This alarm is EM generated and will be problems such as failure to setup the FTP connection to gateway or failure to login. It is different than the inconsistent data (nnESAFault) alarm generated by the hardware while the file transfer is in progress.

The alarm will be cleared by the EM when a successful download takes place.

The new alarm will be displayed at the Alarm Browser at the subnet as well as the well as the alarm browser for each corresponding network element. A log is also generated.

In addition, all the alarms and logs generated for the ITP ESA also apply to ABI ESA.

18.3.1 Explanation

18.3.1.1 nnESADownloadFault

Title: nnESADownloadFault

Name: ESA

Description: This log is generated when the EM is unable to download ESA data to a VMG.

Severity: Critical

Event type: ESA data download failure

18.3.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

18.3.2.1 nnESADownloadFault

***ESA302 Tue Jul 09 14:50:26 EDT 2003 TBL
NnESADOWNLOADFAULT
NE Number: 8 NE Name: co8
State: not acknowledged
Type: Equipment
Cause: Failed to set up FTP connection: login failure!!

Time: Jul 09 14:50:26:616 2003
Severity: critical
Mo: Card.f0.s2.l13.ITP
Description: EM failed to push ESA to VMG

18.3.3 Field descriptions

18.3.3.1 nnESADownloadFault

Table 1 Field descriptions ESA302

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.

Table 1 Field descriptions ESA302

Field	Value	Description
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.

Table 1 Field descriptions ESA302

Field	Value	Description
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
nnESA Fault Type	string	The type of the fault: ESA data download failed
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Warning
MediaGatewayName	string	The name of the Media Gateway control group which found ESA data inconsistent
Description	string	ESA data download failed

18.3.4 Action

nnESADownloadFault:

Check failure cause in alarm or log text and perform manual downloading actions from the corresponding VMG view . The alarm will be cleared by the EM when the download is succesful.

18.3.5 Associated Operational Measurements or Performance Measurements

None.

18.4 Related documentation

1. NORTEL-UEMG-BASE-MIB - MG9000's Enterprise MIB, contains the Alarm Log Table.

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

19: Fault Management (FM): A00003591

19.1 Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “A00003591 - OC3 Channelization ” feature there will be new faults added when the payload selected DS3

19.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

The DS3 alarms will be displayed here..

19.2.1 Faults, Alarms and Logs

There will be new faults generated and cleared by MG9000 when the carrier is channelized and payload selected on the STS1 path is DS3CC or DS3PLCP.

The alarms that can be generated for DS3 will be AIS, LOF and RAI. These faults will be generated when there is a Loss of Frame or some problem at the remote end.

19.3 Alarms

19.3.1 Explanation

19.3.1.1 AlarmIndicationSignal

Title: AlarmIndicatinSignal

Name: ds3ais

Description: This log is generated when a AlarmIndicationSignal fault is received from the Gateway.

19.3.1.2 LossOfFrame

Title: Loss Of Frame

Name: ds3lof

Description: This log is generated when a LossOfFrame fault is received from the Gateway.

19.3.1.3 RemoteAlarmIndication

Title: RemoteAlarmIndication

Name: ds3rai

Description: This log is generated when a RemoteAlarmIndication fault is received from the Gateway

19.3.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

19.3.2.1 STD Format

- **AlarmIndicationSignal**

```
MGCA333 MAR08 06:14:43 3409 TBL  MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 294
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:39:05 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Alarm Indication Signal - Check f
 ar-end carrier faults
Description: (DS3) DS3 AIS
Site   Flr  RPos  Bay_id
FFFF   FF   FFFF  MG9F FFF
```

- **LossOfFrame**
  MGCA334 MAR08 06:12:43 8306 TBL MG9K NorCarrFault
  Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
  Notification Id: 292
  State: not acknowledged
  Category: Communication Alarm
  Cause: Loss Of Frame
  Time: Jan 01 05:37:08 1970
  Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
  Specific Problem: NorCarrFault - DS3 - Loss Of Frame
  Description: (DS3) DS3 LOF
  Site Flr RPos Bay_id
  FFFF FF FFFF MG9F FFF

- **RemoteAlarmIndication**
  MGCA335 MAR08 06:18:43 1111 TBL MG9K NorCarrFault
  Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
  Notification Id: 296
  State: not acknowledged
  Category: Communication Alarm
  Cause: Communications Subsystem Failure
  Time: Jan 01 05:43:02 1970
  Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
  Specific Problem: NorCarrFault - DS3 - Remote Indication Signal - Check
  far-end carrier faults
  Description: (DS3) DS3 RAI
  Site Flr RPos Bay_id
  FFFF FF FFFF MG9F FFF

19.3.2.2 SCC2 Format

- **AlarmIndicationSignal**
  MGCA333 5915 TBL MG9K NorCarrFault
  Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
  Notification Id: 300
  State: not acknowledged
  Category: Communication Alarm
  Cause: Communications Subsystem Failure
  Time: Jan 01 05:54:38 1970
  Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
  Specific Problem: NorCarrFault - DS3 - Alarm Indication Signal - Check f
  ar-end carrier faults
  Description: (DS3) DS3 AIS

Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **LossOfFrame**
  MGCA334 5013 TBL MG9K NorCarrFault
  Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
  Notification Id: 298
  State: not acknowledged
  Category: Communication Alarm
  Cause: Loss Of Frame
  Time: Jan 01 05:53:23 1970
  Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
  Specific Problem: NorCarrFault - DS3 - Loss Of Frame
  Description: (DS3) DS3 LOF
  Site Flr RPos Bay_id
  FFFF FF FFFF MG9F FFF

- **RemoteAlarmIndication**
  MGCA335 6016 TBL MG9K NorCarrFault
  Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
  Notification Id: 301
  State: not acknowledged
  Category: Communication Alarm
  Cause: Communications Subsystem Failure
  Time: Jan 01 05:54:53 1970
  Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
  Specific Problem: NorCarrFault - DS3 - Remote Indication Signal - Check far-end carrier faults
  Description: (DS3) DS3 RAI
  Site Flr RPos Bay_id
  FFFF FF FFFF MG9F FFF

19.3.3 Action

19.3.3.1 AlarmIndicationSignal

This alarm will be cleared when an AlarmIndicationSignal with faultdefinition - clear is received.

19.3.3.2 LossOfFrame

This alarm will be cleared when an AlarmIndicationSignal with faultdefinition - clear is received..

19.3.3.3 RemoteAlarmIndication

This alarm will be cleared when an RemoteAlarmIndication with faultdefinition - clear is received..

19.3.4 Associated Operational Measurements or Performance Measurements

None.

19.4 Related documentation

20: Fault Management (FM): A00003650

20.1 Fault management strategy

This feature provides logs for the MG4K-IP product in SN07. The log series MG4I is introduced by this activity. The following logs are supported:

- MG4I 501 - Stream Control Transmission Protocol (SCTP) IP Control Connection Maintenance (CCMT) Core connection state change
- MG4I 502 - SCTP IPCCM Peer connection state change
- MG4I 300 - Media Integrity Failure

These logs provide the craft with the capability to detect fault conditions and configuration issues.

20.2 Fault management tools and utilities

The logs can be viewed and reporting can be controlled using the existing LOGUTIL CI.

20.3 MG4I 501 Log

Log Title/Log ID: SCTP Core Conn State Change - MG4I 501

20.3.1 Formats

The format for MG4I 501 log report is as follows:

<Alarm Sev.> MG4I501 <date> INFO SCTP Core Conn State Change
State Change From: <SCTP From State> To: <SCTP To State>
Reason : <State Change Reason>
From Node : CORE (<Core IP addr>:<port>; Associd: <SCTP assoc id>)
To Node : SMG4 <SPM no:> (<MG4K IP addr>:<port>)
Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP, ATM, UNK>

Example:

```
*** MG4I501 MAY02 22:04:48 800 INFO SCTP Core Conn State Change
        State Change From: ESTABLISHED To: CLOSED
        Reason : FAR END DISCONNECTED
        From Node : CORE (47.108.11.3:5050; Associd: 10)
            To Node : SMG4 6 (47.142.211.1:5050)
        Location: SPM 6 Type: SMG4 Fabric: IP
```

20.3.2 Explanation

Description: This INFO log is generated when the SCTP IPCCM Core Connection state changes for an MG4K-IP node. IPCCM maintains the SCTP connection for reliable messaging between the call server and the MG4K-IP

node. The state change log from ‘CLOSED’ to ‘ESTABLISHED’ indicates that the connection is up. The state change log from ‘ESTABLISHED’ to ‘CLOSED’ indicates that the connection is down. The trunks will go down and no call processing is possible when the connection is down. This is indicated by log alarm severity of Critical.

20.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
From SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the old SCTP connection state.
To SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the new SCTP connection state.
State Change Reason	1 line of variable text of 60 characters	Indicates the reason for the SCTP connection state change
From Node	CORE (<Call Server IP addr in dotted decimal format>: <Port>; Associd: <Association id>	Indicates the call server SCTP connection end point IP address, port and SCTP association id.
To Node	SMG4 <SPM no: (0 to 85)> (<MG4K IP addr in dotted decimal format>:<Port>)	Indicates the MG4K IP node, SCTP connection end point IP address, port
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location. It can only be an MG4K node with IP Fabric. The SPM node number is the same as that in ‘To Node’ field.

20.3.4 Action

If the SCTP state change is from ‘ESTABLISHED’ to ‘CLOSED’, check the state change reason and corresponding NODE and SPM logs to determine possible causes of SCTP connection failure and attempt to recover the SCTP connection.

20.3.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

20.3.6 Additional information

Not Applicable.

20.4 MG4I 502 Log

Log Title/Log ID: SCTP Peer Conn State Change - MG4I 502

20.4.1 Formats

The format for MG4I 502 log report is as follows:

MG4I502 <date> INFO SCTP Peer Conn State Change
State Change From: <SCTP From State> To: <SCTP To State>
Reason : <State Change Reason>
From Node : SMG4 <SPM no:> (<MG4K IP addr>:<port>; Associd: <SCTP assoc id>)
To Node(s) : <SMG4, IW, GWC> <Node no:> (<Node IP addr>:<port>)
<SMG4, IW, GWC> <Node no:> (<Node IP addr>:<port>)
....
<list of upto 4 peer IP nodes>
Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP, ATM, UNK>

Examples:

MG4I502 MAY02 22:04:48 800 INFO SCTP Peer Conn State Change
State Change From: ESTABLISHED To: CLOSED
Reason : FAR END DISCONNECTED
From Node : SMG4 6 (47.108.11.3:5050; Associd: 10)
To Node : SMG4 5 (47.142.211.1:5050)
Location: SPM 6 Type: SMG4 Fabric: IP

MG4I502 MAY02 22:04:48 0800 INFO SCTP Peer Conn State Change
State Change From: ESTABLISHED To: CLOSED
Reason : REPORTED BY PERIPHERAL
From Node : SMG4 6 (47.108.11.3:*; Associd: *)
To Nodes : SMG4 5 (47.142.211.1:5050)
SMG4 7 (47.142.211.2:5050)
SMG4 10 (47.142.211.23:5050)
SMG4 22 (47.142.211.24:5050)
Location : SPM 6 Type: SMG4 Fabric: IP

20.4.2 Explanation

Description: This INFO log is generated when the SCTP IPCCM Peer Connection from an MG4K-IP node to a peer MG4K-IP node changes state.

IPCCM maintains the SCTP connections for reliable messaging between the MG4K-IP node and all its peer MG4K-IP nodes for peer-peer signalling during call processing. The state change log from ‘CLOSED’ to ‘ESTABLISHED’ indicates that the connection is up. The state change log from ‘ESTABLISHED’ to ‘CLOSED’ indicates that the connection is down. The messages are bounced off the call server when the peer connection is down.

20.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
From SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the old SCTP connection state.
To SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the new SCTP connection state.
State Change Reason	1 line of variable text of 60 characters	Indicates the reason for the SCTP connection state change
From Node	SMG4 <SPM no:(0 to 85)> (<MG4K IP addr in dotted decimal format>: <Port>; Associd: <Association id>	Indicates the MG4K IP node, SCTP connection end point IP address, port and SCTP association id.
To Node list	Upto 4 nodes SMG4 <SPM no: (0 to 85)> (<MG4K IP addr in dotted decimal format>:<Port>)	Indicates the peer MG4K IP node, SCTP connection end point IP address and port for upto 4 peer SCTP connections undergoing state changes.
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location. It can only be an MG4K node with IP Fabric. The SPM node number is the same as that in 'From Node' field.

20.4.4 Action

These logs do not indicate a service affecting change. If the SCTP state change is from 'ESTABLISHED' to 'CLOSED', check the state change reason and corresponding NODE and SPM logs to determine possible causes of SCTP connection failure.

20.4.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

20.4.6 Additional information

In SN07, the peer IP nodes are only MG4K-IP nodes managed by the same call server. The peer nodes may include GWC in a future release.

20.5 MG4I 300 Log

Log Title/Log ID: Media Integrity Failure - MG4I 300

20.5.1 Formats

The format for MG4I 300 log report is as follows:

MG4I300 <date> TBL Media Integrity Failure
Call Type: <Call type string>
Src IP: <Src IP addr>:<port> Dest IP: <Dest IP addr>:<port>
Description : <Media Integrity Failure Reason>
Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP, ATM, UNK>

Example:

MG4I300 SEP04 03:41:44 2801 TBL Media Integrity Failure
Call Type: G711
Src IP: 47.108.11.3:5050 Dest IP:47.142.211.1:5050
Description: RTCP Media Integrity Timer Expired
Location: SPM 1 Type: SMG4 Fabric: IP

20.5.2 Explanation

Description: This TBL log is generated when a media integrity failure has been detected during a call. The corresponding call is taken down.

20.5.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
Call Type	8 character string	Indicates the call type codec (G711, G729)
Src IP	<Src IP addr in dotted decimal format>:<Port>	Source IP address and port
Dest IP	<Dest IP addr in dotted decimal format>:<Port>	Destination IP address and port
Description	1 line of variable text of 50 characters	Indicates the reason for the media integrity failure
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location which reported this failure. It can only be an MG4K node with IP Fabric.

20.5.4 Action

Check the description and investigate the cause of integrity failure.

20.5.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

20.5.6 Additional information

Not Applicable.

20.6 Alarms

Not Applicable.

20.7 Related documentation

Not Applicable.

21: Fault Management (FM): A00003667

21.1 Fault management strategy

There are three changes to the existing SESM fault management structure.

One is the elimination of the SESM alarm acknowledgement function. This is removed because the alarm acknowledgements are being handled at the IEMS level of alarm management. This change will apply to the SESM alarm GUI clients. It is discussed briefly below and more fully in the configuration section.

The second is the update of the SESM communications alarm previously "owned" by the device. The alarm was raised as an alarm from the device that SESM could not communicate with. This was an inaccurate representation of the source of the alarm as the device itself may not have any alarm condition. The alarm was also a critical and this was inaccurate as it did not necessarily mean an outage was occuring or imminent. The alarm has been changed to a major to reflect that the current condition could cause an outage.

The third is the generation of logs on SESM. One each is generated upon startup and shutdown and one when SESM cannot generate alarm notification events. These logs will be sent via the syslog to the SDM.

21.2 Fault management tools and utilities

There are two SESM alarm GUI's. One shows active alarms on the managed devices and the other shows the alarm history. On the active alarm GUI, the ability to acknowledge an alarm will be removed. This function is handled by the IEMS alarm GUI. By removing it, there is no confusion whether an alarm is acknoweldged or not.

The only change to the alarm GUI's will be the removal of the acknowledge options in the active alarm manager and the removal of the "show acknowledged" check box on the alarm history window.

21.3 Logs

21.3.1 Explanation

This log is generated by the SESM alarm system to indicate the system is initializing.

21.3.2 Format

```
COMPACT2 CMT500 JUN30 11:01:55 0580 INFO CMT INFO Init

        CS2K Management Tools Alarm Manager Initialization.
```

Cause – SESM server is restarting.

Action – None.

Interfaces – this is generated by the SESM alarm system via syslog.

21.3.3 Field descriptions

N/A

Table 1 Field descriptions

Field	Value	Description

21.3.4 Action

N/A

21.3.5 Associated Operational Measurements or Performance Measurements

N/A

21.3.6 Additional information

N/A

21.3.7 .Explanation

This log is generated by the SESM alarm system upon shutdown.

21.3.8 Format

```
COMPACT2 CMT501 JUN30 11:01:55 0580 INFO CMT INFO Shutdown
        CS2K Management Tools Alarm Manager Shutting Down.
```

Cause – SESM Server has been shutdown.

Action – A SESM administrator should ensure that the server was intentionally shutdown and that it is being restarted.

Interfaces – this is generated by the SESM alarm system via syslog.

21.3.9 Field descriptions

N/A

Table 2 Field descriptions

Field	Value	Description

21.3.10 Action

A SESM administrator should ensure that the server was intentionally shutdown and that it is being restarted.

21.3.11 Associated Operational Measurements or Performance Measurements

N/A

21.3.12 Additional information

N/A

21.3.13 Explanation

This log is generated by the SESM alarm system to inform northbound alarm clients that alarm notifications cannot be generated. This log will be sent via the SSPFS syslog feed to the customer log.

21.3.14 Format

```
COMPACT2 CMT502 JUN30 11:01:55 0580 INFO CMT INFO

        CS2K Management Tools Alarm Manager failed to raise alarm

        notification due to CORBA failure.  Please check CORBA status on

        CS2K Management Tools server.
```

The is just a sample of how the log might look. The final format will be provided prior to IT.

Cause – CORBA communications on the SESM server or within SESM are failing.

Action – A SESM administrator should check the communications on the SESM server.

Interfaces – this is generated by the SESM alarm system via syslog.

21.3.15 Field descriptions

N/A

Table 3 Field descriptions

Field	Value	Description

21.3.16 Action

The SESM administrator should determine the status of the CORBA communications on the SESM server and the network connectivitiy of that machine.

21.3.17 Associated Operational Measurements or Performance Measurements

N/A

21.3.18 Additional information

This log is intended for users of the SESM CORBA alarm notifications to inform the user that events cannot be generated.

21.4 Alarms

There is one change to an existing alarm. The alarm was previously a device owned alarm represented as GWC398 or UAS398 and was a critical alarm. It has been changed to be owned by the CMT and will be a major alarm now.

For a description of the alarm log formats and fields, please see:

http://ptm -> Documentation -> SN06 -> AlarmLoggingDSUM.doc -> Section 11.

This is the new format of the communication error log. Changed fields in bold.

```
COMPACT2 ** CMT302 JUN30 11:01:55 0580 TBL CMT Fault
        Location: SNMP_NE_Poller
        NotificationID: 0
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jun 30 11:01:55 2003
```

```
Component Id: SNMP Device Poller;Device=rtpsUASa;DeviceID=0x0000006
3000000a12f8e5952
Specific Problem: SNMP Timeout
Description: CMT Unable to communicate with managed device
```

Severity – Major, as it may indicate a network issue or an issue with the device itself, and it could lead to an outage.

Cause – SNMP poller cannot communicate to the network device

Duration – will remain active until communications are reestablished to the device being polled

Action – have a network administrator determine the cause of the SNMP timeout to the device

Interfaces – this is generated by the SNMP poller on SESM

21.5 Related documentation

http://ptm -> Documentation -> SN06 -> AlarmLoggingDSUM.doc -> Section 11.

22: Fault Management (FM): A00003687

22.1 Fault management strategy

The TOPS131 log was added in SN06 by feature A00000816: "TOPS Wireless ADACC with Release." TOPS generates this log in failure situations when interacting with a cell phone caller and a Mobile Switching Center (MSC).

This SN07 feature updates the text title string in the log. The log was formerly titled "TOPS IS-41 Trouble." To make it more general, it is now titled "TOPS Wireless Trouble." An additional line of text is added to identify whether the trouble occurred on an IS-41 or GSM call.

This feature also adds some new reasons to the Reason field.

22.2 Fault management tools and utilities

LOGUTIL and related log tables (LOGCLASS, LOGDEV) can be used to view and collect logs relating to TOPS wireless applications.

22.3 Logs

22.3.1 Explanation

Log Title: TOPS131

Name: TOPS Wireless Trouble (changed from TOPS IS-41 Trouble)

Description: This log is generated in the TOPS switch when problems occur on a wireless ADACC with release call, or when problems occurs when TOPS tries to send a short text message using Short Message Service (SMS).

In the ADACC case, the log indicates TOPS attempted to provide ADACC with Release Link Trunking (RLT) to a wireless customer, but an unexpected problem prevented this.

This log is not generated when the call is disconnected prior to call completion due to normal reasons (e.g. calling party abandons, or operator can't locate DA listing and ends call).

In the SMS case, this log indicates an SMS did not reach the cell phone user. The log text gives an indication of the problem.

Event type: Major. Each log can represent the loss of one call, or that requested information could not be provided. On RLT calls, the wireless customer is disconnected prior to call completion to the requested number.

22.3.2 Format

TOPS131 <mmmdd hh:mm:ss ssdd> TBL TOPS Wireless Trouble
CKT <CPID>
MSC route set: <serving MSC route set from Table C7RTESET>
Called digits: <digits>
Reason: <reason text>
Wireless type: <IS-41 or GSM>

Example:

```
TOPS131 OCT01 15:07:54 7100 TBL TOPS Wireless Trouble
MSC route set:     RTP8_STPA_N_RS
Called digits:     201-220-1234 (TLDN)
Reason:            Failure at MSC
Wireless type:     IS-41
```

Example:

```
TOPS131 OCT01 15:07:54 7100 TBL TOPS Wireless Trouble
CKT  RTPC_RTP8_ISUP    2
MSC route set:     RTP8_STPA_N_RS
Called digits:     619-322-1234 (Destination number)
Reason:            SMS failure: Network problem (2)
Wireless type:     IS-41
```

22.3.3 Field descriptions

This feature does not change TOPS131 fields CKT, MSC route set, or Called digits. This feature adds additional text reasons to the Reason field as indicated in the table in this section. This feature also adds a new field, Wireless type, which indicates whether the log was generated on an IS-41 or GSM call.

The Reason field describes the category of the error. When the log is generated due to a negative acknowledgment from the message center, the exact byte value of the cause code is included in parentheses at the end of the Reason field. The meaning of the byte value can be found in the specifications as follows:

- IS-41-D: Chapter 5, section 6.5.2.125 (SMS Cause Code), table 171
- GSM: 3GPP TS 29.002 V4.12.0 (2003-06), sections 7.6.1 and 12.2.3.

Table 1 Field descriptions

Field	Value	Description
Reason	SMS failure: Network problem <nn>	The message center encountered a network problem and could not process the TOPS SMS.

Table 1 Field descriptions

Field	Value	Description
Reason	SMS failure: Terminal problem <nn>	The message center could not process the TOPS SMS due to problems with the terminal (cell phone) specified by the destination number.
Reason	SMS failure: Radio interface problem <nn>	The message center could not process the TOPS SMS due to problems with the radio interface to the cell phone.
Reason	SMS failure: Miscellaneous problem <nn>	The message center could not process the TOPS SMS for a reason other than the above three. One example is if the format of the TOPS SMS was not understood by the message center.
Reason	SMS failure: Time-out	A response was not received to the TOPS SMS within the time period defined in Table TOPSPARM parameter SMS_TIMEOUT.
Reason	SMS failure: Global title translation	Tables C7GTTYPE and C7GTT cannot accommodate the destination number listed in the log.
Reason	No transaction IDs	No transaction ID could be obtained when TOPS attempted to send an INVOKE, whether for IS-41 WIN, GSM CAMEL, or SMS. This means the message could not be sent.

Table 1 Field descriptions

Field	Value	Description
Reason	WIN: Wireless protocol mismatch	The wireless network protocol established by the IS-41 ANLYZD or GSM InitialDP message did not match the trunk group datafill (RLT_IS41 or RLT_GSM) in Table ISUPTRK when the call arrived. The call cannot proceed because the version of IS-41 or GSM RLT is unknown.
Wireless type	IS-41	The log was generated on a TOPS IS-41 call.
Wireless type	GSM	The log was generated on a TOPS GSM call.

22.3.4 Action

The action taken depends on the contents of the reason field as follows.

Table 2 Reason to action mapping

Reason text	Action
SMS failure: *(any SMS failure except GTT)*	Examine SS7 and TCAP logs on the TOPS switch and at the message center. Use an operator position to send SMS messages and verify the messages arrive at the message center. Use message center tools to verify SMS can be forwarded to the cell phone. If time-outs are occurring, investigate whether the SMS_TIMEOUT parameter in Table TOPSPARM needs to be increased.
SMS failure: Global title translation	Check datafill in Tables C7GTTYPE and C7GTT for the destination number listed in the log. Look for tuples containing MDNMCGT (mobile directory number to message center global title).
No transaction IDs	Contact Nortel Networks. TOPS automatically allocates transaction IDs when needed.
WIN: Wireless protocol mismatch	Correct the datafill mismatch in Table ISUPTRK. The MSC specified in the log is sending one kind of protocol to TOPS, but is datafilled in Table ISUPTRK as another kind.

22.3.5 Associated Operational Measurements or Performance Measurements

Table 3 Reason to OM mapping

TOPS131 reason text	OM
SMS failure: Network problem	Group SMSTOPS, register SMSNETWK
SMS failure: Terminal problem	Group SMSTOPS, register SMSTERM
SMS failure: Radio interface problem	Group SMSTOPS, register SMSRADIO
SMS failure: Miscellaneous problem	Group SMSTOPS, register SMSMISC
SMS failure: Time-out	Group SMSTOPS, register SMSTIME
SMS failure: Global title translation	Group TC7WRLSS, register GTTFAIL
No transaction IDs	Group TC7WRLSS, register NOTRIDS
WIN: Wireless protocol mismatch	None

22.3.6 Additional information

Since short messaging can fail in many expected situations (such as wireless phone powered off, destination number not subscribed to SMS, etc.), the TOPS131 logs can be throttled. A new parameter in Table TOPSPARM, `SMS_LOG_MC_FAILURE`, determines when TOPS131 logs are generated as a result of SMS failure. TOPS131 to be generated in some SMS failure scenarios but not others. See the Configuration chapter for more information.

22.4 Alarms

No new or changed alarms.

22.5 Related documentation

Not applicable.

23: Fault Management (FM): A00003767

23.1 Fault management strategy

Three new alarms are introduced by this activity. These alarms are associated with ABI host XPMs and allow the customer to quickly isolate network messaging issues from other causes of XPM c-side busy.

As with other XPM faults, these alarms affect the DMS alarm banner, show up as an InService TrouBle (ISTB) reason for the applicable ABI XPM, and generate a log message.

23.2 Fault management tools and utilities

No new tools are introduced. These alarms look like other ISTB reasons on any XPM.

23.3 Logs

23.3.1 Explanation

Log Title: PM181

Name: PM181

Description: PM181 logs are existing DMS logs and are used extensively by the GWC in a Succession configuration. This activity extends the use of the PM181 log for Succession. When an ABI messaging alarm (described later) is set or cleared, a PM181 log is reported.

Event type: critical, major or minor depending on the alarm that is generating the log.

23.3.2 Format

Format of the PM181 log has not been changed beyond the formats already in used by the GWC. Information on the GWC use of PM181 can be found in NN10090-911. The following new strings are used. Strings 1, 2 & 3 are concatenated together to form the complete string:

Table 1 New PM181 Log strings

String 1	String 2	String 3
ABI external messaging alarm	Links Down - Severely degraded - Degraded -	Alarm set Alarm cleared

23.3.3 Field descriptions

Unchanged.

23.3.4 Action

An associated alarm is also raised. Please refer to the alarm descriptions below for operating company actions.

23.3.5 Associated Operational Measurements or Performance Measurements

Not applicable

23.3.6 Additional information

Alarm set **Associated alarm message: ABI external messaging alarm Links Down - Alarm Set (or Alarm cleared)**

Severity: Critical; Service Outage

Cause: The messaging links between the ABI card associated with the XPM and the GWC which the XPM subtends have gone down. This causes a service outage of the XPM and all its subtending peripherals (ESA may be in affect).

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover autonomously.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all) of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI card failed or was pulled and not taken out service first
- MG9K OC3 cards taken out of service
- MG9K active OC3 card failed or was pulled and not taken out service first
- Fiber links on MG9K ABI or active OC3 card pulled or failed
- Shelf controller for associated GWC failed, or taken out of service
- Network router failed or taken out of service with no alternative path for packets
- Configuration of router(s) changed so packets can’t get through
- Cables to router(s) failed.

- No Single point of failure, but network message loss is so high that a messaging link can not be sustained (would probably have seen the minor and major alarms earlier).

The alarm is cleared when the message link is re-established, or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

Associated alarm message: ABI external messaging alarm Severely Degraded - Alarm Set (or Alarm cleared)

Severity: Major, service affecting

Cause: Message loss in the network has reached a point where calls may be sporadically starting to fail, loading and RTS'ing peripheral may fail.

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover autonomously.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all) of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI cards in overload
- MG9K OC3 cards in overload
- Shelf controller for associated GWC in overload
- Network router(s) in overload
- Configuration of router(s) changed so there is not sufficient bandwidth

The potential for call failures is high in this state, to the network operator should recover the immediate cause. Additionally, the customer's network operations may want to closely monitor the system and decide if further network capacity is required.

The alarm is cleared when the message link message loss decreases, the critical alarms is raised or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

Associated alarm message: ABI external messaging alarm Degraded - Alarm Set (or Alarm cleared)

Severity: Minor - potential to affect service

Cause: Message retransmission in the network has reached a point where the occasional call fails due to increased latency.

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends. Messages are being lost, but the system is able to recover with message retransmissions. However, if this situation continues to escalate, eventually unrecoverable message loss will occur.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover automonously. The network engineering group should be given the collected information to determine if further network build-out or tweaking of network parameters is required.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all)of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI cards in overload
- MG9K OC3 cards in overload
- Shelf controller for associated GWC in overload
- Network router(s) in overload
- Configuration of router(s) changed so there is not sufficient bandwidth

The alarm is cleared when the message link message loss decreases, the critical or major alarm is raised or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

23.4 Related documentation

The MG9K ABI cards will also being generating similar alarms. The information the for the new alarms at the MG9K element manager can be found in activity A0003571 documentation.

24: Fault Management (FM): A00003933

This section provides information on logs and alarms for the features under the SIP Gateway application umbrella. Separate sections are provided for the Call Processing, Application Maintenance, and Provisioning logs and alarms.

24.1 SIP Gateway application Call Processing Logs and Alarms

The following is a description of logs and alarms generated by the SIP Gateway application Call Processing. Note that these logs and alarms are only generated and reported on the SIP Gateway application.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page.

Note 1: The body of log formats shown in this document are the formats for Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server Web Interface. However the content of the logs will not differ, only the formatting.

Note 2: When viewing logs from an IEMS, log headers may differ slightly from what is shown in this document.

24.1.1 SIP Gateway application Call Processing Logs

The SIP Gateway application Call Processing software produces the following logs:

- SIPC310 - SIP CallP No Database Connection
- SIPC310 (related log) - SIP CallP Database Connection Established
- SIPC 650 - SIP CallP No Data Found
- SIPC301 - All SIP Incoming Msgs Blocked
- SIPC750 - Incoming SIP messages dropped
- STGW700 - SIP Call Processing Application Logs

24.1.1.1 SIPC310 SIP CallP No Database Connection Log

Log SIPC310 "SIP CallP No Database Connection" is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application, a Critical alarm is generated.

Log Title: SIP CallP

Name: SIPC310

Description: No Database Connection

Event type: Trouble

24.1.1.1.1 Format

For the SIPC 310 log, the following are values/explanations of the variable values:

- alarmLevel = CRIT- Indicates it is a critical alarm
- componentID = SIPC
- category = Communications - Indicates communication failure between CallP and the database
- description = No Database Connection
- probableCause = outOfService
- specificProblem = Communication failure with Database
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportName = SIPC
- reportNum = 310
- eventType = TBL
- label = SIP CallP

The following is a sample log:

```
May 19 14:02:54 ngss4 alarmd: SIPC310 CRIT TBL SIP CallP
NCGL=ngss4;Unit=0;SIPC No Database Connection
```

24.1.1.1.2 Action

Establish connectivity between CallP and the Database.

24.1.1.1.3 Associated Operational Measurements or Performance Measurements

None

24.1.1.2 SIPC310 SIP CallP Database Connection Established Log

A second associated SIPC310 log is generated "SIP CallP Database Connection Established" when the connection that caused the first SIPC310 log is re-established and the alarm is cleared.

Log Title: SIP CallP

Name: SIPC3100

Description: Database Connection Established

Event type: Trouble

24.1.1.2.1 Format

For the SIPC 310 alarm and related log, the following are values/explanations of the variable values:

- alarmLevel = None - Indicates that the alarm is cleared
- componentID = SIPC
- category = Communications - Indicates communication failure between CallP and the database has been established
- description = Database Connection Established
- probableCause = outOfService
- specificProblem = Communication Established with Database
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportNum = 310
- eventType = TRBL
- label = SIP CallP

The following is a sample log:

```
May 19 14:03:34 ngss4 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=ngss4;Unit=0;SIPC Automatically cleared due to alarm generator
process death
```

24.1.1.2.2 Action

None

24.1.1.2.3 Associated Operational Measurements or Performance Measurements

None

24.1.1.3 SIPC 650

The SIPC 650 log is an informational log that is generated when the CallP application goes to get data from the database for a particular table and no data is found.

Log Title: IP CallP

Name: SIPC 650

Description: No Data Found

Event type: Info

24.1.1.3.1 Format

For the SIPC 650 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 650
- Alarm Value = NONE
- Event Type = INFO
- label = "No Data Found:" <data type>

The following is a sample log:

```
May 13 13:32:17 JOEBOB sipgwyappln: SIPC650 NONE INFO SIP CallP No
Data Found: ACCESS LINK MAP
```

24.1.1.3.2 Action

None

24.1.1.3.3 Associated Operational Measurements or Performance Measurements

None

24.1.1.4 SIPC301

The SIPC301 log is a critical log that is generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages due to Access Control List being enabled and no valid entries in the Remote SIP server or ACL list.

Log Title: All Incoming SIP Msgs Blocked

Name: SIPC301

Description: ACL enabled without valid entries

Event type: Trouble

24.1.1.4.1 Format

For the SIPC301 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 301
- Alarm Value = CRIT
- Event Type = TBL
- label = “All SIP Incoming Msgs Blocked" <data type>

The following is a sample log:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC301 CRIT TBL All SIP
Incoming Msgs Blocked
```

24.1.1.4.2 Action

None

24.1.1.4.3 Associated Operational Measurements or Performance Measurements

None

24.1.1.5 SIPC750

The SIPC750 log is generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions.

A Minor, Major or Critical log is generated based on the number of SIP messages dropped in last 15 minutes:

- Minor Threshold: 25
- Major Threshold: 100
- Critical Threshold: 500

Log Title: SIP Access Control List

Name: SIPC750

Description: Incoming SIP messages dropped

Event type: Trouble

24.1.1.5.1 Format

For the SIPC301 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 750
- Alarm Value = MIN/MAJ/CRIT
- Event Type = TBL
- label = "SIP Access Control List" <data type>

The following is a sample log:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC750 CRIT TBL Incoming 600
SIP messaged dropped
```

24.1.1.5.2 Action

None

24.1.1.5.3 Associated Operational Measurements or Performance Measurements

None

24.1.1.6 STGW700 - SIP Call Processing Application Logs

The following is a description of the customer logs generated by SIP call processing application. SIP Call Processing Application Logs are INFO logs which can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server.

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: STGW700 NONE INFO SIPCALLP <LogMessage>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <LogMessage>:
  - PostGainNotifyCallp Called on INACTIVE side
  - Sync call to the standby unit failed with callid *callId*
  - GCP NewCall received for Unsupported Agent : *agentType*
  - No more CallDataBlocks to process CallID: *callId*
  - Failed to add ISUP payload for call *callId*
  - Remote SIP server not mapped for SIP LINK Index *SipLinkIdx*
  - No Active Server for SIP Link *SipLinkIdx*
  - HandleNewCall::Failed to Set MDB for callid *callId*
  - No GCP Nodes to process call with callid *callId*
  - Unauthorized Call attempt from MGC *DestMgc*
  - HandleSipUPDATERequest::MDB Parsing for UPDATE failed for callid *callId*
  - HandleACK::MDB Parsing for ACK failed for callid *callId*
  - Handle200OKINVITERecvd::MDB Parsing for 200 OK INVITE failed for callid *callId*
  - Incompatible media format received in 200 OK response to INVITE.
  - Handle200OKINVITERecvd::Failed to send ACK for callid *callId*
  - Handle200OKINVITERecvd::Failed to get Outbound Message for callid *callId*
  - Handle200OKINVITERecvd::Failed to add 305 warning header for callid *callId*

- HandleReINVITE::MDB Parsing for Re INVITE failed for callid *callId*
- HandleSipINFORequest::MDB Parsing for INFO failed for callid *callId*
- HandleACKReINVITE::MDB Parsing for ACK failed for callid *callId*
- new message received with bad syntax start-line. *msgDestName*
- new message received with bad syntax. *msgDestName*
- Unable to Get Received Message (ACK) for callid *callId*
- *Module*:*Procedure* Null App Call Context
- *Module*:*Procedure* Unable to Get Received Message
- Media Error: CALLID: *callId* - 488 Not Acceptable Here Received
- Media Error: CALLID: *callId* - 606 Not Acceptable Received
- Incompatible media format, call rejected.
- Media type not available, call rejected.
- GCP Socket Open Failed
- Failed to get Active IP Address
- Bind for GCP Socket Failed
- supportedExtensionList was Null defaulted to 100rel
- NGSS Profile Data Creation Failed for Server *sipServerName*

Following is a sample STGW700 log:

```
May 11 15:09:33 sp2k-1 sipgwyappln: STGW700 NONE INFO SIPCALLP
supportedExtensionList was Null defaulted to 100rel
```

24.1.2 SIP Gateway application Call Processing Alarms

24.1.2.1 SIP Gateway CallP ACL Trouble Alarm

This alarm is raised when incoming SIP messages are dropped due to Access Control List enforcements. The alarm handler polls for dropped messages every 15 minutes. The severity of the alarm is based on the number of packets dropped in last 15 minute time interval. The severities include

- Minor Threshold: A minor alarm is raised if 25 or more messages (but less than 100) are dropped.
- Major Threshold: A major alarm is raised if 100 or more messages (but less than500) are dropped.
- Critical Threshold: A major alarm is raised if 500 or more messages are dropped.

If no messages are dropped in the next 15 minutes, the raised alarmed is cleared.

SIPC 750 logs are generated for each of the alarms as described in logs section.

24.2 SIP Gateway Application Maintenance Logs and Alarms

The following is a description of logs and alarms generated by the SIP Gateway Application Maintenance software. Note that these logs and alarms are only generated and reported on the SIP Gateway application, and are not resident on the DMS core for example.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page.

The following information corresponds to the content delivered in the SN07 release, and may be updated for following releases.

24.2.1 SIP Gateway Application Maintenance Logs

The SIP Gateway Application Maintenance software produces the following logs:

- SIPM500 - SIP Gateway Maintenance State Change Log
- SIPM300 - SIP Gateway Maintenance Trouble Log
- SIPM301 - SIP Gateway Maintenance Trouble Alarm Log
- SIPM302 - SIP Gateway Maintenance Sync Trouble Alarm Log

24.2.1.1 SIPM500 - SIP Gateway Maintenance State Change Log

This is an INFO log which is generated any time the SIP Gateway Application maintenance state changes.

Following is the format of this log:

```
<Date> <Time> <DeviceName> sipgwymtc: SIPM500 NONE INFO SIP Gateway Maintenance State Change
        [Administrative : <AdminFrom> -> <AdminTo>]
        [Operational    : <OperFrom>  -> <OperTo>]
        [Control        : <CtrlFrom>  -> <CtrlTo>]
        [Procedural     : <ProcFrom>  -> <ProcTo>]
        [User Requested : <Yes|No>]
        [Reason         : <StateChangeReason>]
        [Web User ID    : <webuserid>]
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <AdminFrom> and <AdminTo>:
  - — Locked
  - — Unlocked
  - — Shutting Down

- <OperFrom> and <OperTo>:
  - — Enabled
  - — Disabled
- <CtrlFrom> and <CtrlTo>:
  - — Suspended
  - — Not Suspended
- <ProcFrom> and <ProcTo>:
  - — Terminating
  - — Not Terminating
- <StateChangeReason>:
  - — Unsuspend command issued
  - — Suspend command issued
  - — Lock command issued
  - — Lock command in progress
  - — Lock operation complete
  - — Unlock command issued
  - — Shut Down command issued
  - — Shut Down operation complete
  - — System originated change of state
  - — Timeout waiting to terminate call processing
  - — Audit Failure
  - — Timer Problem
  - — Data corruption detected
- <webuserid>: If applicable, this is the web interface login ID of the user performing the maintenance that caused the state transition. If not applicable, this value is left blank.

Following is a sample SIPM500 log:

```
Apr 12 10:45:06 RTPF-SIP0 sipgwymtc: SIPM500 NONE INFO SIP Gateway Maintenance State Change
        [Administrative : Locked          -> Unlocked]
        [Operational    : Enabled         -> Enabled]
        [Control        : Not Suspended   -> Not Suspended]
        [Procedural     : Not Terminating -> Not Terminating]
        [User Requested : Yes]
        [Reason         : Unlock command issued]
        [Web User ID    : mtc]
```

24.2.1.2 SIPM300 - SIP Gateway Maintenance Trouble Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Application Maintenance software encounters an unexpected condition.

Following is the format of this log:

```
<Date> <Time> <DeviceName> sipgwymtc: SIPM300 NONE TBL  SIP Gateway Maintenance Trouble
        [Reason Text : <TroubleReason>]
        [Error Code  : <ErrorCode>]
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <TroubleReason>:
  - — SAM to Web Server message send failure
  - — SAM to SIP CallP message send failure
  - — Been Terminating too long. Timer Expired.
  - — SAM Wait Timer Messaging Timeout
  - — SAM/SIP CallP Audit Messaging Timeout
  - — Failed to set the SIP Gateway Application state
  - — SIP Gateway Application process death
  - — Failed to start the SIP Gateway Application process
  - — Failed to set a timer
  - — SIP CallP created, but not in the requested state
  - — SIP CallP created, but failed to reply to SAM
  - — SIP CallP on the Inactive failed to respond to a request
  - — SIP CallP on the Inactive failed to get to the requested state
  - — SAM failed to send a reply to a platform swact request
  - — SAM failed a Swact Request due to an invalid Swact Request
  - — SAM failed a Graceful Swact Request due to being marked to do a COLD Swact
  - — SAM failed a Swact Precheck Request due to option = FORCE
  - — SAM failed a Swact Precheck or PreSwact request due to option = NOW
  - — SAM failed a Swact Request due to an invalid option
  - — SAM failed a Swact Request due to an unacceptable platform status

- SAM failed a Swact Request due to not being In-Sync
- Swact Precheck Failed due to failure received in SIP CallP response
- Swact Precheck Failed due to failure to notify SIP CallP
- Swact Precheck Failed due to timeout waiting on SIP CallP response
- Swact PreSwact Failed due to failure received in SIP CallP response
- Swact PreSwact Failed due to failure to notify SIP CallP
- Swact PreSwact Failed due to timeout waiting on SIP CallP response
- Swact AbortSwact Failed due to failure received in SIP CallP response
- Swact AbortSwact Failed due to failure to notify SIP CallP
- Swact AbortSwact Failed due to timeout waiting on SIP CallP response
- Swact PostSwact Failed due to failure received in SIP CallP response
- Swact PostSwact Failed due to failure to notify SIP CallP
- Swact PostSwact Failed due to timeout waiting on SIP CallP response
- Disable PreCheck Failed due to failure received in SIP CallP response
- Disable PreCheck Failed due to timeout waiting on SIP CallP response
- Disable PreDisable Failed due to failure received in SIP CallP response
- Disable PreDisable Failed due to timeout waiting on SIP CallP response
- Disable AbortDisable Failed due to failure received in SIP CallP response
- Disable AbortDisable Failed due to timeout waiting on SIP CallP response
- Swact PreSwact Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to failure received from the mate SAM
- Disable PreDisable Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to timeout waiting on mate SAM response
- Disable AbortDisable Failed due to failure received from the mate SAM
- Disable AbortDisable Failed due to failure to notify SIP CallP
- Disable AbortDisable Failed due to timeout waiting on mate SAM response
- Disable Request Failed due to Callback called with existing disable request outstanding

- — Disable Request Failed due to Callback called when platform not active and enabled
- — Disable Inactive Failed due to Callback called when platform not in duplex
- — Disable Inactive PreCheck Failed due to Callback called when SAM had a conflicting wait state
- — Disable Inactive PreDisable Failed due to Callback called when SAM had a conflicting wait state
- — Disable Inactive AbortDisable Failed due to Callback called when SAM had a conflicting wait state
- — Disable PreCheck Failed due to failure to notify SIP CallP
- — Disable PreDisable Failed due to failure to notify the Mate SAM
- — Disable AbortDisable Failed due to failure to notify the Mate SAM
- — Disable Active Failed due to Callback called when platform was in duplex
- — Disable Active Graceful Failed due to Callback called when SIP State was not suspended
- — Disable Callback called with invalid request
- — SAM received a response to a Swact request that contained an invalid request
- — SAM received a response to a Swact request that contained an invalid option
- — SAM received a response to a Swact request that contained an invalid result
- — Mate SAM failed a Prepare For COLD Swact request, reverting to a WARM swact
- — Failed to notify the Mate SAM to Prepare For COLD Swact request, reverting to a WARM swact
- — Timed out waiting on the Mate SAM to respond to a Prepare For COLD Swact request, reverting to a WARM swact
- — SAM failed to register with DataSync

- <ErrorCode>: This is an integer code used for debugging. -1 is the default value.

Following is a sample SIPM300 log:

```
Apr  6 13:24:47 RTPF-SIP0 sipgwymtc: SIPM300 NONE TBL  SIP Gateway Maintenance Trouble
        [Reason Text : SIP Gateway Application process death]
        [Error Code  : -1]
```

24.2.1.3 SIPM301 - SIP Gateway Maintenance Trouble Alarm Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered.

Following is the format of this log:

```
<Date> <Time> <DeviceName> alarmd: SIPM301 <AlarmSeverity> TBL  SIP Gateway Maintenance Trouble
Alarm : <DeviceInfo> <AlarmRaiseLowerText>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <AlarmSeverity>: The current severity of the alarm:
  - CRIT
  - NONE
- <DeviceInfo>: Info that specifies the device to which the alarm pertains
- <AlarmRaiseLowerText>:
  - SIP Gateway Application System Busy
  - SIP Gateway Application System Busy - Alarm Cleared

Following are sample SIPM301 logs:

```
Apr  6 14:39:00 RTPF-SIP0 alarmd: SIPM301 CRIT TBL  SIP Gateway Maintenance Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy


Apr  6 14:39:01 RTPF-SIP0 alarmd: SIPM301 NONE TBL  SIP Gateway Maintenance Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy - Alarm Cleared
```

24.2.1.4 SIPM302 - SIP Gateway Maintenance Sync Trouble Alarm Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Maintenance Sync Trouble Alarm is raised or lowered. This occurs when the SIP Gateway application state gets out of sync, or gets back in sync in a duplex Session Server configuration.

Following is the format of this log:

```
<Date> <Time> <DeviceName> alarmd: SIPM302 <AlarmSeverity> TBL  SIP Gateway Maintenance Sync
Trouble Alarm : <DeviceInfo> <AlarmRaiseLowerText>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <AlarmSeverity>: The current severity of the alarm:
  - — MAJOR
  - — NONE
- <DeviceInfo>: Info that specifies the device to which the alarm pertains
- <AlarmRaiseLowerText>:
  - — SIP Gateway Application Mtc Out Of Sync
  - — SIP Gateway Application Mtc Out Of Sync - Alarm Cleared

Following are sample SIPM302 logs:

```
Apr 13 09:13:15 RTPF-SIP0 alarmd: SIPM302 MAJOR TBL  SIP Gateway Maintenance Sync Trouble Alarm
: NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application Mtc Out Of Sync

Apr 13 09:13:45 RTPF-SIP0 alarmd: SIPM302 NONE TBL  SIP Gateway Maintenance Sync Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application Mtc Out Of Sync - Alarm Cleared
```

24.2.2 SIP Gateway Application Maintenance Alarms

Following are the two alarms the SIP Gateway Application Maintenance software may produce:

- SIP Gateway Maintenance Trouble Alarm
- SIP Gateway Maintenance Sync Trouble Alarm

24.2.2.1 SIP Gateway Maintenance Trouble Alarm

This is a critical alarm that is raised when the SIP Gateway Application transitions to a state that indicates it should be in-service, but is not, and the Session Server unit the application is running on is in an enabled operational state. This “system busied” state is represented by state values as follows:

- Administrative State = Unlocked
- Operational State = Disabled
- Procedural Status = “-” or Not Terminating
- Control Status = “-” or Not Suspended

Call processing cannot occur while in this state.

When the SIP Gateway Application transitions out of this state (automatically or manually) this alarm is lowered. It is also lowered if the Session Server unit the application is running on leaves the enabled operational state.

When this alarm is raised, the system will attempt recovery immediately. If immediate recovery is not successful, reattempts are made automatically every 30 seconds.

A manual method to attempt recovery from this state would entail issuing the following commands from the SIP Gateway Maintenance web browser interface:

- Lock command
- Unsuspend command
- Unlock command

Refer to the SIPM301 logs described above which are generated when this alarm is raised or lowered.

24.2.2.2 SIP Gateway Maintenance Sync Trouble Alarm

This is a major alarm that is raised when the Session Server the SIP Gateway Application is running on is in a duplex configurations with both units in an

enabled operational state, and the SIP Gateway application state becomes out of sync between the two Session Server units.

This alarm is lowered if the Session Server leaves the duplex configuration with both units in an enabled operational state, or if the SIP Gateway application state becomes synchronized between the two Session Server units.

The SIP Gateway application should attempt to sync itself automatically every 30 seconds. If there repeated failures, a manual method to attempt recovery from this condition would entail issuing the following commands from the SIP Gateway Maintenance web browser interface:

- Lock command
- Suspend command
- Unsuspend command
- Unlock command

Refer to the SIPM302 logs described above which are generated when this alarm is raised or lowered.

24.3 Session Server Provisioning Logs and Alarms

The following is a description of logs and alarms generated by the Session Server Provisioning software. The alarms and logs are generated in response to database connectivity changes of state detected by the provisioning watchdog program.

They can be viewed via the CS 2000 Session Server Manager Platform Main web browser page via the ‘Alarms’ and ‘Customer Logs’ buttons.

24.3.1 Session Server Provisioning Logs

The Session Server provisioning software produces the following logs:

- DBSE300 - Database Connectivity Change Log

24.3.1.1 DBSE300 - Solid Database connectivity change Log

This is a Trouble (TBL) log which is generated any time a change in database connectivity is detected. It reports ‘**No Solid DB Connection**’ when database connectivity is lost. It reports ‘**Solid DB Connection Restored**’ when database connectivity is reestablished.

Log Title: No Solid DB Connection

Name: DBSE300

Description: No Database Connection

Event type: Trouble

The DBSE300 "No Database Connection" log is generated in tandem with a Critical alarm due to a loss of connectivity between the Session Server provisioning watchdog program and the Solid database.

Following is the format of this log:

- reportName = DBSE
- reportNum = 300
- eventType = TBL
- alarmValue =
  - CRIT
  - None

- label = **No Solid DB Connection** ~ when database connectivity is lost.
- label = **Solid DB Connection Restored** ~ when database connectivity is restored.

24.3.2 Example Logs

The following is a sample log when the database connection is lost.:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL No Solid DB Connection No
Database Connection
```

The following is a sample log when the database connectivity is restored:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL Solid DB Connection
Restored No Database Connection
```

24.3.3 Action

Take corrective action to restore the unresponsive database.

24.3.4 Associated OMs

None.

24.3.5 Associated Alarms

Critical No Database Connection Alarm

24.4 Session Server Provisioning Alarms

The Session Server Provisioning software produces a critical alarm when it detects a loss of connectivity to the database. An example of this alarm follow:

```
Communications   Out of Service   Monday March 22nd 2004 09:34:54 AM
Critical   No Database Connection
```

When this alarm is raised the provisioning watchdog software will attempt to switch activity to the mate copy of the Session Server platform only if connectivity to the mate's database can be verified.

24.4.1 Action

Take corrective action to restore the unresponsive database.

24.4.2 Associated Logs

DBSE300

25: Fault Management (FM): A00003947

25.1 Fault management strategy

25.2 Fault management tools and utilities

25.3 Logs

25.3.1 Explanation

Log Title:IWBM 800

Name: 1st Threshold Exceeded

Description:The number of interworking bridges in use has exceed a predefined 1st threshold percent of all bridges in the pool
Event type:

Log Title:IWBM 801

Name: 1st Threshold cleared

Description: The number of interworking bridges in use has fallen below the predefined 1st Threshold percent of all bridges in the pool.
Event type:

Log Title:IWBM 802

Name: 2st Threshold Exceeded

Description: The number of interworking bridges in use has exceed a predefined 2nd threshold percent of all bridges in the pool
Event type:

Log Title:IWBM 803

Name: 2nd Threshold Cleared

Description: The number of interworking bridges in use has fallen below the predefined 2nd Threshold percent of all bridges in the pool

Event type:

25.3.2 Format

RTP7 ** IWBM800 SEP17 12:16:55 6600 1st Threshold Exceeded
The number of interworking bridges in use has
exceeded 70 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: 600
Bridge Pool: ENET_to_ATM

RTP7 ** IWBM800 SEP17 12:16:56 6600 1st Threshold Cleared
The number of interworking bridges in use has
fallen below 65 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: 725

Bridge Pool: ENET_to_ATM

RTP7 ** IWBM802 SEP17 12:16:57 6600 2nd Threshold Exceeded
The number of interworking bridges in use has
exceeded 90 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: 200

Bridge Pool: ENET_to_ATM

RTP7 ** IWBM800 SEP17 12:16:58 6600 2nd Threshold Cleared
The number of interworking bridges in use has
fallen below 85 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: 310

Bridge Pool: ENET_to_ATM

Note: This feature is only enhancing the existing IWBM 800, 801, 802 and 803 logs to display bridge pool information. The existing fileds have not been changed. The bridge pool information will be displayed only when the office parameter MULTINET_DISPLAY_ACTIVE is set to “YES”.

25.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Bridge Pool	BRDGGRP datafilled in table NETBRDGE	Identifies the name of the core managed bridge group (pool). Must be datafilled in Table CLLI

25.3.4 Action

Not changed by thei feature

25.3.5 Associated Operational Measurements or Performance Measurements

Not changed by the feature

25.3.6 Additional information

None

25.4 Related documentation

26: Fault Management (FM): A00003971

26.1 Fault management strategy

As a part of this activity the following enhancements are done.

- Some of the existing logs generated for SPMs shall be modified to provide additional data.
- Two new SPM logs, SPM 682 and SPM 683 shall be implemented to report on conditions related to manual reset of CEM/RM and CEM swact trigger respectively.
- A new NODE log, NODE602 shall be implemented to report on the CEM state transition reasons. This log is generated only when the CEM state transitions from Insv to Istb or Insv to Sysb. This log provides the reason for the state transition.

26.2 Fault management tools and utilities

Logutil

26.3 Logs

This section gives details of each log modified/added.

26.3.1 SPM300

26.3.1.1 Explanation

Log Title: Device Fault report

Name: SPM 300

Description:

This log is generated when a fault occurs on a SPM device.

Event type: TBL

26.3.1.2 Format

Figure 1 shows the format and an example of the SPM 300 log after the completion of this activity.

Figure 1 Format and example of SPM 300 log

Format of SPM 300 log

```
<office_id> <alarm> SPM300 <mmmdd hh:mm:ss ssdd> TBL Device Fault Report
          Location   : SPM : <spm_number> <cpk_type> : <cpk_number> Activity:<A or I>
          Status     : <one of the 3 strings given below>
          Problem Description: <text up to 16 chars>
          <text up to 64 chars>
          Action: Replace the following cards in the ordered list.
          Cardlist:
          <device_cardlist>
          Location: <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 300 log

```
STEC207AT ***  SPM300 JUL28 07:02:21 6701 TBL  Device Fault Report
          Location   : SPM : 25   VSP : 7 Activity : A
          Status     : Fault Raised
          Problem Description: Critical
            8I: RM reset reason: Last Gasp
          Action     : Replace the following cards in the order listed.
          Cardlist   :
            Site     Flr   Row FrPos ShfPos ShfPec    Slot
            HOST     3     A   0    59      NTLX66AA  4
            HOST     3     A   0    43      NTLX82AA  8
```

26.3.1.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the device. The status field indicates ‘Fault Raised’ instead of ‘Alarm Raised’. The following table describes the modified fields.

Table 1 SPM 300 field details

Field	Modified/ Added	Value	Description
Activity	Added	A or I	This indicates activity status of the device. A - Active; I - Inactive;
Status	Modified	Fault Raised Fault Cleared Info Only	This indicates whether fault was raised/ cleared or whether the log is meant just for information only.

26.3.1.4 Action

Not applicable.

26.3.1.5 Associated Operational Measurements or Performance Measurements

None.

26.3.1.6 Additional information

None.

26.3.2 SPM500

26.3.2.1 Explanation

Log Title: Device State change report

Name: SPM 500

Description:

This log is generated when a state change occurs on a SPM RM.

Event type: INFO

26.3.2.2 Format

Figure 2 shows the format and an example of the SPM 500 log after completion of this activity.

Figure 2 Format and example of SPM 500 log

Format of SPM 500 log

```
<office_id> <alarm> SPM500 <mmmdd hh:mm:ss ssdd> INFO Device State Change
          Location   : SPM : <spm_number> <cpk_type> : <cpk_number>
          From       :<state> <activity status>
          To         :<state> <activity status>
          Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 500 log

```
RTPY07AW ***  SPM500 AUG28 03:06:11 7700 INFO Device State Change
                   Location: SPM : 10   DLC : 0
                   From    : InSv (Active  )
                   To      : SysB (Inactive)
```

26.3.2.3 Field descriptions

The newly added string along with the state ‘Active/Inactive’ indicates the activity status of the device on which state change is being reported.

Table 2 SPM 500 field details

Field	Modified/ Added	Value	Description
From	Modified	Active/Inactive	In addition to the state of the device, the activity before transition is also indicated.
To	Modified	Active/Inactive	In addition to the state of the device, the activity after transition is also indicated.

26.3.2.4 Action

Not applicable.

26.3.2.5 Associated Operational Measurements or Performance Measurements

None.

26.3.2.6 Additional information

None.

26.3.3 SPM650

26.3.3.1 Explanation

Log Title: SPM Bootloader log (loading passed)

Name: SPM 650

Description:

This log is generated when a SPM bootloader completes load transfer successfully.

Event type: Not applicable

26.3.3.2 Format

Figure 3 shows an format and example of the SPM 650 log after completion of this activity.

Figure 3 Format and example of SPM 650 log

Format of SPM 650 log

```
RTPY07AW      SPM650 <mmmdd hh:mm:ss ssdd> PASS
                 SPM Device Loader Success
        Report:          <report seq. num> OF <total num. of report>
        Device:          SPM <spm num> <device type> <device unit no> Activity : <A or I>
        Result:          Passed
        Load File:       <load file name>
        Elapsed Time:    <elapsed hour>:<elapsed min>:<elapsed sec>
        KiloByte Loaded: <kiloByte downloaded>
```

Example of SPM 650 log

```
RTPY07AW      SPM650 AUG28 02:46:52 8400 PASS
                 SPM Device Loader Success
        Report:          1 OF 1
        Device:          SPM 10 VSP 2 Activity : I
        Result:          Passed
        Load File:       DSP20AM_010012
        Elapsed Time:    00:03:49
        KiloByte Loaded: 2926
```

26.3.3.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the device. The following table gives details of the newly added field.

Table 3 SPM 650 field details

Field	Modified/ Added	Value	Description
Activity	Added	A or I	This indicates activity status of the device. A - Active I - Inactive

26.3.3.4 Action
Not applicable.

26.3.3.5 Associated Operational Measurements or Performance Measurements
None.

26.3.3.6 Additional information
None.

26.3.4 SPM651

26.3.4.1 Explanation
Log Title: SPM Bootloader log (loading Failed)

Name: SPM 651

Description:

This log is generated when a SPM bootloader fails to transfer load.

Event type: Not applicable

26.3.4.2 Format
Figure 4 shows the format and an example of the SPM 651 log after completion of this activity.

Figure 4 Format and example of SPM 651 log

Format of SPM 651 log

```
RTPY07AW   *  SPM651 <mmmdd hh:mm:ss ssdd> FAIL
                 SPM Device Loader Failure
        Report:          <report seq. num> OF <total num. of report>
        Device:          SPM <spm num> <device type> <device unit no> Activity : <A or I>
        Result:          Failed
        Load File:       <load file name>
        Elapsed Time:    <elapsed hour>:<elapsed min>:<elapsed sec>
        Failure Reason:  <kiloByte downloaded>
```

Example of SPM 651 log

```
RTPY07AW   *  SPM651 AUG28 02:11:03 3800 FAIL
                 SPM Device Loader Failure
         Report:          1 OF 1
         Device:          SPM 10 VSP 2 Activity : I
         Result:          Failed
         Load File:       DSP20AM_010012
         Elapsed Time:    00:00:46
         Failure Reason:  Loading Aborted
```

26.3.4.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the device. The following table gives details of the new field added.

Table 4 SPM 651 new field details

Field	Modified/ Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A - Active I - Inactive

26.3.4.4 Action

Not applicable.

26.3.4.5 Associated Operational Measurements or Performance Measurements

None.

26.3.4.6 Additional information

None.

26.3.5 SPM684

26.3.5.1 Explanation

Log Title: Erase Flash log

Name: SPM 684

Description:

This log is generated when a EraseFl command is executed on a CEM MAP.

Event type: INFO

26.3.5.2 Format

Figure 5 shows the format and an example of the SPM 684 log after completion of this activity.

Figure 5 Format and example of SPM 684 log

```
Format of SPM684 log

<Office id> SPM684 <mmmdd hh:mm:ss ssdd>INFO ERASE FLASH
Location: SPM : <spm no> CEM : <unit no> Activity : <A or I>
Userid : <userid>
Description:<one of the 4 strings given below>
Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>


string1 : ERASE FLASH INITIATED
string2 : ERASE FLASH COMPLETED
string3 : ERASE FLASH FAILED
string4 : ERASE FLASH REJECTED


Example of SPM log

RTPY07AW      SPM684 AUG28 03:04:25 4800 INFO ERASE FLASH
        Location    : SPM :  10   CEM : 0 Activity : I
        Userid      : USER1
        Description : ERASE FLASH COMPLETED
```

26.3.5.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the device. The following table gives details about the new field.

Table 5 SPM 651 new field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A -Active I -Inactive

26.3.5.4 Action

Not applicable.

26.3.5.5 Associated Operational Measurements or Performance Measurements

None.

26.3.5.6 Additional information

None.

26.3.6 SPM301

26.3.6.1 Explanation

Log Title: Device Patching Report

Name: SPM 301

Description:

This log is generated when patching fails on a SPM device.

Event type: TBL

26.3.6.2 Format

Figure 6 shows the format and an example of the SPM 301 log after completion of this activity.

Figure 6 Format and example of SPM 301 log

Format of SPM301 log

```
<office_id> <alarm> SPM301 <mmmdd hh:mm:ss: ssdd> TBL  Device Patching Report
         Location   : SPM : <spm_number> <cpk_type> : <cpk_number> Activity:<A or I>
         Status     : <one of the 2 strings given below>
         Location: <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

string 1 : Patching operation failure set
string 2 : Patching operation failure cleared

Example of SPM301 log

```
INTL7006CD  **  SPM301 JAN01 09:50:33 1600 TBL  Device Patching Report
          Location   : SPM : 2   CEM : 1 Activity: I
          Status     : Patching operation failure set
```

26.3.6.3 Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The following table gives details about the new field.

Table 6 SPM 301 new field details

Field	Modified/ Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A -Active I -Inactive

26.3.6.4 Action

Not applicable.

26.3.6.5 Associated Operational Measurements or Performance Measurements

None.

26.3.6.6 Additional information

None.

26.3.7 SPM311

26.3.7.1 Explanation

Log Title: SW exception Report

Name: SPM 311

Description:

This log is generated when software error (SWERR) occurs on a SPM device.

Event type: TBL

26.3.7.2 Format

Figure 7 shows the format and an example of the SPM 311 log after completion of this activity.

Figure 7 Format and example of SPM 311 log

Format of SPM311 log

```
<office_id> <alarm> SPM311 <mmmdd hh:mm:ss ssdd> TBL SW Exception Report
      SPM <node number> <circuit pack> <circuitpackno> : <activity>              Time: <timestamp>
        Filename: <filename>              LineNumber: <linenumber>
        TaskID: <task id>      Index: <index number>          Reason: <reason>
        TaskName: <taskname string>
        ErrStr:    <error string>
        ErrData: <error data>
        Traceback: <traceback>
```

Example of SPM311 log

```
MSH306BB      SPM311 FEB24 03:10:47 5519 TBL  SW Exception Report
           SPM  12 CEM   1 : I                      Time: 03:10:47.145
           Filename: isupSgrpDDMData.cpp      LineNumber: 489
           TaskID: 000000DF      Index:           Reason:
           TaskName: processMipArbitrati
           ErrStr:
           ErrData:   00376230 026B6D24 026B6D1C 026B6D40 00D1FA58
           Traceback: 00D1FD14 00CEA1A4 00D2D044 00D2F598 00D2F894 00D2E87C
```

26.3.7.3 Field descriptions

The newly added field ‘TaskName’ gives the task name for the task Id. The following table gives details about the new field.

Table 7 SPM 311 field details

Field	Modified/ Added	Value	Description
TaskName	Added	String	This indicates taskname corresponding to the taskID field.

26.3.7.4 Action

Not applicable.

26.3.7.5 Associated Operational Measurements or Performance Measurements

None.

26.3.7.6 Additional information

None.

26.3.8 SPM312

26.3.8.1 Explanation

Log Title: Trap log

Name: SPM 312

Description:

This log is generated when a trap occurs in a SPM device.

Event type: TBL

26.3.8.2 Format

Figure 8 shows the format and an example of the SPM 312 log after completion of this activity.

Figure 8 Format and example of SPM 312 log

Format of SPM312 log

```
<office_id> <alarm> SPM312 <mmmdd hh:mm:ss ssdd> TBL Trap
          SPM <node number> <circuit pack> <circuitpackno> : <activity>          Time: <timestamp>
             TaskID: <task id>  TrapNo: <trap number>
             TaskName: <taskname string>
             Instr:   <instruction>      Flt: <fault>     Vector: <vector>
             Traceback: <traceback>
```

Example of SPM312 log

```
MG4K106BG ***  SPM312 MAR03 03:37:59 8963 TBL  Trap
               SPM  64 CEM   0 : A                       Time: 03:37:59.155
               TaskID: 000000D3  TrapNo: 00000001
               TaskName: OmSubsystemStart
               Instr:  009CFB00     Flt: 00000000     Vector: 00000300
              Traceback: 009CF44C 00774B44 01608508 FDFDFDFD FDFDFDFD FDFDFDFD
                         FDFDFDFD FDFDFDFD FDFDFDFD FDFDFDFD
```

26.3.8.3 Field descriptions

The newly added field ‘TaskName’ gives the task name corresponding to the the task Id displayed in the log. The new field is described in the following table.

Table 8 SPM 312 field details

Field	Modified/ Added	Value	Description
TaskName	Added	String	This indicates taskname corresponding to the taskID field.

26.3.8.4 Action

Not applicable.

26.3.8.5 Associated Operational Measurements or Performance Measurements

None.

26.3.8.6 Additional information

None.

26.3.9 SPM331

26.3.9.1 Explanation

Log Title: Failed Device Protection Switch

Name: SPM 331

Description:

This log is generated when sparing fails/is rejected or when PROTFAIL alarm is cleared on a SPM device.

Event type: TBL

26.3.9.2 Format

Figure 9 shows the format and an example of the SPM 331 log after completion of this activity.

Figure 9 Format of SPM 331 log

Format of SPM 331 log

```
<office_id> <alarm> SPM331 <mmmdd hh:mm:ss ssdd> TBL Failed Device Protection Switch
                    Location:  SPM : <spm_number> <cpk_type> : <cpk_number>
                    Status  : <one of the strings given below>
                    Description: <Description string>
                    Reason  : <Failure Reason string>
                    Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 331 log

```
MSH207BL ***  SPM331 NOV27 02:32:27 1100 TBL  Failed Device Protection Switch
                  Location: SPM : 25   VSP : 0
                  Status  : Alarm Raised
                  Description: Manual spare from VSP 1 to VSP 0 failed.
                  Reason  :  dest Config failed!
```

26.3.9.3 Field descriptions

The newly added field ‘Reason’ indicates the Reason for the protection switch failure/refusal. The following table gives details of the new and modified fields.

Table 9 SPM 331 field details

Field	Modified/ Added	Value	Description
Reason	Added	string	This indicates reason for failure/rejection of protection switching for the device.

26.3.9.4 Action
Not applicable.

26.3.9.5 Associated Operational Measurements or Performance Measurements
None.

26.3.9.6 Additional information
None.

26.3.10 SPM682

26.3.10.1 Explanation
Log Title: Resetmod

Name: SPM 682

Description:

This log is generated when CEM/RM is manually reset on the MAP. This log is generated in the following conditions

1> When resetmod command is initiated from the MAP
2> When resetmod command is completed
3> When resetmod command fails
4> When resetmod command is aborted
5> When reset via mate is initiated (on CEM) from the MAP
6> When reset firmware is initiated from the MAP

Event type: INFO

26.3.10.2 Format
Figure 10 shows the format and examples of the SPM 682 log .

Figure 10 Format of SPM 682 log

Format of SPM682 log

```
<Office id> SPM682 <mmmdd hh:mm:ss ssdd> INFO RESETMOD
Location: SPM : <spm no>  <cpk_type> : <cpk_number>
Userid : <userid>
Description:<one of the 7 strings given below>
Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Description strings:

```
Resetmod Initiated
Resetmod Completed
Resetmod Firmware Initiated
Resetmod ViaMate Initiated
Resetmod Rejected
Resetmod Failed
Resetmod Aborted
```

Example of SPM 682 log

```
STEC207AS      SPM682 JUL16 07:31:58 7311 INFO RESETMOD
                Location    : SPM :  25   CEM : 0
                Userid      : USER1
                Description : Resetmod initiated



STEC207AS      SPM682 JUL16 07:31:58 7311 INFO RESETMOD
                Location    : SPM :  25   DSP : 1
                Userid      : USER1
                Description : Resetmod initiated
```

When the resetmod command is issued with the option nowait, the logs are as follows

```
RSN07AOINDY1      SPM682 OCT18 14:59:57 4700 INFO RESETMOD
        Location    : SPM :   1   CEM: 1
        Userid      : ADMIN
        Description : Resetmod initiated


RSN07AOINDY1      SPM682 OCT18 15:04:17 4500 INFO RESETMOD
        Location    : SPM :   1   CEM: 1
        Userid      :
        Description : Resetmod Completed
```

26.3.10.3 Field descriptions

The following table describes each field in detail.

Table 10 SPM 682 field details

Field	Value	Description
INFO RESETMOD	Constant	Indicates that the log is a info log and related to resetmod
spm number	Numeric	Indicates the spm number on which resetmod was initiated
cpk_type	String	This is the circuitpack type on which the manual reset was issued.
cpk_number	Numeric	This is the circuit pack number on which manual reset was issued.
UserId	string	Gives the login ID of the user who issued the reset command.
Description	Resetmod Initiated Resetmod Completed Resetmod Aborted Resetmod Failed Resetmod Firmware Initiated Resetmod ViaMate Initiated Resetmod Rejected	This is a description of the resetmod status.

26.3.10.4 Action

Not applicable.

26.3.10.5 Associated Operational Measurements or Performance Measurements

None.

26.3.10.6 Additional information

None.

26.3.11 SPM683

26.3.11.1 Explanation

Log Title: CEM swact trigger

Name: SPM 683

Description:

This log is generated when CEM swact occurs.

Event type: INFO

26.3.11.2 Format

Figure 11 shows the format of the SPM 683 log .

Figure 11 Format of SPM 683 log

Format of SPM 683 log

```
<office_id> <alarm> SPM683 <mmmdd hh:mm:ss ssdd> INFO CEM Swact Trigger
                    Location:  SPM : <spm_number>
                    Swact Reason: <Description string>
                    Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 683 log

```
MSH207BL      SPM683 NOV27 00:45:30 3300 INFO CEM Swact
                  Location    : SPM : 25   CEM : 0
                  Swact Reason: System Cold switch from CEM 0 to CEM 1.
                                CEM SWACT due to Critical Fault. See NODE logs.
                  Location: SPM  25  Type: DMSCP


MSH207BL      SPM683 NOV27 00:45:05 1900 INFO CEM Swact
                  Location    : SPM : 25   CEM : 0
                  Swact Reason: Manual switch from CEM 0 to CEM 1.
                                No other details.
                  Location: SPM  25  Type: DMSCP
```

26.3.11.3 Field descriptions

The following table describes each field in detail.

Table 11 SPM 683 field details

Field	Value	Description
INFO CEM Swact trigger	Constant	This indicates that the log is a information log related to CEM swact trigger.
spm number	Numeric	Indicates the SPM number on which CEM swact occurred.
Status	No Alarm	Gives the status of the alarm.
Description	String	This gives the description of what triggered the CEM swact.

26.3.11.4 Action

Not applicable.

26.3.11.5 Associated Operational Measurements or Performance Measurements

None.

26.3.11.6 Additional information

None.

26.3.12 NODE 600

26.3.12.1 Explanation

Log Title: System Recovery Action

Name: NODE 600

Description:

This log is generated when a system recovery is happening on a node/unit

Event type: INFO

26.3.12.2 Format

Figure 12 shows an example and format of the NODE 600 log . The activity status is displayed in the log only if the architecture type is not load shared.

Figure 12 Format and example of NODE600 log

Format of NODE600 log

```
NODE600 mmmdd hh:mm:ss ssdd INFO TBL System Recovery Action
  Location= <node>
  Trouble= <trouble_code>
  Action= <user_action>
  Activity=<Activity status A or I>
  Integrated Node Maintenance Detailed Information
  Trouble Reason= <INM trouble condition reason>
```

Example of NODE600 log

```
RTPY07AW     NODE600 AUG28 01:04:40 8300 INFO System Recovery Action
        Location: SPM 12 Unit 1
         System recovery is in progress
         Activity: I
         Integrated Node Maintenance Detailed Information
                  INM retry audit trigger received
                  Information for analysis, no immediate action required
```

26.3.12.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the unit.

Table 12 NODE 600 field details

Field	Modified/ Added	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A -Active I - Inactive

26.3.12.4 Action

Not applicable.

26.3.12.5 Associated Operational Measurements or Performance Measurements

None.

26.3.12.6 Additional information

26.3.13 NODE601

26.3.13.1 Explanation

Log Title: System Status Notification

Name: NODE 601

Description:

This log is generated indicating a status notification.

Event type: INFO

26.3.13.2 Format

Figure 13 shows the format of the NODE 601 log .

Figure 13 Format of NODE 601 log

```
NODE601 <mmmdd hh:mm:ss ssdd> INFO System Status Notification
        Location: <node> <Unit number>
         Activity: <activity status A or I>
         Integrated Node Maintenance Detailed Information
         <Detailed information>
```

Example of NODE 601 log

```
RTP5     NODE601 JUL01 12:23:05 4627 INFO System Status Notification
        Location: SPM 1 Unit 1
         Activity : I
         Integrated Node Maintenance Detailed Information
         Data not synchronized
         Loadname mismatch
         Check datafill and correct if necessary
         Datafill Loadname does not match Loadname in PM
```

26.3.13.3 Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

Table 13 SPM 601 field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A - Active I - Inactive

26.3.13.4 Action

Not applicable.

26.3.13.5 Associated Operational Measurements or Performance Measurements

None.

26.3.13.6 Additional information

None.

26.3.14 NODE302

26.3.14.1 Explanation

Log Title: Software Alarm

Name: NODE 302

Description:

This log is generated when a software fault or alarm occurs.

Event type: TBL

26.3.14.2 Format

Figure 14 shows the format of the NODE 302 log .

Figure 14 Format of NODE 302 log

NODE 302 <mmmdd hh:mm:ss> <ssdd> TBL Software Alarm
Location: <NODE>
Activity:<Activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: Details of trouble

Example of NODE302 log

NODE 302 <mmmdd hh:mm:ss> <ssdd> TBL Software Alarm
Location: SPM 1 Unit 1
Activity: I
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: <Details of trouble>

26.3.14.3 Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

Table 14 NODE 302 field details

Field	Added/Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A - Active I - Inactive

26.3.14.4 Action

Not applicable.

26.3.14.5 Associated Operational Measurements or Performance Measurements

None.

26.3.14.6 Additional information

None.

26.3.15 NODE303

26.3.15.1 Explanation

Log Title: Wrong Application Data

Name: NODE 303

Description:

This log is generated when Wrong Application Data due to manual or system initiated activities is detected.

Event type: TBL

26.3.15.2 Format

Figure 15 shows the format of the NODE 303 log .

Figure 15 Format of NODE 303 log

Format and example of NODE log

NODE 303 <mmmdd hh:mm:ss> <ssdd> TBL Wrong Application Data
Location: <NODE>
Trouble: <Trouble_Type>
Action: <User_Action>
Activity:<Activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: CEM in Slot <slot_number(7or 8)> has Application Data of CEM <cem_number(0 or 1)>

```
NODE303 FEB15 01:57:54 2112 TBL Wrong Application Data
Location: SPM 0 Unit 1
Trouble:  CEM has Application Data of Mate CEM
Action:   Check LINK300 Logs & reconnect DS512 Links correctly
Activity: I
Integrated Node Maintenance Detailed Information
Trouble Reason:  DS-512 Link/Links may be misconnected.
Trouble Detail:  CEM in Slot 8 has Application Data of CEM 0.
```

26.3.15.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the unit.

Table 15 NODE 303 field details

Field	Added/Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A- Active I-Inactive

26.3.15.4 Action
Not applicable.

26.3.15.5 Associated Operational Measurements or Performance Measurements
None.

26.3.15.6 Additional information
None.

26.3.16 NODE326

26.3.16.1 Explanation
Log Title: Hardware Fault

Name: NODE 326

Description:

This log is generated when a hardware fault occurs.

Event type: TBL

26.3.16.2 Format
Figure 16 shows the format of the NODE 326 log .

Figure 16 Format of NODE 326 log

NODE326 <mmmdd hh:mm:ss ssdd> TBL Hardware Fault
Location: <node> <unit number>
Status: <Alarm status>
Trouble: <trouble_code>
Action: <user_action>
Activity: <activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <INM trouble condition reason>
Trouble Detail: <trouble detail>

Example of NODE326 log

```
RSN07AOINDY1  ** NODE326 OCT02 14:55:30 3300 TBL  Hardware Fault
        Location: SPM 3 Unit 0
        Status:   Alarm raised
        Trouble:  Card fault
        Action:   Restore communication with the Resource Processor
         Activity: I
         Integrated Node Maintenance Detailed Information
         Trouble Reason:  Link isolation condition
         Trouble Detail:  Link/Messaging hardware
```

26.3.16.3 Field descriptions

The newly added field ‘Activity’ indicates the activity status of the unit.

Table 16 NODE 326 field details

Field	Added/ Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A-Active I-Inactive

26.3.16.4 Action

Not applicable.

26.3.16.5 Associated Operational Measurements or Performance Measurements

None.

26.3.16.6 Additional information

None.

26.3.17 NODE602

26.3.17.1 Explanation

Log Title: CEM State Change Reason Report

Name: NODE 602

Description:

This log is generated when a CEM unit of an SPM transitions from Insv to Sysb or Insv to Istb.

Event type: INFO

26.3.17.2 Format

Figure 17 shows the format of the NODE 602 log .

Figure 17 Format of NODE 602 log

```
<office_id> <alarm> NODE602 <mmmdd hh:mm:ss ssdd> INFO CEM State Change Reason Report
        Location:  SPM : <spm_number> CEM : <Unit number>
        Reason  : <Description string>
        Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of NODE602 log

```
MSH207BL     NODE602 DEC01 00:38:58 1500 TBL  CEM State Change Reason Report
        Location: SPM:  10   CEM :  0
        Reason  : /RmmMgr/CfltSet
        Location: SPM  10  Type: SMG4      Fabric: ATM
```

26.3.17.3 Field descriptions

The fields in the NODE 602 log are explained below in Table 17, “NODE 602 field details,” on page 2188.

Table 17 NODE 602 field details

Field	Value	Description
INFO CEM State Change Reason Report	Constant	This indicates that the log is a information log related to CEM state change reason.
spm number	Numeric	Indicates the SPM number on which CEM state transition occurred.

Field	Value	Description
CEM unit number	Numeric	This gives the unit number of the CEM which underwent a state transition.
Reason	String	This gives the description of the reason for CEM state transition.

26.3.17.4 Action

Not applicable.

26.3.17.5 Associated Operational Measurements or Performance Measurements

None.

26.3.17.6 Additional information

None.

26.4 Related documentation

None.

27: Fault Management (FM): A00004045

This section provides information on logs and alarms for the features under the Session Server platform.

27.1 Session Server Platform Logs and Alarms

This section describes the logs and alarms generated by the Nortel Carrier Grade Link (NCGL) session server. The logs and alarms can be viewed via the web browser interface on the Succession Communication Server 2000 NCGL Platform Manager - via Alarms panel and Customer Logs panel.

Session Server Alarms/Logs

The NCGL session server platform generate the following logs categories::

- Raid Alarms/Logs
  - — XTS391
  - — XTS691
- Chassis Hardware Alarms/Logs
  - — XTS392
  - — XTS692
- File system Alarms/Logs
  - — XTS395
  - — XTS695
- Platform Maintenance.
  - — XTS300
  - — XTS600
  - — XTS301
  - — XTS601
  - — XTS302
  - — XTS602
  - — XTS303
  - — XTS603
  - — XTS305
  - — XTS605
  - — XTS306

  - XTS606
- Application Maintenance.
  - XTS315
  - XTS615
  - XTS316
  - XTS616
- Network Connectivity Maintenance.
  - XTS331
  - XTS631
  - XTS335
  - XTS635
  - XTS336
  - XTS636
  - XTS351
  - XTS651
- Node Maintenance.
  - XTS355
  - XTS655
  - XTS670
  - XTS671

Field Description

The NCGL alarm/logs are made of the following fields shown in the table given below.

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NCGL or application process unit that generates the report
Log Number	Alphanumeric	The component prefix and number of the log

Severity	Alphanumeric	The log severity (may be related to alarm severity)
Event Type	Alphanumeric	The type of trouble recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

Few example of alarms are given below

Apr 29 10:33:05 yang alarmd: XTS391 MINOR INIT Array Rebuilding NCGL=yang; Array: '/dev/md1' (ntvg) Status: The array is currently being rebuilt.

May 10 13:48:12 yin alarmd: XTS391 MAJOR UNEQ Disk Missing NCGL=yin;Unit=0; Array: '/dev/md1' (ntvg) Status: A physical disk has been removed from the array.

May 6 14:30:09 yin alarmd: XTS691 NONE INIT Array Rebuilt NCGL=yin;Unit=0; Array: '/dev/md1' (ntvg) The array has been rebuilt.

May 10 13:48:37 yin alarmd: XTS691 NONE UNEQ Array Rebuilding NCGL=yin;Unit=0; Array: '/dev/md1' (ntvg) Disk inserted

27.1.1 Raider Alarms/Logs

The Raider software produces the following logs:

27.1.1.1 XTS391

27.1.1.1.1 Explanation

In the event of a disk failure, the fault is reported as an alarm to the SAM XTS and an XTS391 log report is generated. LEDs on the face of the SAM-XTS platform also indicate the failure. Alarm is raised at the STORM Manager and a log report is generated.

The SAM-XTS platform uses two 68.37 GB drives mirrored in a RAID-1 configuration. The SAM-XTS platform mirrors its own load locally, in addition to exported file systems, so that the unit can boot even in the event of one disk failure.

Disk Array Rebuilding alarm indicates that the disk array is being rebuilt after a disk replacement or an uncontrolled shutdown.

27.1.1.1.2 Format

- **When Disk Failure occurs**
  - Alarm/Log: Disk Failure
  - Type: Equipment
  - ID: inputOutputDeviceError
  - Event: FAIL
  - Label: Disk Failure
  - Severity: Major (1 disk fail) or Critical (2 disk fail or removed)
- **When Disk is missing**
  - Alarm/Log: Disk Missing
  - Type: Equipment
  - ID: underlyingResourceUnavailable
  - Event: UNEQ
  - Label: Disk Missing
  - Severity: Major (1 disk removed)
- **When Disk array is rebuilding**
  - Alarm/Log: Disk Rebuilding
  - Type: Equipment
  - ID: performanceDegraded
  - Event: INIT
  - Label: Array Rebuilding
  - Severity: Minor (array rebuilding)

27.1.1.1.3 Field descriptions

See section 12.1

27.1.1.1.4 Action

Check the application status and performance on disk outages.

Click on the Disk services panel tab.

Review the RAID Array Status table.

Under Disk Service Frame, Disk Maintenance window has Disk Insert option if one of the disk is removed it can be inserted if disk is error free.

Monitor the rebuild by periodically clicking the web browser reload button until the rebuild completes.

When the rebuild completes, the alarm clears and an information only XTS691 log report is generated.

27.1.1.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.1.1.6 Additional information

None

27.1.1.2 XTS691

27.1.1.2.1 Explanation

When XTS391 alarm is cleared. XTS391 alarm are due to

Array Rebuilt or Disk Failure or Disk Missing or Array Rebuilding

27.1.1.2.2 Format

- **When Disk Alarms are cleared**
  - Alarm/Log: Disk Rebuilding Clear
  - Event: None
  - Label: "Array Rebuilt" or "Disk Failure" or "Disk Missing" or "Array Rebuilding"
  - Severity: None
  - Log ID: 691

27.1.1.2.3 Field descriptions

See section 12.1

27.1.1.2.4 Action

None

27.1.1.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.1.2.6 Additional information

None

27.1.2 Chassis Hardware Alarms/Logs

The Chassis Hardware related alarms/logs are as follows:

27.1.2.1 XTS392

27.1.2.1.1 Explanation

When there is platform hardware failure an XTS392 alarm is raised on the Alarms panel of the NCGL Session server unit.

27.1.2.1.2 Format

- **Alarm/Log: Magneto Hardware Chassis Fault Alarms / Logs**
  - Type: eAPC_Equipment
  - ID: equipmentMalfunction
  - Event: Fail
  - Label: Chassis Fault
  - Severity: Major
- **Alarm/Log: Self Test Unavailable**
  - Type: eAPC_Equipment
  - ID: underlyingResourceUnavailable
  - Event: UNEQ
  - Label: Self Test
  - Severity: Minor
- **Alarm/Log: Self Test Hardware Error**
  - Type: eAPC_Equipment
  - ID: equipmentMalfunction
  - Event: FLT
  - Label: Self Test
  - Severity: Critical
- **Alarm/Log: Self Test Query Error**
  - Type: eAPC_Equipment
  - ID: communicationsSubsystemFailure
  - Event: FLT

- Label: Self Test
- Severity: Major

- **Alarm/Log: Self Test Corrupted Error**
  - Type: eAPC_Equipment
  - ID: equipmentMalfunction;
  - Event: FLT
  - Label: Self Test
  - Severity: Major
- **Alarm/Log: Self Test Device Failure**
  - Type: eAPC_Equipment
  - ID: equipmentMalfunction;
  - Event: FLT
  - Label: Self Test
  - Severity: Major

27.1.2.1.3 Field descriptions

See section 12.1

27.1.2.1.4 Action

Click on the System Status panel tab.

Review the Chassis Information table.

Record the error message, gather XTS log reports, and contact Nortel Networks support personnel for assistance.

27.1.2.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.2.1.6 Additional information

None

27.1.2.2 XTS692

27.1.2.2.1 Explanation

When XTS392 alarm is cleared this log is generated.

27.1.2.2.2 Format

- Alarm/Log: Self Test Device Clear
  - — Event: None
  - — Label: "Self Test" or "Chassis OK"
  - — Severity: None
  - — Log ID: 692

27.1.2.2.3 Field descriptions

See section 12.1

27.1.2.2.4 Action

None

27.1.2.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.2.2.6 Additional information

None

27.1.3 File System Alarms/Logs

The Magnum software produces the following logs:

27.1.3.1 XTS395

27.1.3.1.1 Explanation

An alarm is raised on the Alarms panel of the SAM XTS when the filesystem Threshold Crossed or when there is an error in Filesystem.

Minor severity alarms indicate that the filesystem is full and a request to write data to the filesystem by the system test process failed.

Critical severity alarms indicate that the system encountered an error with at least one of the following sequential operations:

- — create a directory on the filesystem
- — create a file on the filesystem
- — write to the file (if only this test fails because the filesystem is too full, the alarm is minor)

- read from the file
- delete the file
- delete the directory

27.1.3.1.2 Format

- **Alarm/Log: Self Test Device Filesystem Threshold Exceeded**
  - Type: QualityOfService
  - ID: thresholdCrossed;
  - Event: THR
  - Label: Threshold exceeded
  - Severity: Minor or Major or Critical
- **Alarm/Log: Filesystem Test Failure**
  - Type: Equipment
  - ID: inputOutputDeviceError;
  - Event: FLT
  - Label: Filesystem Error
  - Severity: Minor (low disk space) or Critical (filesystem test fail)

27.1.3.1.3 Field descriptions

See section 12.1

27.1.3.1.4 Action

Click on the Disk service panel tab.

Review the Filesystem Information table.

If the alarm is minor, determine if the filesystem size is engineered too low.If so, increase the size of the filesystem, and the alarm will clear. Determine how the space is being used.

If the alarm is Critical, contact Nortel Networks support personnel for assistance.

27.1.3.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.3.1.6 Additional information

May 4 13:02:58 fred alarmd: XTS395 MINOR FLT Filesystem Error NCGL=fred;Unit=0 Status: Alarm raised. Filesystem is < /boot >. Test results: Stat(Success) CreateDir(Success) CreateFile(Success) WriteFile(No space left on device) ReadFile(Success) RemoveFile(Success) RemoveDir(Success)

27.1.3.2 XTS695

27.1.3.2.1 Explanation

When XTS395 alarm is cleared his log is generated.

27.1.3.2.2 Format

- **Alarm/Log: Clear Logs**
  - — Event: None
  - — Label: "Threshold exceeded" or "Filesystem Error"
  - — Severity: None
  - — Log ID: 695

27.1.3.2.3 Field descriptions

See section 12.1

27.1.3.2.4 Action

None

27.1.3.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.3.2.6 Additional information

None

27.1.4 Platform Maintenance Alarms/Logs

The Madman & Swmon software produces the following logs:

27.1.4.1 XTS300

27.1.4.1.1 Explanation

An alarm is raised on the Alarms panel of the NCGL session server. An XTS300 log report is generated and is available for viewing from the Customer Logs panel of the NCGL session server.

This alarm is raised when Memory usage on the NCGL session server unit is excessive.

27.1.4.1.2 Format

- **Alarm/Log: OutofMemory**
  - Type: QualityOfService
  - ID: outOfMemory
  - Event: FLT
  - Label: Memory
  - Severity:Minor,Major or Critical

27.1.4.1.3 Field descriptions

27.1.4.1.4 Action

Click on the System Status panel tab.

Review the Memory Information table.

For minor or major : Monitor the alarm and contact Nortel Networks support personnel.

For critical : Check the unit activity status and swact if the unit is Active. Then do rebootmate the failure NCGL Session server unit from the Admin panel of Active unit. Contact Nortel Networks support personnel for additional support if the alarm persist.

27.1.4.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.1.6 Additional information

None

27.1.4.2 XTS600

27.1.4.2.1 Explanation

When XTS300 minor, major or critical alarm is cleared, a INFO alarm/log XTS600 is generated.

27.1.4.2.2 Format

- **Alarm/Log: Application Memory**
  - — Type: QualityOfService
  - — ID: outOfMemory
  - — Event: INFO
  - — Label: Application Memory Alarm Cleared
  - — Severity:NONE

27.1.4.2.3 Field descriptions

See section 12.1

27.1.4.2.4 Action

None

27.1.4.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.2.6 Additional information

None

27.1.4.3 XTS301

27.1.4.3.1 Explanation

When too many processes are waiting in the process queue an alarm is raised on the Alarms panel of the NCGL session server. An XTS300 log report is generated and is available for viewing from the Customer Logs panel of the NCGL session server.

27.1.4.3.2 Format

- Alarm/Log: CPU Load
  - — Type: QualityOfService
  - — ID: cpuCyclesLimitExceeded

— Event: FLT

— Label: CPU Load

— Severity:Minor,Major or Critical

27.1.4.3.3 Field descriptions

See section 12.1

27.1.4.3.4 Action

Click on the System Status panel tab.

Review the current load average from the CPU Information table and the number of zombie processes from the Process Information table.

If zombie processes are present the CPU alarm is minor or major :

Zombie processes could be causing the CPU high load. Wait for a period of low office traffic, and reboot the NCGL session server unit from the Admin panel.

If the CPU alarm is minor or major and no zombie processes are present:

The unit is in a period of heavy load. Monitor the CPU load by clicking the reload button. Also look into Additional information given below for any cause and related diagnosing.

The CPU alarm is critical but the 1 minute and 5 minute loads are less than the 15 minute load

The unit endured a prolonged period of heavy load but the load is diminishing. Monitor the CPU load by clicking on the reload button. If the CPU load is falling, continue to monitor the load and refer to Additional information given below for information about diagnosing this alarm.

The CPU alarm is critical and the load for all time periods is rising

The load exceeds the capacity of the unit. reboot the unit from the Admin panel.

27.1.4.3.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.3.6 Additional information

Consider the following factors that could cause a temporary rise in CPU load:

Rebuilding a disk array while under heavy load

A SIP call processing application image dump while under heavy load

Lack of free space on the "/" filesystem. This mount point is a ramdisk and cannot be increased. An alarm report indicate a lack of storage.

Excessive network traffic on the Communications Server LAN (CS LAN).

27.1.4.4 XTS601

27.1.4.4.1 Explanation

This alarm is reported when XTS301 minor/major/critical alarm is cleared

27.1.4.4.2 Format

- **Alarm/Log: CPU Alarm Cleared**
  - Type: QualityOfService
  - ID: cpuCyclesLimitExceeded
  - Event: INFO
  - Label: CPU Alarm Cleared
  - Severity:NONE

27.1.4.4.3 Field descriptions

See section 12.1

27.1.4.4.4 Action

None

27.1.4.4.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.4.6 Additional information

None

27.1.4.5 XTS302

27.1.4.5.1 Explanation

When Not enough space is available to meet storage needs.an alarm is raised on the Alarms panel of the NCGL session server. An XTS302 log report is generated and is available for viewing from the Customer Logs panel of the NCGL session server.

27.1.4.5.2 Format

- **Alarm/Log: Disk/Storage FLT**
  - Type: ProcessingError
  - ID: storageCapacityProblem
  - Event: FLT
  - Label: Disk
  - Severity:Minor,Major or Critical

27.1.4.5.3 Field descriptions

See section 12.1

27.1.4.5.4 Action

Click on the Disk Service panel tab.

Review the Filesystem Information table.

If the alarm is raised against the “/” filesystem Contact Nortel Networks support personnel.

If the alarm is raised against the /boot filesystem Remove previous software loads from the Admin panel.

Else increase the size of the filesystem. Refer to Increasing filesystem size in Configuration management document.

27.1.4.5.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.5.6 Additional information

None

27.1.4.6 XTS602

27.1.4.6.1 Explanation

This alarm is reported when XTS302 minor/major/critical alarm is cleared.

27.1.4.6.2 Format

- **Alarm/Log: Disk Alarm Cleared**
  - Type: ProcessingError
  - ID: storageCapacityProblem
  - Event: INFO
  - Label: Disk Alarm Cleared
  - Severity: NONE

27.1.4.6.3 Field descriptions

See section 12.1

27.1.4.6.4 Action

None

27.1.4.6.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.6.6 Additional information

None

27.1.4.7 XTS303

27.1.4.7.1 Explanation

When the number of zombie processes has exceeded the threshold specified on the System panel an alarm is raised on the Alarms panel of the NCGL session server. An XTS303 log report is generated and is available for viewing from the Customer Logs panel of the NCGL session server.

27.1.4.7.2 Format

- **Alarm/Log: Zombie Process**

- Type: QualityOfService
- ID: thresholdCrossed
- Event: FLT
- Label: Zombie Process
- Severity: Minor,Major or Critical

27.1.4.7.3 Field descriptions

See section 12.1

27.1.4.7.4 Action

Click on the System Status panel tab.

Review the number of zombie processes.

If the alarm is minor or major and no CPU threshold crossing alarms are present

Wait for a period of low office traffic, reboot the unit from the Admin panel.

The alarm is minor or major and CPU threshold crossing alarms are present or the alarm is critical

Reboot the unit from the Admin panel.

27.1.4.7.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.7.6 Additional information

None

27.1.4.8 XTS603

27.1.4.8.1 Explanation

This alarm is reported when XTS303 minor/major/critical alarm is cleared.

27.1.4.8.2 Format

- **Alarm/Log: Zombie Process Alarm Cleared**
  - Type: QualityOfService
  - ID: thresholdCrossed

— Event: INFO

— Label: Zombie Process Alarm Cleared

— Severity:NONE

27.1.4.8.3 Field descriptions

See section 12.1

27.1.4.8.4 Action

None

27.1.4.8.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.8.6 Additional information

None

27.1.4.9 XTS305

27.1.4.9.1 Explanation

The platformsoftware lost time synchronization to one or more Network Time Protocol (NTP) servers or the drift is excessive.

27.1.4.9.2 Format

- **Alarm/Log: NTP Related**
  - — Type: Communications
  - — ID: communicationsProtocolError
  - — Event: FLT
  - — Label: NTP Error
  - — Severity:Minor, Major or Critical

27.1.4.9.3 Field descriptions

See section 12.1

27.1.4.9.4 Action

Click on the Services panel tab.

Review the NTP related information.

The provisioned NTP information is displayed. Ensure that the IP addresses in the remote column match the NTP servers provisioned at the NCGL session server unit. If provision data is right, refer to NTP product document or Contact Nortel Networks support personnel.

27.1.4.9.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.9.6 Additional information

None

27.1.4.10 XTS605

27.1.4.10.1 Explanation

This alarm is reported when XTS305 minor/major/critical alarm is cleared.

27.1.4.10.2 Format

- **Alarm/Log:NTP Alarm Cleared**
  - Type: Communications
  - ID: communicationsProtocolError
  - Event: INFO
  - Label: NTP Alarm Cleared
  - Severity: NONE

27.1.4.10.3 Field descriptions

See section 12.1

27.1.4.10.4 Action

None

27.1.4.10.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.10.6 Additional information

None

27.1.4.11 XTS306

27.1.4.11.1 Explanation

The CPU utilization for one or more time segments has exceeded the threshold.

27.1.4.11.2 Format

- **Alarm/Log: CPU Utilization**
  - Type: QualityOfService
  - ID: cpuCyclesLimitExceeded
  - Event: FLT
  - Label: CPU Utilization
  - Severity:Minor, Major or Critical

27.1.4.11.3 Field descriptions

See section 12.1

27.1.4.11.4 Action

Click on the System Status panel tab.

Review the of CPU Utilization.

If the alarm is critical monitor the status and performance of the application.

27.1.4.11.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.11.6 Additional information

None

27.1.4.12 XTS606

27.1.4.12.1 Explanation

This alarm is reported when XTS306 minor/major/critical alarm is cleared.

27.1.4.12.2 Format

- **Alarm/Log:CPU Utilization Cleared**
  - Type: QualityOfService
  - ID: cpuCyclesLimitExceeded,
  - Event: INFO
  - Label: CPU Utilization Cleared
  - Severity:NONE

27.1.4.12.3 Field descriptions

See section 12.1

27.1.4.12.4 Action

None

27.1.4.12.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.12.6 Additional information

None

27.1.4.13 XTS309

27.1.4.13.1 Explanation

The unit has a bus fault, Error Checking and Correction (ECC) memory fault, or a parity error or any hardware component failure.

27.1.4.13.2 Format

- **Alarm/Log: Hardware FLT**
  - Type: Equipment
  - ID: equipmentMalfunction
  - Event: FLT
  - Label: Hardware Fault
  - Severity:Minor, Major or Critical

27.1.4.13.3 Field descriptions

See section 12.1

27.1.4.13.4 Action

Click on the Alarm panel tab.

Review the Hardware fault alarms.

If the severity is minor & unit is Inactive, Jam the unit from active unit. Perform a reboot on the faulty unit and Unjam it from active unit when its back to service.

If the severity is critical reboot the unit. In case of failure even after reboot, Contact Nortel Networks support personnel.

27.1.4.13.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.13.6 Additional information

None

27.1.4.14 XTS609

27.1.4.14.1 Explanation

This alarm is reported when XTS309 minor/major/critical alarm is cleared.

27.1.4.14.2 Format

- **Alarm/Log:Hardware Fault Cleared**
  - Type: Equipment
  - ID: equipmentMalfunction
  - Event: INFO
  - Label: Hardware Fault Cleared
  - Severity: NONE

27.1.4.14.3 Field descriptions

See section 12.1

27.1.4.14.4 Action

None

27.1.4.14.5 Associated Operational Measurements or Performance Measurements

None

27.1.4.14.6 Additional information

None

27.1.5 Application Alarms/Logs

The Application software produces the following logs:

27.1.5.1 XTS315

27.1.5.1.1 Explanation

This alarm is reported during swact operation when the unit State has changed from Standby Enabled to Standby Disabled."

27.1.5.1.2 Format

- **Alarm/Log: Application Out-of-Sync**
  - Type: ProcessingError
  - ID: applicationSubsystemFailure
  - Event: FLT
  - Label: Application Out-of-Sync (simplex)
  - Severity:Minor, Major or Critical

27.1.5.1.3 Field descriptions

See section 12.1

27.1.5.1.4 Action

Click on the Alarm panel tab.

Review the Application fault alarms.

This alarm is raised during a transition state. No action is required.

27.1.5.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.5.1.6 Additional information

None

27.1.5.2 XTS615

27.1.5.2.1 Explanation

This alarm is reported after successful swact operation when unit State has changed from Standby Disabled to Standby Enabled.

27.1.5.2.2 Format

- **Alarm/Log:Application In-Sync**
  - Type: ProcessingError
  - ID: applicationSubsystemFailure
  - Event: INFO
  - Label: Application In-Sync
  - Severity:NONE

27.1.5.2.3 Field descriptions

See section 12.1

27.1.5.2.4 Action

None

27.1.5.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.5.2.6 Additional information

None

27.1.5.3 XTS316

27.1.5.3.1 Explanation

The alarm has minor severity if the alarm is raised against the inactive application. The alarm has critical severity if the alarm is raised against the active application.

27.1.5.3.2 Format

- **Alarm/Log: Application Out-of-Service**

- Type: ProcessingError
- ID: outOfService
- Event: FLT
- Label: Application Out-of-Service
- Severity:Minor, Major or Critical

27.1.5.3.3 Field descriptions

See section 12.1

27.1.5.3.4 Action

Click on the Alarm panel tab.

Review the Application fault alarms.

This alarm is raised during a transition state. No action is required.

27.1.5.3.5 Associated Operational Measurements or Performance Measurements

None

27.1.5.3.6 Additional information

None

27.1.5.4 XTS616

27.1.5.4.1 Explanation

This alarm is reported when XTS316 minor/major/critical alarm is cleared.

27.1.5.4.2 Format

- **Alarm/Log:Application In-Service**
  - Type: ProcessingError
  - ID: outOfService
  - Event: INFO
  - Label: Application In-Service
  - Severity: NONE

27.1.5.4.3 Field descriptions

See section 12.1

27.1.5.4.4 Action

None

27.1.5.4.5 Associated Operational Measurements or Performance Measurements

None

27.1.5.4.6 Additional information

None

27.1.6 Network Maintenance Alarms/Logs

The Netmon software produces the following logs:

27.1.6.1 XTS331

27.1.6.1.1 Explanation

A remote host monitor has failed. This failure indicates a loss of connectivity to the monitored unit.

27.1.6.1.2 Format

- **Alarm/Log: Mate Connectivity**
  - Type: Communications
  - ID: communicationsSubsystemFailure
  - Event: FLT
  - Label: Mate Connectivity
  - Severity:Minor, Major or Critical

27.1.6.1.3 Field descriptions

See section 12.1

27.1.6.1.4 Action

Click on the Network Connectivity panel tab.

Review the Network connectivity Information.

Use the following list of possible causes to clear the alarm:

- The unit is offline due to maintenance or an uncontrolled failure
- Communication to the unit is unavailable due to a router failure or misconfiguration
- Cable failure at the remote unit

27.1.6.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.1.6 Additional information

None

27.1.6.2 XTS631

27.1.6.2.1 Explanation

This alarm is reported when XTS331 minor/major/critical alarm is cleared.

27.1.6.2.2 Format

- **Alarm/Log : Mate Connectivity Restored**
  - Type: Communications
  - ID: communicationsSubsystemFailure
  - Event: INFO
  - Label: Mate Connectivity Restored
  - Severity: NONE

27.1.6.2.3 Field descriptions

See section 12.1

27.1.6.2.4 Action

None

27.1.6.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.2.6 Additional information

None

27.1.6.3 XTS335

27.1.6.3.1 Explanation

A major severity alarm indicates that one of the Ethernet links is unavailable. A critical severity alarm indicates that both of the Ethernet links are unavailable. If both Ethernet links are unavailable, the Call Agent reboots.

27.1.6.3.2 Format

- **Alarm/Log: Link Connectivity**
  - Type: Communications
  - ID: communicationsSubsystemFailure
  - Event: FLT
  - Label: Link Connectivity
  - Severity:Minor, Major or Critical

27.1.6.3.3 Field descriptions

See section 12.1

27.1.6.3.4 Action

Click on the Network Connectivity panel tab.

Review the Network connectivity Information.

Follow Action suggested in Mate Connectivity section XTS331.

If Link0, Link1 in-service (INSV) and the alarm persists, contact Nortel Networks support personnel. 4 This procedure is complete.

27.1.6.3.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.3.6 Additional information

None

27.1.6.4 XTS635

27.1.6.4.1 Explanation

This alarm is reported when XTS335 minor/major/critical alarm is cleared.

27.1.6.4.2 Format

- **Alarm/Log : Link Connectivity Restored**
  - Type: Communications
  - ID: communicationsSubsystemFailure
  - Event: INFO
  - Label: Link Connectivity Restored
  - Severity: NONE

27.1.6.4.3 Field descriptions

See section 12.1

27.1.6.4.4 Action

None

27.1.6.4.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.4.6 Additional information

None

27.1.6.5 XTS336

27.1.6.5.1 Explanation

A major severity alarm indicates that one Ethernet link does not have network connectivity. A critical severity alarm indicates that both Ethernet links do not have network connectivity.

27.1.6.5.2 Format

- **Alarm/Log: Network Connectivity**
  - Type: Communications
  - ID: communicationsSubsystemFailure

— Event: FLT

— Label: Network Connectivity

— Severity:Minor, Major or Critical

27.1.6.5.3 Field descriptions

See section 12.1

27.1.6.5.4 Action

Click on the Network Connectivity panel tab.

Review the Network connectivity Information .

Follow Action suggested for Mate Connectivity log XTS331.

If link connectivity is restored and the alarm persists, contact Nortel Networks support personnel.

27.1.6.5.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.5.6 Additional information

None

27.1.6.6 XTS636

27.1.6.6.1 Explanation

This alarm is reported when XTS336 minor/major/critical alarm is cleared.

27.1.6.6.2 Format

- **Alarm/Log : Network Connectivity Restored**
  — Type: Communications
  — ID: communicationsSubsystemFailure
  — Event: INFO
  — Label: Network Connectivity Restored
  — Severity: NONE

27.1.6.6.3 Field descriptions

See section 12.1

27.1.6.6.4 Action

None

27.1.6.6.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.6.6 Additional information

None

27.1.6.7 XTS351

27.1.6.7.1 Explanation

A major severity alarm indicates that one Ethernet link does not have network connectivity. A critical severity alarm indicates that both Ethernet links do not have network connectivity

27.1.6.7.2 Format

- **Alarm/Log: No Mate Communication (simplex)**
  - Type: ProcessingError
  - ID: underlyingResourceUnavailable
  - Event: FLT
  - Label: No Mate Communication (simplex)
  - Severity:Minor, Major or Critical

27.1.6.7.3 Field descriptions

See section 12.1

27.1.6.7.4 Action

Click on the Network Connectivity panel tab.

Review the Network connectivity Information .

Follow Action suggested for Mate Connectivity log XTS331.

If link connectivity is restored and the alarm persists, contact Nortel Networks support personnel.

27.1.6.7.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.7.6 Additional information

None

27.1.6.8 XTS651

27.1.6.8.1 Explanation

This alarm is reported when XTS351 minor/major/critical alarm is cleared.

27.1.6.8.2 Format

- **Alarm/Log : Mate Communication Restored**
  - Type: ProcessingError
  - ID: underlyingResourceUnavailable
  - Event: INFO
  - Label: Mate Communication Restored
  - Severity: NONE

27.1.6.8.3 Field descriptions

27.1.6.8.4 Action

None

27.1.6.8.5 Associated Operational Measurements or Performance Measurements

None

27.1.6.8.6 Additional information

None

27.1.7 Node Maintenance

When Node maintenance action is performed, the following alarm/logs are generated.

27.1.7.1 XTS355

27.1.7.1.1 Explanation

The inactive unit is jammed to prevent a Switch of Activity (SWACT).

27.1.7.1.2 Format

- **Alarm/Log: Jam Inactive Unit**
  - Type: ProcessingError
  - ID: underlyingResourceUnavailabe
  - Event: FLT
  - Label: Jam Inactive Unit
  - Severity: Major or Critical

27.1.7.1.3 Field descriptions

See section 12.1

27.1.7.1.4 Action

This alarm is expected during an upgrade or unit replacement. No action is required.

27.1.7.1.5 Associated Operational Measurements or Performance Measurements

None

27.1.7.1.6 Additional information

None

27.1.7.2 XTS655

27.1.7.2.1 Explanation

This alarm is reported when XTS355 minor/major/critical alarm is cleared.

27.1.7.2.2 Format

- **Alarm/Log : Release Jam on Inactive unit**

- Type: ProcessingError
- ID: underlyingResourceUnavailable
- Event: INFO
- Label: Release Jam on Inactive unit
- Severity: NONE

27.1.7.2.3 Field descriptions

See section 12.1

27.1.7.2.4 Action

None

27.1.7.2.5 Associated Operational Measurements or Performance Measurements

None

27.1.7.2.6 Additional information

None

27.1.7.3 XTS670

27.1.7.3.1 Explanation

This alarm is reported when a swact is initiated on the system

27.1.7.3.2 Format

- **Alarm/Log : SWACT Failover Started**
  - Type: No_Problem_Category
  - ID: noProbableCause
  - Event: INFO
  - Label: SWACT Failover Started
  - Severity: NONE

27.1.7.3.3 Field descriptions

See seaction 12.1

27.1.7.3.4 Action

None

27.1.7.3.5 Associated Operational Measurements or Performance Measurements

None

27.1.7.3.6 Additional information

None

27.1.7.4 XTS671

27.1.7.4.1 Explanation

This alarm is reported when swact is finished on the unit.

27.1.7.4.2 Format

- **Alarm/Log : SWACT Failover Finished**
  - Type: No_Problem_Category
  - ID: noProbableCause
  - Event: INFO
  - Label: SWACT Failover Finished
  - Severity: NONE

27.1.7.4.3 Field descriptions

See section 12.1

27.1.7.4.4 Action

None

27.1.7.4.5 Associated Operational Measurements or Performance Measurements

None

27.1.7.4.6 Additional information

None

28: Fault Management (FM): A00004045

28.1 Fault management strategy

The CLIDN for DMS-250 feature provides the same CLIDN call tracing capability using the TRK605 log as the existing DMS-100/200 CLIDN functionality.

28.2 Fault management tools and utilities

N/A.

28.3 Logs

28.3.1 Explanation

Log Title: TRK605

Name: ICT Calling Line Identification

Description: This log is generated when the SOC UTRS0012 is ON and the called number is data filled in table CLIDN in a DMS-250 toll switch. The TRK605 log is used in a toll switch to identify the origination number when the called number is being traced.

Event type: Minor alarm condition.

28.3.2 Format

The log report format for TRK605 is as follows:

* TRK605 mmmdd hh:mm:ss ssdd ALARM INFO ICT Calling Line Ident

INCOMING TRUNK = <CKT CLLI>

OUTGOING TRUNK = <CKT CLLI>

CALLED NUMBER = NXXNXXXXXX

SOURCE = CALLING NUMBER/CHARGE NUMBER/ UNAVAILABLE

CALLID = XXXXXX

TIME: MONTH: DAY HH:mm:ss

An example of log report TRK605 follows:

* TRK605 SEP27 14:23:29 5908 INFO ICT Calling Line Ident

INCOMING TRUNK = CKT DCEA20C7DR01 1

OUTGOING TRUNK = CKT DCEA21C7DR02 1

CALLED NUMBER = 2018212345

ORIGINATION NUMBER = 8146119871

SOURCE = CALLING NUMBER

CALLID = 852346

TIME: SEP27 14:23:29

28.3.3 Field descriptions

The following table describes each field in the log report:

Table 1 Field descriptions

Field	Value	Description
*	Alarm	One asterik indicates that the generation of this log report represents a minor alarm condition.
INCOMING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the incoming trunk.
OUTGOING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the outgoing trunk.
CALLED NUMBER	Digits 0-9	This field identifies the called number that is being traced.
ORIGINATING NUMBER	Digits 0-9 or '$'	This field identifies either the calling number, charge number or billing number from the incoming trunk call information. The CLIDN for DMS-250 feature attempts to get the calling number first. If the calling number is not available, the charge number is used. If the charge number is not available, the billing number is used. If neither the calling, charge nor billing number is available, this field will display '$'.

Table 1 Field descriptions

Field	Value	Description
SOURCE	Calling Number, Charge Number or Unavailable	This field identifies from what the originating number is derived. If the originating number cannot be derived, '$' will appear in the ORIGINATING NUMBER field and the SOURCE field will display "UNAVAILABLE".
CALLID	6 digit number; Digits 0-9 used	This field identifies the call process id number.
TIME	Month, Day, Hour, Minute and Second	This field identifies the date and time the call was logged.

28.3.4 Action

Action to be taken is determined by the local telephone company.

28.3.5 Associated Operational Measurements or Performance Measurements

There are no associated OM registers.

28.3.6 Additional information

On the DMS-250, the TRK605 log is generated for EANT, PRI, DAL, ONAL, ONAT and IMT trunk types.

The TRK605 log was introduced to the DMS-100/200 by feature AN1658.

28.4 Alarms

The TRK605 log is a minor alarm condition.

28.5 Related documentation

AN1658 - Inter-Switch Call Trace (ICT) Feature

29: Fault Management (FM): A00004260

29.1 Fault management strategy

This section describes troubleshooting for the new XPKT806 and XPKT807 logs, which assist with current strategy of troubleshooting XPKT301 logs.

29.2 Fault management tools and utilities

Tools used are LOGUTIL, for the new logs described below, and MAPCI, which has the new APPL;PKT;SPM_ATM Map levels to assist with troubleshooting the new XPKT806 and XPKT807 logs.

29.3 XPKT806 Logs

29.3.1 Explanation

Log Title: XPKT806

Name: TBL ATM PACKET ALARM

Description: Reported when the number of XPKT301 logs against a SPM node crosses (i.e. meets or exceeds) the threshold. The threshold value and duration of the collection interval (called a “raise cycle”) are defined in the OPTCN section.

The “nn PKT” major alarm is raised under the APPL banner in MAPCI;MTC whenever one or more nodes have the XPKT806 alarm raised. See OPTCN section on MAPCI;MTC level for more details.

Event type: Major

29.3.2 Format

```
MG4K107BH  **  XPKT806  <mmmdd hh:mmm:ss seq#> TBL  ATM Packet Alarm
         Status  : Alarm Raised
         Problem : Node reached threshold of <hits> XPKT301 failures
                   at <CycleDur> minutes into a <CycleMax> minute raise cycle.
         Troubleshooting : MAPCI;MTC;APPL;PKT;SPM_ATM or refer to NTPs.
         Location: SPM  <SPMNUM>  Type: <SPM Class>      Fabric: <Fabric>


MG4K107BH  **  XPKT806 OCT31 11:55:30 7100 TBL  ATM Packet Alarm
         Status  : Alarm Raised
         Problem : Node reached threshold of 2 XPKT301 failures
                   at 3 minutes into a 15 minute raise cycle.
         Troubleshooting : MAPCI;MTC;APPL;PKT;SPM_ATM or refer to NTPs.
         Location: SPM  60  Type: SMG4      Fabric: ATM
```

29.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
<mmmdd hh:mmm:ss seq#>	numeric	Date, Time, and Log Sequence number
<hits>	1..32767	Number of XPKT301 logs that impacted this SPM node during the cycle. This number will match the RAISE_THRESHOLD value since alarm is raised as soon as threshold is crossed.
<CycleDur>	1..1440	Number of minutes that elapsed (i.e. duration) in the current cycle when the alarm was raised.
<CycleMax>	1..1440	Maximum minutes in the cycle - same as RAISE_CYCLE in the office parameter that controls the threshold.
<SPMNUM>	0..85	Number of SPM that raised this alarm
<SPM Class>	SMG4, IW, or DPT	SPM Class of the node where IW is IW with BRDG_ONLY, and DPT is IW with DPT_ONLY.

29.3.4 Action

Alarm will clear automatically if the number of XPKT301 failures diminishes. The MAPCI;MTC;APPL;PKT;SPM_ATM Map level provides helpful commands for troubleshooting XPKT806 alarms. Also refer to the existing NTP troubleshooting procedures for XPKT301 logs.

29.3.5 Associated Operational Measurements or Performance Measurements

Feature A00004430 is creating new OMs in SN07 to track the XPKT301 hits on a per node basis.

29.3.6 Additional information

None

29.4 XPKT807 Logs

29.4.1 Explanation

Log Title: XPKT807

Name: INFO ATM PACKET ALARM

Description: Reported when the XPKT806 alarm clears for a SPM node. The clearing is done when the number of XPKT301 logs against the node does not exceed the threshold. The threshold value and duration of the collection interval (called a “clear cycle”) are defined in the OPTCN section.

Event type: None

29.4.2 Format

There are four different formats for the XPKT807 log, where the difference between the formats is the text in the “Reason:” field, which will indicate the four different ways the alarm can be cleared.

29.4.2.1 XPKT807 for Automatic Clearing when Threshold Met

This format is used when the XPKT806 alarm is automatically cleared by the system after the threshold is not exceeded when the clear cycle expires. This is the most common way of clearing the alarm.

```
RSN07BD     XPKT807 <mmmdd hh:mmm:ss seq#> INFO ATM Packet Alarm
        Status: Alarm Cleared Automatically
        Reason: Node had <hits> XPKT301 failures in a <CycleMax> minute clear
                cycle with a threshold of <Thresh> XPKT301 failures.
        Location: SPM <SPMNUM>  Type: <SPM Class>  Fabric: <Fabric>

RSN07BD     XPKT807 SEP30 12:58:04 1100 INFO ATM PACKET ALARM
        Status: Alarm Cleared Automatically
        Reason: Node had 0 XPKT301 failures in a 15 minute clear
                cycle with a threshold of 0 XPKT301 failures.
        Location: SPM 39  Type: SMG4  Fabric: ATM
```

29.4.2.2 XPKT807 for Manual Clearing by Map Command

This format is used when the XPKT806 alarm is manually cleared via the CLEAR command at the MAPCI;MTC;APPL;PKT;SPM_ATM level:

```
RSN07BD     XPKT807 <mmmdd hh:mmm:ss seq#> INFO ATM Packet Alarm
```

```
        Status: Alarm Cleared Manually by User <user>
        Reason: Cleared by MAPCI;MTC;APPL;PKT;SPM_ATM;CLEAR command.
                Node had <hits> XPKT301 failures before clear cycle aborted.
        Location: SPM <SPMNUM>  Type: <SPM Class>  Fabric: <Fabric>

RSN07BD     XPKT807 SEP30 12:58:04 1100 INFO ATM PACKET ALARM
        Status: Alarm Cleared Manually by User ADMIN
        Reason: Cleared by MAPCI;MTC;APPL;PKT;SPM_ATM;CLEAR command.
                Node had 0 XPKT301 failures before clear cycle aborted
        Location: SPM 39  Type: SMG4  Fabric: ATM
```

29.4.2.3 XPKT807 for Manual Clearing by Disabling Feature

This format is used when the XPKT806 alarm is manually cleared via Table OFCENG by setting the sub-parameter RAISE_THRESHOLD to zero for one of these tuples:

1. XPKT806_SMG4_RAISE_CLEAR
2. XPKT806_IW_RAISE_CLEAR
3. XPKT806_DPT_RAISE_CLEAR

Setting the RAISE_THRESHOLD to zero will disable XPKT806 reporting for the supported SPM type. See the OPTCN section for more details on the above office parameters.

```
RSN07BD     XPKT807 <mmmdd hh:mmm:ss seq#> INFO ATM Packet Alarm
        Status: Alarm Cleared Manually by User <user>
        Reason: Cleared by disabling feature in Table OFCENG.
                Node had <hits> XPKT301 failures before clear cycle aborted.
        Location: SPM <SPMNUM>  Type: <SPM Class>  Fabric: <Fabric>

RSN07BD     XPKT807 SEP30 12:58:04 1100 INFO ATM PACKET ALARM
        Status: Alarm Cleared Manually by User ADMIN
        Reason: Cleared by disabling feature in Table OFCENG.
                Node had 0 XPKT301 failures before clear cycle aborted
        Location: SPM 39  Type: SMG4  Fabric: ATM
```

29.4.2.4 XPKT807 for Automatic Clearing when Node Deleted

This format is used when the XPKT806 alarm is automatically cleared for a node that has XPKT806 alarm present and is then deleted.

```
RSN07BD     XPKT807 <mmmdd hh:mmm:ss seq#> INFO ATM Packet Alarm
        Status: Alarm Cleared Automatically
        Reason: Cleared since node has been deleted.
                Node had <hits> XPKT301 failures before clear cycle aborted.
        Location: SPM <SPMNUM>  Type: <SPM Class>  Fabric: <Fabric>

RSN07BD     XPKT807 SEP30 12:58:04 1100 INFO ATM PACKET ALARM
        Status: Alarm Cleared Automatically
        Reason: Cleared since node has been deleted.
                Node had 0 XPKT301 failures before clear cycle aborted
```

```
Location: SPM 39  Type: SMG4  Fabric: ATM
```

29.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
<mmmdd hh:mmm:ss seq#>	numeric	Date, Time, and Log Sequence number
<user>	string	Login ID of user that executed command that caused manual clearing of the alarm.
<hits>	1..32767	Number of XPKT301 logs that impacted this SPM node during the cycle.
<CycleMax>	1..1440	Number of minutes in a clear cycle - same as CLEAR_CYCLE in the office parameter that controls the threshold.
<Thresh>	1..32767	Number of XPKT301 hits allowed against the node for alarm to clear. Same as CLEAR_THRESHOLD in the office parameter that controls the threshold.
<SPMNUM>	0..85	Number of SPM that cleared the XPKT806 alarm.
<SPM Class>	SMG4, IW, or DPT	SPM Class of the node where IW is IW with BRDG_ONLY, and DPT is IW with DPT_ONLY.

29.4.4 Action

None - just a notification that the previous XPKT806 major alarm has now cleared for this SPM node. The MAPCI;MTC;APPL;PKT;SPM_ATM Map level provides helpful commands for troubleshooting XPKT806 alarms.

29.4.5 Associated Operational Measurements or Performance Measurements

Feature A00004430 is creating new OMs in SN07 to track the XPKT301 hits on a per node basis.

29.4.6 Additional information

None

29.5 Alarms

A new “nn PKT” major alarm is introduced under the APPL banner for the MAPCI;MTC level. See the OPTCN section for details.

A new XPKT806 log with major alarm is introduced. See details above in the section for “XPKT806 Logs”.

29.6 Related documentation

None

30: Fault Management (FM): A00004271

30.1 Fault management strategy

A log is needed to provide real-time indication when a SIPT call is not allowed to proceed due to the SOC LIMIT setting of either CS2B0008 or CS2B0009.

30.2 Fault management tools and utilities

DMS logutil system.

30.3 Logs

30.3.1 Explanation

Log Title: NGSS 700

Name: CS2CS CALL REJECTED

Description: This log is generated when a SIPT CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC. The SIPT call is not allowed to complete through the NGSS.

Event type: Call setup failure.

30.3.2 Format

```
NGSS700 <mmmdd hh:mmm:ss ssdd> INFO CS2CS CALL REJECTED
 NGSS CS2CS call limit has been reached
 A new LIMIT for SOC CS2B0008 may be needed.
```

30.3.3 Field descriptions

There are no fields associated with this log, only text indicating SOC CS2B0008's LIMIT setting is being exceeded.

30.3.4 Action

The SOC LIMIT setting for the SIP Call Server SOC CS2B0008 option may need to be increased.

30.3.5 Associated Operational Measurements or Performance Measurements

The CS2CSOV register in OM group NGSSOM is pegged.

30.3.6 Additional information

None.

30.3.7 Explanation

Log Title: NGSS 701

Name: CS2AS CALL REJECTED

Description: This log is generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC. The SIPT call is not allowed to complete through the NGSS.

Event type: Call setup failure.

30.3.8 Format

```
NGSS701 <mmmdd hh:mmm:ss ssdd> INFO CS2AS CALL REJECTED
 NGSS CS2AS call limit has been reached
 A new LIMIT for SOC CS2B0009 may be needed.
```

30.3.9 Field descriptions

There are no fields associated with this log, only text indicating SOC CS2B0009's LIMIT setting is being exceeded.

30.3.10 Action

The SOC LIMIT setting for the SIP Call Server SOC CS2B0009 option may need to be increased.

30.3.11 Associated Operational Measurements or Performance Measurements

The CS2ASOV register in OM group NGSSOM is pegged.

30.3.12 Additional information

None.

30.4 Related documentation

31: Fault Management (FM): A00004391

31.1 Fault management strategy

There are 3 existing logs which are slightly modified for this feature. The modified logs are E911212, E911213, and E911214.

The modification is very minor. Each of these logs prints out a position ID and login ID when the 911 PSAP is using ACD. The fields used to display these IDs are increasing from 4 digits to 5 digits.

31.2 Fault management tools and utilities

Not Applicable

31.3 E911 212 Logs

31.3.1 Explanation

Log Title: E911 212

Name: E911 Call Event Record

Description: All E911 calls produce this log when either party disconnects.

31.3.2 Format

This is an existing log. Its function and basic format is unchanged by this activity.

If the E911 PSAP is using an ACD group for its agents, this log will print a position ID (POSID) and a login ID (LOGINID) associated with the agent who took the call. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000.

31.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
POSID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

Table 1 Field descriptions

Field	Value	Description
LOGINID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

31.3.4 Action

No new action is required beyond the standard procedures for E911 212 logs.

31.3.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

31.3.6 Additional information

None.

31.4 E911 213 Logs

31.4.1 Explanation

Log Title: E911 213

Name: ACD PSAP Agent Login

Description: This log is produced when an ACD PSAP Agent logs in.

31.4.2 Format

This is an existing log. Its function and basic format is unchanged by this activity.

When an ACD PSAP agent logs in, this log is produced. It contains an AGENT POSITION ID and an AGENT LOGIN ID associated with the agent logging in. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000.

31.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
AGENT POSITION ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.
AGENT LOGIN ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

31.4.4 Action

No new action is required beyond the standard procedures for E911 213 logs.

31.4.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

31.4.6 Additional information

None.

31.5 E911 214 Logs

31.5.1 Explanation

Log Title: E911 214

Name: ACD PSAP Agent Logout

Description: This log is produced when an ACD PSAP agent logs out.

31.5.2 Format

This is an existing log. Its function and basic format is unchanged by this activity.

When an ACD PSAP agent logs out, this log is produced. It contains an AGENT POSITION ID and an AGENT LOGIN ID associated with the agent logging out. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000

31.5.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
AGENT POSITION ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.
AGENT LOGIN ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

31.5.4 Action

No new action is required beyond the standard procedures for E911 214 logs.

31.5.5 Associated Operational Measurements or Performance Measurements

Not Applicable.

31.5.6 Additional information

None.

31.6 Alarms

Not Applicable

31.7 Related documentation

None.

32: Fault Management (FM): A00004430

32.1 Fault management strategy

32.2 Fault management tools and utilities

32.3 Logs

32.3.1 XPKT301 and XPKT302

Log Title: ***XPKT301***

Name: UNI Connection Failure

The XPKT301 log replaces the ATM606 log in SN07. The ATM606 log was introduced on the SMG4 in SN05, and was expanded to include MG9K and MG9K ABI nodes in SN06.

The XPKT301 log is generated when a UNI Release/Release Complete message is received by a Succession line or trunk peripheral where the release cause in the message indicates a failure, i.e. not normal clearing. The Core is sent an ATM SVC failure message from either an SPM based AAL1 node (SMG4, IW SPM, or DPT SPM), or from an MG9K Gateway, through a Gateway Controller (GWC). The log can be used to troubleshoot system configuration and setup problems.

In SN07 the XPKT301 is the only log generated by SPM based AAL1 nodes, and represents both ATM SVC setup call failures, and ATM SVC mid-call failures.

NOTE In SN07, for MG9K and MG9K ABI nodes, the XPKT301 log represents ATM SVC call setup failures. (The XPKT302 log is generated for MG9K and MG9K ABI established calls).

Event type: INFO

Log Title: ***XPKT302***

Name: UNI Mid-call Failure

Description: This log is generated when a UNI Release/Release Complete message is received by a Succession line or trunk peripheral and the release

cause in the message indicates a failure, i.e. not normal clearing, for established MG9K or MG9K ABI node calls.

The log can be used to troubleshoot system configuration and setup problems.

The XPKT302 log is introduced in SN07 and is generated by MG9K Gateway or MG9K ABI nodes for established calls.

Event type: INFO

32.3.2 Format

The format of the XPKT301 and XPKT302 logs are almost identical to the ATM606 log, except for three new fields. New fields are introduced for the originating and terminating nodes (Orig Node, Term Node). A new DEBUG field is also introduced for future use by Gateways to send information back to the Core for Field Support trouble shooting.

32.3.2.1 SPM originated logs

The first example is for SPM originated logs, logs pertaining to ATM connections made by an SPM. This example also illustrates an optional last line applicable to **all** SPM ATM-related logs that is present when SPM_ENHANCED_OUTPUT in table OFCVAR is set to ON.

CS0004BB XPKT301 JAN17 09:27:41 1800 INFO UNI Connection Failure
Location: SPM 2
Type: SMG4
Orig Agent: CKT MGEA22C7DR01 1
Orig Node: SPM 2
Term Agent: CKT MGEA27C7DR06 1
Term Node: SPM 2
Called Number: 5018271111
Call ID: 42565634
CAUSE = 3 NO_ROUTE_TO_DEST
DEBUG: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Location: SPM 2 Type: SMG4 Fabric: ATM

32.3.2.2 MG9K Orignated, MG9K ITP Hosted Lines

CS0004BB XPKT301 JAN17 09:27:44 1800 INFO UNI Connection Failure
Location: SLOA 23 3
Type: MG9K
Orig Agent: HURR 02 5 01 74 DN 619522087
Orig Node: SLOA 23 3
Term Agent: HURR 02 5 04 30 DN 6195220943
Term Node: SLOA 23 3

Called Number: 6195220943
Call ID: 42565699
CAUSE = 3 NO_ROUTE_TO_DEST
DEBUG: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

32.3.2.3 MG9K Originated, ABI Hosted Lines

RTP7 XPKT301 FEB11 11:40:22 3600 INFO UNI Connection Failure
Location: SMA2 0
Type: MG9K-ABI
Orig Agent: HOST 00 0 07 19 DN 6136212587
Orig Node:
Term Agent: RDT1 24 0 00 26 DN 6136212301
Term Node: SMA2 0
Called Number: 6212301
CallID: 47907279
Cause: 41 TEMP_FAILURE
DEBUG: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

32.3.2.4 XPKT301 log(s) - MG9K ABI line to legacy line established call

These two XPKT logs were generated for an estabished MG9K ABI line to legacy line call. This call involved two SVC connections: one (1) for the IW SPM which connected the legacy line to the ATM network and one (1) for the MG9K ABI line connection to the ATM network. One XPKT 301 log is generated for the IW SPM, and one XPKT302 log is generated for the MG9K ABI.

RTP7 XPKT301 FEB14 11:31:22 7001 INFO UNI Connection Failure
Location: SPM 3
Type: IW
Orig Agent: RDT1 24 0 00 26 DN 6136212301
Orig Node: SMA2 0
Term Agent: HOST 00 0 07 19 DN 6136212587
Term Node:
Called Number: 6212587
CallID: 43647418
Cause: 41 TEMP_FAILURE
DEBUG: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Location: SPM 3 Type: IW Fabric: ATM

RTP7 XPKT302 FEB14 11:31:22 7102 INFO UNI Mid-call Failure
Location: SMA2 0
Type: MG9K-ABI
Orig Agent: RDT1 24 0 00 26 DN 6136212301

Orig Node: SMA2 0
Term Agent: HOST 00 0 07 19 DN 6136212587
Term Node:
Called Number: 6212587
CallID: 43647418
Cause: 41 TEMP_FAILURE
DEBUG: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

32.3.2.5 MG9K Originated, ABI Hosted Trunks

CS0004BB XPKT301 JAN17 09:27:41 1800 INFO UNI Connection Failure
Location: RCC 3
Type: MG9K-ABI
Orig Agent: CKT MGEA60TWMFWK 1
Term Agent: CKT S5S4D0D0TR1 1600
Called Number: 5018271111
Call ID: 42565634
CAUSE = 41 TEMP_FAILURE

32.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Location	SPM <nn> or <site, frame, unit/shelf> or <trunk PM name, PM #>	Identifies the node or subnode hosting the line/trunk whose bearer connection received the UNI Release/ Release Complete with failure cause. This is the master node that requested the ATM connection.
Type	SMG4 or IW or MG9K or MG9K-ABI	Identifies the type of the node associated with the location.

Table 1 Field descriptions

Field	Value	Description
Orig. Agent	CKT/DPT, CLLI, CIC or LEN, DN	Identification and properties of the originating agent in the affected call
Orig. Node	- SPM <nn> or - MG9K <lgrp - name> - MG9K-ABI (pm name)	- SPM and number - MG9K Lgrp name from table lgrpinv - the name of the ABI peripheral that has its DS-512 fiber connected to the MG9K Gateway,
Term. Agent	CKT/DPT, CLLI, CIC or LEN, DN	Identification and properties of the terminating agent in the affected call
Term. Node	- SPM <nn> or - MG9K <lgrp - name> - MG9K-ABI (pm name)	- SPM and number - MG9K Lgrp name from table lgrpinv - the name of the ABI peripheral that has its DS-512 fiber connected to the MG9K Gateway,
Called Number	<digit string>	The called number of the affected call
CallID	<digits>	The DMS Core Call Identifier for the affected call
Cause	digits, text	The UNI release/ release complete cause value and associated text as defined in the Q2931 standard.

Table 1 Field descriptions

Field	Value	Description
Debug	Nil values in SN07	Future use for Gateways to send information back to the Core to allow Nortel Network engineers to trouble shoot External Network problems.

32.3.4 Action

No immediate action is required. These logs are informational and intended to help with diagnosing call completion problems.

32.3.5 Associated Operational Measurements or Performance Measurements

Whenever this log is generated a subsequent integrity lost event will occur and this latter event will cause the ISCONBAD OM to be pegged if the agent attempting the ATM connection is an ISUP agent.

32.3.5.1 OM group AL1SVCOM register pegs in SN07

At the time the XPKT301 or XPKT302 logs are generated, corresponding nodal tuples in new OM group AL1SVCOM are also pegged.

```
AL1SVCOM

CLASS: ACTIVE
START:2004/02/14 11:10:00 SAT; STOP: 2004/02/14 11:11:21 SAT;
SLOWSAMPLES:       1 ; FASTSAMPLES:       8 ;

   KEY (SVC_OM_PM_INFO1)
   INFO (SVC_OM_TUPLE_DATA1)

   NOSVCAT   NOSVCAT2   NOSVCFL   ISSVCAT
    ISSVCAT2   ISSVCFL   DPTSVCA   DPTSVCA2
    DPTSVCF   NRTEDEST   NOUSRRES   VPCINAVL
    BWTHNAVL   TEMPFAIL   RESUNAVL   OTH_CC

  72
    IW SPM   3
       1      0      1      1
       0      1      0      0
       0      0      0      0
       0      0      0      0
```

```
101
MG9K ABI SMA2   0
      1     0     1     1
      0     1     0     0
      0     0     0     0
      0     0     0     0

118
MG9K SLOA 23 3
      2     0     2     2
      0     2     0     0
      0     0     0     0
      0     2     0     0
```

32.3.6 Additional information

NA

32.4 Related documentation

33: Fault Management (FM): A00005016

33.1 Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “New VMG Out of Service Alarms” feature there will be new faults added to provide the reason why a VMG is out of service.

33.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

Gateway Status Config in Switched Lines Services GUI - the current list of Megaco faults will also be displayed here.

33.2.1 Faults, Alarms and Logs

There will be new VMG Out Of Service faults raised and cleared by the MG9000 to indicate the specific reason the VMG is out of service.

Some of these faults will have a severity of WARNING. These faults will be raised for issues that are most likely caused by user intervention: locking cards, setting VMG administrative state to Out of Service and restarting cards.

All of the other faults raised must assume that there is a problem that is preventing the VMG from going into service and have a severity of CRITICAL, same as the existing VMG300 fault.

33.3 Alarms

33.3.1 Explanation

33.3.1.1 vmgAdminStatusOutOfService

LogID: VMG322

Title: vmgAdminStatusOutOfService

Name: VMG Admin State is OOS

Description: Admin State Out Of Service - Call Processing Out of Service

Severity: Warning

Event type: TBL (Trouble)

33.3.1.2 vmgInitializing

LogID: VMG325

Title: vmgInitializing

Name: VMG Initializing

Description: VMG Initializing - Call Processing Out of Service.

Severity: Warning

Event type: TBL (Trouble)

33.3.1.3 vmgOOSCardLocked

LogID: VMG323

Title: vmgOOSCardLocked

Name: VMG OOS-card locked

Description: Card Locked - Call Processing Out of Service.

Severity: Warning

Event type: TBL (Trouble)

33.3.1.4 vmgOOSCardDisabled

LogID: VMG324

Title: vmgOOSCardDisabled

Name: VMG OOS-card disabled

Description: Card Disabled - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.1.5 vmgOOSLineMtcNotReady

LogID: VMG328

Title: vmgOOSLineMtcNotReady

Name: VMG OOS- Line Maintenance is not Ready

Description: Line Maintenance Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.1.6 vmgOOSMegacoMtcNotReady

LogID: VMG329

Title: vmgOOSMegacoMtcNotReady

Name: VMG OOS- Megaco Maintenance is not Ready

Description: Megaco Maintenance Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.1.7 vmgOOSGWCUnreachable

LogID: VMG373

Title: vmgOOSGWCUnreachable

Name: VMG OOS- GWC is not reachable

Description: GWC Unreachable - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.1.8 vmgOOSNoReplyFromGWC

LogID: VMG374

Title: vmgOOSNoReplyFromGWC

Name: VMG OOS- no reply from GWC

Description: GWC Reachable But No Reply To Service Change - Check LGRP/GWC state - Call Processing Out of Service

Severity: Critical

Event type: TBL (Trouble)

33.3.1.9 vmgOOSAAL1BearerOnPairNotReady

LogID: VMG376

Title: vmgOOSAAL1BearerSubsystemOnPairNotReady

Name: VMG OOS- AAL1 bearer subsystem not ready

Description: AAL1 Bearer Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.1.10 vmgOOSIPBearerOnPairNotReady

LogID: VMG377

Title: vmgOOSIPBearerSubsystemOnPairNotReady

Name: VMG OOS- IP bearer subsystem not ready

Description: IP Bearer Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

33.3.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

The following sections show the STD format for each of the faults.

33.3.2.1 vmgAdminStatusOutOfService

```
250Q MG9K     ***  VMG322 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - VMG Admin Status Out Of Service
        Description: Admin State Out Of Service - Call Processing Out of Service
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.2 vmgInitializing

```
250Q MG9K     ***  VMG325 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - VMG is Initializing
        Description: VMG Initializing - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.3 vmgOOSCardLocked

```
250Q MG9K     ***  VMG323 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - Card is Locked
        Description: Card Locked - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.4 vmgOOSCardDisabled

```
250Q MG9K     ***  VMG324 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - Card is Disabled
        Description: Card Disabled - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.5 vmgOOSLineMtcNotReady

```
250Q MG9K     ***  VMG328 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
      Specific Problem: Specific Problem: NnMegacoFault - Line Maintenance is not ready
        Description: Line Maintenance Not Ready - Call Processing Out of Service
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.6 vmgOOSMegacoMtcNotReady

```
250Q MG9K     ***  VMG329 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - Megaco Maintenance is not ready
        Description: Megaco Maintenance Not Ready - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.7 vmgOOSGWCUnreachable

```
250Q MG9K     ***  VMG373 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault- Ping to reachGWC failed
        Description: GWC Unreachable - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.8 vmgOOSNoReplyFromGWC

```
250Q MG9K     ***  VMG374 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - GWC did not reply to service change
        Description: GWC Reachable But No Reply To Service Change - Check LGRP/GWC
state - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
```

```
        HOST   03   A0    MG9F 006
```

33.3.2.9 vmgOOSAAL1BearerOnPairNotReady

```
250Q MG9K     ***  VMG376 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - AAL1 bearer subsystem not ready
        Description: AAL1 Bearer Not Ready - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.2.10 vmgOOSIPBearerOnPairNotReady

```
250Q MG9K     ***  VMG377 MAY18 10:44:31 4200 TBL  MG9K NnMegacoFault
        Location: 18-c418_sanity-Frame006.Shelf2.Slot12
        Notification Id: 469
        State: not acknowledged
        Category: Equipment Alarm
        Cause: Equipment Malfunction
        Time: Jan 01 19:31:52 1970
        Component Id: Card.frame1.shelf2.slot12.ITP
        Specific Problem: NnMegacoFault - IP bearer subsystem not ready
        Description: IP Bearer Not Ready - Call Processing Out of Service.
        Site   Flr  RPos  Bay_id
        HOST   03   A0    MG9F 006
```

33.3.3 Action

33.3.3.1 vmgAdminStatusOutOfService

To clear this, change the Admin status in the Gateway Status Config tab of the Switched Lines Services GUI to In Service

33.3.3.2 vmgInitializing

This alarm is raised at initial VMG creation, while waiting for a reply form the GWC when the VMG Admin status is changed to InService or as the active ABI/ITP is coming up out of a restart. There is no clearing procedure for this alarm. During a restart, this is raised as long as 15 minutes. During the first 15 minutes after a restart of an ITP pair, no other out of service VMG alarms are raised against the VMG, except the Card Locked and Admin State Out of Service faults. If the VMG is still Out of Service 15 minutes after the restart, the alarm will be cleared and replaced by the appropriate VMG fault indicating the fault condition at that time.

33.3.3.3 vmgOOSCardLocked

To clear this, unlock the active ITP or ABI.

33.3.3.4 vmgOOSCardDisabled

This alarm indicates the ITP or ABI card's status is disabled. The ITP or ABI card view or Alarm Browser will provide more information about what is preventing the card from going enabled. When the card's status goes to enabled, this alarm will be cleared.

33.3.3.5 vmgOOSLineMtcOnPairNotReady

This alarm indicates Line Maintenance on the ITP or ABI is not ready for call processing support. If this is raised when the card is enabled, then this is most likely a software error condition. If the ITP or ABI is disabled, the Line Maintenance fault is usually raised as well. Locking and unlocking the card might cause this condition to clear.

33.3.3.6 vmgOOSMegacoMtcOnPairNotReady

This fault would be raised because of a software error condition. Locking and unlocking the card might cause this condition to clear.

33.3.3.7 vmgOOSGWCUnreachable

This alarm indicates the GWC is not responding to pings from the ITP or ABI and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG.

It could mean a number of things:

- If this VMG has never been in service, it could be because an invalid VMG IP address was provisioned. If the address is incorrect, then delete and re-add the VMG with the correct IP address
- It could be an issue with the network interface or edge router - most likely there will also be a Wanbuilder Heartbeat alarm - resolve the issue with that alarm
- If there is not a Wanbuilder Heartbeat alarm and Wanbuilder Heartbeat was turned on for the Call Control subnet (ITPs) or ABI subnet (ABIs) then this is likely a network issue - do pings/traceroutes to isolate the issue further
- Also verify that the pair of GWC cards is unlocked. If the active GWC is locked, it will not respond to pings.

33.3.3.8 vmgOOSNoReplyFromGWC

This alarm indicates the GWC is not responding to Megaco messages for this VMG and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG.

It could mean a number of things, including:

- The LGRP for this VMG is not in a ready state. Check the LGRP state using MAPCI ; PM on the core.
- If this is a VMG for an ABI pair that has never been in service, it could mean that the core or MG9K EM is provisioned with the incorrect address for this VMG. Correct the VMG IP address in the datafill in the core or re-provision the VMG with the correct address in the MG9K EM.
- GWC pair has been set to man busy or has issues - check the GWC status in CS2M.

33.3.3.9 vmgOOSAAL1BearerOnPairNotReady

This usually indicates a software error situation on either the DCC or ITP. Lock and unlocking the ITP, ABI or DCC card(s) involved might clear this.

33.3.3.10 vmgOOSIPBearerOnPairNotReady

This is usually because the Call Control Subnet was not provisioned on the DCC. Go to LCI and provision the Call Control Subnet. As such, this fault is usually card to see if that clears the issue. If the Call Control Subnet has been provisioned and this fault does not clear, then this is likely a software error - lock and unlock the ITP/ABI card to see if that clears the issue.

33.3.3.11 VMG300

Most of the time, this alarm will be raised only for transient situations, and should either be cleared or replaced by a different alarm within 15 seconds. The two exceptions to this are:

- if the active card is at SN07 or greater, but the inactive card is on a pre-SN07 software release.
- the ITP or ABI pair is on SN07, but the DCC is on a pre-SN07 release

Until the inactive card and DCC are upgraded to SN07 or greater, the active card will raise only the VMG300 fault when the VMG is out of service. To clear this, follow the instructions for the various faults in this section until the alarm is cleared.

33.3.4 Associated Operational Measurements or Performance Measurements

None.

33.4 Related documentation

34: Fault Management (FM): A00005073

34.1 Fault management strategy

In case of file transfer error , SDMB375 is generated on the Core with the proper information. The SDMB375 is not a new log.It is also raises a major or critical alarm on certain error conditions. .

34.2 Fault management tools and utilities

34.3 Logs

34.3.1 Explanation

The SDMB375 log is generated whenever SFTP or the base file transfer systems encounters a problem. Where appropriate, it raises a major or critical alarm. The TEXT portion of the log provides an explanation of the problem. SDMB375 logs is generated to indicate the trouble condition.

Log Title:. SDMB375

Name: SDM BILLING FILE TRANSFER

Description: To indicate an error occur in SBA secure file transfer

Event type: Trouble (TBL)

34.3.2 Format

Figure 1 SDMB375 log format

**SDMB375 <date> <time> <seq#> <event type> SDM BILLING FILE TRANSFER STREAM=<stream>: <destination>: <specific resolution>

***SDMB375 <date> <time> <seq#> <event type> SDM BILLING FILE TRANSFER STREAM=<stream>: <destination>: <specific error>

Note : The ** in the log indicates the major event and *** in the log indicates the critical event

Example:

** SDMB375 MAR12 00:33:16 9921 TBL SDM BILLING FILE TRANSFER

STREAM= AMA: TEST: Not logged in or login incorrect.

34.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Stream	string SIZE(4)	stream name
destination	string SIZE(15)	The name of the destination
specific error (variable field)	string SIZE varies	sftp specific error message and the possible action should be taken

34.3.4 Action

Follow the recommended action in the specific error field.
next line of support should be contacted.

34.3.4.1 Additional information

The SDMB375 log is generated whenever SFTP or the base file transfer systems encounters a problem. Where appropriate, it raises a major or critical alarm. The TEXT portion of the log provides an explanation of the problem.

Example:

** SDMB375 MAR12 01:59:48 5404 TBL SDM BILLING FILE TRANSFER

STREAM= AMA: TEST: Not logged in or login incorrect

*** SDMB375 MAR12 01:59:48 5505 TBL SDM BILLING FILE TRANSFER

STREAM= AMA: TEST: SFTP session failed. Max retries encountered

34.3.5 SDMB675

34.3.5.1 Explanation:

The SDMB675 log is generated whenever SFTP or the base file transfer system displays an informative message. The <destination>: <specific resolution> portion of the log provides an explanation of the information. SDMB675 logs is generated to indicate the cleared trouble condition.

Log Title: SDMB675

Name: SDM BILLING FILE TRANSFER

Description: To indicate the cleared error condition.

Event type: Info(INFO)

34.3.5.2 Format

Figure 2 SDMB 675 log format

SDMB675 <date> <time> <seq#> <event type> SDM BILLING FILE TRANSFER
STREAM=<stream>: <destination>: <specific resolution>

Example:

SDMB675 MAR13 01:46:43 5836 INFO SDM BILLING FILE TRANSFER

STREAM= AMA: TEST: Retrying one more time

34.3.5.3 Field descriptions

Field	Value	Description
Stream	string SIZE(4)	stream name
destination	string SIZE(15)	The name of the destination
specific resolution (variable field)	string SIZE varies	An explanation of the information.

34.3.5.4 Additional information

The SDMB675 log is generated whenever SFTP or the base file transfer system displays an informative message. The <destination>: <specific resolution> portion of the log provides an explanation of the information.

Example:

SDMB675 MAR13 01:46:43 5836 INFO SDM BILLING FILE TRANSFER

STREAM= AMA: TEST: Retrying one more time

34.4 Alarms

On error conditions, Major or critical alarm is raised on SDMBIL alarm slot on the core. The “major” alarm is raised if SFTPW will attempt re-try or “critical” alarm is raised if SFTP does not re-try due to exceeded re-try limit

Alarm format: SFTW

C

The corresponding log for the alarm detail will also be generated to indicate the error.

Example:

critical: AMA: SFTPW: TEST: SFTP session failed. Max retries encounter.

34.4.1 Major Alarm:

Alarm format: **SFTPW**

M

The corresponding log for alarm detail will also be generated to indicate the error.

Example:

Major:AMA:SFTPW: TEST: Not logged in or login incorrect

34.4.2 Associated Operational Measurements or Performance Measurements

34.5 Related documentation

35: Fault Management (FM): A00005074

35.1 Fault management strategy

Prior to this activity, OMDD used only the standard file transfer protocol for performing file transfers. This activity introduces an optional secure outbound file transfer mechanism for OMDD. Now OMDD can perform outbound file transfers in two ways: standard or secure. This activity does not modify the existing mechanism for fault management in OMDD file transfers. If a file transfer (either secure or standard) fails, a customer log (SDMO375) will be generated. The text of the log will indicate the reason for failure of file transfer.

35.2 Fault management tools and utilities

The existing OM file transfer log SDMO375 will be used by this activity to indicate failures in secure file transfer. The text of SDMO35 will indicate the actual reason for file transfer failure.

35.3 Logs

35.3.1 Explanation

Log Title: SDMO375

Name:SDM OM FILE TRANSFERDescription: This log indicates that OMDD outbound file transfer from the SDM to the OSS has failed. This is an already existing log.

Event type:MAJOR

35.3.2 Format

<mm dd hh:mmm:ss> <sdm/cbm name> syslog: SDMO375 MAJOR TBL SDM OM FILE TRANSFER ODM FTP:<reason for ftp failure>

35.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
<mm dd hh:mmm:ss>	date and time	Date and time when the log is generated

Table 1 Field descriptions

Field	Value	Description
<sdmname>	sdm/cbm name	The hostname of the SDM/CBM where the log is generated
SDMO375	SDMO375	Log name
<reason for ftp failure>	Text String	The actual reason for ftp failure.

35.3.4 Action

From the reason text, identify the reason for failure of file transfer and follow the standard procedures to rectify it.

35.3.5 Associated Operational Measurements or Performance Measurements

None

35.3.6 Additional information

No alarms are created or modified by this activity.

35.4 Related documentation

SDM product documentation: Fault Management.

36: Fault Management (FM): A00005160

36.1 Fault management strategy

This feature does not change the fault management strategy for XA-Core Ethernet interface cards or for the OSSAIN product. It does modify the reason texts that can appear in two OSSAIN log reports.

36.2 Fault management tools and utilities

Unchanged.

36.3 Logs

This activity modifies the values that can appear in the existing OAIN606 and OAIN607 logs. It does not add any new logs or change the format of any existing logs.

36.3.1 Explanation

Log Title: OAIN606

Name: UNDELIVERABLE MESSAGE

Description: This log is generated when OSSAIN data communication software cannot route an incoming message to the appropriate software to process it. The reason text in the log indicates why the message could not be routed.

Event type: INFO

36.3.2 Format

The format is unchanged. Following is an example.

```
RTPC07BZ  OAIN606 MAR12 13:56:45 8500 INFO UNDELIVERABLE MESSAGE
        MESSAGE PROTOCOL RELEASE:   5
        MESSAGE PROTOCOL INCREMENT: 0
        SENDERS PROTOCOL RELEASE:   5
        SENDERS PROTOCOL INCREMENT: 0
        NODE NAME: TO_RTPV                          NODE ID: 70
        SESSION POOL NAME:                          SESSION POOL ID: 0
        SESSION ID: 0
        MESSAGE CLASS: OSAC NODE CLASS              MESSAGE CLASS ID: 22
        NETWORK ADDRESS : 47 245 9 1 : 5290
        REASON: MSG RECEIVED AT UNEXPECTED DESTINATION ADDRESS
        MESSAGE:
        160000003600120000050005460064 00FF0082A1
        26000202640102020B0282041A0005E016002000
        000300FFF52F0109FFFFFFFFFFFFFFFFFFFFFFFF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
```

36.3.3 Field descriptions

The overall field descriptions are unchanged. The values that can appear in the REASON field are changed as follows:

- INVALID NETWORK ADDRESS

  This value, which could appear in earlier releases, no longer appears as of SN07/ISN07. It is replaced by MSG RECEIVED WITH UNEXPECTED SOURCE ADDRESS

- MSG RECEIVED WITH UNEXPECTED SOURCE ADDRESS

  This new reason indicates that the source IP address, port, or both in the incoming message do not match switch datafill for the node whose node name and ID are shown in the log. The NETWORK ADDRESS field shows the actual source address. The most likely explanation is incorrect datafill for the node's IP address at the switch at which the log is generated. Another possibility is that the security of the service provider's network may have been compromised, and a rogue node may be sending OAP messages to the switch.

- MSG RECEIVED AT UNEXPECTED DESTINATION ADDRESS

  This new reason indicates that a message incoming from the node whose name and ID are shown in the log was delivered to a core IP address other than the one datafilled in the switch for the far-end node. The NETWORK ADDRESS in the log is the actual destination address at which the message was received.

  The most likely explanation is that the node that sent the message is configured to have the wrong one of the core's IP addresses. If the switch where the log was generated is datafilled to use an EIU for messaging with the far-end node, the IP address in table IPNETWRK at the switch should be configured in the far-end node as the switch address. If the switch is datafilled to use XA-Core Ethernet interface for messaging with the node, the CM IP address datafilled against the node in table OANODINV in the switch should be configured in the node as the switch IP address.

  Another possibility is that the security of the service provider's network may have been compromised in a way that causes messages to be misrouted.

Note the REASON field can also have other values, which are unchanged by this feature.

36.3.4 Action

Check parallel datafill between the node that sent the message and the switch at which the log was generated. Check for logs or alarms at the node that sent the message. If the problem is not resolved, contact the next level of support.

36.3.5 Associated Operational Measurements or Performance Measurements

Unchanged.

36.3.6 Explanation

Log Title: OAIN607

Name: TRANSPORT INTERFACE ERROR

Description: This log indicates that OSSAIN software encountered an error when interfacing with lower-layer transport software in the switch.

Event type: INFO

36.3.7 Format

The format is unchanged. Following is an example.

```
RTPC07BZ  OAIN607 FEB29 13:03:30 7499 INFO TRANSPORT INTERFACE ERROR
        NODE NAME: TEST_NODE1                    NODE ID: 185
        SESSION POOL NAME:                       SESSION POOL ID: 0
        MESSAGE CLASS:                           MESSAGE CLASS ID: 256
        NETWORK ADDRESS : 47 142 224 185 : 7000
        REASON: XAETHR TRANSMIT FAILURE
        MESSAGE:
        0001000000260012080009000020000008300FF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
        00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
```

36.3.8 Field descriptions

The overall field descriptions are unchanged. This activity adds one new value that can appear in the REASON field:

- XAETHR TRANSMIT FAILURE

  This value indicates that the OSSAIN attempted to send a message using the XA-Core Ethernet interface, but the lower-layer transport software reported back to OSSAIN that the message could not be sent. The cause of the problem is more likely to be in lower-layer software or hardware than in OSSAIN code.

36.3.9 Action

Investigate the underlying transport facilities. Check logs for any that might suggest the root cause of the transport failure. Investigate at MAP levels MAPCI;MTC;XAC;IO and MAPCI;MTC;XAC;ETHR. The peg counts in CI XAIPTOOL may be useful.

36.3.10 Associated Operational Measurements or Performance Measurements

Unchanged.

36.3.11 Additional information

OSSAIN does not generate an OAIN607 log if the reason for failure to send an OAP message via XA-Core Ethernet interface is that no route exists for the source IP address. In this case, the problem is definitely with the underlying transport, and OAIN logs would only clutter up the reporting and possibly make it more difficult to troubleshoot the underlying problem. The underlying transport always raises an XAC alarm when there is no route for messages from a CM host IP address.

36.4 Related documentation

Refer to 297-8403-901, OSSAIN User's Guide, for information about OSSAIN fault management.

37: Fault Management (FM): A00005192

37.1 Fault management strategy

37.2 Fault management tools and utilities

37.3 Link Condition Change Log

37.3.1 Explanation

Log Title: SDM633

Name: SDM LINK CONDITION CHANGE

Description: CBM custlog log to indicate a change in the condition of a CBM link.

Event type: Info

37.3.2 Format

```
SDM633 NONE INFO SDM LINK CONDITION CHANGE
        Link: domain <domain num> port <port num>
        From: <previous link condition>
          To: <new link condition>

SDM633 NONE INFO SDM LINK CONDITION CHANGE
        Link: domain 0 port 0
        From: closed
          To: mtc-open
```

37.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Link: domain	0 or 1	CBM domain number
Link: port	0 or 1	CBM port number
From:	closed, mtc-open, open	previous link condition
To:	closed, mtc-open, open	new link condition

37.3.4 Action

None.

37.3.5 Associated Operational Measurements or Performance Measurements

Associated alarm message: No heartbeat response received.

Severity: Major

Condition: response to CBM 800 heartbeat not received from core.

Action: Check for link faults at cbmmtc HW level. Check for closed link conditions at cbmmtc core level.

Log Title: SDM336 MINOR, SDM636 NONE

Examples:

Alarm Raised Log:

SDM336 MAJOR Alarm raised or updated.
Heartbeat alarm
TimeStamp: Tue Apr 27 12:52:52 2004
ComponentID: CLASS=NET;NETTYPE=CORE
Category: Communications
Probable Cause: communicationsProtocolError
Specific Problem: No heartbeat response received.

Alarm Cleared Log:

SDM636 NONE Alarm raised or updated.
Heartbeat alarm
TimeStamp: Tue Apr 27 15:38:12 2004
ComponentID: CLASS=NET;NETTYPE=CORE
Category: Communications
Probable Cause: noProbableCause
Specific Problem: Heartbeat response received.

Associated alarm message: Crossed Link: link 0 (domain 0 port 0) crossed with link 0 (domain 0 port 1)

Severity: Major

Condition: two link connections are physically crossed.

Action: Fix the crossed link connections.

Log Title: SDM314 MAJOR, SDM614 NONE

Examples:

Alarm Raised Log:

SDM314 MAJOR Alarm raised or updated.
Major Crossed Link: link 0 (domain 0 port 0) crossed with link 1 (domain 0 port 1)
TimeStamp: Mon Mar 29 17:47:26 2004
ComponentID: CLASS=HW;HWTYPE=CROSS_LINK_0
Category: Communications
Probable Cause: configurationOrCustomizationError
Specific Problem:

Alarm Cleared Log:

SDM614 NONE Alarm raised or updated.
Cleared Crossed Link: link 0 (domain 0 port 0) crossed with link 1 (domain 0 port 1)
TimeStamp: Mon Mar 29 17:47:26 2004
ComponentID: CLASS=HW;HWTYPE=CROSS_LINK_0
Category: Communications
Probable Cause: noProbableCause
Specific Problem:

Associated alarm message: OC3 Card Fault: [receive/transmit] fault on link <num> (domain <num> port <num>)

Severity: Major

Condition: signal on receive/transmit fibre to OC3 card is faulty or not present.

Action: check receive/transmit fibre connection.

Log Title: SDM334 MAJOR, SDM634 NONE

Examples:

Alarm Raised Log:

SDM334 MAJOR Alarm raised or updated.
Major OC3 Card Fault: receive fault on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 20:07:21 2004
ComponentID: CLASS=HW;HWTYPE=OC3_FAULT_0
Category: Communications
Probable Cause: equipmentMalfunction
Specific Problem:

Alarm Cleared Log:

SDM634 NONE Alarm raised or updated.
Cleared OC3 Card Fault: receive fault on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:01:10 2004
ComponentID: CLASS=HW;HWTYPE=OC3_FAULT_0
Category: Communications
Probable Cause: noProbableCause
Specific Problem:

Associated alarm message: Link Fault: <fault description> on link <num> (domain <num> port <num>)

Severity: Minor

Condition: diagnostics indicate minor link fault

Action: Report the full text of the alarm to the support group.

Log Title: SDM335 MINOR, SDM635 NONE

Examples:

Alarm Raised Log:

SDM335 MINOR Alarm raised or updated.
Minor Link Fault: Bad Incoming CRCs on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:47:06 2004
ComponentID: CLASS=HW;HWTYPE=LINK_FAULT_0
Category: Communications
Probable Cause: equipmentMalfunction
Specific Problem:

Alarm Cleared Log:

SDM635 NONE Alarm raised or updated.
Cleared Link Fault: Bad Incoming CRCs on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:47:06 2004
ComponentID: CLASS=HW;HWTYPE=LINK_FAULT_0
Category: Communications
Probable Cause: noProbableCause
Specific Problem:

37.4 Related documentation

38: Fault Management (FM): A00005322

38.1 Fault management strategy

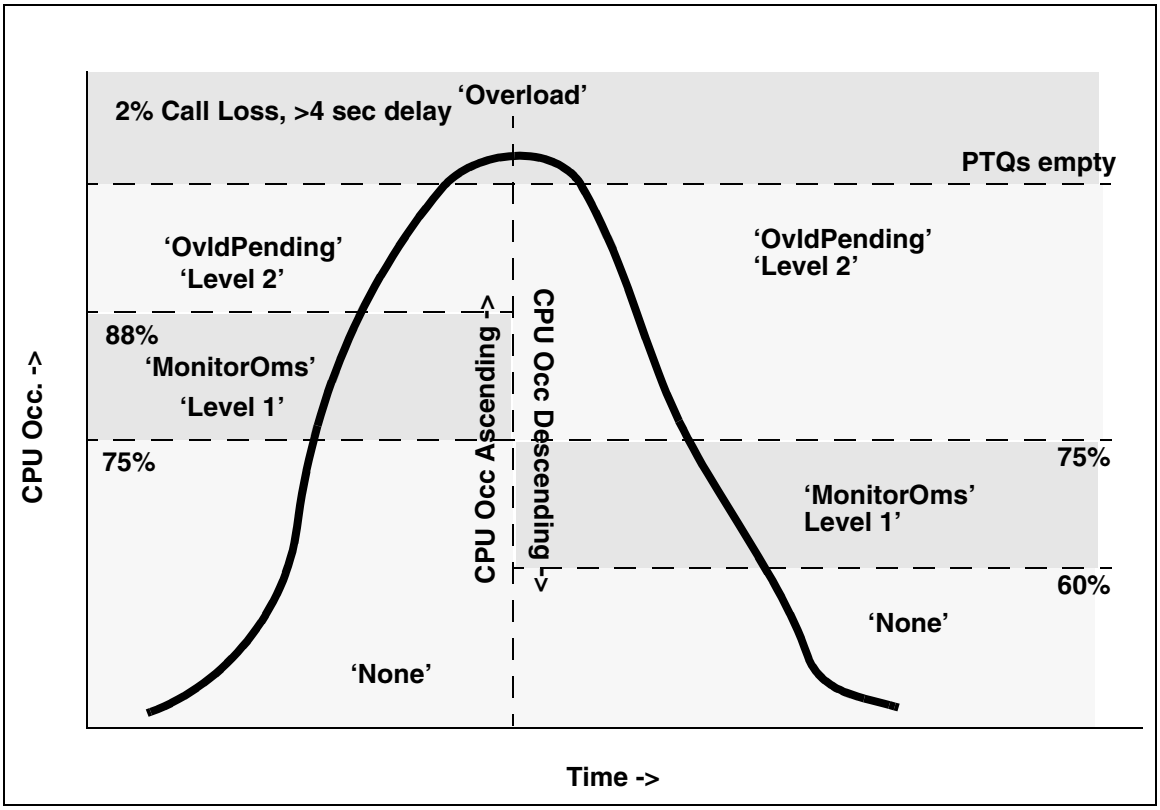
This feature introduces several changes into the reporting of ATMRM resource exhaustion and CEM overload conditions. Since the ATMRM resources are integral to call processing on the MG4K/IW variants of the SPM peripheral node, attempts are made to make ATMRM resource exhaustion conditions very visible. To this end, depending upon the severity of the ATMRM resource exhaustion:

- CEM CALLP can go into Overload which results in SPM399 Overload logs, Minor alarm, CEM state change to ISTb, Node state change to Istb (NODE500, NODE602), MAPCI MIP strings indicating Overload and "querypm flt reason" indicating an overload condition being generated.
- On the ATMRM, a minor alarm will be raised, RM state change to ISTb (SPM500 state change and SPM300 fault reason logs), MAPCI MIP strings indicating Overload and "querypm flt reason" indicating an overload condition will be generated.

The severity of ATMRM resource exhaustion is reported via predefined utilization levels. Each level has a different onset and abatement value to prevent quick entry/exit (jitter) from a single level at a boundary value. The ATMRM resource utilization levels (NONE, LEVEL1 and LEVEL2) are transferred to the CEM and are applied to CEM resources. As a result, the ATMRM and CEM share resource utilization levels. For the case of CPU occupancy/CALLP flow control, these levels are as follows:

- None: Exit: 75% (Level 1 Onset), Onset: 0% (system initialization) or 60% (Level 1 abatement) - The monitored resource is below 75% utilization since last being in "Level 1" or since system initialization.
- Level 1: Onset: 75%, Exit: 88% (Level 2 onset), Abatement: 60% (Level 1 onset) - The CPU resource utilization was initially above its engineering level of 75% and has not dropped below 60% utilization since the initial 75% level was encountered.
- Level 2: Onset: 88%, Exit: Overload triggered, Abatement: 75% - The CPU resource is dangerously overused. CALLP flow control has been triggered to delay call originations in order to lessen CPU occupancy.
- Overload: Onset: Any call delayed by flowcontrol for more than 4 seconds or more than 2% of the calls have been discarded. Abatement: No calls are being delayed. Overload determination is not resource based, it is determined by the characteristics of the states of the calls in flow control.

Figure 1 CPU Occupancy and Resource Utilization Level



The following table shows the maintenance interaction mapped to CPU resource levels. The shaded entries are the new interactions introduced by this feature. Please note, with introduction of this feature, the ATMRM CPU resource level will effect existing maintenance interactions for the CEM.

.

Table 1 Maintenance Interactions for each ATMRM Resource Utilization Level

Mtc Interaction	No Overload	Level 1 Resource Utilization	Level 2 Resource Utilization	CALLP Overload (call state based)
CEM Flowcontrol	Off	Off	On	On
CEM Alarms	None	None	Minor	Minor
ATMRM Alarms	None	Minor	Minor	Minor
CEM State	InSv	InSv	ISTb	ISTb
ATMRM State	InSv	ISTb	ISTb	ISTb
Node State	InSv	InSv	ISTb	ISTb

Changing Existing Interaction

New Interaction

Table 1 Maintenance Interactions for each ATMRM Resource Utilization Level

Mtc Interaction	No Overload	Level 1 Resource Utilization	Level 2 Resource Utilization	CALLP Overload (call state based)
CEM MIP	None	"Monitor OMs"	"Overload Pending"	"Overload"
ATMRM MIP	None	"Monitor OMs"	"Overload Pending"	"Overload Pending"
CEM Logs				
SPM399	None	"Monitor OMs"	"Overload Pending"	"Overload"
NODE500	None	None	ISTb State Change	None
NODE602	None	None	"Reached or Nearing Overload"	None
ATMRM Logs				
SPM300	None	"Monitor OMs"	"Overload Pending"	None
SPM500	None	ISTb State Change	None	None

Please note, the above table indicates the interactions visible when entering or being in high resource utilization levels. When abating the "Level 1" state and returning to the "No Overload" state, alarms are extinguished, MIP strings are cleared, module states are returned to InSv and the logs indicate overload states have cleared, resources utilization levels have returned to normal, and module states are back to InSv.

38.2 Fault management tools and utilities

This feature is not introducing new mechanisms for fault reporting. Existing CORE based tools/mechanisms are being utilized.

38.2.1 Logs

The CORE base **LOGUTIL** command can be used to view the following logs. These logs are existing log classes, but now are being triggered via resource exhaustion/overload conditions on the ATMRM with new fault text.

- NODE500 "Node State Change",
- NODE602 "CEM State Change Reason Report"
- SPM399 "SPM Overload Report",
- SPM300 "Device Fault Report"
- SPM500 "Device State Change".

Depending upon the state of the CEM/ATM RM experiencing the resource exhaustion condition, a minimum of 2 of the above logs types will be generated and possibly, all 5 types of logs will be generated. At the very least, the 2 report logs (SPM399 “SPM Overload Report” and SPM300 “Device Fault Report”) will be generated. These two “Report” logs contain the detailed information needed to identify the “Resource Exhaustion” event.

38.2.2 Alarms

This feature introduces new conditions in which Spectrum device alarms are generated. A minor alarm is raised against an ATMRM when it experiences resource exhaustion. When the CEM’s CALLP performance degrades sufficiently, the CEM will raise a minor alarm. When the active CEM raises an alarm, the NODE will raise a similar alarm. To view which node is alarmed:

MAPCI;MTC;PM;POST SPM <Alarm Type: {Minor, Major, Crit}>

To see details of the alarm:

MAPCI;MTC;PM;POST SPM <SPM Number>; querypm flt

A useful mechanism to determine the current alarm state of all devices within a single node, is the “querypm flt reason” MAPCI command. It will elaborate on the reasons behind a device being alarmed. To view the peripheral faults:

MAPCI;MTC;PM;POST SPM <SPM Number>;querypm flt reason

38.2.3 State Changes

To indicate a device’s resource exhaustion/overload state, a device’s maintenance state can be degraded from “InSv” to “Istb”. If the device is the active CEM, a degraded device state will also degrade the node state in a similar manner. To view the degraded nodes:

MAPCI;MTC;PM;POST SPM <State: {SysB, ManB, OffL, CBsy, ISTb, InSv}>

The above command only posts the node by state, not the individual devices. Once the node is posted, the “querypm flt reason” can be used to indicate the device degradation reasons.

38.2.4 Maintenance Operation Strings

To view the current resource exhaustion/overload state of a Spectrum device, the device must be selected.

MAPCI;MTC;PM;POST SPM <SPM Number>;SELECT <Device Type: {CEM, ATM}> <Device Number {0,1}>

On the maintenance status line, the device's resource exhaustion/overload state will be visible if said condition exists. These status indicators are:

- "Monitor OMs",
- "Ovld Pending",
- "Overload".

38.3 Logs

38.3.1 ATM605

This feature removes the generation of the ATM605 log. The ATM605 is replaced with the SPM300 "Device Fault Report" log.

38.3.1.1 Explanation

Log Title: ATM 605

Name: ATM Overload Event

Description: This log is generated on the DMS CORE whenever an Spectrum ATMRM enters/leaves pre-defined resource utilization levels. Resource utilization levels are commonly referred to as overload levels.

Event type: Threshold

38.3.1.2 Format

```
<LABCLLI> ATM605 <MMMdd hh:mm:ss SSSS> INFO  ATM Overload Event
           Location: SPM <xx> ATM RM
           Description: <Description String>
```

38.3.1.3 Examples

38.3.1.3.1 Exiting Level 1 Resource Utilization

```
MSH207BW      ATM605 FEB25 12:58:22 5209 INFO ATM Overload Event
               Location: SPM 4 ATM RM
               Description: ATM RM Not in Overload
```

38.3.1.3.2 Entering Level 1 Resource Utilization/Exiting Level 2 Resource Utilization

```
MSH207BW      ATM605 FEB25 14:14:00 5236 INFO ATM Overload Event
               Location: SPM 4 ATM RM
               Description: ATM RM Near Overload
```

38.3.1.3.3 Entering Level 2 Resource Utilization

```
MSH207BW       ATM605 FEB25 14:40:09 5009 INFO ATM Overload Event
                Location: SPM 4 ATM RM
                Description: ATM RM In Overload
```

38.3.1.4 Field descriptions

The following table describes the variable fields (fields within "<>" "38.3.1.2 Format" on page 2277):

Table 2 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
XX	00 to 85	CEM number of the SPM for which the log is generated.
Description String	1) ATM RM Not in Overload 2) ATM RM Near Overload 3) ATM RM in Overload 4) Invalid ATM Overload Level Received from ATM	The set of possible strings for the ATMRM when traversing various resource utilization levels. String "1" is an error clearing event. The subsequent strings are for error notification events.

The 3 "Description Strings" indicate the 3 following events respectfully:

1. Active ATMRM's CPU occupancy has dropped below 60%.
2. Active ATMRM's CPU occupancy initially exceeds 75% and subsequently exceeds 60%.
3. Active ATMRM's CPU occupancy initially exceeds 88% and subsequently exceeds 75%.
4. Unknown error has been encountered - contact Nortel support personnel.

38.3.1.5 Action

None. Log is being replaced with SPM300 "Device Fault Report".

38.3.1.6 Associated Operational Measurements or Performance Measurements

None. Log is being replaced with SPM300 “Device Fault Report”.

38.3.1.7 Additional information

None. Log is being replaced with SPM300 “Device Fault Report”.

38.3.2 SPM399

38.3.2.1 Explanation

Log Title: SPM 399

Name: SPM Overload Report

Description: This log is generated whenever a Spectrum CEM enters/leaves pre-defined overload conditions.

This feature augments the conditions in which this log is generated. With this feature, the CEM overload states are effected by the ATM RM resource utilization levels. As a result, the ATM RM resource utilization levels can trigger the generation of this log.

Event type: Trouble

38.3.2.2 Format

Format has not changed

```
<LABCLLI> <*> SPM399 <MMMdd hh:mm:ss SSSS> TBL  SPM Overload Report
        SPM   <xx> CEM   <y> : <Activity> <state> Time: <hh:mm:ss.SSS>
        Reason: <Reason string>
        Prev: <previous state> Curr: <current state> Diagnostic: <#HHHH>
        Action: <Action string>
        Location: SPM <SPM no> Type: <Type> Fabric: <Fabric>
```

38.3.2.3 Example

38.3.2.3.1 Entering Monitor OMs

```
MSH207BW      SPM399 MAR02 11:59:47 8100 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 11:59:43.685
        Reason:     Overload OMs initiated
        Prev: None           Curr: MonitorOMs     Diagnostic: #0000
        Action:     Check SPMACT and SPMOVLD OMs
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.2.3.2 Enter Overload Pending

```
MSH207BW   *  SPM399 MAR02 11:59:51 8600 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 11:59:51.040
        Reason:     CEM in Overload Pending state
        Prev: MonitorOMs     Curr: OvldPending    Diagnostic: #2000
        Action:     Check SPMACT and SPMOVLD OMs
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.2.3.3 Entering Overload

```
MSH207BW  **  SPM399 MAR02 11:59:57 4500 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 11:59:55.555
        Reason:     CEM experiencing Overload
        Prev: OvldPending    Curr: Overload       Diagnostic: #206e
        Action:     Contact next level of support
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.2.3.4 Exiting Overload

```
MSH207BW   *  SPM399 MAR02 12:12:51 2200 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 12:12:45.620
        Reason:     CEM in Overload Pending state
        Prev: Overload       Curr: OvldPending    Diagnostic: #306e
        Action:     Check SPMACT and SPMOVLD OMs
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.2.3.5 Exiting Overload Pending

```
MSH207BW      SPM399 MAR02 12:13:19 2900 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 12:13:19.340
        Reason:     Overload Pending cleared
        Prev: OvldPending    Curr: MonitorOMs     Diagnostic: #1000
        Action:     Check SPMACT and SPMOVLD OMs
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.2.3.6 Exiting Monitor OMs

```
MSH207BW      SPM399 MAR02 12:13:28 3600 TBL  SPM Overload Report
        SPM   4 CEM   1 : A                      Time: 12:13:28.020
        Reason:     Overload cleared
        Prev: MonitorOMs     Curr: None           Diagnostic: #0000
        Action:     None
        Location: SPM   4  Type: SMG4      Fabric: ATM
```

38.3.2.4 Field descriptions

Field contents have not changed.

Table 3 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
*	Priority of Alarm - Two asterisks (**), one asterisk (*) or empty space	Two asterisks (**) appear for a log of 'Major' severity, one asterisk (*) appears for a log of severity 'Minor' and empty space appears for a log of severity 'No Alarm'.
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	CEM number of the SPM for which the log is generated.
Activity	A,I	Activity of the CEM. 'A' for Active and 'I' for Inactive.
State	INSV,ISTB,MANB,SYSB	State of the CEM.
hh:mm:ss.SSS	hh - 00 to 23 mm - 00 to 59 ss - 00 to 59 SSS - 000 to 999	Time when the error/ error-clearing event happened in the SPM. This time will be earlier than the time that appears on the first line because the event happens in the SPM first and then the core generates the log.

Table 3 Field descriptions

Field	Value	Description
Reason	1) “Overload OMs initiated” 2) “CEM in Overload Pending state” 3) “CEM experiencing Overload” 4) “Overload Pending cleared” 5) “Overload cleared”	These are the five possible strings that can appear in the ‘Reason’ field of the log. The first three reasons are for error scenarios and the fourth one is for the error-clearing scenario.
Prev	1)”None” 2) “MonitorOMs” 3)”OvldPending” 4)”Overload”	This field gives the overload condition of the SPM before the error/error-clearing event happened.
Curr	1)”None” 2) “MonitorOMs” 3)”OvldPending” 4)”Overload”	This field gives the current overload condition of the SPM.
Diagnostics	“#0000” to “#FFFF”	This field is for the designers who are doing the trouble-shooting. The craft need not look in to this field.
Action	1)”Check SPMACT and SPMOVLD OMs.” 2) “Contact your next level of support.” 3)”None.”	This field gives the craft information on the action that needs to be taken. The string 1) is for logs generated for “Check OMs” and “Overload Pending”. String 2) is generated in addition to String 1) when an “Overload” event occurs. The last string is for logs generated for an error-clearing scenario.
SPM no	00 to 85	SPM number
Type	DMSCP,SMG4,IW	Variant of the SPM
Fabric	ATM,IP,ENET	The switching fabric

The CEM now incorporates the ATM RM's resource utilization level into the generation of the SPM399. As a result, the ATM RM resource levels can trigger the SPM399 logs under the following condition:

1. Overload OMs initiated - ATM RM's CPU occupancy initially exceeds 75%, then subsequently exceeds 60%.
2. CEM in Overload Pending state - ATM RM's CPU occupancy initially exceeds 88%, then subsequently exceeds 75%. The overload pending state can also be entered when the CEM has exited overload conditions.
3. CEM experiencing Overload - The ATM RM ***cannot*** trigger this transition. The ATM RM can influence/contribute to this state, but it cannot be the trigger. This transition is triggered when CEM CALLP has delayed calls for more than 4 seconds, or when over 2% of calls have been tossed. Overload is exited only when there are no more delayed/tossed calls on the CEM.
4. Overload Pending cleared - ATM RM's CPU occupancy initially exceeds 88%, then subsequently drops below 75%.
5. Overload cleared - ATM RM's CPU occupancy has dropped below 60%

38.3.2.5 Action

The 'Action' field of the log contains the action that is needed to be taken by the craft. For the situations when the SPM is leaving an overload condition, the 'Action' field will have 'None' and no action need be taken.

1. Check SPMACT and SPMOVLD OMs - Consult these OM groups on the DMS CORE. Consultation should indicate that the amount of traffic being presented to the Spectrum exceeds the engineering guidelines. The craft should re-engineer traffic sources to bring traffic levels presented to the Spectrum to within published guidelines.
2. Contact your next level of support - Contact Nortel support personnel.
3. None - For the situations when the SPM is leaving an overload condition, no action is required.

38.3.2.6 Associated Operational Measurements or Performance Measurements

In the OM group SPMOVLD, the OVLDNUM register is pegged when the SPM enters the 'Overload' condition and register OVLDUSG maintains the number of seconds the SPM was in the 'Overload' condition in the present OM collection interval. Similarly, the register OVLDPNUM is pegged when the SPM enters the 'Overload Pending' condition and register OVLDPUSG maintains the number of seconds the SPM was in the 'Overload Pending' condition in the present OM collection interval.

Looking at the “TRK” OM group for the trunk groups terminating on the overloaded Spectrum should indicate the source of the overload. The “CONNECT” OM indicates the number of calls successfully connected by this Spectrum for this trunk group. The “INCATOT” OM indicates the number total incoming connect requests for this trunk group for this Spectrum. If these two OMs are not equal, then call failures have occurred and need to be further investigated. Depending upon office configuration/traffic scenarios, all trunk groups terminating on this Spectrum may have to have these OM added together for the analysis to be meaningful.

38.3.2.7 Additional information

a. A00002431 - SP20 “LX82BA Capacity Delivery” - Enhances CALLP Flowcontrol interaction

b. A00002432 - SP20 “SPM Enhanced Overload OMs and Logs”- Enhances overload reporting.

38.3.3 SPM300

38.3.3.1 Explanation

Log Title: SPM300

Name: SPM300 Device Fault Report

Description: This feature adds new conditions for the generation of this existing log class.

With this feature, when ATM RM resource utilization crosses several pre-defined thresholds, instances of this log will be generated indicating resource utilization levels.

This log replaces the ATM605 log.

Event type: Trouble

38.3.3.2 Format

The format of this log has not changed. New descriptive strings have been added to describe the ATM RM’s resource utilization levels.

```
<LABCLLI> <*> SPM300 <MMMdd hh:mm:ss SSSS TBL  Device Fault Report
          Location    : SPM :<XX> ATM : <Y> Activity : <Activity1>
          Status      : <Status String>
          Problem Description: <Problem Description String>
          <Slot Number><Activity2>: <Problem Refinement String>
          Action      : <Action String>
          Cardlist    :
            No Cardlist Available.
```

38.3.3.3 Examples

38.3.3.3.1 Clearing ATMRM Resource Utilization Issues

```
MSH207BW      SPM300 FEB25 14:40:19 5900 TBL  Device Fault Report
          Location   : SPM : 4   ATM : 0 Activity : A
          Status     : Info Only
          Problem Description: No Problem
            8A: Resources OK
          Action     : No Action Required.
          Cardlist   :
            No Cardlist Available.
```

38.3.3.3.2 Entering Monitor OMs

```
MSH207BW   *  SPM300 FEB25 14:13:59 5000 TBL  Device Fault Report
          Location   : SPM : 4   ATM : 0 Activity : A
          Status     : Fault Raised
          Problem Description: Non Critical
            8A: Monitor OMs - Check SPMACT and SPMOVLD OMs
          Action     : Refer to NTPs for Alarm Clearing Procedures.
          Cardlist   :
            No Cardlist Available.
```

38.3.3.3.3 Entering Overload Pending

```
MSH207BW   *  SPM300 FEB25 14:14:08 3100 TBL  Device Fault Report
          Location   : SPM : 4   ATM : 0 Activity : A
          Status     : Fault Raised
          Problem Description: Non Critical
            8A: Ovld Pending
          Action     : Refer to NTPs for Alarm Clearing Procedures.
          Cardlist   :
            No Cardlist Available.
```

38.3.3.4 Field descriptions

Table 4 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
*	Priority of Alarm - One asterisk (*) or empty space	One asterisk (*) appears for a log of severity ‘Minor’ and empty space appears for a log of severity ‘No Alarm’.

Table 4 Field descriptions

Field	Value	Description
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	ATM RM number of the SPM for which the log is generated.
Activity1	A,I	Activity of the ATM RM. ‘A’ for Active and ‘I’ for Inactive.
Status String	1) “Info Only”, 2) “Fault Raised”	Log reason indication - The first string indicates no issues exists. The second string indicates an error condition.
Problem Description String	1) “No Problem”, 2) “Non Critical”	Severity of the fault - The first string indicates no issues exists. The second string indicates an error condition.
Slot Number	7,8	Slot Number of CEM which maintains the ATMRM
Activity2	A,I	Activity of the CEM. ‘A’ for Active and ‘I’ for Inactive.
Problem Refinement String	1) “Resources OK”, 2) “Monitor OMs - Check SPMACT and SPMOVLD OMs”, 3) “Ovld Pending”	ATM RM Resource Utilization level. First refinement indicates the condition has cleared. The subsequent 2 refinements indicate an error condition.
Action String	1) “Refer to NTPs for Alarm Clearing Procedures.”, 2) “No Action Required.”	Action the craft can preform.

38.3.3.5 Action

Same actions are to be preformed as when similar SPM399 logs are generated.
For more details, see“38.3.2.5 Action” on page 2283.

38.3.3.6 Associated Operational Measurements or Performance Measurements

Same analysis is to be preformed as when similar SPM399 logs are generated. For more details, see “38.3.2.6 Associated Operational Measurements or Performance Measurements” on page 2283.

38.3.3.7 Additional information

Please consult the same information as when the SPM399 logs are generated. For more details, see “38.3.2.7 Additional information” on page 2284.

38.3.4 NODE500

38.3.4.1 Explanation

Log Title: Node 500

Name: Node State Change

Description: This log is generated whenever a Spectrum node or Spectrum CEM changes state.

This feature adds new triggers for the generation of this log. The ATM RM resource levels are factored into the generation of this log in the same manner as the CEM resources are currently factored.

In the case of ATMRM resource exhaustion, when this log is triggered the following logs will also be generated. These other logs provide the reason behind the NODE/CEM state change.

- SPM399 SPM Overload Report
- SPM300 Device Fault Report

Event type: Information

38.3.4.2 Format

This feature is not changing the format of this log type. There are two formats for this log class: 1) Node State change, 2) CEM state change.

38.3.4.2.1 Node State Change

```
<LABCLLI> <*> NODE500 <MMMdd hh:mm:ss SSSS> INFO Node State Change
        Location: SPM  <xx>
        From:     <Node State>  ( <Connectivity State> )
        To        <Node State>  ( <Connectivity State> )
```

38.3.4.2.2 CEM State Change

```
<LABCLLI> <*> NODE500 <MMMdd hh:mm:ss SSSS> INFO Node State Change
        Location: SPM  <xx> Unit <y>
        From:     <Node State>  ( <Connectivity State>, <Activity State> )
        To        <Node State>  ( <Connectivity State>, <Activity State> )
```

38.3.4.3 Examples

38.3.4.3.1 Node ISTb State Change

```
MSH207BW   * NODE500 MAR04 09:21:26 7500 INFO Node State Change
        Location: SPM 10
        From:     InSv ( Connected )
          To:     ISTb ( Connected )
```

38.3.4.3.2 Node InSv State Change

```
MSH207BW     NODE500 MAR04 09:21:14 7200 INFO Node State Change
        Location: SPM 10
        From:     ISTb ( Connected )
          To:     InSv ( Connected )
```

38.3.4.3.3 CEM ISTb State Change

```
MSH207BW   * NODE500 MAR04 09:49:40 0000 INFO Node State Change
        Location: SPM 10 Unit 1
        From:     InSv ( Connected, Active )
          To:     ISTb ( Connected, Active )
```

38.3.4.3.4 CEM InSv State Change

```
MSH207BW     NODE500 MAR04 09:21:14 7100 INFO Node State Change
        Location: SPM 10 Unit 1
        From:     ISTb ( Connected, Active )
          To:     InSv ( Connected, Active )
```

38.3.4.4 Field descriptions

This feature is not changing the format of this log type.

Table 5 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
*	Priority of Alarm - One asterisk (*) or empty space	One asterisk (*) appears for a log of severity ‘Minor’ and empty space appears for a log of severity ‘No Alarm’.

Table 5 Field descriptions

Field	Value	Description
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	CEM number of the SPM for which the log is generated.
Node State	InSv, ISTb	The ISTb condition indicates the NODE/ CEM is experiencing ATMRM resource exhaustion. The InSv condition indicates no such condition exists.
Connectivity State	Connected, Isolated	CORE Connectivity Indicator - Nodes/CEM experiencing resource exhaustion should always be ”Connected”
Activity State	Active, Inactive	CEM’s Activity State - Only Active CEMs should experience resource exhaustion.

38.3.4.5 Action

In the case of ATMRM resource exhaustion, the following 3 log types will also be generated:

- NODE602 “CEM State Change Reason Report”,
- SPM300 “Device Fault Report” and a
- SPM399 “SPM Overload Report”.

See the “Action” sections associated with the above 3 log types for corrective action.

38.3.4.6 Associated Operational Measurements or Performance Measurements

See “38.3.2.6 Associated Operational Measurements or Performance Measurements” on page 2283 for details

38.3.4.7 Additional information

Please consult the same information as when the SPM399 logs are generated. For more details, see “12.3.3.7 Additional information” on page 99.

38.3.5 NODE602

38.3.5.1 Explanation

Log Title: Node 602

Name: CEM State Change Reason Report

Description: This log is generated whenever a Spectrum CEM changes state. The fault string “Unit reached or nearing OVERLOAD” is generated only when the active CEM enters the Level 2 overload state. There is no abatement log.

This feature adds new triggers for the generation of this log. The ATM RM resource levels are factored into the generation of this log in the same manner as the CEM resources are currently factored.

In the case of ATMRM resource exhaustion, when this log is triggered, the following logs will also be generated. These other logs provide the reason behind the NODE/CEM state change.

- NODE500 Node State Change
- SPM399 SPM Overload Report
- SPM300 Device Fault Report

Event type: Trouble

38.3.5.2 Format

This feature is not changing the format of this log type. A new reason string has been added.

```
<LABCLLI> NODE602 <MMMdd hh:mm:ss SSSS> TBL  CEM State Change Reason Report
        Location: SPM  <xx>   CEM :  <y>
        Reason  : CPU: Unit reached or nearing OVERLOAD.
        Location: SPM  <xx>  Type: SMG4      Fabric: ATM
```

38.3.5.3 Example

```
MSH207BW     NODE602 MAR16 13:31:15 7757 TBL  CEM State Change Reason Report
        Location: SPM:  10   CEM :  0
        Reason  : CPU: Unit reached or nearing OVERLOAD.
        Location: SPM  10  Type: SMG4      Fabric: ATM
```

38.3.5.4 Field descriptions

This feature is not changing the format of this log type.

Table 6 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	CEM number of the SPM for which the log is generated.

38.3.5.5 Action

In the case of ATMRM resource exhaustion, the following 3 log types will also be generated:

- NODE500 “Node State Change”,
- SPM300 “Device Fault Report” and a
- SPM399 “SPM Overload Report”.

See the “Action” sections associated with the above 3 log types for corrective action.

38.3.5.6 Associated Operational Measurements or Performance Measurements

See “38.3.2.6 Associated Operational Measurements or Performance Measurements” on page 2283 for details

38.3.5.7 Additional information

Please consult the same information as when the SPM399 logs are generated. For more details, see “12.3.3.7 Additional information” on page 99.

38.3.6 SPM500

38.3.6.1 Explanation

Log Title: SPM 500

Name: Device State Change

Description: This class of logs are generated when a Spectrum Resource Module changes state.

This feature does not change the information contained in this log class. This feature adds a new trigger for the generation of this type of log.

When the ATM RM experiences initial resource exhaustion, or recovers from resource exhaustion, this log will be triggered. Please note, in the case of ATM RM resource exhaustion, when this log is generated, it will be accompanied by a SPM300 “Device Fault Report” and a SPM399 “SPM Overload Report”.

Event type: Information

38.3.6.2 Format

This feature does not change the format or contents of this log class.

```
<LABCLLI> <*> SPM500 <MMMdd hh:mm:ss SSSS> INFO Device State Change
         Location: SPM : <xx>   ATM : <y>
         From    : <State String>  (<Activity String>)
         To      : <State String>  (<Activity String>)
```

38.3.6.3 Examples

38.3.6.3.1 Istb Device State Change

```
MSH207BW *  SPM500 FEB25 14:13:59 5135 INFO Device State Change
        Location: SPM : 4   ATM : 0
        From    : InSv (Active  )
        To      : ISTb (Active  )
```

38.3.6.3.2 Insv Device State Change

```
MSH207BW    SPM500 FEB25 14:40:19 5817 INFO Device State Change
        Location: SPM : 4   ATM : 0
        From    : ISTb (Active  )
        To      : InSv (Active  )
```

38.3.6.4 Field descriptions

Field descriptions are not changes by this feature.

Table 7 Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
Priority of Alarm	One asterisk (*) or empty space	One asterisk (*) appears for a log of severity ‘Minor’ and empty space appears for a log of severity ‘No Alarm’.

Table 7 Field descriptions

Field	Value	Description
MMMdd hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	CEM number of the SPM for which the log is generated.
State String	InSv, ISTb	Device State - An ATMRM should be InSv when there is no resource exhaustion, else ISTb.
Activity String	Active, Inactive	Identifies the sparing state of the ATM RM. Only the “Active” ATMRM should experience resource exhaustion.

38.3.6.5 Action

In the case of ATMRM resource exhaustion, the following 2 log types will also be generated:

- SPM300 “Device Fault Report” and a
- SPM399 “SPM Overload Report”.

See the “Action” sections associated with the above 2 log types for corrective action.

38.3.6.6 Associated Operational Measurements or Performance Measurements

In the case of ATMRM resource exhaustion, the following 2 log types will also be generated:

- SPM300 “Device Fault Report” and a
- SPM399 “SPM Overload Report”.

See “38.3.2.6 Associated Operational Measurements or Performance Measurements” on page 2283 for details

38.3.6.7 Additional information

Please consult the same information as when the SPM399 logs are generated. For more details, see “12.3.3.7 Additional information” on page 99.

38.4 Alarms

This feature does not introduce any new alarms. It provides new conditions for the triggering the existing ISTb alarm on both the ATMRM and the CEM.

The resource exhaustion based ISTb alarm for the ATMRM is triggered before the similar alarm for the CEM. The CEM ISTb alarm will only be triggered for ATMRM resource utilization level of Level 2 and/or the CEM reaching a similar resource utilization level.

38.4.1 Format

This feature does not change the format of this existing alarm. The following output is from the "**MAPCI;MTC;PM;POST SPM <xx>;QUERYPM FLT**" command.

```
ATM  <Active ATMRM #> ISTb Act   Alarm: ISTB     Severity: Minor    Action: RPT
```

Field descriptions are not changed by this feature.

Table 8 Field descriptions

Field	Value	Description
`ATM`	All valid RM types.	Indicates the RM type generating the alarm.
`<Active ATMRM #>`	0,1	RM number of the active unit.
`ISTb`	ISTb	RM device state. Only the "ISTb" state is allowed for the "ISTb" alarm.
`Act`	Act	Activity of the ATMRM generating the alarm. Only the active ATMRM can generate this log for an overload condition.
`Alarm: ISTB`	ISTb	Alarm type. Only "ISTb" is allowed.
`Severity: Minor`	Minor	Alarm severity. Only "Minor" is allowed for an overload condition.
`Action: RPT`	RPT, NORPT	Indicates whether a log is to be generated for this alarm type. In table MNNODE a tuple for this node exists that indicates for an ISTb alarm, a SPM300 "Node State Change" and/or a SPM500 "Device State Change" log will be generated.

38.4.2 Associated Alarm Message

To look at other output to refine the "ISTb" alarm conditions, use the "**MAPCI;MTC;PM;POST SPM <xx>; QUERYPM FLT REASON**" command.

For a Level 1 ATMRM resource exhaustion condition, the output will be:

```
ATM <Active ATMRM #> ISTb NonCritical faults:
ApplicationFlt: Monitor OMs - Check SPMACT and SPMOVLD OMs
```

For a Level 2 ATMRM resource exhaustion condition, the output will be:

```
ATM <Active ATMRM #> ISTb NonCritical faults:
  ApplicationFlt: Ovld Pending
CEM <Active CEM #> ISTb NonCritical faults:
  CPU: Unit reached or nearing OVERLOAD
```

For a CEM CALLP Overload condition, the output will be:

```
ATM <Active ATMRM #> ISTb NonCritical faults:
  ApplicationFlt: Overload
CEM <Active CEM #> ISTb NonCritical faults:
  CPU: Unit reached or nearing OVERLOAD
```

38.4.3 Severity

Minor

38.4.4 Cause or Condition

The ATMRM resource exhaustion triggered ISTb alarm is triggered by any form of resource exhaustion (i.e. high rates of traffic) in the ATMRM. The CEM alarm is raised when the ATMRM enters Level 2 resource exhaustion (i.e. ATMRM CPU occupancy is initially greater than 88%, then greater than 75%).

38.4.5 Duration

The ATMRM resource exhaustion triggered alarm will exist as long as the ATMRM is experiencing any form of resource exhaustion. The CEM alarm is raised when the ATMRM enters Level 2 resource exhaustion.

38.4.6 Action

As specified in the SPM399 “Overload Report” log.

38.4.7 Association

For full association, see Table 1, “Maintenance Interactions for each ATMRM Resource Utilization Level,” on page 2274.

38.5 Maintenance Operation Strings

The Maintenance Operation strings (also known as MIP Strings (Maintenance In Progress)) displays the current maintenance status of the posted device.

This feature extends the current CEM overload MIP strings functionality to the ATMRM.

38.5.1 Format

This feature adds the overload status MIP string to the ATMRM.

To view the current resource exhaustion/overload state of an ATMRM module, the module must be selected.

MAPCI;MTC;PM;POST SPM <SPM Number>;SELECT ATM <Module Number {0,1}>

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .        .        .        .        .        .        .        .        .        .

ATM                                  SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                    0        0        0        0        0      100
 2               SPM                   0        0        0        0        0       85
 3 ListSet         ATM                 0        0        0        0        0        2
 4
 5               SPM 4    ATM 0    Act    InSv          <MIP String>
 6 Tst
 7 Bsy           Loc : Row G  FrPos 41 ShPos  0 ShId 0 Slot  1   Prot Grp : 1
 8 RTS           Default Load: ATC20CF                          Prot Role: Working
 9 OffL
10 LoadMod       ATM:
11
12 Next
13 Select_
14 QueryMod
15 ListAlm
16 Prot
17 SPERFORM
18
   DOC
Time  12:01  >
```

This feature does not change the format of this display.

Table 9 Field descriptions

Field	Value	Description
MIP String	“”, “/Monitor OMs”, “/Ovld Pending”.	Indicates the current maintenance operations of the posted device.

- “” (no string): Device is not experiencing resource exhaustion.
- “/Monitor OMs”: Resource utilization is at Level 1 (See “Fault management strategy” on page 2273. for resource level description,
- “/Ovld Pending”: Resource utilization is at Level 2.
- Please note, the “/Overload” MIP string does not exist for the ATMRM. Only CEMs can be in this state as it indicates that CEM CALLP is experiencing overload.

38.5.2 Cause or Condition

The ATMRM resource exhaustion triggered MIP strings is triggered by any form of resource exhaustion (i.e. high rates of traffic) in the ATMRM. The CEM MIP string can be raised when the ATMRM enters any level of resource exhaustion.

38.5.3 Duration

The ATMRM resource exhaustion triggered MIP string will exist as long as the ATMRM is experiencing any form of resource exhaustion The CEM MIP string is raised when the ATMRM enters any level of resource exhaustion.

38.5.4 Action

As specified in the SPM399 “Overload Report” log.

38.5.5 Association

For full association, see Table 1, “Maintenance Interactions for each ATMRM Resource Utilization Level,” on page 2274.

On the maintenance status line, the module’s resource exhaustion/overload state will be visible if said condition exists. These status indicators are:

38.6 Related documentation

a. A00002431 - SP20 “LX82BA Capacity Delivery” - Enhances CALLP Flowcontrol interaction

b. A00002432 - SP20 “SPM Enhanced Overload OMs and Logs”- Enhances overload reporting.

39: Fault Management (FM): A00005363

39.1 Fault management strategy

Logs are used for fault management.

39.2 Fault management tools and utilities

The VPTRACE tool is used to turn on VAMP logs.

39.3 Logs

39.3.1 VAMP901

The VAMP901 log is enhanced for the following two purposes:

- to display the new Business Customer ID parameter, and
- the AMA Digits parameter has an additional value possible in the Digits Type subfield (300)

39.3.1.1 Explanation

Log Title: VAMP901

Name: Variable AIN Message Platform 901 Log

Description: The VAMP901 log report is generated when a message is received via the VAMP framework. The VAMP framework captures the messages only when message logging has been enabled with the VPTRACE tool. For more detailed information, refer to NTP 297-2621-370--UCS DMS-250 NetworkBuilder Application Guide. This log is intended for lab use only and is not suitable for live switches due to the number and size of reports.

Event type: Info

39.3.1.2 Format

The new Business Customer ID parameter appears in the VAMP901 log with the other parameters. Its display format is shown below.

```
AMABUSCSTID: <string of digits>
```

39.3.1.3 Field descriptions

The new field AMABUSCSTID consists of a string of digits

Table 1 Field descriptions

Field	Value	Description
AMABUSCSTID	Vector of 11 digits	Digits

Field name: AMABUSCSTID
Field optionality: optional, variable
Type: Alphanumeric
Size: 7 bytes
Value(s): See field descriptions above
Descriptions: See field descriptions above
NTP table reference: N/A

39.3.1.4 Action

None

39.3.1.5 Associated Operational Measurements or Performance Measurements

None

39.3.1.6 Additional information

None

39.4 Related documentation

None

40: Fault Management (FM): A00005375

40.1 Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “New Shelf Discovery Alarms” feature there will be new faults added to provide the reason when shelf discovery failed due to a particular card or due to an incompatible card.

40.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

40.2.1 Faults, Alarms and Logs

There will be new Shelf faults raised and cleared by the MG9000 to indicate the specific reason the shelf discovery failed.

40.3 Alarms

40.3.1 Explanation

40.3.1.1 SHELFCOMPATIBILITY

Title: shelfCompatibility

Name: Incompatible Shelf

Description: This log is generated when a shelfCompatibility fault is received from the MG9kEM server.

40.3.1.2 CARDDISCOVERY

Title: cardDiscovery

Name: Card Discovery failure

Description: This log is generated when a cardDiscovery fault is received from the MG9kEM server.

40.3.1.3 CARDDISCPOWIO

Title: cardDiscPowIo

Name: Discovery failure for IO card

Description: This log is generated when a cardDiscPowIo fault is received from the MG9kEM server.

40.3.1.4 CARDDISPOWSIC

Title: cardDiscPowSic

Name: Discovery failure for SIC card

Description: This log is generated when a cardDiscPowSic fault is received from the MG9kEM server.

40.3.1.5 CARDDISCSLOT2

Title: cardDiscSlot2

Name: Discovery failure for card in Slot 2

Description: This log is generated when a cardDiscSlot2 fault is received from the MG9kEM server.

40.3.1.6 CARDDISCSLOT3

Title: cardDiscSlot2

Name: Discovery failure for card in Slot 3

Description: This log is generated when a cardDiscSlot3 fault is received from the MG9kEM server.

40.3.1.7 CARDDISCSLOT4

Title: cardDiscSlot4

Name: Discovery failure for card in Slot 4

Description: This log is generated when a cardDiscSlot4 fault is received from the MG9kEM server.

40.3.1.8 CARDDISCSLOT5

Title: cardDiscSlot5

Name: Discovery failure for card in Slot 5

Description: This log is generated when a cardDiscSlot5 fault is received from the MG9kEM server.

40.3.1.9 CARDDISCSLOT6

Title: cardDiscSlot6

Name: Discovery failure for card in Slot 6

Description: This log is generated when a cardDiscSlot6 fault is received from the MG9kEM server.

40.3.1.10 CARDDISCSLOT7

Title: cardDiscSlot7

Name: Discovery failure for card in Slot 7

Description: This log is generated when a cardDiscSlot7 fault is received from the MG9kEM server.

40.3.1.11 CARDDISCSLOT8

Title: cardDiscSlot8

Name: Discovery failure for card in Slot 8

Description: This log is generated when a cardDiscSlot8 fault is received from the MG9kEM server.

40.3.1.12 CARDDISCSLOT9

Title: cardDiscSlot9

Name: Discovery failure for card in Slot 9

Description: This log is generated when a cardDiscSlot9 fault is received from the MG9kEM server.

40.3.1.13 CARDDISCSLOT10

Title: cardDiscSlot10

Name: Discovery failure for card in Slot 10

Description: This log is generated when a cardDiscSlot10 fault is received from the MG9kEM server.

40.3.1.14 CARDDISCSLOT11

Title: cardDiscSlot11

Name: Discovery failure for card in Slot 11

Description: This log is generated when a cardDiscSlot11 fault is received from the MG9kEM server.

40.3.1.15 CARDDISCSLOT12

Title: cardDiscSlot12

Name: Discovery failure for card in Slot 12

Description: This log is generated when a cardDiscSlot12 fault is received from the MG9kEM server.

40.3.1.16 CARDDISCSLOT13

Title: cardDiscSlot13

Name: Discovery failure for card in Slot 13

Description: This log is generated when a cardDiscSlot13 fault is received from the MG9kEM server.

40.3.1.17 CARDDISCSLOT14

Title: cardDiscSlot14

Name: Discovery failure for card in Slot 14

Description: This log is generated when a cardDiscSlot14 fault is received from the MG9kEM server.

40.3.1.18 CARDDISCSLOT15

Title: cardDiscSlot15

Name: Discovery failure for card in Slot 15

Description: This log is generated when a cardDiscSlot15 fault is received from the MG9kEM server.

40.3.1.19 CARDDISCSLOT16

Title: cardDiscSlot16

Name: Discovery failure for card in Slot 16

Description: This log is generated when a cardDiscSlot16 fault is received from the MG9kEM server.

40.3.1.20 CARDDISCSLOT17

Title: cardDiscSlot17

Name: Discovery failure for card in Slot 17

Description: This log is generated when a cardDiscSlot17 fault is received from the MG9kEM server.

40.3.1.21 CARDDISCSLOT18

Title: cardDiscSlot18

Name: Discovery failure for card in Slot 18

Description: This log is generated when a cardDiscSlot18 fault is received from the MG9kEM server.

40.3.1.22 CARDDISCSLOT19

Title: cardDiscSlot19

Name: Discovery failure for card in Slot 19

Description: This log is generated when a cardDiscSlot19 fault is received from the MG9kEM server.

40.3.1.23 CARDDISCSLOT20

Title: cardDiscSlot20

Name: Discovery failure for card in Slot 20

Description: This log is generated when a cardDiscSlot20 fault is received from the MG9kEM server.

40.3.1.24 CARDDISCSLOT21

Title: cardDiscSlot21

Name: Discovery failure for card in Slot 21

Description: This log is generated when a cardDiscSlot21 fault is received from the MG9kEM server.

40.3.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

40.3.2.1 SHELFCOMPATIBILITY

- **STD Format:**

```
SHLF392 MAR08 04:58:42 8781 TBL  MG9K NorShelfFault
    Location: 8-CO8-Frame123.Shelf2
    Notification Id: 125
    State: not acknowledged
    Category: Equipment Alarm
    Cause: Equipment Malfunction
    Time: Jan 01 03:05:03 1970
    Component Id: Shelf.frame0.shelf2
    Specific Problem: NorShelfFault - Shelf Compatibility
    Description: testing
    Site   Flr  RPos  Bay_id
    HOST   00   A0    MG9F 123
```

- **SCC2 Format:**

```
SHLF392 8168 TBL  MG9K NorShelfFault
    Location: 8-CO8-Frame123.Shelf2
    Notification Id: 3
    State: not acknowledged
    Category: Equipment Alarm
    Cause: Equipment Malfunction
    Time: Jan 01 02:30:17 1970
    Component Id: Shelf.frame0.shelf2
    Specific Problem: NorShelfFault - Shelf Compatibility
    Description: asf
    Site   Flr  RPos  Bay_id
    HOST   00   A0    MG9F 123
```

40.3.2.2 CARDDISCOVERY

- **STD Format:**

```
SHLF393 MAR08 04:55:43 6680 TBL  MG9K NorShelfFault
    Location: 8-CO8-Frame123.Shelf2
    Notification Id: 126
    State: not acknowledged
    Category: Equipment Alarm
    Cause: Equipment Malfunction
    Time: Jan 01 02:40:06 1970
    Component Id: Shelf.frame0.shelf2
    Specific Problem: NorShelfFault - Card Discovery
    Description: testing
    Site   Flr  RPos  Bay_id
    HOST   00   A0    MG9F 123
```

- **SCC2 Format:**

```
SHLF393 6612 TBL  MG9K NorShelfFault
    Location: 8-CO8-Frame123.Shelf2
```

Notification Id: 4
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:40:06 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.3 CARDDISCPOWIO

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 127
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power IO
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 887 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 5
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:13 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power IO
Description: asdf
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.4 CARDDISCPOWSIC

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 128
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction

Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power SIC
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9279 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 6
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:31 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power SIC
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.5 CARDDISCSLOT2

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 129
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 2
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 7
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 2
Description: testing
Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

40.3.2.6 CARDDISCSLOT3

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 130
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 3
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 8
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 3
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.7 CARDDISCSLOT4

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 131
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 4
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2

Notification Id: 9
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 4
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.8 CARDDISCSLOT5

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 132
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 5
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 10
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 5
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.9 CARDDISCSLOT6

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 133
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction

Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 6
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 11
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 6
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.10 CARDDISCSLOT7

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 134
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 7
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 12
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 7
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.11 CARDDISCSLOT8

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 135
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 8
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 13
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 8
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.12 CARDDISCSLOT9

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 136
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 9
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 14

State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 9
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.13 CARDDISCSLOT10

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 137
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 10
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 15
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 10
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.14 CARDDISCSLOT11

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 138
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970

Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 11
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 16
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 11
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.15 CARDDISCSLOT12

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 139
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 12
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 17
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 12
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.16 CARDDISCSLOT13

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 140
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 13
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 18
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 13
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.17 CARDDISCSLOT14

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 141
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 14
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 19

State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 14
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.18 CARDDISCSLOT15

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 142
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 15
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 20
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 15
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.19 CARDDISCSLOT16

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 143
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970

Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 16
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 21
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 16
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.20 CARDDISCSLOT17

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 144
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 17
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 22
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 17
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.21 CARDDISCSLOT18

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 145
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 18
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 23
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 18
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.22 CARDDISCSLOT19

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 146
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 19
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 24

State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 19
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.23 CARDDISCSLOT20

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 147
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 20
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 25
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 20
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.2.24 CARDDISCSLOT21

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 148
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970

Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 21
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 26
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 21
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

40.3.3 Action

40.3.3.1 SHELFCOMPATIBILITY

To clear this, insert a compatible card in the slot. for example put a NY30AA card if the active mate card is a NY30AA

40.3.3.2 CARDDOSCOVERY

Insert a good card

40.3.3.3 CARDDISCPOWIO

Insert a good IO card

40.3.3.4 CARDDISCPOWSIC

Insert a good SIC card.

40.3.3.5 CARDDISCSLOT2

Insert a good card in the slot.

40.3.3.6 CARDDISCSLOT3

Insert a good card in the slot.

40.3.3.7 CARDDISCSLOT4

Insert a good card in the slot.

40.3.3.8 CARDDISCSLOT5

Insert a good card in the slot.

40.3.3.9 CARDDISCSLOT6
Insert a good card in the slot.

40.3.3.10 CARDDISCSLOT7
Insert a good card in the slot.

40.3.3.11 CARDDISCSLOT8
Insert a good card in the slot.

40.3.3.12 CARDDISCSLOT9
Insert a good card in the slot.

40.3.3.13 CARDDISCSLOT10
Insert a good card in the slot.

40.3.3.14 CARDDISCSLOT11
Insert a good card in the slot.

40.3.3.15 CARDDISCSLOT12
Insert a good card in the slot.

40.3.3.16 CARDDISCSLOT13
Insert a good card in the slot.

40.3.3.17 CARDDISCSLOT14
Insert a good card in the slot.

40.3.3.18 CARDDISCSLOT15
Insert a good card in the slot.

40.3.3.19 CARDDISCSLOT16
Insert a good card in the slot.

40.3.3.20 CARDDISCSLOT17
Insert a good card in the slot.

40.3.3.21 CARDDISCSLOT18
Insert a good card in the slot.

40.3.3.22 CARDDISCSLOT19
Insert a good card in the slot.

40.3.3.23 CARDDISCSLOT20
Insert a good card in the slot.

40.3.3.24 CARDDISCSLOT21
Insert a good card in the slot.

40.3.4 Associated Operational Measurements or Performance Measurements

None.

40.4 Related documentation

Configuration Management (CN)

Introduction

This chapter describes impacts to configuration management, such as hardware/software requirements, data schemas, and service orders for the features planned for this release. Only those features with configuration-management impacts are listed.

Featid	Title
A00001847.AA31	ABI Expansion Datafill
A00001890.AA31	Refer to A00001888
A00001893	MG9K Imaging
A00001898.AA29	ABI RMM Support
A00002009.AA04	Enhance Display on PSET
A00002012.AA13	XA-Core CMIC/RTIF HIOP Maintenance Software
A00002013.AA06	Intelligent Network T1 Timer Expiry Message Suppression
A00002020.AB10	ESA Translation Download
A00002146.AA09	MAPCI ABI Link Test & Legacy Comparison
A00002196.AA14	Enhanced Do Not Disturb
A00002380.AA21	MG9K ABI ESA
A00002431.AA16	LX82BA Capacity Delivery
A00002433.AA07	XA-Core Baseline Control
A00002510.AA08	LANCOMM IP over IRM
A00002538.AA19	Performance Measurements Tools

A00002555.AA03	SERVORD Manipulation of the GND Option
A00002558.AA07	LDI display for Class phone
A00002585	TMM Support For PTS Trunk, POST by Carrier
A00002607.AA11	ABI XPM SITE and MG9K Location support
A00002746.AB01	ABI XPM Fault Isolation & QueryPM
A00002760.AA11	Panther Enhancements For Hybrid Office Support
A00002858.AA26	Node ISTB for SPM Carrier Outage
A00002900.AA09	China INAP Compliance Enhancement Part 2
A00002901.AA07	Enhanced Meet-Me Conference (EMMC)
A00002960.AA12	Originator Identification Screening
A00002970.AA11	SMG4 Remote Site Provisioning
A00002979.AA07	Panther Electronic Software Delivery
A00003073.AA29	SimRing Deny Redirection (SRDR)
A00003074.AA	MG9000 Manager Capacity Increase
A00003454	Secure_and_Firewall_Compatible_CS2M_and_UE9KEM_Client_GUI_Communication
A00003459.AA18	SSC re-architecture: SYSB Line alarm/log and LGRP alarm/pm map support
A00003486.AA13	Gateway location information
A00003487.AA27	SN07 Trimodal Call Server Features
A00003489.AA09	ABI SMS Support
A00003490.AA21	Support for ABI XPM Tuple Change - XA-Core
A00003506.AA15	H.248 Per Trunk Signalling (PTS) Development
A00003531	MG9K EM – Frame location enhancements
A00003567	MG9000 Element Manager support for ABI ESA

A00003571	
A00003591	MG9000 OC3 Channelization support from EM
A00003615	SSPFS packaging/patch enhancements
A00003630.AA18	TGCP for the Cable Market
A00003667	SESM NB Alarm Interface Changes required for OSS
A00003669.AA08	Media Gateway 4000 - Internet Protocol (MG4K-IP) Prep Feature
A00003672.AA02	NTLZ20CA Core Definition
A00003687.AA06	TOPS Wireless Intelligent Network Integration
A00003767.AA29	IP ABI PPVM Robustness & Msg Loss Alarms
A00003773.AA08	Trunk Group Based Quality of Service (QOS) Operational Measurement (OM) support for MG4K-IP
A00003789.AA14	INTRA IMT CAUSE Enhancements
A00003905.AA07	DIRP Enhancements for Billing
A00003923.AA13	CTX / RES SCAI Redirection
A00003933.AA07	Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application
A00003947.AA16	Trimodal LOGs and Operational Measurements (OM)
A00003948	Tri-modal provisioning
A00003971.AA10	SPM Log Robustness
A00003995	SN07 H.323 Gateway Change Capability
A00004005.AA12	Nortel Carrier Grade Linux (NCGL) platform “Session Server”
A00004036.AA42	Off-Board Service Control
A00004045.AA06	Calling Line Identification Directory Number (CLIDN) for DMS-250
A00004046.AA10	Echo Cancellation Support for TriModal Call Server 2000

A00004126.AA13	SPM ECAN Control Enhancement
A00004131.AA16	UCS PRI B-Channel Negotiation
A00004137.AA12	ANI Billing
A00004260.AA24	XPKT301 Alarm Banner for MG4K/IW/DPT
A00004271.AA08	SIP App Server SOC
A00004391	ACD Agent Expansion from 9,999 to 30,000 Agents
A00004414.AA03	SIP Call Server SOC
A00004500.AA15	IN TCAP Messaging on IP
A00004872.AA25	Services Support for the UA-IP Solution
A00005007.AA11	Cause Indicators parameter support for DTAG AMA Enhancement
A00005016	VMG Out of Service Alarms
A00005073.AA18	SBA Outbound Connection Security
A00005074.AA07	OMDD: Outbound Connection Security
A00005160.AA10	OSSAIN XA-Core Data Messaging Capacity Enhancements
A00005190.AA09	CBM 800 OC3 Core Node and Link Maintenance
A00005193.AA04	9+1 Performance Measurements Tools Support
A00005363.AA16	CAIN FlexCDR Enhancements
A00005734.AA04	Multiple Time Zone (MTZ) support for CICM lines
A00006483.AA02	Audio Server Node Announcement Capacity Increase to 1280
A00006693	XA-Core IO Capacity Monitoring Toolset

1: Configuration (CN): A00001847

This chapter documents the changes in the Data Schema introduced by activity A00001847. Specifically there are changes to the behavior of table LTCINV that are documented.

Note: The FN/CN sections for activity A00001847 include the related information for a number of activities due to the close association of all these activities. The activities that are included in this group are:

- A00001847 - ABI Expansion Datafill
- A00001909 - ABI Trunk Support for RCC
- A00001936 - MG9K ABI Expansion - Node and Link Mtc

1.1 Hardware and Software Requirements

Not Required

1.2 Initial Configuration

Not Required

1.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Required

1.4 Upgrade Impact

Not Required

1.5 Data schema (DS) (CM, MIBS, RDB)

1.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	CHANGED	UNCHANGED (NEW)

1.5.2 Table/MIB/Remote Database Schema information

1.5.2.1 Name: LTCINV

Full Table Name: Line/Trunk Controller Inventory Table

1.5.2.1.1 Functional description

Table LTCINV lists all the line and trunk controlling peripherals that were historically directly connected to the ENET (although this is no longer the case as of SN05 with the additional of the EXTDS512 optional field). Tuples are added to this table for the following peripheral types (this is not an exhaustive list and only includes those which are relevant to this activity):

1. LGC/LGCI (although no distinction is made in the table itself)
2. LTC/LTCI (although no distinction is made in the table itself)
3. SMA2

Prior to this activity the EXTDS512 optional attribute was only allowed to be provisioned on the LGCI and SMA2 types of peripherals. After this activity the entire peripheral list shown above will be allowed to have the EXTDS512 optional attribute assigned to them.

There is no change in the format of the table or in the format of the optional field, all that has been changed is the types of peripherals that are allowed to have the field provisioned. All other types of peripherals that can be added in table LTCINV will continue to receive an error message if the EXTDS512 field is provisioned.

Note: Please refer to the documentation for SN05 activity A59038361 for more detailed information of the initial EXTDS512 design.

1.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged (SERVRINV must be datafilled prior to adding EXTDS512 peripherals in LTCINV).

1.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	Unchanged by this activity.	Unchanged by this activity.	All existing tuples, regardless of whether the EXTDS512 attribute is provisioned or not, have the physical space allocated for the information contained in this field; therefore, there is no memory impact from this activity as the memory is already allocated for all tuples in this table.

1.5.2.1.4 Fields/OIDs

The following table lists fields for LTCINV.

CSLNKTAB = “$”

OPT_ATTR = EXTDS512

When provisioning an external (non-ENET hosted) peripheral in LTCINV the EXTDS512 OPT_ATTR must be added. This optional attribute includes the IP Address of the DS512 (ABI) card in the MG9000 and Gateway Controller host name (as provisioned in table SERVRINV).

It should be noted that the CSLNKTAB portion of the tuple is not datafilled when adding external XPMs. The content of the CSLNKTAB field is automatically generated by the LTCINV code and no longer refers to real C-side links to the ENET. A “$” should be entered when prompted for the CSLNKTAB entry (this is unchanged from SN05 behavior).

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSLNKTAB	Changed	Unchanged from SN05	None	For External XPMs this field no longer contains real C-side ENET links. Instead, "$" should be entered when prompted for this field. With this activity you should now enter "$" when provisioning External LTC/LTCI/ LGC tuples in LTCINV.
OPT_ATTR (EXTDS512)	Changed	Unchanged from SN05	Unchanged from SN05	When datafilling external LTC/LTCI/ LGC peripherals you should add this field and enter the IP address of the DS512 card in the MG9000 and the name of the host GWC (from table SERVRINV).

1.5.2.1.5 Datafill example

The following example shows sample datafill for table LTCINV. The changes from standard ENET-based peripheral datafill is highlighted with **bold** characters.

```
TABLE: LTCINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LTCNAME:
>ltc 5
ADNUM:
>1001
FRTYPE:
>ltei
FRNO:
>0
SHPOS:
>32
```

```
FLOOR:
>1
ROW:
>d
FRPOS:
>32
EQPEC:
>6X02NA
LOAD:
>QLI18AH
EXECTAB:
>POTS   POTSEX
EXECTAB:
>KEYSET   KSETEX
EXECTAB:
>$
CSLNKTAB:
>$
OPTCARD:
>UTR15
OPTCARD:
>MSG6X69
OPTCARD:
>CMR13
CMRLOAD:
>CMR10A
OPTCARD:
>ISP
SLOT_NUMBER:
>16
OPTCARD:
>$
TONESET:
>northaa
PROCPEC:
>SX05AA $ SX05AA $
EXTLINKS:
>0
E2LOAD:
>SXFWAJ01
OPT_ATTR:
>EXTDS512
IPADDR:
>192   2   7  69
GWC_HOST:
>GWC 3
OPT_ATTR:
>$
PEC6X40:
>6X40FC
EXTSHELF: N
>
```

The following shows the range values for the OPTATTR field of table LTCINV. Note that this has not changed from the SN05 version.

```
TABLE: LTCINV
>ran
 1 LTCNAME           XPM_KEY
 2 ADNUM             ADMIN_NUMBER
 3 FRTYPE            FRAME_NAME
```

```
 4 FRNO              FRAME_NO
 5 SHPOS             SHELF_POS
 6 FLOOR             FLOOR_POS
 7 ROW               ROW_POS
 8 FRPOS             FRAME_POS
 9 EQPEC             PEC
10 LOAD              NPMLOAD_INFO
11 EXECTAB           TERM_EXEC_TC_TAB
12 CSLNKTAB          XPM_NET_CSLINK_TC_TAB
13 OPTCARD           EXT_OPT_CARD_TC_TAB
14 TONESET           TONE_SET_TYPE
15 PROCPEC           XPM_PEC_AREA_TAB
16 EXTLINKS          NUM_EXT_LNKS_RANGE
17 E2LOAD            NPMLOAD_INFO
18 OPTATTR           LTCINV_OPT_ATTR_VECTOR
19 PEC6X40           NT_6X40_PEC
20 EXTINFO           EXTENSION_INFO
LOGICAL TUPLE TYPE: LTC_LOGTUPLE
>ran 18
18 OPTATTR           LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
        OPT_ATTR               LTCINV_OPT_ATTR REFINEMENTS:
        {EXTDS512}             MULTIPLE WITH
             IPADDR            TABLE OF 4 {0 TO 255}'S
             GWC_HOST          MULTIPLE WITH
                  PMTYPE       PM_TYPE
                  PMNO         {0 TO 255}
        OTHERWISE              LTCINV_OPT_ATTR_NIL_DATA
>
```

1.5.2.1.6 Table release history update

The following changes were made:

1. EXTDS512 OPT_ATTR is now allowed for LTC/LTCI/LGC peripheral types.
2. "$" should be entered in the CSLNKTAB field for external XPMs (the C-side link information will be generated automatically).

1.5.2.1.7 Supplementary information

Limitations:

- The CSLNKTAB and EXTDS512 optional attribute must align in each tuple in LTCINV. This means that if EXTDS512 exists then a "$" must have been entered in the CSLNKTAB field. A tuple must be either ENET based on External but not a combination of both.
- Multiple tuples of each type (ENET and External) can exist in the table at the same time.
- The EXTDS512 optional attribute can be provisioned only against LTC, LGC, LTCI, LGCI, and SMA2 peripheral types. Attempting to add the optional attribute to other peripheral types will result in the tuple failing verification and an error will be displayed.

- The derived CSLNKTAB entries for External XPMs cannot be changed by the user.
- The ability to change the Host Gateway Controller for External XPMs is not allowed.
- The EXTDS512 optional attribute cannot be added to an existing tuple using the change command in table control, nor can it be removed using change.

1.5.2.1.8 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

1.6 Service Orders (SO) (CM & SESM)

Not Required

1.7 Software optionality control (SOC)

Not Required

1.8 Element Management

Not Required

1.9 Command interface changes

1.9.1 Directory: MAPCI;MTC;PM

1.9.1.1 Directory description

No new commands or paramenters have been introduced, however due to the ABI supported host XPMs in this feature, certain maintenance functions and states will be supported for the ABI host XPMs. When an ABI peripheral (LTC, LTCI, LGC, LGCI, or SMA2) subtending a GWC is posted the display looks just like it did for the same peripheral posted as a direct HOST peripheral (legacy).

1.9.1.2 Accessing directory: PM

1.9.1.2.1 Access to directory or MAP level and return to CI

The updated displays are accessed through the PM (peripherals) level of the maintenance (MTC) level of the DMS core command interface (MAPCI).

1.9.2 Command: TRNSL C

1.9.2.1 Command type: Listed MENU

1.9.2.2 Command target: All

But will only appear for Succession ABI peripherals.

1.9.2.3 Command availability: RES

1.9.2.4 Command description

TRNSL C (translate c-side links) is not a new command, however when an LTC, LTCI, LGC, LGCI, or SMA2 subtends a GWC (gateway controller), the TRNSL C will display the c-side links of the peripheral as connecting to a GWC.

Each c-side link will simply reflect the name of the gateway controller to which it subtends. Link 0, 1, 4 and 5 (the message links) reflect the actual status of the c-side links. Currently, the speech links have the following string hardcoded as their status “**;Cap S;Status:OK”.

It is important to note that TRNSL C indicates only which GWC supertends the ABI peripheral, it does not display the MG9K or ABI card that is in use for the messaging path.

1.9.2.5 Command syntax

Table 4 TRNSL C command parameters and variables

Command	Parameters and variables
TRNSL C	unchanged
Parameters and variables	unchanged

1.9.2.6 Qualifications and warnings

The TRNSL C command will provide the user with the following additional information when a GWC is involved:

“Please refer to the DS512 Interface EM for all link maintenance commands.”

It should be noted that maintenance actions on the c-side links (e.g. bsy link 0, rts link 1, etc.) can only be performed on the c-side message links for ABI peripherals.

1.9.2.7 Example

Usage example for **“MAPCI;MTC;PM; POST <XPM>;TRNSL C “ command**

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 AMDI    RExFlt  NODLOG    .      3 SPM     .       .     53CC.   1 Min   SDM
   M                              *C*                     *C*
 LGC                            SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit         PM               1       0       5       5      14      16
  2 Post_        LGC              0       0       0       2       0       1
  3 ListSet
  4              LGC    13 InSv  Links_OOS: CSide  0 , PSide  0
  5 Trnsl_     Unit0:    Inact InSv
  6 Tst_       Unit1:    Act   InSv
  7 Bsy_        Trnsl   c
  8 RTS_        Link  0: GWC 0              8;Cap MS;Status:OK
;MsgCond:OPN,
  9 OffL        Restrict
 10 LoadPM_     Link  1: GWC 0              9;Cap MS;Status:OK
;MsgCond:OPN,
 11 Disp_       Restrict
 12 Next        Link  2: GWC 0             **;Cap  S;Status:OK
 13 SwAct       Link  3: GWC 0             **;Cap  S;Status:OK
 14 QueryPM     Link  4: GWC 0             10;Cap MS;Status:OK
;MsgCond:OPN,
 15 DCH         Unrestrict
 16             Link  5: GWC 0             11;Cap MS;Status:OK
;MsgCond:OPN,
 17 PERFORM     Unrestrict
 18 ISG         Link  6: GWC 0             **;Cap  S;Status:OK
```

Message link status is reflected accurately

Speech link state is hardcoded.

Shows which GWC is used to control packet c-side connections for this ABI peripheral.

PM can be SMA2, LTC, LTCI, LGC, or LGCI

1.10 Security

Not Required

1.11 Configuration Walkthrough

Not Required

2: Configuration (CN): A00001890

2.1 Hardware and Software Requirements

The following activities provide support for MG9000 line testing through the CS2000 in the SN06.2 release:

- A00001890
- A00001888

The following sections describe the hardware and software required to support the functionality delivered under the above listed activities.

2.1.1 Hardware Requirements

2.1.1.1 CS2000 Hardware

The following hardware is required to provide the CS2000 line test support:

2.1.1.1.1 Trunk Modules

The CS2000 supports an array of test heads and supporting hardware. These circuit packs are contained in trunk modules. Examples of the supported trunk modules are the TM8, ISM, MTM and RMM.

2.1.1.1.2 Test Circuits

The following CS2000 test heads and supporting hardware are required to support MG9000 line testing:

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)
- NT2X10/NT2X11 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)

The CS2000 also requires the following supporting equipment for MLT test trunks:

- NT2X57 SD Card

Additional details on the circuit packs listed above are provided in TAM-1001-018 DMS-100 Family Quick Reference Guide. This is available through Helmsman.

The information on the quantities required for each circuit pack is provided in the EI section of this activity.

2.1.1.1.3 MTA Matrix

The CS2000 supports two types of test heads: transmission test heads and metallic test heads. The transmission test heads connect to the line under test through the bear network. The metallic test heads connect to the line under test through a metallic test access matrix.

The metallic test access matrix is a matrix with the metallic test heads connected to the horizontal leads on the matrix and the line concentrating devices connected to the vertical leads on the matrix. This matrix allows any test head to be cross connected to any line, thus allowing the test heads to be shared across all line access devices.

The CS2000 supports the following cards for implementing the MTA matrix:

- NT3X09BA 8x8 Matrix Card

The trunk modules also contain the MTA matrix cards.

2.1.1.1.4 Horizontal Connectivity

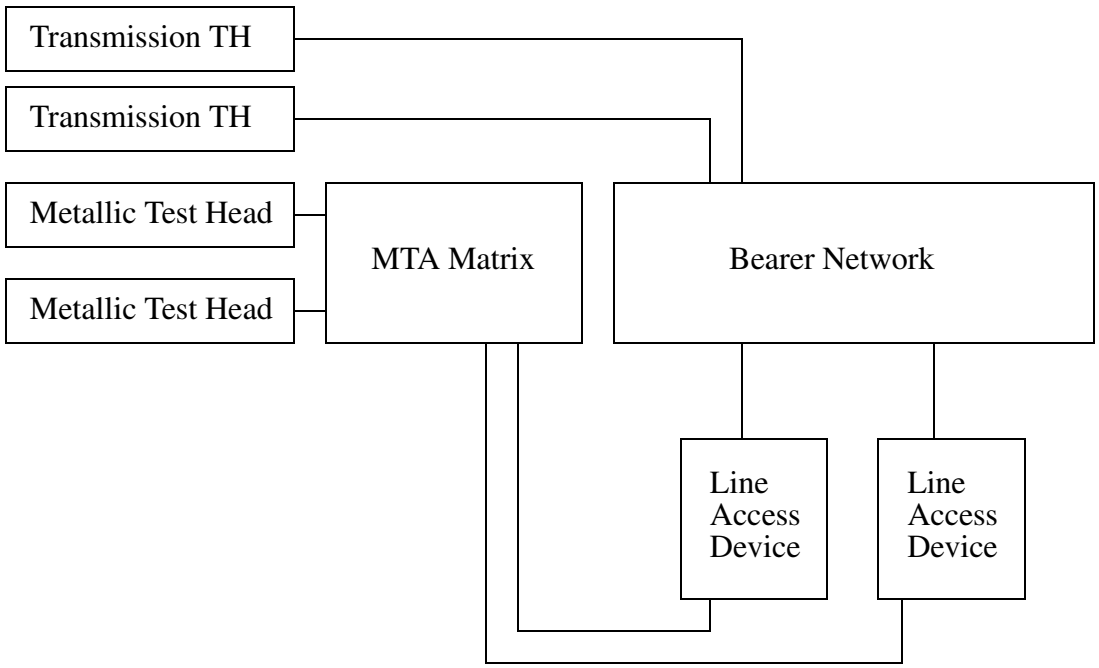
As noted above, the metallic test heads must be wired to the horizontal leads on the MTA matrix.

2.1.1.1.5 Vertical Connectivity

As notes above, the test access ports on the line concentrating devices must be wired to the vertical leads on the MTA matrix.

2.1.1.1.6 Test Configuration Diagram

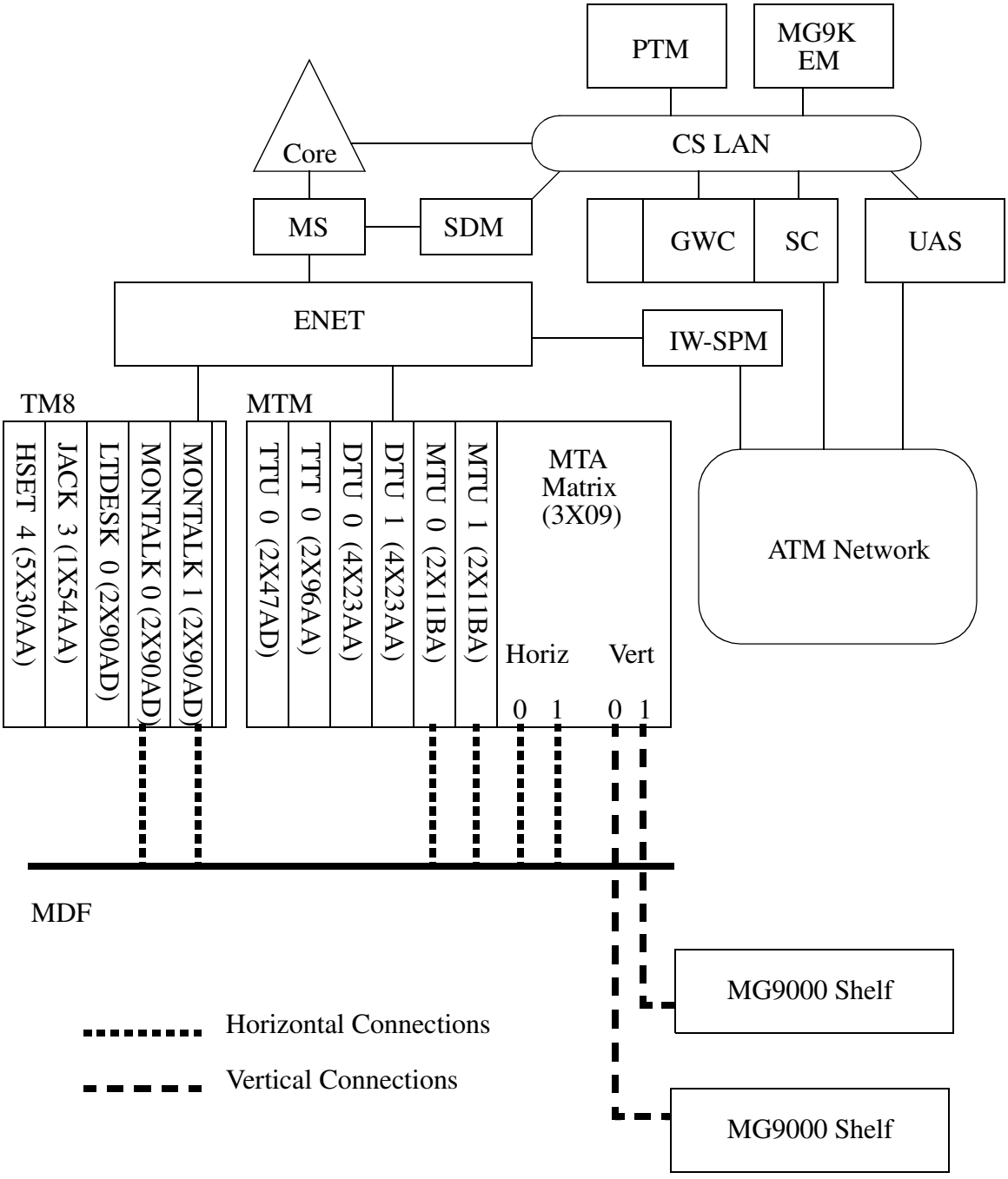
The following diagrams illustrate the hardware configuration required to support CS2000 based line testing for MG9000 lines.



The above diagram is a logical view of the test equipment.

- The transmission test heads have access to the bearer network. These test heads are connected to the line access devices through the bearer network.
- The metallic test heads are connected to the horizontal leads on the MTA matrix. The line access devices are connected to the vertical leads on the MTA matrix. In this configuration, any metallic test head can be cross connected to any line on any line access device.

The following figure gives are more detailed view of the physical implementation.


PTM
MG9K EM
Core
CS LAN
MS
SDM
GWC
SC
UAS
ENET
IW-SPM
TM8
MTM
HSET 4 (5X30AA)
JACK 3 (1X54AA)
LTDESK 0 (2X90AD)
MONTALK 0 (2X90AD)
MONTALK 1 (2X90AD)
TTU 0 (2X47AD)
TTT 0 (2X96AA)
DTU 0 (4X23AA)
DTU 1 (4X23AA)
MTU 0 (2X11BA)
MTU 1 (2X11BA)
MTA Matrix (3X09)
Horiz
Vert
0 1 0 1
ATM Network
MDF
MG9000 Shelf
MG9000 Shelf
Horizontal Connections
Vertical Connections

2.1.1.1.7 References

NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides a more complete description of the test equipment and the provisioning of the test equipment.

NTP 297-8991-805 DMS-100 Family Hardware Description Manual provides additional details on the hardware described above.

NTP 50041.08 DMS-100/200 Hardware Planning Guide

2.1.1.2 MG9000 Hardware

The MG9000 requires the following hardware to support the SN06.2 line test content provided by activities A00001888 and A00001890:

- MTA-TRC pack per node per frame
- SIC card per shelf.

2.1.1.3 3rd Party Gateways

The CS2000 line test functionality will support any 3rd party gateway that supports the H.248 extension added by activities A00001890 and A00001888. However, this document does not provide specific information on the hardware requirements for 3rd party gateways.

2.1.2 Software Requirements

There are 5 types of equipment/connectivity datafilled required to support the CS2000 line test functionality provided by activities: A00001888 and A00001890.

- First the trunk modules that will contain the CS2000 test equipment are provisioned.
- Second, the CS2000 test heads and supporting hardware are provisioned.
- Third, the MTA (Metallic Test Access) matrix for the CS2000 is provisioned.
- Fouth, the metallic test head connectivity to the horizontals on the MTA matrix are provisioned.
- Fifth, the line concentrating device connectivity to the verticals on the MTA matrix are provisioned.

Note that additional datafill is required for individual line test applications. For example, the subscriber premise tests are supported for MG9000 lines in the SN06.2 release (DSCKT, SSMAN, Station Ringer). The subscriber premise tests require translations in the CS2000 to function correctly.

This document does not provide details on the provisoining and translations required for the individual line test applications. The provisioning and translations for individual line test applications are already documented in NTP 297-1001-594 DMS-100 Family Line Maintenance Guide, and the existing provisioning and translations methods apply to LGRP lines on the CS2000.

2.1.2.1 Trunk Module Provisioning

The trunk modules are provisioned in table TMINV and RMMINV. The CS2000 uses the same trunk module provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provide details on trunk module provisioning for the CS2000.

2.1.2.2 Test Head and Supporting Hardware Provisioning

The test heads and supporting hardware are provisioned in tables TRKGRP and TRKMEM. The CS2000 uses the same test head provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on test head provisoning for the CS2000.

2.1.2.3 MTA Matrix Provisioning

The MTA matrix is provisioned in table MTAMDRVE. The CS2000 uses the same MTA matrix provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on MTA matrix provisioning for the CS2000.

2.1.2.4 Horizontal Connectivity Provisioning

The horizontal connectivity is provisioned in table MTAHORIZ. The CS2000 uses the same horizontal connectivity provisioning as the DMS-100. NTP 297-1001-594 DMS-100 Family Line Maintenance Guide provides details on the horizontal connectivity provisioning for the CS2000.

2.1.2.5 Vertical Connectivity Provisioning

Vertical connectivity provisioning for LGRPs differs from the vertical connectivity provisoning for existing DMS-100 peripherals. Additional details on LGRP vertical connectivity are provided below.

Table LGRPINV and MTAVERT are used to provision the metallic connections from MG9000 shelves to verticals on the MTA matrix. The following figure shows examples of provisioning these tables for MG9000 to MTA matrix connectivity.

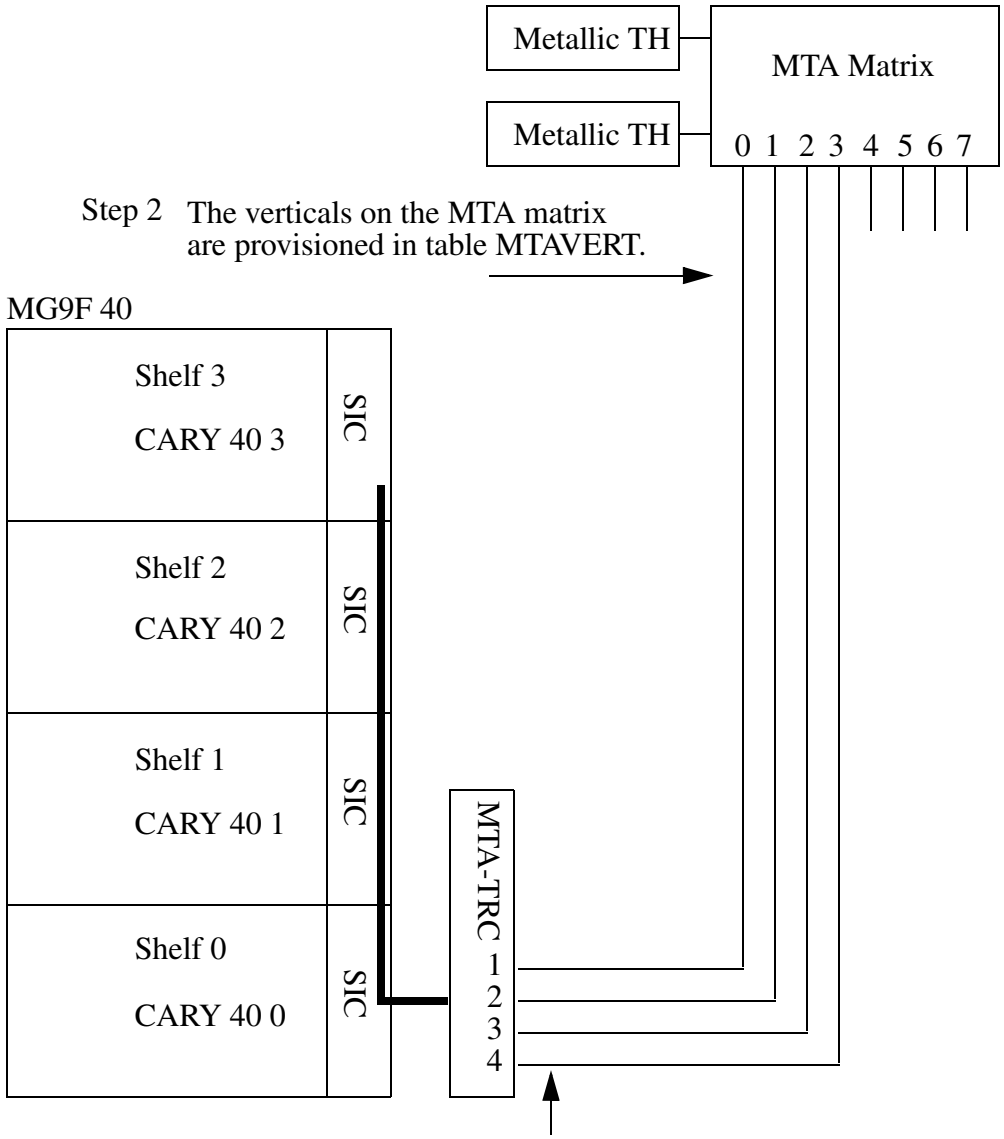


Table LGRPINV

```
CARY 40 0  GWC 0  S  MTSTAPT  CARY  (0  1) $
CARY 40 1  GWC 0  S  MTSTAPT  CARY  (1  2) $
CARY 40 2  GWC 0  S  MTSTAPT  CARY  (2  3) $
CARY 40 3  GWC 0  S  MTSTAPT  CARY  (3  4) $
```

Table MTAVERT

```
0  G  (O  CARY  40  0) $
1  G  (O  CARY  40  1) $
2  G  (O  CARY  40  2) $
3  G  (O  CARY  40  3) $
```

Vertical
Metallic Test Access Point

Provisioning Rules for MG9000 Verticals

1. The metallic test access connections for the MG9000s are provisioned in table LGRPINV first, and then in table MTAVERT.
2. Table LGRPINV allows up to 8 metallic test access points (with verticals) to be provisioned per LGRP. This is for future flexibility to increase the number of simultaneous tests per MG9000. **At this time, the user should only provision a single metallic test access point per LGRP in table LGRPINV (each LGRP being a single MG9000 shelf**).
3. LGRPs are assigned to verticals in table MTAVERT. Before an LGRP is assigned to a vertical in table MTAVERT, the tuple for the LGRP in table LGRPINV must have a metallic test access point associated to the vertical.

As noted in the rules, only a one metallic test access point and vertical should be assigned to an LGRP in the SN06.2 release. A single physical MG9000 can support up to 16 shelves; however, a single physical MG9000 can only support 8 metallic test access points. When an MG9000 grows beyond 8 shelves, verticals must be shared across multiple shelves. The provisioning recommendations for SN06.2 are as follows:

a. For MG9000 nodes that have 8 or less shelves, each shelf on the MG9000 should be assigned to a unique metallic test access point and vertical.

b. As an MG9000 grows beyond 8 shelves, the metallic test access points and verticals used on shelves 0-7 should be reused on shelves 8-15 in sequential fashion.

c. If wideband testing is required on the MG9000 to support DSL lines, then one (or more) of the metallic test access points should be reserved for the wideband test head.

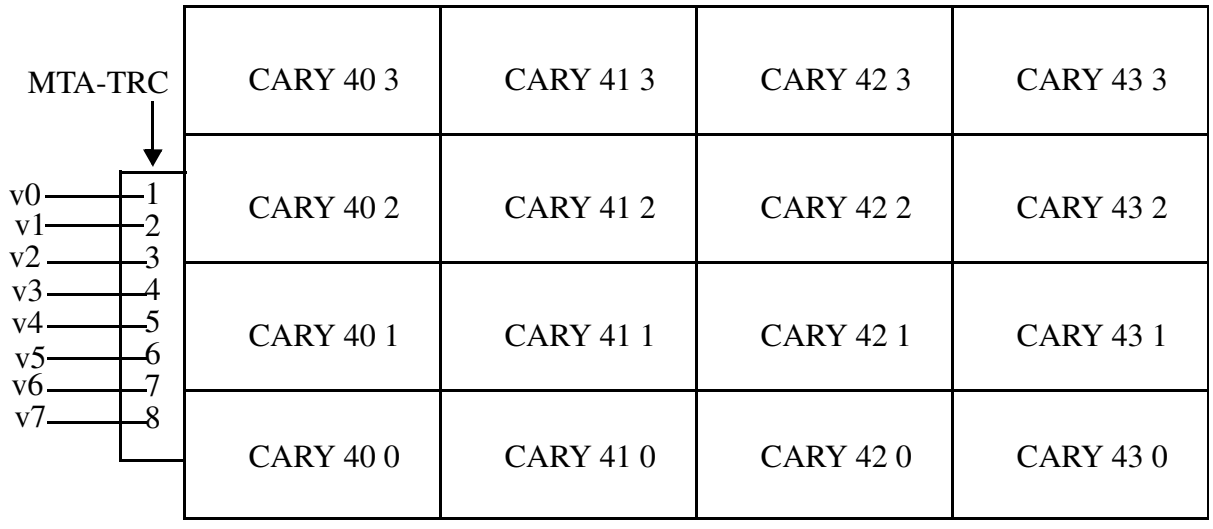
Example 1 : All 8 metallic test access points assigned to verticals.

The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node is in the CARY site and it occupies frame 40 41 42 and 42. This examples hows all 8 metallic test access points wired to verticals on the MTA matrix.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
------------------------------------------------------------------------
CARY 40 0  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2  GWC 0  S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3  GWC 0  S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0  GWC 0  S (MTSTAPT CARY (4 5) $ ) $
```

```
CARY 41 1  GWC 0  S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2  GWC 0  S (MTSTAPT CARY (6 7) $ ) $
CARY 41 3  GWC 0  S (MTSTAPT CARY (7 8) $ ) $
CARY 42 0  GWC 1  S (MTSTAPT CARY (0 1) $ ) $
CARY 42 1  GWC 1  S (MTSTAPT CARY (1 2) $ ) $
CARY 42 2  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 42 3  GWC 1  S (MTSTAPT CARY (3 4) $ ) $

CARY 43 0  GWC 1  S (MTSTAPT CARY (4 5) $ ) $
CARY 43 1  GWC 1  S (MTSTAPT CARY (5 6) $ ) $
CARY 43 2  GWC 1  S (MTSTAPT CARY (6 7) $ ) $
CARY 43 3  GWC 1  S (MTSTAPT CARY (7 8) $ ) $

TABLE: MTAVERT

VERT VERTCONN
------------------------
0  G  ( O CARY 40 0 ) (O CARY 42 0) $
1  G  ( O CARY 40 1 ) (O CARY 42 1) $
2  G  ( O CARY 40 2 ) (O CARY 42 2) $
3  G  ( O CARY 40 3 ) (O CARY 42 3) $
4  G  ( O CARY 41 0 ) (O CARY 43 0) $
5  G  ( O CARY 41 1 ) (O CARY 43 1) $
6  G  ( O CARY 41 2 ) (O CARY 43 2) $
7  G  ( O CARY 41 3 ) (O CARY 43 3) $
```



In this configuration, a single vertical will be shared across as many as 1024 lines.

Example 2 : Two metallic test access points reserved for widband testing

The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node is in the CARY site and it occupies frame 40 41 42 and 42. This example shows only 6 metallic test access points wired to verticals on the MTA matrix.

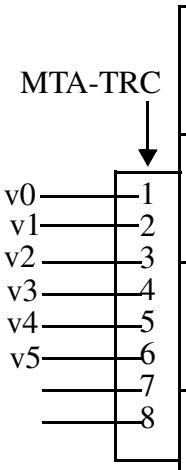
TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
------------------------------------------------------------------------
CARY 40 0  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2  GWC 0  S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3  GWC 0  S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0  GWC 0  S (MTSTAPT CARY (4 5) $ ) $
CARY 41 1  GWC 0  S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2  GWC 0  S (MTSTAPT CARY (0 1) $ ) $
CARY 41 3  GWC 0  S (MTSTAPT CARY (1 2) $ ) $
CARY 42 0  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 42 1  GWC 1  S (MTSTAPT CARY (3 4) $ ) $
CARY 42 2  GWC 1  S (MTSTAPT CARY (4 5) $ ) $
CARY 42 3  GWC 1  S (MTSTAPT CARY (5 6) $ ) $
CARY 43 0  GWC 1  S (MTSTAPT CARY (0 1) $ ) $
CARY 43 1  GWC 1  S (MTSTAPT CARY (1 2) $ ) $
CARY 43 2  GWC 1  S (MTSTAPT CARY (2 3) $ ) $
CARY 43 3  GWC 1  S (MTSTAPT CARY (3 4) $ ) $
```

TABLE: MTAVERT

```
VERT VERTCONN
-----------------------
0  G  ( O CARY 40 0 ) (O CARY 41 2) (O CARY 43 0)$
1  G  ( O CARY 40 1 ) (O CARY 41 3) (O CARY 43 1)$
2  G  ( O CARY 40 2 ) (O CARY 42 0) (O CARY 43 2)$
3  G  ( O CARY 40 3 ) (O CARY 42 1) (O CARY 43 3)$
4  G  ( O CARY 41 0 ) (O CARY 42 2) $
5  G  ( O CARY 41 1 ) (O CARY 42 3) $
```

In this example, a single vertical can be shared by up to 1536 lines.



CARY 40 3	CARY 41 3	CARY 42 3	CARY 43 3
CARY 40 2	CARY 41 2	CARY 42 2	CARY 43 2
CARY 40 1	CARY 41 1	CARY 42 1	CARY 43 1
CARY 40 0	CARY 41 0	CARY 42 0	CARY 43 0

2.1.2.6 Provisioning Example

2.1.2.6.1 Trunk Module Provisioning

First, the trunk modules must be provisioned. This includes shelves such as the TM8, MTMs and RMMs. In the example given, RMMs are not shown. However, RMMs can be used in the remote sites for MG9000 line testing. The sample datafill given shows a single MTM and TM8 shelf for this CS2000.

Note: all tables are shown in packeted format.

TABLE: TMINV

TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS LKDATA EQPEC LOAD EXECS SCTMLOC

TM8 0 TME 0 18 1 D 28 0 32 0 0 2X52AG BTMKA02 TM8EX SHELF
MTM 0 TME 0 52 1 D 28 0 32 5 0 2X58CB MTMKA02 MTMEX SHELF

2.1.2.6.2 Test Head and Supporting Hardware Provisioning

The test heads and supporting hardware are provisioned next. These circuits are provsioned thru tables TRKGRP and TRKMEM. The following test heads and inteface circuits are required to support MG9000 line testing:

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)
- NT2X10/NT2X11 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)

TABLE: TRKGRP

GRPKEY GRPTYP TRAFSNO PADGRP NCCLS GRPINFO

TTU MAINT 0 NPDGP NCIT 2X47AD
TTT MAINT 0 NPDGP NCIT 2X96AA
DTU MAINT 0 NPDGP NCRT 4X23AA
MTU MAINT 0 NPDGP NCRT 2X11BA
MONTALK MAINT 0 NPDGP NCRT 2X90AD
HSET MAINT 0 NPDGP NCRT 5X30AA
JACK MAINT 0 NPDGP NCRT 1X54AA
LTDESK TD 0 NPDGP NCOT NIL MIDL IC NPRT NSCR 613 613 LCL N N BASIC N

TABLE: TRKMEM

CLLI EXTRKNM SGRP MEMVAR

TTU 0 0 MTM 0 21
TTT 0 0 MTM 0 16
DTU 0 0 MTM 0 18
DTU 1 0 MTM 0 19
MTU 0 0 MTM 0 10
MTU 1 0 MTM 0 11
MONTALK 0 0 TM8 0 8
MONTALK 1 0 TM8 0 10
HSET 4 0 TM8 0 2
JACK 3 0 TM8 0 18
LTDESK 0 0 TM8 0 6

2.1.2.6.3 MTA Matrix Provisioning

After the test heads and supporting circuits are provisioned, the MTA (Metallic Test Access) matrix is provisioned for the CS2000. The MTA matrix is provisioned through table MTAMDRVE. This examples shows an MTA matrix with a single MTA matrix card. The CS2000 supports an MTA matrix

that is significantly larger. The MTA matrix for a CS2000 is created by linking together multiple MTA cards in both the vertical and horizontal directions.

TABLE: MTAMDRVE

```
MTAMEM VERT HORIZ TMTYPE TMNO TMCKTNO MTACARD
-------------------------------------------
0 0 0 MTM 0 6 3X09BA
```

2.1.2.6.4 Horizontal Connectivity Provisioning

After provisioning the MTA matrix for the office, the test heads are assigned to horizontals on the MTA matrix. The example shows a pair ofMTU (Metallic Test Units) connected to the first two horizontals on theMTA matrix along with a single analog test trunk for supporting external test systems such as: Access Care, 4TEL and Loop Care.

TABLE: MTAHORIZ

```
HORIZ HORIZGRP HORIZAGT MTAGRP
-----------------------------
0 0 L MTU 0 Y (0 0) $
1 0 L MTU 1 N (0 1) $
3 0 T LTDESK 0 (0 3) $
```

2.1.2.6.5 Vertical Connectivity Provisioning

After provisioning the test head connectivity to the horizontals on the MTA matrix, the line concentrating devices are assigned to verticals on the MTA matrix. For LGRPs, verticals are assigned to specific MG9000 metallic test access points and shelves through tables LGRPINV and MTAVERT.

The following example shows two separate LGRPs. For CARY 77 1, the entry in LGRPINV associates vertical 0 with metallic test access point 1 on the gateway. For CARY 40 2, the entry in LGRPINV associates vertical 1 with metallic test access point 1 on the gateway.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
-------------------------------------------------------------------------
CARY  77 1  GWC   5   S (MTSTAPT CARY ( 0 1) $)$
CARY  40 2  GWC   5   S (MTSTAPT CARY ( 1 1) $)$
```

TABLE: MTAVERT

VERT VERTCONN
---
0 G (O CARY 77 1) $
1 G (O CARY 40 2) $

2.2 Initial Configuration

N/A

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

2.4 Upgrade Impact

N/A

2.5 Data schema (DS) (CM, MIBS, RDB)

Existing tables are used.

2.6 Service Orders (SO) (CM & SESM)

N/A

2.7 Software optionality control (SOC)

N/A

2.8 Element Management

N/A

2.9 Command interface changes

2.9.1 Directory: LTP

2.9.1.1 Directory description

This level contains the line test position menu commands.

2.9.1.2 Accessing directory: LTP

2.9.1.2.1 Access to directory or MAP level and return to CI

MAPCI;MTC;LNS;LTP

2.9.2 Command: LTP Commands

2.9.2.1 Command type: Listed MENU

2.9.2.2 Command target: BRISC, POWERPC

2.9.2.3 Command availability: RES

2.9.2.4 Command description

No changes in functionality.

2.9.2.5 Command syntax

No changes in syntax.

Table 1 <CommandName> command parameters and variables

Command	Parameters and variables

2.9.2.6 Qualifications and warnings

N/A

2.9.2.7 Responses

2.9.2.7.1 New CM LGRP messages to support MAP-Based Line Test for MG9000

Other messages than the ones listed below are output but they are not unique to Succession. The ones listed below are unique to Succession.

Table 2 MAP outputs with associated meanings and actions

Responses
For unsupported commands: “This command is not valid for Call Server LGRP lines.” **Meaning:** Self-explanatory **System or user actions:** None
For all commands: “This command is not valid for non-MG9000 lines.” **Meaning:** Self-explanatory **System or user actions:** None

Table 2 MAP outputs with associated meanings and actions

Responses
For VDC, VAC: “Failed to determine the split capabilities for this Call Server LGRP line.” **Meaning:** Could not get the test session for this LGRP. **System or user actions:** Check logs.
For VDC, VAC,LTA: “LTA IN requires split-in metallic access which is not supported for this Call Server LGRP line.” **Meaning:** Split capability is not right. **System or user actions:** None
For RES: “LTA IN command is not valid for RES on Call Server LGRP lines.” **Meaning:** Self-explanatory **System or user actions:** None
For CAP: “LTA IN command is not valid for CAP on Call Server LGRP lines.” **Meaning:** Self-explanatory **System or user actions:** None
For LNTST: “LTA IN command is not valid for LNTST on Call Server LGRP lines.” **Meaning:** Self-explanatory **System or user actions:** None
For metallic tests: “Unable to determine metallic test equipment provisioned” “Verify the MTSTAPT option exists for the entry in table LGRPINV” **Meaning:** Could not retrieve MTSTAPT from LGRPINV provisioned data **System or user actions:** Check table LGRPINV, option MTSTAPT.
For metallic tests: “Unable to get the test point index from LGRPINV” “Test cannot be performed” **Meaning:** Could not find available vertical type test point. **System or user actions:** Check table LGRPINV.

Table 2 MAP outputs with associated meanings and actions

Responses
For metallic tests: “Vertical is not datafilled in MTAVERT” “Test cannot be performed” **Meaning:** Self-explanatory. **System or user actions:** Check table MTAVERT.
For metallic tests: “TAN vertical is not assigned” “Test canot be performed” **Meaning:** Self-explanatory. **System or user actions:** Check table MTAVERT.
For MONLTA or TALKLTA: “Cannot get line state” **Meaning:** Self-explanatory. **System or user actions:**
For LTA: “Talk connected” “LTA operations not valid on Call Server LGRP lines” **Meaning:** Do not allow the LTA IN or LTA OUT commands for LGRP lines if either monlta or talklta is in progress. LGRP line maintenance performs a true split-in when the LTA IN command is performed and a split-out when the LTA OUT command is performed. The monlta and talklta commands use bridge mode by design. For LGRP lines, once the bridge is lost by a LTA IN or LTA OUT, it can not be re-established using the LTA command. **System or user actions:** Wait until TALKLTA is complete.
For LTA: “Monitor connected: “LTA operations not valid on Call Server LGRP lines” **Meaning:** Do not allow the LTA IN or LTA OUT commands for LGRP lines if either monlta or talklta is in progress. LGRP line maintenance performs a true split-in when the LTA IN command is performed and a split-out when the LTA OUT command is performed. The monlta and talklta commands use bridge mode by design. For LGRP lines, once the bridge is lost by a LTA IN or LTA OUT, it can not be re-established using the LTA command. **System or user actions:** Wait until MONLTA is complete.

Table 2 MAP outputs with associated meanings and actions

Responses
For LTA: “Failed to determine the split capabilities of the LGRP.” “Test not performed.” **Meaning:** Could not get the test session for this LGRP. **System or user actions:** Check logs.
For TSTRING: “To test the ringing function for Call Server LGRP lines, please run the DIAG command.” **Meaning:** self-explanaory **System or user actions:** Execute the DIAG command.
For DIAG, “This Call Server LGRP line has no serving metallic test equipment.” “”*** WARNING *** This command will cause the EBS set to lose” “ power and its previous volume setting” **Meaning:** self-explanaory **System or user actions:** None.
“Failed to determine the termination state” **Meaning:** Could not determine the state of the line to be tested. So, line test cannot be performed on this line. **System or user actions:** Check the termination status at the gateway.
“Failed to put the termination in the test state” and/or “Check the termination status at the gateway” **Meaning:** Could not put the state of the line to be tested in the termination state. So, line test cannot be performed on this line. **System or user actions:** Check the termination status at the gateway.
The line is an ESA call” **Meaning:** self-explanaory **System or user actions:** None.

Table 2 MAP outputs with associated meanings and actions

Responses
The line is out of service at the gateway” **Meaning:** The gateway has explicitly stated that this line is Out of Service. So, line test cannot be performed on this line. **System or user actions:** Check the Circuit State at the MG9000 Element Manager.
RTPU07AX ***+LINE100 AUG25 12:39:40 5000 PASS LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Card Diagnostic OK ACTION REQUIRED None CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Test session not available ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Call server software error ACTION REQUIRED Check logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Call server processing failure ACTION REQUIRED Check logs CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Invalid data ACTION REQUIRED Check logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Base messaging failure ACTION REQUIRED Check logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Gateway processing failure ACTION REQUIRED Chk GW logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT No card present in slot ACTION REQUIRED Insert card CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT Linecard is in an invalid state ACTION REQUIRED Chk ln state CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:36:05 0800 FAIL LN_DIAG SLOA 78 1 20 00 DN 2145207800 DIAGNOSTIC RESULT TRC not operated ACTION REQUIRED Check TRC CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT TRC not connected ACTION REQUIRED Check TRC CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Gateway resources not available ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Connection Fault ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Action not supported by gateway ACTION REQUIRED CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Unexpected gateway reply ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Gateway reply timeout ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT MTA connection failure at gateway ACTION REQUIRED Try again CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Test failed: Single-end ACTION REQUIRED Replace card CARD TYPE RDTLSG Note: Instead of ‘Single-end’, could be the following: ’Off-hook ’, ’On-hook ’, ’Single-party ringing’, ’Tip ringing, ANI gnd’, ’Pos coin off-hook ’, ’Neg coin off-hook ’, ’Coin collect ’, ’Coin return ’, ’Pos coin presence ’, ’Neg coin presence ’, ’Reverse battery ’, ’Positive Ring Party ’, ’Positive Tip Party ’, ’Idle channel noise ’, ’Echo return loss ’, ’Carrier channel loss’

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT GWC processing error ACTION REQUIRED Chk GWC logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Node data missing in GWC ACTION REQUIRED Chk GWC data CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Gateway is out of service in GWC ACTION REQUIRED Chk GW state CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Line data missing in GWC ACTION REQUIRED Chk GWC data CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Line out of service in GWC ACTION REQUIRED Chk ln state CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT No response from gateway ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Gateway processing error ACTION REQUIRED Chk GW logs CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Line data missing in gateway ACTION REQUIRED Chk GW data CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Line data mismatch in gateway ACTION REQUIRED Chk GW data CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Test resources unavailable at gateway ACTION REQUIRED Chk Gateway CARD TYPE RDTLSG

Table 2 MAP outputs with associated meanings and actions

Responses
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Test resources busy at gateway ACTION REQUIRED Try again CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Linecard hardware mismatch ACTION REQUIRED Replace Card CARD TYPE RDTLSG
RTPU07AX ***+LINE101 AUG25 12:48:23 5700 FAIL LN_DIAG SLOA 43 1 08 00 DN 2145208300 DIAGNOSTIC RESULT Connection Fault ACTION REQUIRED Try again CARD TYPE TTU
RTPU07BA ***+LINE101 SEP15 13:02:20 1300 FAIL LN_DIAG SLOA 77 1 20 03 DN 2145207703 KEY 1 DIAGNOSTIC RESULT No Signalling to Set 0/10 ACTION REQUIRED Chk Card&Set CARD TYPE RDTEBS

2.9.2.8 Example

Table 3 Usage examples for <CommandName> command

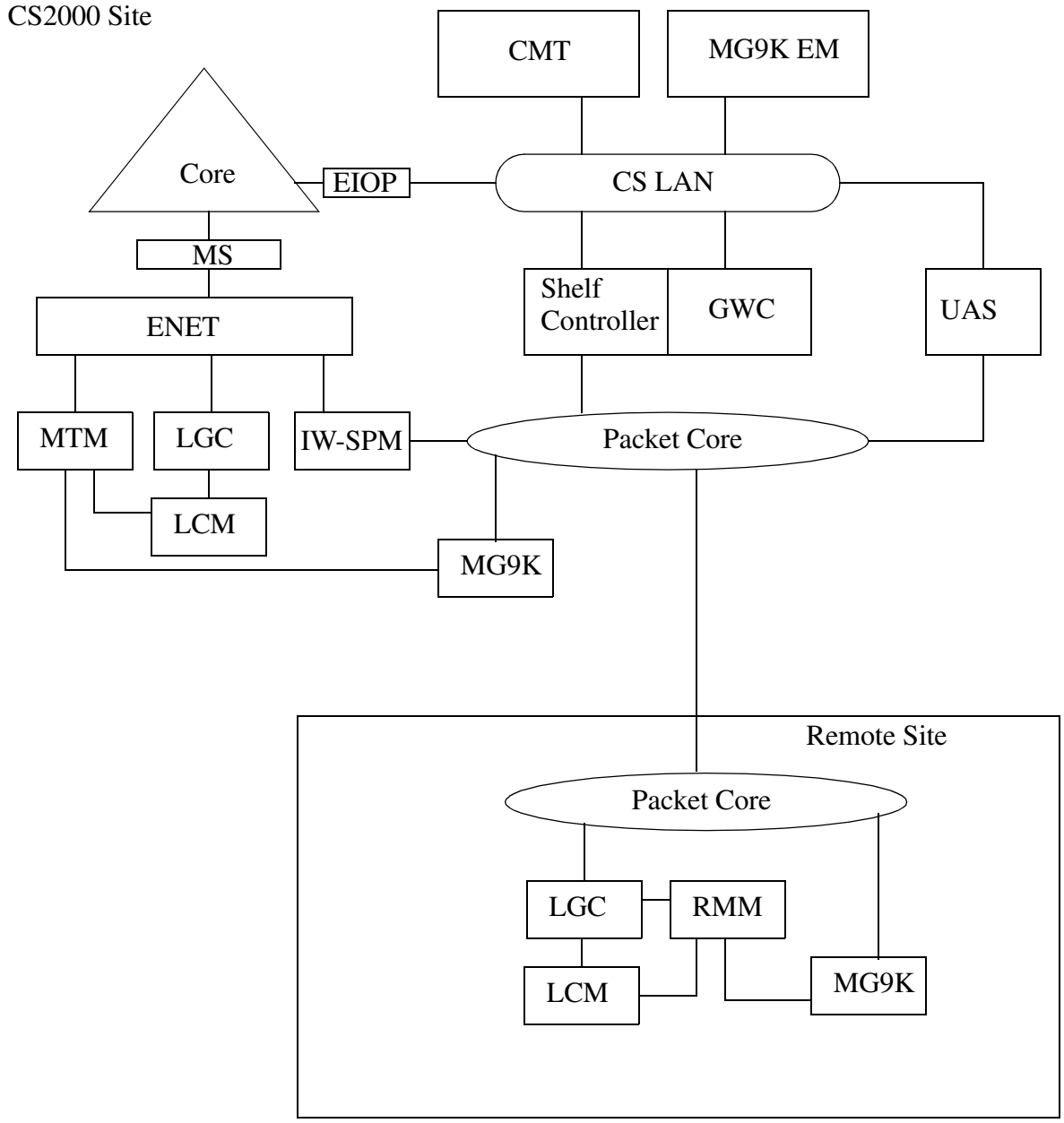
Description of task:	
Description of task	
Command: MAP response:	

2.10 Security

N/A

2.11 Configuration Walkthrough

The following diagram shows an example network deployment.


CS2000 Site
CMT
MG9K EM
Core
EIOP
CS LAN
MS
ENET
Shelf Controller
GWC
UAS
MTM
LGC
IW-SPM
Packet Core
LCM
MG9K
Remote Site
Packet Core
LGC
RMM
LCM
MG9K

3: Configuration (CN): A00001893

3.1 Hardware and Software Requirements

This feature requires the SN07 Media Gateway 9000 Element Manager, the Network Patch Manager and Media Gateway 9000 Device Software as well as the SSPFS platform software.

3.2 Document Name and Version

Document Name:
MG9K_Imaging_CN.fm

Version:

/main/pnmdoc/1

3.3 Upgrade Impact

This feature impacts MG9K Device upgrades by allowing the craft person to upgrade an MG9K Device with a new load, patch the load with all available patches for the load and execute an image.

The execution of the image will create a device load with a ".tar" file extension (ex. SCOA07AA_GZ.tar). This image load will contain the software load *and* the patches.

The user will then have the ability to upgrade the remaining devices in the office with the newly imaged load.

The availability of the image command could potentially reduce the amount of time an upgrade takes significantly

3.3.1 Dump and Restore

N/A

3.3.2 Element Management Upgrade

This feature will create a ".tar" load file during the imaging process that can be used to upgrade MG9K Devices of the same load type.

3.4 Element Management

This feature adds new commands to the Media Gateway 9000 Element Manager Graphical User Interface and the Network Patch Manager Graphical User and Command Line User Interface.

3.4.1 Media Gateway 9000 Element Manager

This feature adds new commands to the Media Gateway 9000 Element Manager Graphical User Interface and the Network Patch Manager Graphical User and Command Line User Interface.

3.4.2 Initial MG9K Element Manager Configuration

This feature will change/update two configuration scripts for the MG9K EM Server; *mg9kconfig.sh* and *mg9kserver config*.

3.4.2.0.1 mg9kconfig.sh

Today, the mg9kconfig.sh script must be executed before the MG9K EM Server can be started. Therefore, this script will be modified to ask the user for the following information:

- Image Server - the load server where the load images will be stored
- Image Server User ID - the user id for the load server that has ftp access. **NOTE: the ftp user must have over write privileges on the server**.
- Image Server password - the password for the load server user id
- Supercore IMA Image Directory - directory where the image for this load type will be stored.
- SuperCore OC2 Image Directory - directory where the image for this load type will be stored.
- ITP Image Directory - directory where the image for this load type will be stored.
- ITX Image Directory - directory where the image for this load type will be stored.
- DS1 Image Directory - directory where the image for this load type will be stored.
- ABI Image Directory -directory where the image for this load type will be stored.

The mg9kconfig.sh script will provide a default Image Directory for the user that will be located at: /swd/mg9k.

The following figure shows the final output from the mg9kconfig.sh script that the user will see and verify before starting the MG9K EM Server.

Figure 1 Script output of the mg9kconfig.sh verification

```
************************************************************
      Setup Server As                    : MASTER
     Master Server IP Address            : wnc0s00v
      SESM IP Address                    : 47.142.164.250
      Security Authentication Host       : 47.142.164.250
      Oracle IP Address                  : 47.142.164.250
      Initialize Database                : YES
      Maintenance Release Upgrade        : NO
      Image Server                       : 47.142.164.250
      Image Server User ID               : maint
     SuperCore IMA Image Directory       : /swd/mg9k/sci
     SuperCore OC3 Image Directory       : /swd/mg9k/sco
      ITP Image Directory                : /swd/mg9k/itp
      ITX Image Directory                : /swd/mg9k/itx
      ABI Image Directory                : /swd/mg9k/abi
      DS1 Image Directory                : /swd/mg9k/ds1

************************************************************
```

3.4.2.0.2 mg9kimpl

The mg9kimpl script exists today and is available so that the user can change information the MG9K EM Server utilizes. This script is accessed by typing **./ mg9kserver config**. This feature will provide a "*Change Imaging Server Settings*" Menu in this script so that the default software imaging parameters can be changed without executing the entire mg9kconfig.sh script again. The following figures show how the menu is displayed.

Figure 2 Main Configuration Menu for the MG9K EM Server

```
Main Configuration Menu

1) Change Distribution Policy
2) Change SESM IP Address
3) Change Oracle IP Address
4) Change Debug Level for logs
5) Change Persistence settings
6) Change ESA data download settings
7) Change Imaging Server settings
8) Display current settings
9) Exit from Main Menu
Please make a selection =>
```

Figure 3 Image Configuration Menu for the MG9K EM Server

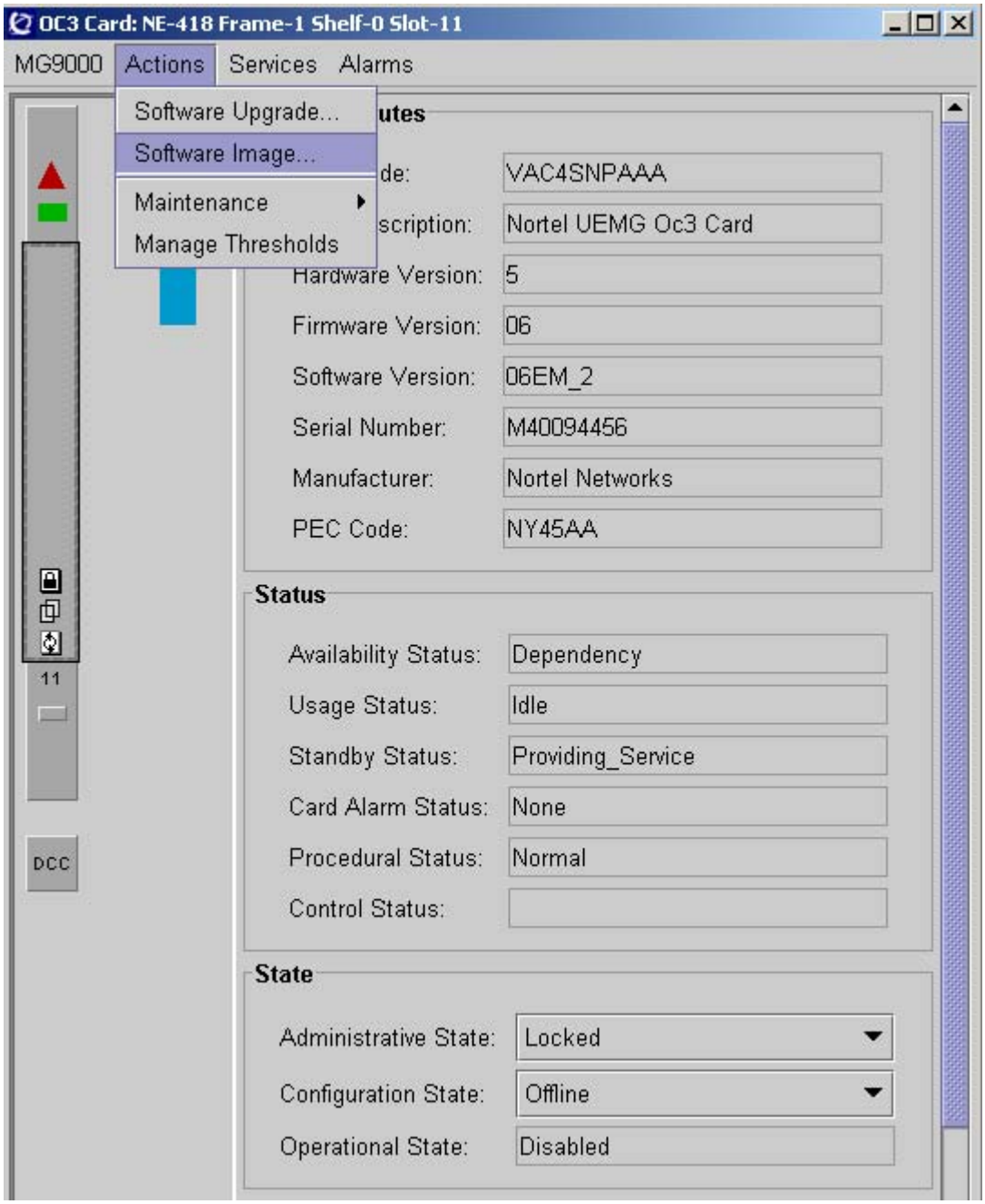
```
.
  Image Configuration Menu

1) Change Image Server IP
2) Change Image Server User ID and password
3) Change Image Server default directories
4) Exit to Main Menu
Please make a selection =>
```

3.4.2.1 MG9K EM GUI

This feature changes the MG9K EM GUI at the card level only. An additional item named *Software Image* will be added to the *Actions* menu. The Software Image function is performed on a **per card basis** and is only available for the SuperCore OC3, SuperCore IMA, ITP, ITX, DS1 and ABI cards.

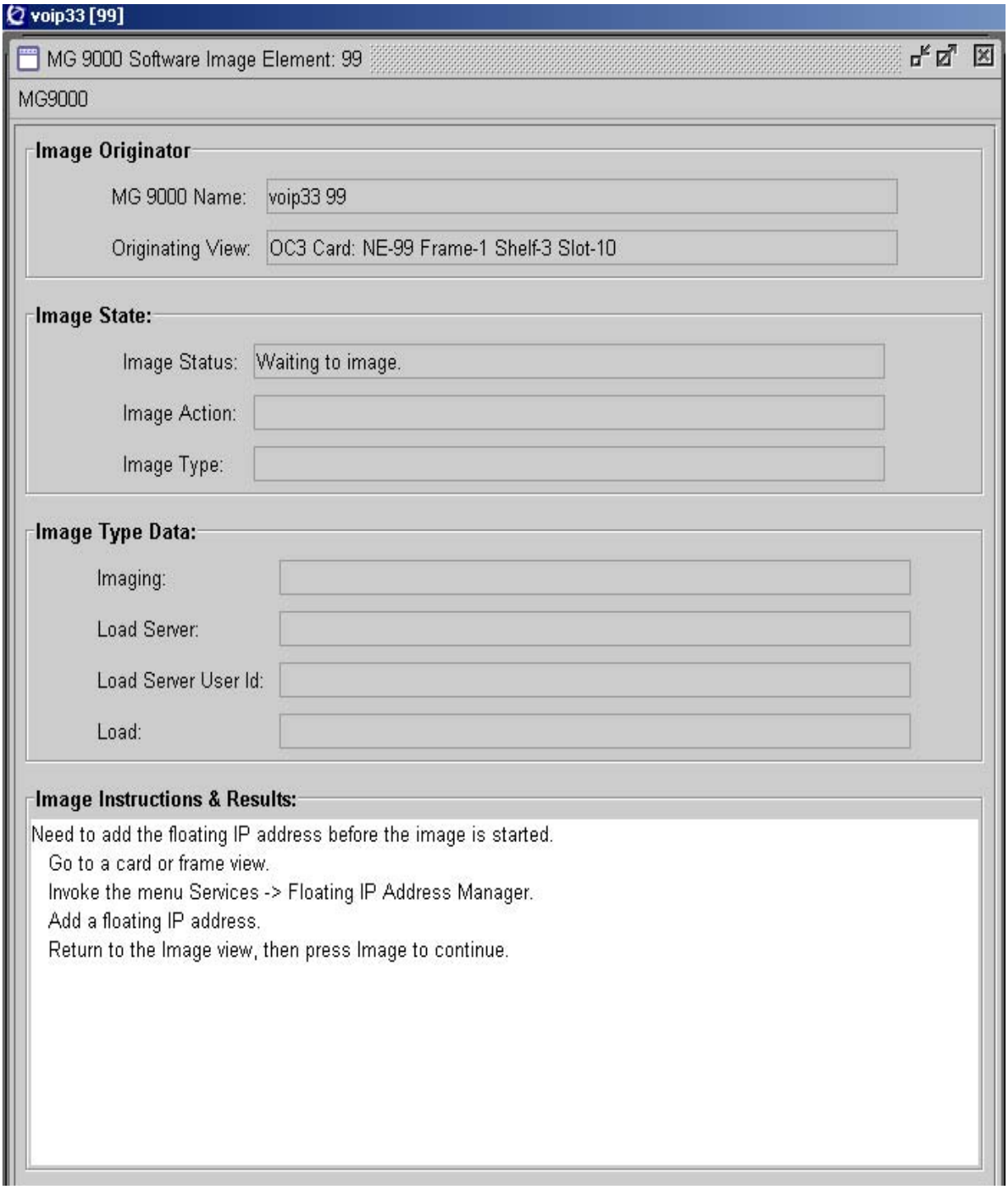
The following figures show the Software Imaging GUI interface for the MG9K EM.

Figure 4 MG9K EM GUI Card View



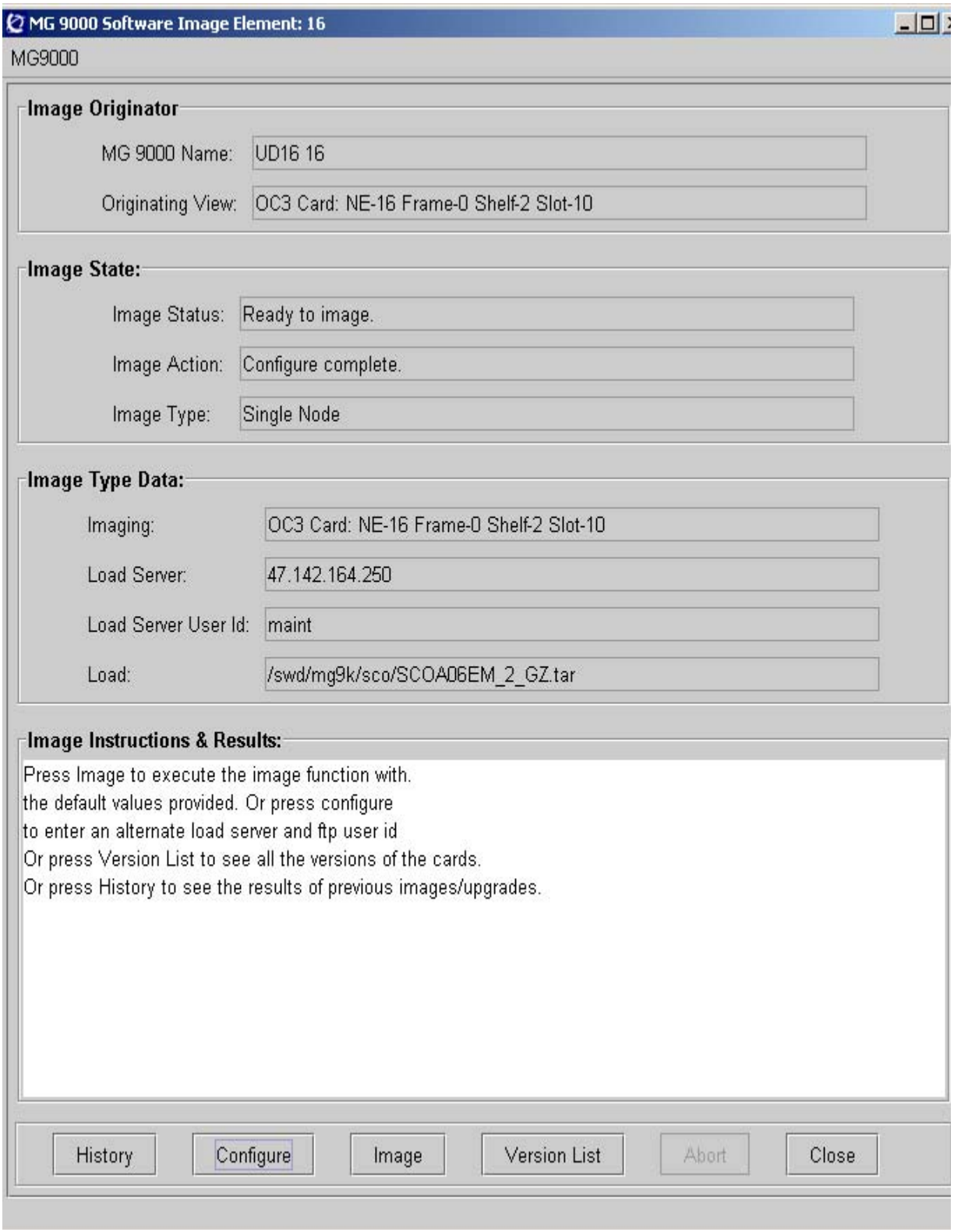
After selecting the Software Image tab, the MG9K Image GUI appears. The next figure shows the message if the Floating IP has not been configured.

Figure 5 Floating IP Not configured



After the floating IP has been configured, the MG9K Image GUI can be re-entered and should look as follows:

Figure 6 MG9K EM Image GUI



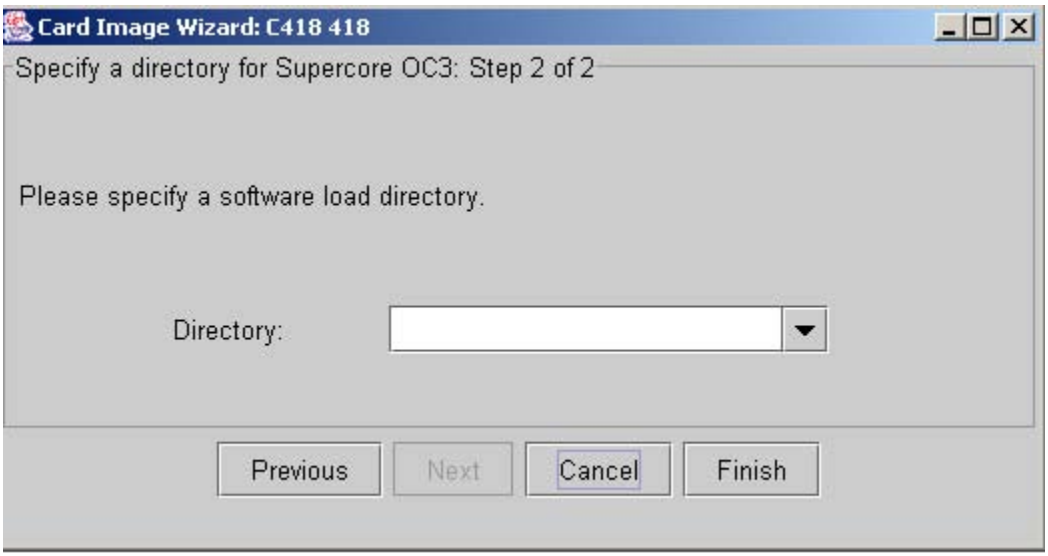
From figure 6, notice that there is a *Configure* button. If the user wishes to change the default server IP, server user ID, server password or directory, they can do so by clicking on the *Configure* button. **Note**: *Configure* only changes these values for this session. It does not change the default values permanently.

The following two figures show the *Configure* menus.

Figure 7 Server Configure Menu

The Server User Identifer *must* be an FTP user that has overwrite access on the load server.

Figure 8 Server Directory Menu



As part of manual imaging, the MG9K EM will obtain patch information from the Network Patch Manager. This information will help the user to determine if there is any reason the device load should not be imaged. If the NPM determines any of the following conditions, a *Warning* message will be sent to the user:

- the device load contains obsolete patches
- the device load contains patches that are on hold
- the device itself is on hold
- the device load is at a lower patch level then the previously image load.

A *Failure* message will be sent to the user if communication with the NPM cannot be obtained. However, in all of these instances, the user will have the ability to override these conditions and continue with the image.

3.4.2.2 FTP User Configuration

This feature requires that the FTP server that is used for images have an FTP user configured that has read AND overwrite access to the server. After an image file is created once, every subsequent image of that load will be overwritten. NOTE: only the image file will be overwritten, not the original load file.

3.4.2.3 Image File

The imaged file name is pre-determined and **CANNOT** be configured. The imaged file name will be based on the name of the load file with a ".tar" extension. For example, if the file name of the load is SCOA07AA_GZ, the imaged load file name will be SCOA07AA_GZ.tar. This is the name of the load file that should be used when the user is ready to upgrade or re-load devices from disk.

The imaged load will be placed in the directory that the user specified during initial configuration of the MG9K EM Server or in the configuration entered via the Image Configuration Panels shown in figures 6 and 7.

3.4.3 Network Patch Manager

The NPM will offer the ability to image an MG9K Device via a new maintenance command; *SmartImage*. This new maintenance command will "look and feel" like the other maintenance commands in the NPM.

Unlike manual imaging from the MG9K EM, the *SmartImage* command utilizes a patching criteria that will determine if the devices that the user wishes to image *should* be imaged. The following sections discuss the patching criteria, NPM GUI and NPM CLUI changes as well as other changes to the NPM that will be necessary for the this feature.

3.4.3.1 Security

This feature requires the user to have a security level of emsadm in order to execute the *SmartImage* command.

3.4.3.2 Logs

This feature will not add new log numbers for the SmartImage command. This feature will utilized the NPM maintenance log numbers that are currently available for maintenance commands.

3.4.3.3 NPM PreDefined Device Sets

This feature will introduce two new predefined device sets to the NPM:

- MG9KDevices
- GWCDevices

Each of these sets will include all of the devices of the device type they reference. For example, MG9K Devices will include all of the MG9K type devices; OC3, ITP, ITX, DS1, and ABI. It will be recommended that the user utilize these sets when executing the *SmartImage* command.

3.4.3.4 NPM Patching Criteria

Basically, the criteria for the SmartImage command boils down to which device(s) contains the highest patch content.

Because this is the “focus” of the criteria, it is essential that the user be aware of what they are doing when they image a device from the NPM. It is **highly** recommended that the user only use the “device sets” that will be provided as part of this feature. Otherwise, an image of a device could be taken that does not contain the highest patch content.

The tables below show an example of how the patching criteria will work for the SmartImage Command.

Table 1 shows a list of all the MG9K Devices, registered in the NPM, sorted by loadname.

Table 1 Sorted devices and loads

Loadname	Device
SCOA07AB	UD16_16_62_OC3_0_2_10
	UD16_16_62_OC3_0_2_11
	UD17_17_72_OC3_0_2_10
	UD17_17_72_OC3_0_2_11
ITPA07AB	UD16_16_62_ITP_0_2_12
	UD16_16_62_ITP_0_2_13
	UD16_16_62_ITP_1_2_12
ITPA07AA	UD16_16_62_ITP_1_2_13
ITXA07AB	UD16_16_62_ITX_0_2_14
	UD16_16_62_ITX_0_2_15
	UD17_17_72_ITX_0_2_14
	UD17_17_72_ITX_0_2_15

Once all of the devices are sorted, the NPM looks at specific fields to determine if each device is a candidate for imaging. The following table shows the fields used and what impact they have on each device as it is evaluated.

Table 2 Patching Criteria

Field	Description	Impact on Imaging
AppLevel	Contains an integer value to indicate the number of patches applied to the device.	If zero patches are applied, the device is not a candidate for imaging.

Table 2 Patching Criteria

Field	Description	Impact on Imaging
ActLevel	Contains an integer value to indicate the number of patches activated in the device.	If all the devices for a particular load are at the same applevel, this field is used as a “tie breaker” to determine if a device should be imaged.
Hold	Contains Y or N to indicate whether the device is on hold.	If the device is on hold (Y), the device is not a candidate for imaging.
Patches on Hold	Contains an integer to indicate how many patches are on hold.	If the device contains any patches that are on hold, the device is not a candidate for imaging.
Obsolete Patches	Contains an integer value to indicate how many obsolete patches.	If the device contains any patches that are obsolete, the device is not a candidate for imaging.

Table 3 shows an example the patching criteria field values for each device.

Table 3 Patching Criteria Fields

Loadname	Device	App-Level	Act-Level	Patches on Hold	Obsolete Patches	Hold	Include
SCOA07AB	UD16_16_62_OC3_0_2_10	5	0	0	0	N	Y
	UD16_16_62_OC3_0_2_11	5	0	0	0	N	Y
	UD17_17_72_OC3_0_2_10	5	0	0	0	N	Y
	UD17_17_72_OC3_0_2_11	5	0	0	0	N	Y
ITPA07AB	UD16_16_62_ITP_0_2_12	3	0	0	0	N	Y
	UD16_16_62_ITP_0_2_13	2	0	0	0	N	Y
	UD16_16_62_ITP_1_2_12	5	0	0	0	Y	N
ITPA07AA	UD16_16_62_ITP_1_2_13	5	0	0	1	N	N
ITXA07AB	UD16_16_62_ITX_0_2_14	0	0	0	0	N	N
	UD16_16_62_ITX_0_2_15	0	0	0	0	N	N
	UD17_17_72_ITX_0_2_14	0	0	0	0	N	N
	UD17_17_72_ITX_0_2_15	0	0	0	0	N	N

From Table 3, let's evaluate which devices were chosen as candidates for imaging. We will look at the devices that were not chosen for imaging later in this section.

Table 4 Candidates Devices for Imaging

Candidate Devices	
Group 1	UD16_16_62_OC3_0_2_10
	UD16_16_62_OC3_0_2_11
	UD17_17_72_OC3_0_2_10
	UD17_17_72_OC3_0_2_11
Group 2	UD16_16_62_ITP_0_2_12

The five devices from Table 4 were chosen because they were not on hold and they had the highest level of patches applied to their load without any of the patches being obsolete or on hold.

Once the candidate device list is determined, the NPM then looks at the previously imaged AppLevel and ActLevel fields for each load.

If the AppLevel for the devices in a group are at a higher or lower level then the previously imaged levels, a device from the group will be chosen for imaging.

If the AppLevel is the same as the Previously Imaged AppLevel, the ActLevel will be used as a "tie breaker" to determine if an image should occur. If the ActLevel is the same, none of the devices will be imaged because the levels are the same level as the previous image.

NOTE: MG9K Devices do not currently support activation type patches, however, this patching criteria will continue to utilize this field as part to the criteria to determine the candidate device list, so that the patching criteria can be keep generic.

Table 5 Chosen Devices for Imaging

Candidate Devices		Current AppLevel	Current Actlevel	Previous Imaged AppLevel	Previous Imaged ActLevel
Group 1	UD16_16_62_OC3_0_2_10	5	0	4	0
	UD16_16_62_OC3_0_2_11	5	0	4	0
	UD17_17_72_OC3_0_2_10	5	0	4	0
	UD17_17_72_OC3_0_2_11	5	0	4	0
Group 2	UD16_16_62_ITP_0_2_12	3	0	4	0

Once the NPM determines that a group of devices should be imaged, from this point on, the NPM views the devices in each group as “equals” and simply chooses the first device in the group to be imaged; as shown in Table 6.

Table 6 Chosen Devices for Imaging

Chosen Devices	
1	UD16_16_62_OC3_0_2_10
2	UD16_16_62_ITP_0_2_12

Now that we know which devices will be chosen for imaging, let’s take a closer look at why some of the devices were not chosen for imaging.

Table 7 Devices NOT chosen for imaging

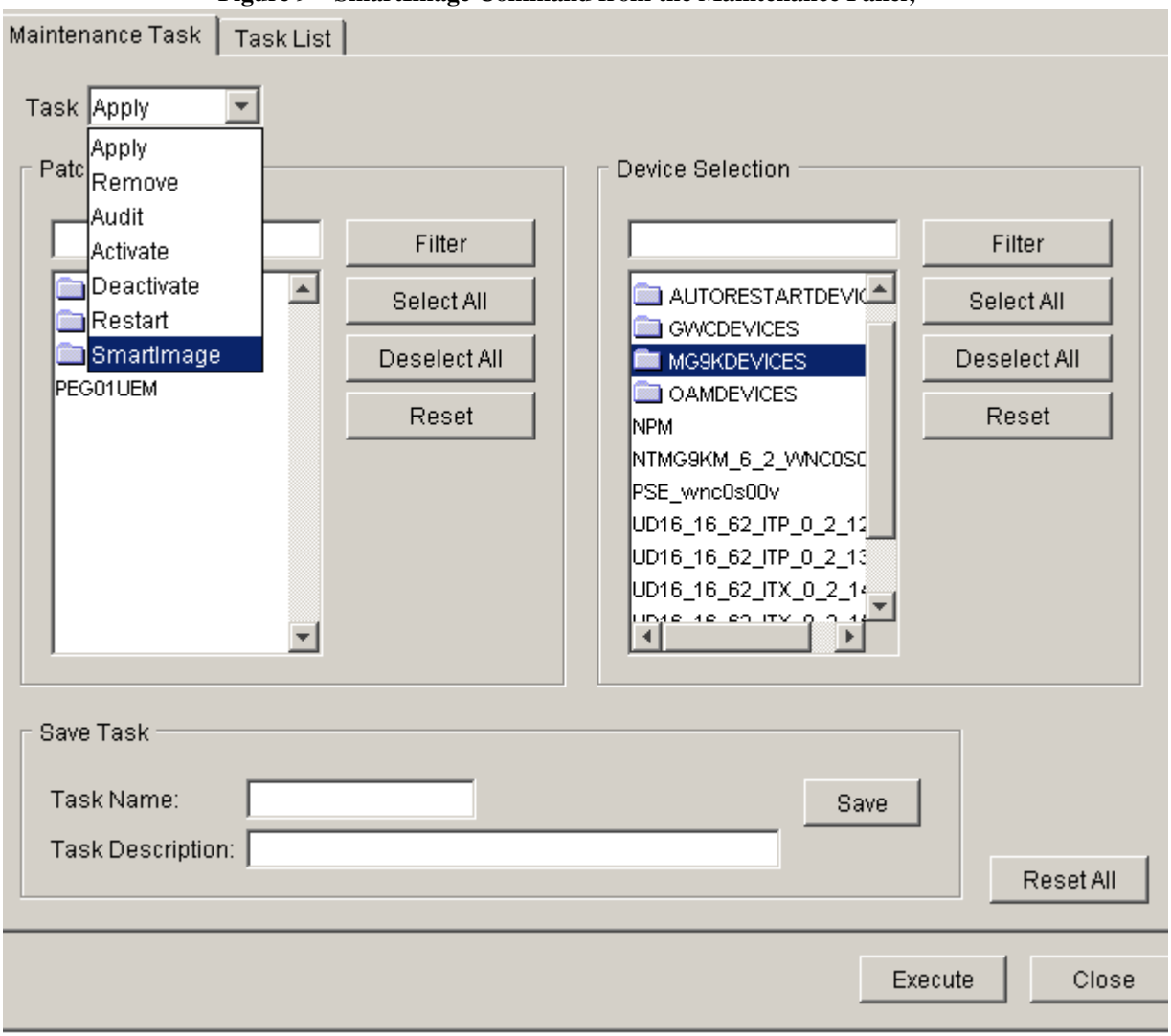
Loadname	Device	AppLevel	ActLevel	Patches on Hold	Obsolete Patches	Hold
ITPA07AB	UD16_16_62_ITP_0_2_13	2	0	0	0	N
	UD16_16_62_ITP_1_2_12	5	0	0	0	Y
ITPA07AA	UD16_16_62_ITP_1_2_13	5	0	0	1	N
ITXA07AB	UD16_16_62_ITX_0_2_14	0	0	0	0	N
	UD16_16_62_ITX_0_2_15	0	0	0	0	N
	UD17_17_72_ITX_0_2_14	0	0	0	0	N
	UD17_17_72_ITX_0_2_15	0	0	0	0	N

- Device UD16_16_62_ITP_0_2_13, was not chosen for imaging because it does not contain as high of a patch content as UD16_16_62_ITP_0_2_12.
- Device UD16_16_62_ITP_1_2_12, was not chosen for imaging because the device is on hold.
- Device UD16_16_62_ITP_1_2_13, was not chosen for imaging because the device load contains an obsolete patch.
- Device UD16_16_62_ITX_0_2_14, UD16_16_62_ITX_0_2_15, UD17_17_72_ITX_0_2_15 and UD17_17_72_ITX_0_2_15 were not chosen for imaging because there are not patches currently applied to either device.

3.4.3.5 NPM GUI

The following figures show example output of the *SmartImage* command and results (Note the example output here, is not the example that is shown in the table example shown in section 2.2.2.4):

Figure 9 SmartImage Command from the Maintenance Panel;



After choosing the *SmartImage* Command and the selected devices, the user can click the *Execute* button. Once this button is clicked a warning message is displayed to the user to ensure that they agree that the devices chosen are the ones that they want evaluated.

Figure 10 Warning message for the SmartImage Command

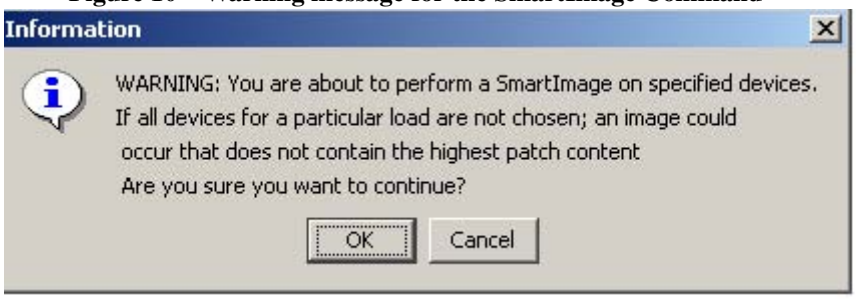


Figure 11 Pre-results for the SmartImage Command

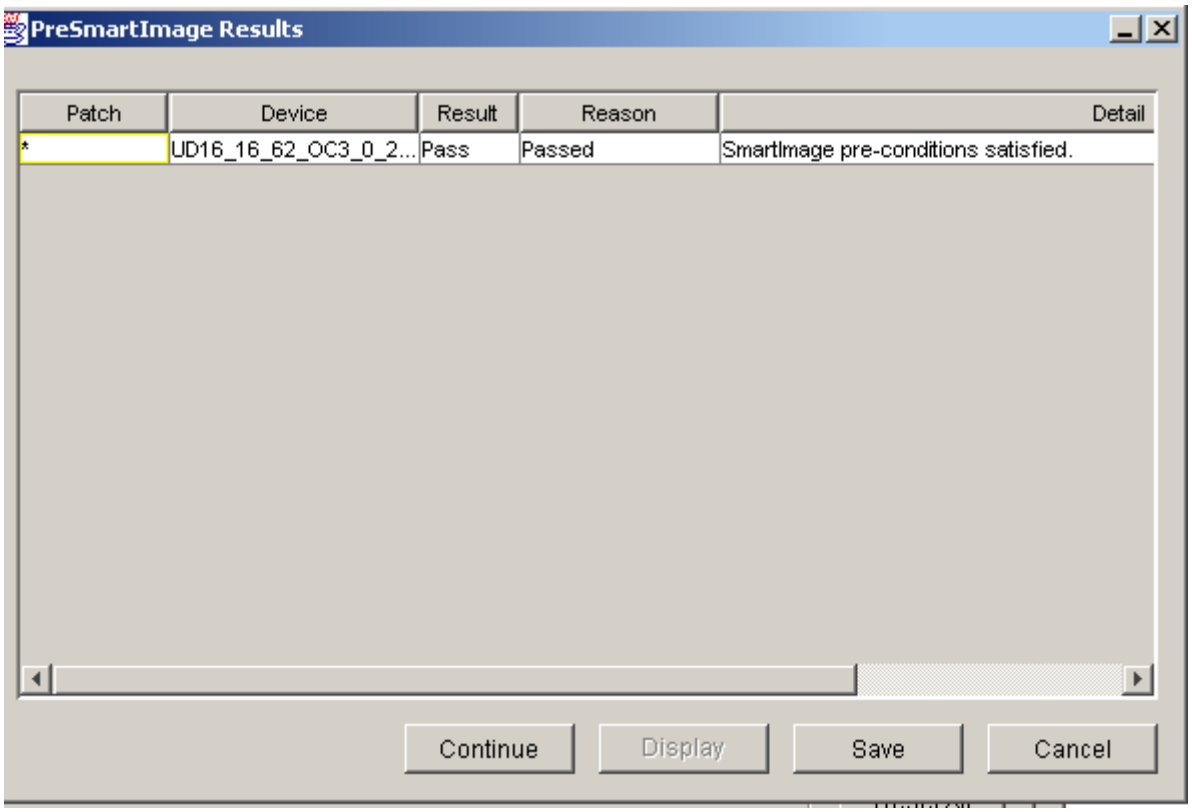
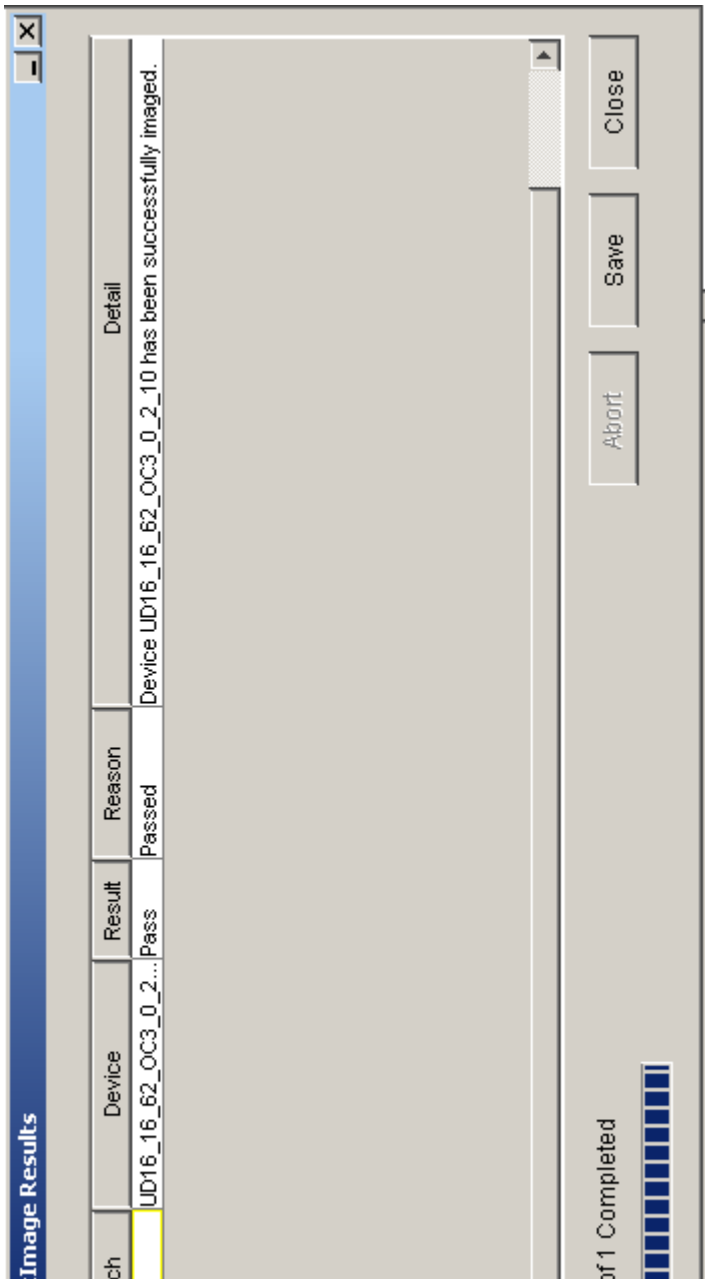


Figure 12 Final results from the SmartImage Command



3.4.3.6 NPM CLUI

This feature changes the NPM CLUI by adding the new SmartImage command. The command will execute just as it does in the NPM GUI. The following is an example of the command and output.

NPM CLUI SmartImage Command Output

```
npm>smartimage SET MG9KDEVICES
WARNING: You are about to perform a smartimage on the specified devices.
Note that if all devices for a particular load are not chosen
for imaging. A device may be chosen that does not contain the
the highest patch content.
If you wish to continue with this maintenance request enter Yes (Y or y).
Otherwise, just enter return.
#y

Patch: *
Device: UD16_16_62_OC3_0_2_10
Result: true
Reason: Passed
Details: SmartImage pre-conditions satisfied.


If you wish to continue with this maintenance request enter Yes (Y or y).
Otherwise, just enter return.
#y

npm>
Patch: *
Device: UD16_16_62_OC3_0_2_10
Reason: Passed
Detail: Device UD16_16_62_OC3_0_2_10 has been successfully imaged.
```

3.4.3.7 Scheduling SmartImage

The SmartImage command can be scheduled in the NPM via the NPM GUI or NPM CLUI and executed nightly, weekly or monthly. It is recommended that if SmartImage is scheduled on a nightly basis, that autoapply is also scheduled and executed before the SmartImage task is executed.

The following figures show some of the steps involed to schedule the SmartImage task.

3.4.3.7.1 Scheduling a SmartImage from the NPM GUI

Figure 13 Saving the SmartImage Task

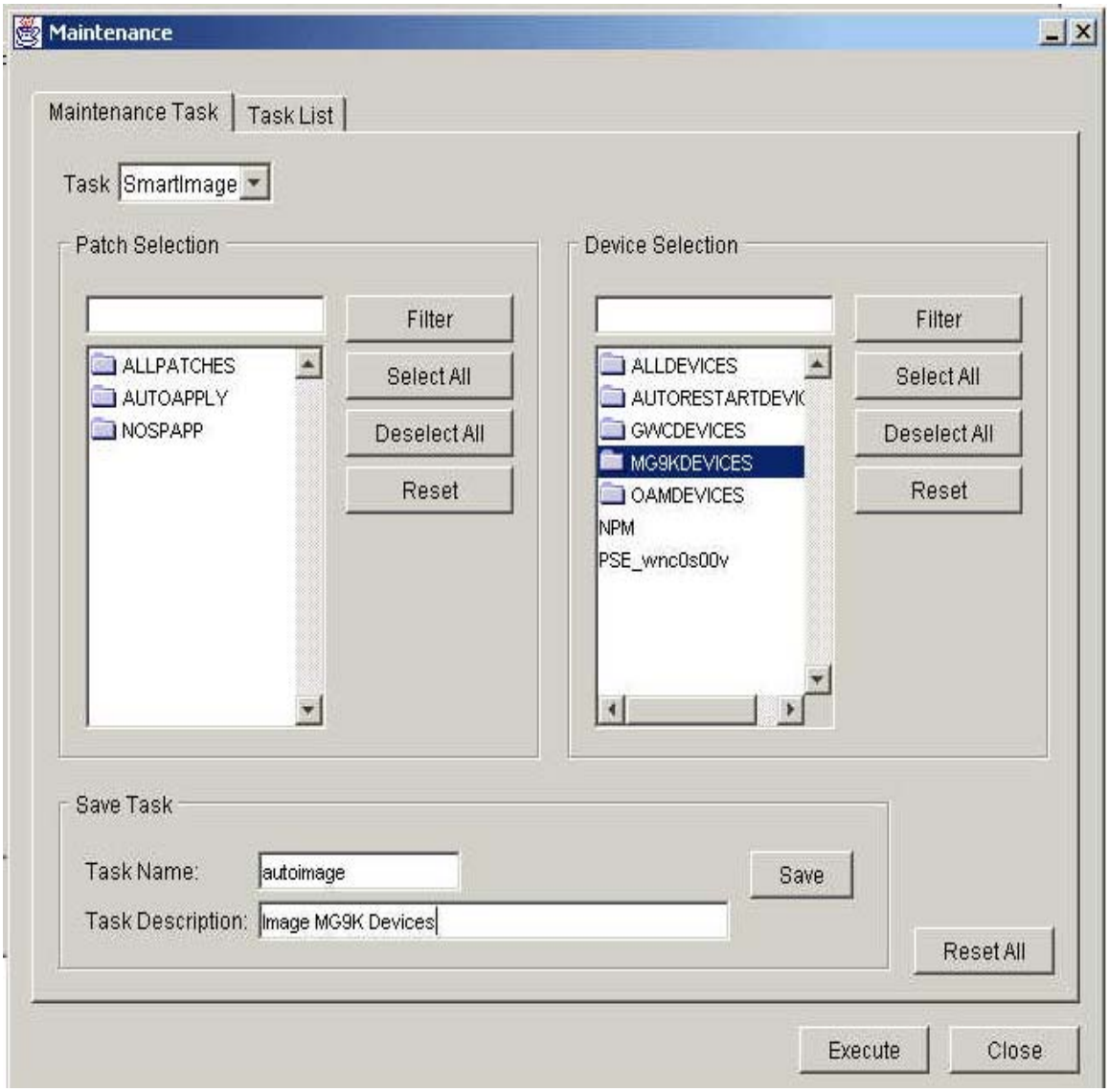


Figure 13 shows the SmartImage Task being saved and called *autoimage*.

After the task is saved it will show up as an available task to be scheduled in the NPM System Scheduler. The following figures show how to get to the NPM System plan and how to edit the plan to include the *autoimage* task.

Figure 14 Selection of the System Plans menu

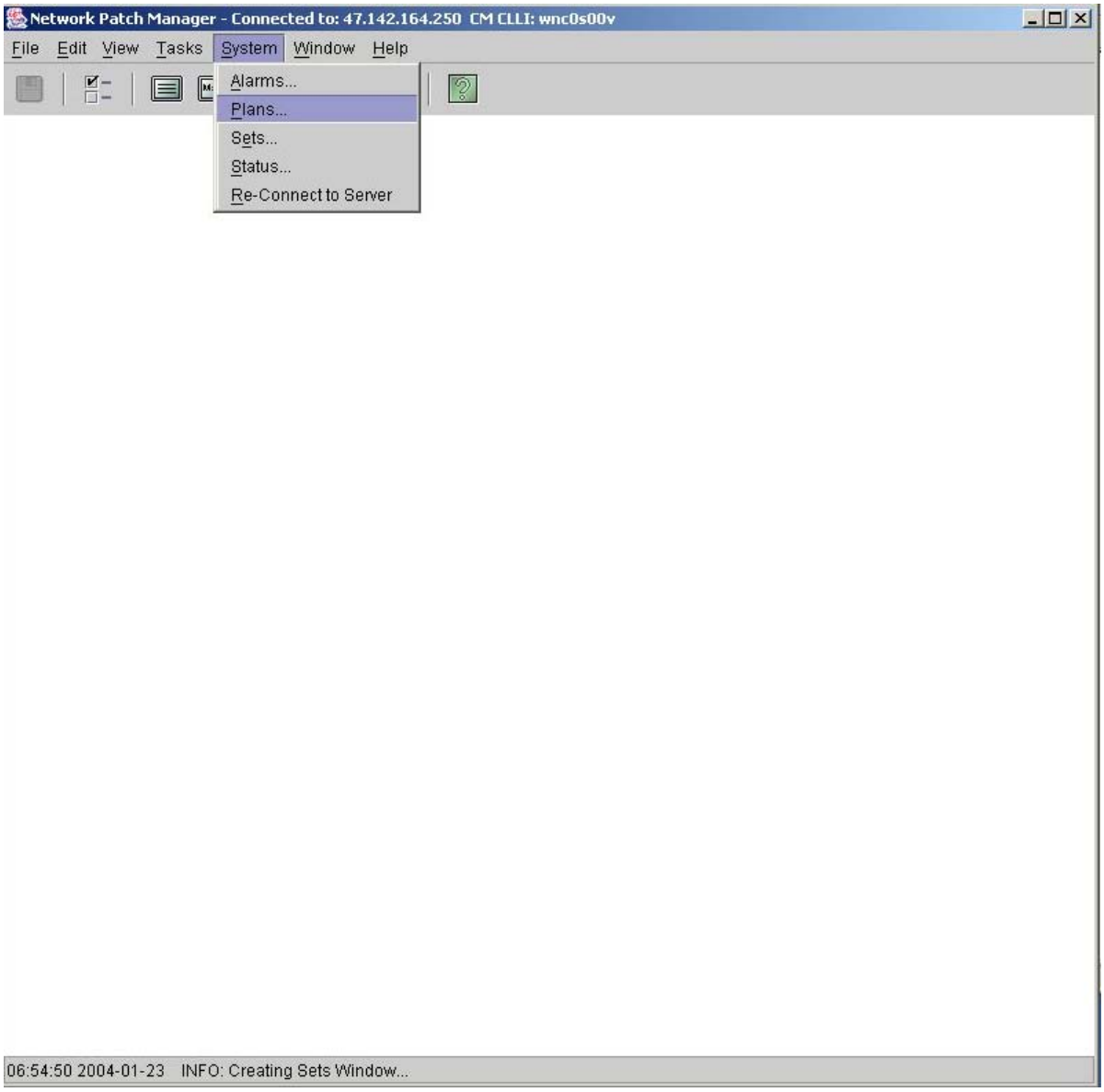


Figure 15 Selection of the System Plan for editing

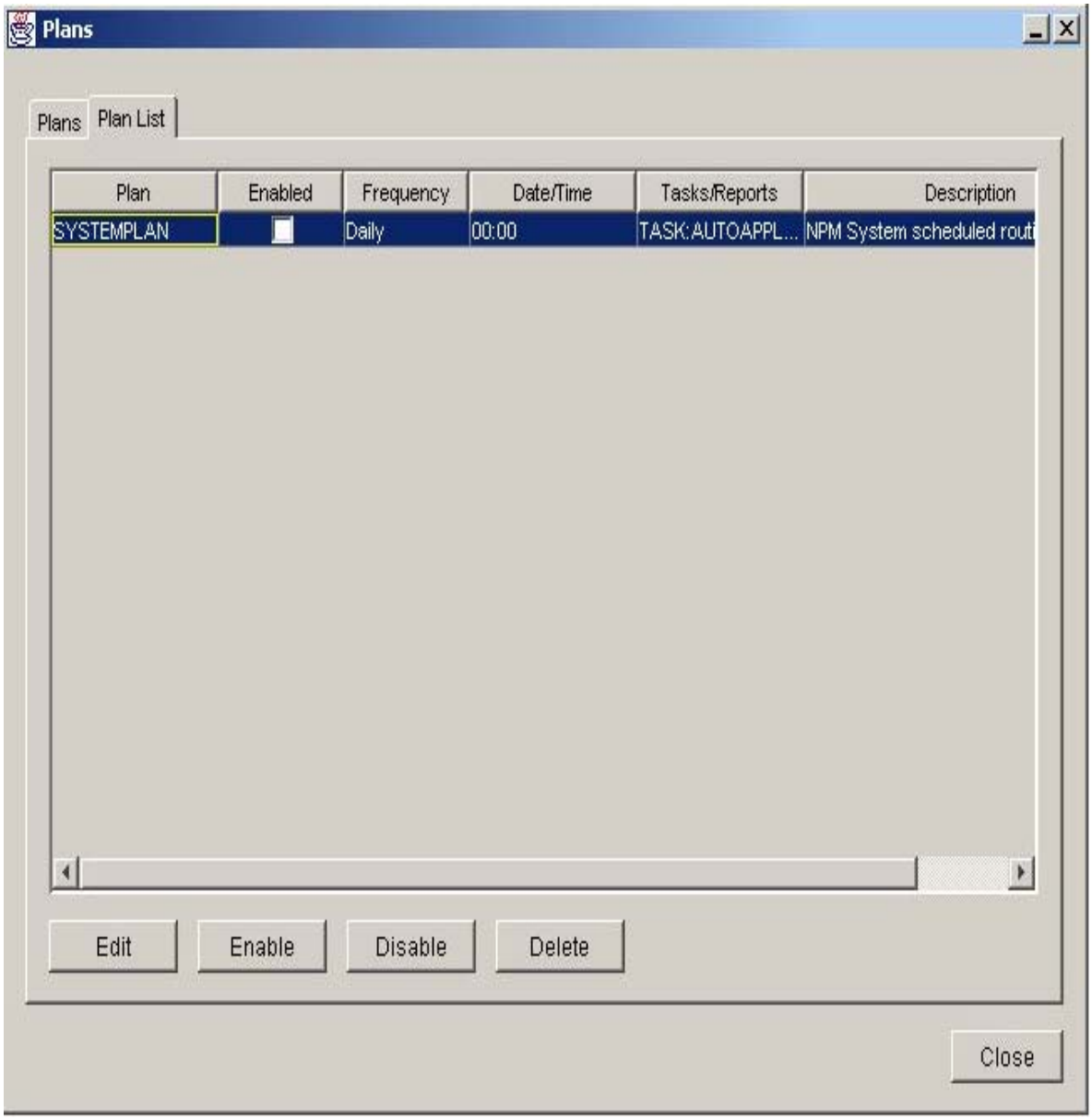
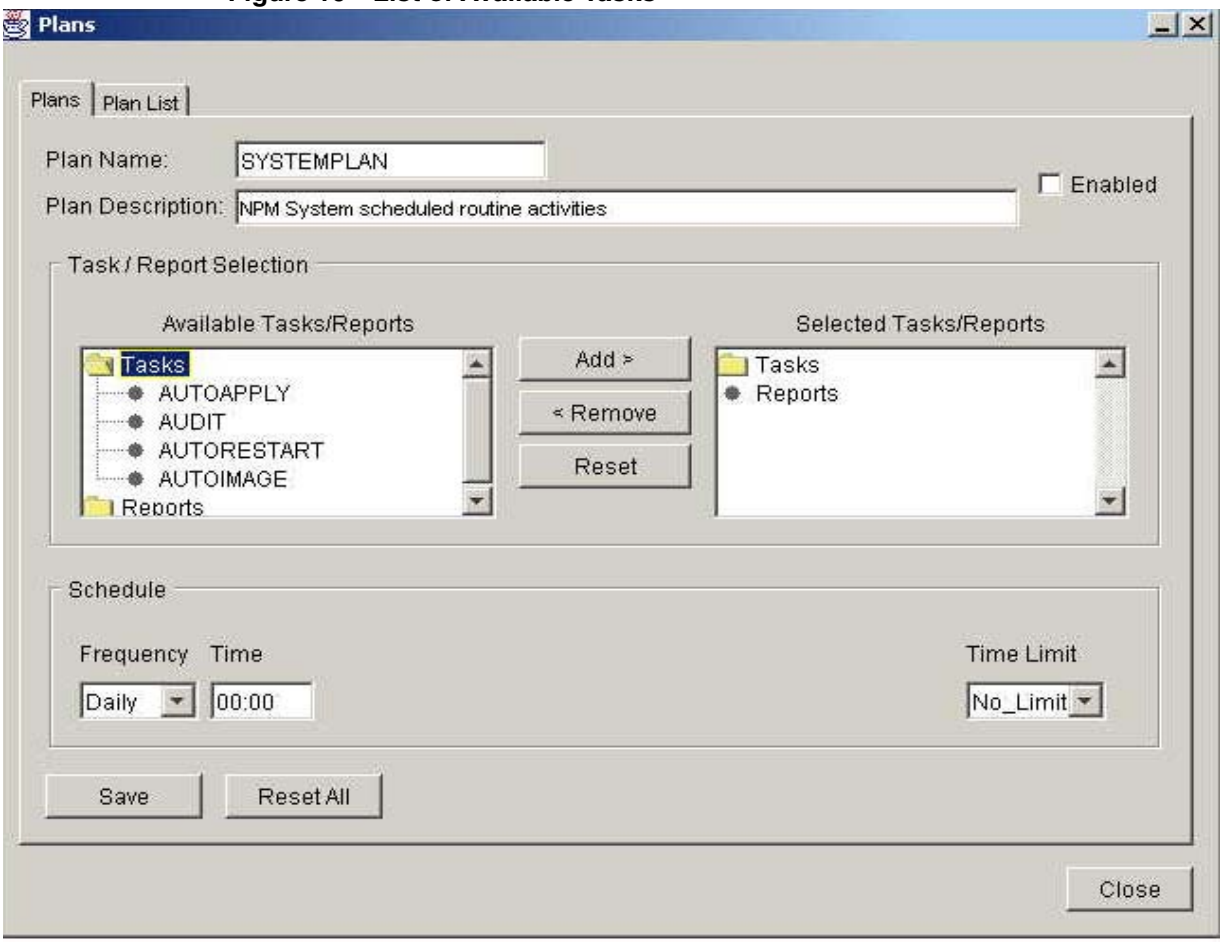
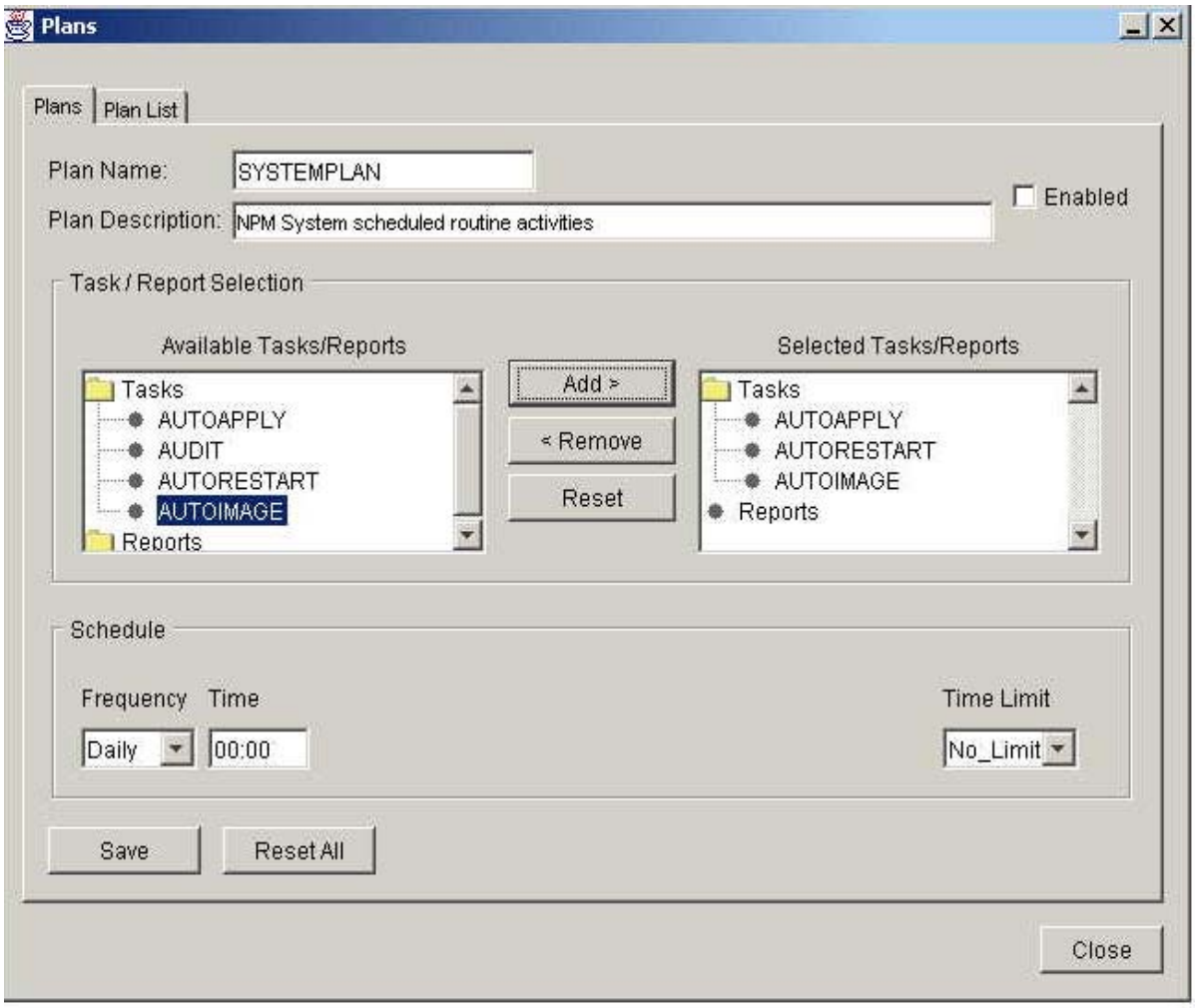


Figure 16 List of Available Tasks



The newly added *AUTOIMAGE* task can be added to the selected number of tasks to execute, as shown in figure 15.

Figure 17 Imaging added to the System Plan



3.4.3.7.2 Scheduling a SmartImage task from the NPM CLUI

The following figures shows how to save, add and schedule a *SmartImage* task from the NPM CLUI.

Figure 18 Scheduling SmartImage Task from NPM CLUI

```
npm>newtask MG9K_IMAGE_TASK SMARTIMAGETASK"MG9K AUTO IMAGING
" MG9KDEVICES
Task created successfully.


npm>sched SYSTEMPLAN TASK MG9K_IMAGE_TASK Add
Done.


npm>updplan SYSTEMPLAN Daily"1-24-04 00:00 " No_Limit"Nightly Maintenance"
Plan updated successfully.


npm>enableplan SYSTEMPLAN ON
Done.
```

3.5 Hardware Requirements or Dependencies

None

3.6 Software Requirements or Dependencies

This feature requires the SN07 MG9K EM, NPM and MG9K Device Software.

3.7 Limitations and restrictions

The following items are listed here as limitations from this feature:

- **SmartImage is dependant on the default information that is input at configuration time of the MG9K EM Server. If this information is not available, the user will not be able to SmartImage or auto image.**
- **SmartImage or auto imaging for the customer who does not *specialize* his office. It is for the customer who patches all devices with the same patches.**
- **The patching criteria looks at the levels of patches in a device load. Therefore is a user patches a device with 4 patches, images the device, then removes the patches and then applies 4 different patches; the level of patches since the last image has not changed and the device will not be imaged.**

- **Due to the fact that two MG9K EM Servers execute on the same SSPFS box at one time during upgrades; the customer must be aware that when the mg9kconfig.sh script asks for the image user id and image server password, they must be the same for both MG9K EM Servers executing. This is due to the fact that there will only be one secure password file for the imaging server per SSPFS platform. However, the additional information the user provides via the mg9kconfig.sh script can be different, including the image server IP and load image directories.**
- **The load server used must have FTP read/overwrite access.**

3.8 Interactions

None

3.9 Glossary

MG9K EM - Media Gateway 9000 Element Manager

NPM - Network Patch Manager

GUI - Graphical User Interface

CLUI - Command Line User Interface

4: Configuration (CN): A00001898

This chapter documents the configuration related changes for activity A00001898. Specifically there are changes in the provisioning system (as captured in the Data Schema Section) as well as changes in the maintenance system (as captured in the Command Interface Section). All sections that are not relevant for this activity are tagged as Not Applicable.

4.1 Hardware and Software Requirements

- The RMM has been installed
- A DS30A card has been inserted into the host peripheral (LTC, LGC, or SMA2) in the appropriate slot
- The host XPM and the RMM are connected via a DS30A cable
- The software for this activity is installed in the XACore
- The required SMA2 load (if the RMM is connected to an SMA2) is installed in the XPM

4.2 Initial Configuration

Not Applicable

4.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

4.4 Upgrade Impact

The RMM load is unchanged by this activity and therefore is not required to be upgraded from the currently available load. All other loads are upgraded in the standard fashion and the upgrade procedure is not impacted by this activity.

The feature impacts Core, GWC, and XPM software. The standard DMS processes for upgrade order applies to ABI XPMs. With regard to GWCs and XPMs, the XPMs are upgraded first, followed by the GWCs.

4.5 Data schema (DS) (CM, MIBS, RDB)

4.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TABLE LTCPSINV	Changed	Unchanged

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TABLE RMMINV	Changed	Unchanged
TABLE LTCINV	Changed	Unchanged

4.5.2 Table/MIB/Remote Database Schema information

4.5.2.1 Name: TABLE LTCPSINV

Long Table Name: Line Trunk Controller P-Side Inventory

4.5.2.1.1 Functional description

Table LTCPSINV lists all the P-Side links for each of the XPMs datafilled in table LTCINV. A tuple in this table is automatically created when a tuple is added in LTCINV, and is only modified (tuples are not manually added or deleted in this table) by the craftsperson to indicate what types of links are available on the P-Side of the XPM.

This activity modifies the handling of the P-Side links for the SMA2 peripheral type. All other peripheral types are unaffected by this activity.

Prior to this activity the SMA2 was only allowed to have DS-1 or DCH type P-Side devices. With the implementation of this activity support is provided for a single DS30A P-Side link on the SMA2. This is specifically being added to allow the SMA2 to have an RMM subtending it. The RMM is connected to it's host peripheral via a single DS30A link.

The format of LTCPSINV in not changed, all that is done is to allow the provisioning of a DS30A type link on the SMA2.

4.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

4.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCPSINV	Unchanged by this activity	Unchanged by this activity	Unchanged by this activity.

4.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for LTCPSINV.

EXP_TAB = "<LINK NUMBER (0-53)> DS30A"

When modifying the LTCPSINV entry for the SMA2 the EXP_TAB entry is changed to be a P-Side type of DS30A from NILTYPE.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
EXP_TAB	Changed	Unchanged from the existing set of P-side types.	DS30A	EXP_TAB refers to the expanded table of P-side links that is available for CPM-based peripherals (of which the SMA2 is one). The EXP_TAB allows the entry of up to 54 P-side links on the XPM, which is what is available when the SMA2 is setup with an extension shelf. This activity adds the capability to add a DS30A link on the P-side of the SMA2 XPM, specifically on link 52 only.

4.5.2.1.5 Datafill example

The following example shows sample datafill for table LTCPSINV. The changes from the prior allowed SMA2 peripheral datafill is highlighted with **bold** characters. This example is for an SMA2 without at extension shelf, but the DS30A provisioning is identical (ie: link 52 is always used) for a single shelf system.

```
CI:
>
>table ltcpsinv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCPSINV
>pos sma2 3
      SMA2   3
          Y (0 DS1 DEFAULT N) (1 DS1 DEFAULT N)
          (2 DS1 DEFAULT N) (3 DS1 DEFAULT N) (4 NILTYPE ) (5 NILTYPE )
          (6 NILTYPE ) (7 NILTYPE ) (8 NILTYPE ) (9 NILTYPE ) (10 NILTYPE )
          (11 NILTYPE ) (12 NILTYPE ) (13 NILTYPE ) (14 NILTYPE )
          (15 NILTYPE ) (16 NILTYPE ) (17 NILTYPE ) (18 NILTYPE )
          (19 NILTYPE ) (20 NILTYPE ) (21 NILTYPE ) (22 NILTYPE )
```

```
          (23 NILTYPE ) (24 NILTYPE ) (25 NILTYPE ) (26 NILTYPE )
          (27 NILTYPE ) (28 NILTYPE ) (29 NILTYPE ) (30 NILTYPE )
          (31 NILTYPE ) (32 NILTYPE ) (33 NILTYPE ) (34 NILTYPE )
          (35 NILTYPE ) (36 NILTYPE ) (37 NILTYPE ) (38 NILTYPE )
          (39 NILTYPE ) (40 NILTYPE ) (41 NILTYPE ) (42 NILTYPE )
          (43 NILTYPE ) (44 NILTYPE ) (45 NILTYPE ) (46 NILTYPE )
          (47 NILTYPE ) (48 NILTYPE ) (49 NILTYPE ) (50 NILTYPE )
          (51 NILTYPE ) (52 NILTYPE ) (53 NILTYPE ) $
>change
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
EXP_PSIDES: Y
>
EXP_TAB: 0     DS1          DEFAULT N
>
EXP_TAB: 1     DS1          DEFAULT N
>
EXP_TAB: 2     DS1          DEFAULT N
>
EXP_TAB: 3     DS1          DEFAULT N
>
EXP_TAB: 4 NILTYPE
>
EXP_TAB: 5 NILTYPE
>
EXP_TAB: 6 NILTYPE
>
EXP_TAB: 7 NILTYPE
>
EXP_TAB: 8 NILTYPE
>
EXP_TAB: 9 NILTYPE
>
EXP_TAB: 10 NILTYPE
>
EXP_TAB: 11 NILTYPE
>
EXP_TAB: 12 NILTYPE
>
EXP_TAB: 13 NILTYPE
>
EXP_TAB: 14 NILTYPE
>
EXP_TAB: 15 NILTYPE
>
EXP_TAB: 16 NILTYPE
>
EXP_TAB: 17 NILTYPE
>
EXP_TAB: 18 NILTYPE
>
EXP_TAB: 19 NILTYPE
>
EXP_TAB: 20 NILTYPE
>
EXP_TAB: 21 NILTYPE
>
EXP_TAB: 22 NILTYPE
>
EXP_TAB: 23 NILTYPE
>
EXP_TAB: 24 NILTYPE
>
```

```
EXP_TAB: 25 NILTYPE
>
EXP_TAB: 26 NILTYPE
>
EXP_TAB: 27 NILTYPE
>
EXP_TAB: 28 NILTYPE
>
EXP_TAB: 29 NILTYPE
>
EXP_TAB: 30 NILTYPE
>
EXP_TAB: 31 NILTYPE
>
EXP_TAB: 32 NILTYPE
>
EXP_TAB: 33 NILTYPE
>
EXP_TAB: 34 NILTYPE
>
EXP_TAB: 35 NILTYPE
>
EXP_TAB: 36 NILTYPE
>
EXP_TAB: 37 NILTYPE
>
EXP_TAB: 38 NILTYPE
>
EXP_TAB: 39 NILTYPE
>
EXP_TAB: 40 NILTYPE
>
EXP_TAB: 41 NILTYPE
>
EXP_TAB: 42 NILTYPE
>
EXP_TAB: 43 NILTYPE
>
EXP_TAB: 44 NILTYPE
>
EXP_TAB: 45 NILTYPE
>
EXP_TAB: 46 NILTYPE
>
EXP_TAB: 47 NILTYPE
>
EXP_TAB: 48 NILTYPE
>
EXP_TAB: 49 NILTYPE
>
EXP_TAB: 50 NILTYPE
>
EXP_TAB: 51 NILTYPE
>
EXP_TAB: 52 NILTYPE
>52 DS30A
EXP_TAB: 53 NILTYPE
>
TUPLE TO BE CHANGED:
      SMA2   3
          Y (0 DS1 DEFAULT N) (1 DS1 DEFAULT N)
          (2 DS1 DEFAULT N) (3 DS1 DEFAULT N) (4 NILTYPE ) (5 NILTYPE )
          (6 NILTYPE ) (7 NILTYPE ) (8 NILTYPE) (9 NILTYPE ) (10 NILTYPE )
          (11 NILTYPE ) (12 NILTYPE ) (13 NILTYPE ) (14 NILTYPE )
```

```
          (15 NILTYPE ) (16 NILTYPE ) (17 NILTYPE ) (18 NILTYPE )
          (19 NILTYPE ) (20 NILTYPE ) (21 NILTYPE ) (22 NILTYPE )
          (23 NILTYPE ) (24 NILTYPE ) (25 NILTYPE ) (26 NILTYPE )
          (27 NILTYPE ) (28 NILTYPE ) (29 NILTYPE ) (30 NILTYPE )
          (31 NILTYPE ) (32 NILTYPE ) (33 NILTYPE ) (34 NILTYPE )
          (35 NILTYPE ) (36 NILTYPE ) (37 NILTYPE ) (38 NILTYPE )
          (39 NILTYPE ) (40 NILTYPE ) (41 NILTYPE ) (42 NILTYPE )
          (43 NILTYPE ) (44 NILTYPE ) (45 NILTYPE ) (46 NILTYPE )
          (47 NILTYPE ) (48 NILTYPE ) (49 NILTYPE ) (50 NILTYPE )
          (51 NILTYPE ) (52 DS30A ) (53 NILTYPE ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
SMA2 3 UNIT 1 is not in service and not accepting static data.
Static data will be sent on next RTS.
WARNING: Static data needs to be updated for:
         SMA2 3
         BSY the INACTive unit, RTS and SWACT the peripheral.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

4.5.2.1.6 Table release history update

The following changes have been made to table LTCPSINV in this release:

1. A single DS30A type P-side link can be added to SMA2 peripherals on link 52.

4.5.2.1.7 Supplementary information

There are a number of restrictions on how the provisioning of the DS30A link on the SMA2 can be done. The following list defines the set of restrictions.

Note: DS30A provisioning, and any associated restrictions, for LTCs and LGCs have not been changed and are not impacted by the restrictions listed here. These restrictions apply to the SMA2 only.

Limitations:

- There can be a maximum of 1 P-side DS30A link on an SMA2, and hence a maximum of 1 RMM subtending an SMA2.
- The DS30A uses link 52 regardless of whether this is a single or extension shelf system. Prior to this activity link 52 was not used by the SMA2 and therefore using this link does not impact any existing configurations. Any attempt to add the DS30A on a link other than 52 will result in an error.
- The DS30A cards can only be located in slots 13 and 15 of the main shelf of an SMA2 system (regardless of whether the system has an extension shelf or not). Due to a backplane restriction the cards will not fit into any other slot in the main shelf. The DS30A cards cannot be placed into any slot in the extension shelf.

  Note: Slots 13 and 15 of existing SMA2 systems will have a 0X50AA filler cards in them prior to this activity. These slots were previously unused by the SMA2 as there was no supported card that fit into these slots. To add

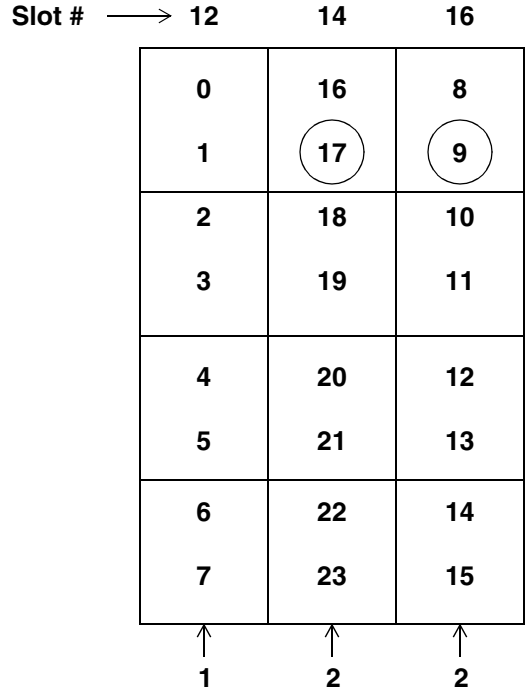
the MX74 DS30A cards to an SMA2 these filler cards will need to be removed to allow installation.

Note: Two DS30A cards need to be installed into the SMA2 to ensure that the DS30A link is kept in service at all times as one card serves each unit of the XPM. Port 52 only terminates on the back of slot 15 in the SMA2 due to the hardware design of the shelf, but the two DS30A cards are linked on the backplane of the shelf to allow either card to communicate on port 52 depending on which card is active.

- There are no restrictions on the provisioning of DS-1s/DCHs and the DS30A link in an SMA2 as the DS30A uses a link number that is not used by any of the other type of p-side links.

Figure 1, "SMA2 Existing Slot and Link Usage Restrictions - Main Shelf" and Figure 2, "SMA2 Existing Slot and Link Usage Restrictions - Extension Shelf" show the existing slot and link restrictions for the SMA2. These diagrams are duplicates of those found in the existing SMA2 (ESMA) Maintenance NTP (297-8263-550) in the “SMA2 Hardware” Chapter. They are provided here for reference only. The NTP diagrams are the master copies of these and take presidence over these versions.

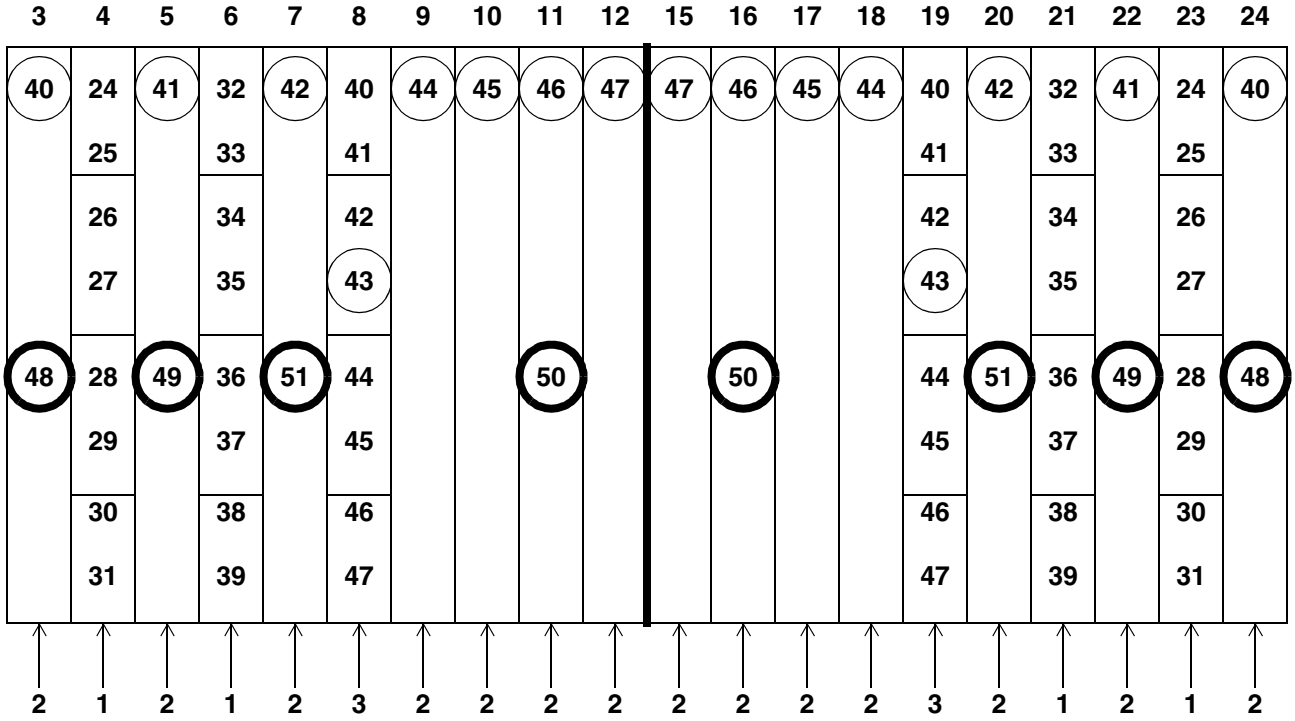
Figure 1 SMA2 Existing Slot and Link Usage Restrictions - Main Shelf



The bottom numbers indicate the type of cards that can be contained in the slot:
1 = DS-1
2 = DS-1 or DCH

NOTE: The allowed link numbers for DCH are circled.

Figure 2 SMA2 Existing Slot and Link Usage Restrictions - Extension Shelf



The bottom numbers indicate the type of cards that can be contained in the slot:
1 = DS-1 Only
2 = DCH Only
3 = DS-1 or DCH

NOTE: The allowed link numbers for DCH are circled, with the normal bold circles being those for the DCH links in the special initial configuration (48 DS-1s and 4 DCHs). The non-bold circles indicate the possible locations for the DCHs when not in the special initial configuration. The link numbers that are not circled are those used by the DS-1 cards with the exception of 43, which can be a DS-1 link or a DCH link depending on which type of card is in slot 8/19.

4.5.2.1.8 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

4.5.2.2 Name: TABLE RMMINV

Long Table Name: Remote Maintenance Module Inventory

4.5.2.2.1 Functional description

Table RMMINV contains the inventory list for all the RMMs provisioned in the office. Each tuple contains the RMM's site, the PEC code for the hardware,

information about the RMM load, the EXEC lineup for the RMM, and finally, a pointer to the C-side peripheral upon which the RMM is hosted.

This activity has altered this table to allow the C-side PM to include a new set of allowable XPM types, including LGC, LTC, and SMA2.

Note: Although official support of the LTC is added with this activity there are no code changes needed for this as the table already allowed an LTC to be the host peripheral for an RMM prior to this release.

Note: It should also be noted that LGCI and LTCIs are also supported as host peripherals for the RMM; however, the distinction between the LTC/LGC and their ISDN counterparts (LTCI/LGCI) is strictly done based on where ISDN subtending devices are provisioned on the host. There is no actual LTCI or LGCI XPM type defined in the DMS, they are known only as LTCs or LGCs.

4.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

4.5.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RMMINV	Unchanged by this activity	Unchanged by this activity	Unchanged by this activity.

4.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for RMMINV.

CSPMINFO = “<RMMSMA2 or RMMLTC> <XPM Key from LTCINV> <Port Number of DS30A Link from LTCPSINV>”

For Example:

CSPMINFO = “RMMSMA2 SMA2 0 52”

where “SMA2 0” is the XPM key from LTCINV and “52” is the port number in LTCPSINV of a DS30A link on SMA2 0.

Note: It should be noted that the RMM Selector for the LTC and LGC peripherals is the same (RMMLTC). This is due to the fact that these two

peripherals are simply variations of the same hardware, and are also treated identically in the software.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSPMINFO	Changed	New RMM Selector of RMMSMA2 has been defined for adding RMMs to SMA2 ABI XPMs.	RMMSMA2	When RMMSMA2 is entered as the RMM Selector for the CSPMINFO field the user is then prompted for the SMA name/number and the DS30A port to use. The DS30A port number must match that provisioned in table LTCPSINV for the SMA2 (52 is the only allowed link number for a DS30A on an SMA2).
CSPMINFO	Changed	The handling of the CSIDEPM has been modified such that when an RMM Selector of RMMLTC is entered the allowed C-side PM types now includes LTC and LGC.	CSIDEPM	When RMMLTC is entered as the RMM Selector for the CSPMINFO field the user is then prompted for the name/number of the LTC/LGC and the DS30A port to use (fields CSIDEPM and CSIDPORT). The DS30A port number must match that provisioned in table LTCPSINV for the XPM.

4.5.2.2.5 Datafill example

The following 3 examples show sample datafill for table RMMINV. The first example shows the provisioning of an RMM hosted on an SMA2, the second shows the provisioning of an RMM on an LTC, and the third shows the provisioning of an RMM on an LGC. The changes from the prior allowed datafill is highlighted with **bold** characters.

Example #1 - RMM hosted on SMA2:

```
CI:
>table rmminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: RMMINV
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RMMNAME:
>rmms rmm 8
FRTYPE:
>mis
FRNO:
>5
SHPOS:
>44
FLOOR:
>3
ROW:
>c
FRPOS:
>2
EQPEC:
>6x13aa
LOAD:
>rmm10a
EXECS:
>rsmex
RMMSELECTOR:
>rmmsma2
CSIDEPM:
>sma2 3
CSIDPORT:
>52
TUPLE TO BE ADDED:
RMMS        RMM   8    MIS    5    44     3   C     2 6X13AA   RMM10A
   RSMEX RMMSMA2       SMA2      3 52
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Static data update for GWC  0 UNIT 0 submitted.
Static data update for GWC  0 UNIT 1 submitted.
SMA2 3 UNIT 0 is not in service and not accepting static data.
Static data will be sent on next RTS.
SMA2 3 UNIT 1 is not in service and not accepting static data.
Static data will be sent on next RTS.
Static data updates completed.
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

Example #2 - RMM hosted on LTC:

```
CI:
>table rmminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: RMMINV
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RMMNAME:
>rmms rmm 5
```

```
FRTYPE:
>mis
FRNO:
>4
SHPOS:
>20
FLOOR:
>2
ROW:
>m
FRPOS:
>1
EQPEC:
>6x13aa
LOAD:
>rmm10a
EXECS:
>rsmex
RMMSELECTOR:
>rmmltc
CSIDEPM:
>ltc 0
CSIDPORT:
>18
TUPLE TO BE ADDED:
RMMS        RMM   5    MIS    4    20     2   M     1 6X13AA   RMM10A
   RSMEX  RMMLTC        LTC      0 18
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Static data update for LTC  0 UNIT 0 submitted.
Static data update for LTC  0 UNIT 1 submitted.
Static data updates completed.
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

Example #3 - RMM hosted on LGC:

```
CI:
>table rmminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: RMMINV
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RMMNAME:
>rmms rmm 5
FRTYPE:
>mis
FRNO:
>4
SHPOS:
>20
FLOOR:
>2
ROW:
>m
FRPOS:
>1
EQPEC:
>6x13aa
LOAD:
```

```
>rmm10a
EXECS:
>rsmex
RMMSELECTOR:
>rmmltc
CSIDEPM:
>lgc 1
CSIDPORT:
>12
TUPLE TO BE ADDED:
RMMS        RMM   5    MIS    4    20     2   M     1 6X13AA   RMM10A
   RSMEX  RMMLTC        LGC 1 12
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Static data update for LGC 1 UNIT 0 submitted.
Static data update for LGC 1 UNIT 1 submitted.
Static data updates completed.
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

4.5.2.2.6 Table release history update

The following changes have been made to table RMMINV in this release:

1. New RMMSELECTOR of RMMSMA2 has been added.
2. CSIDEPM of SMA2 is now allowed when the RMMSELECTOR is RMMSMA2.
3. The CSIDPORT for SMA2 type CSIDEPM must be between 0 and 53, and must match that provisioned in table LTCPSINV for the SMA2 (port 52, although there is no specific error checking for this in RMMINV, it is enforced through table LTCPSINV).
4. For RMMSELECTOR of RMMLTC the following peripheral types are now supported for the CSIDEPM field:
   — LTC
   — LGC
5. The CSIDPORT for peripherals with a RMMSELECTOR of RMMLTC must be between 0 and 19.

4.5.2.2.7 Supplementary information

Limitations:

- The RMM is only supported on the LGC, LTC, and SMA2 ABI XPMs. It should also be noted that the RMM is not supported on the legacy (ENET-based) versions of these peripheral types.
- The CHANGE operation cannot alter the content of the C-side Port portion of the tuple. Any attempt to alter this value will result in an error and the tuple will be rejected by table control. If the C-side port information needs to be altered then the RMM must be deleted and re-added to the table. Note

that this is not new behavior, it simply reflects the existing restriction for RMMs.

4.5.2.2.8 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

4.5.2.3 Name: TABLE LTCINV

Long Table Name: Line Trunk Controller Inventory

4.5.2.3.1 Functional description

Table LTCINV contains a list of all the provisioned LTC-type peripherals in the system. ABI-based XPMs are datafilled in this table and are distinguished by the addition of the EXTDS512 optional attribute to their tuples.

This activity alters the functionality of LTCINV to allow the provisioning of a new type of EXEC for the SMA2 peripherals. To support the functionality of the RMM on the SMA2 the RSMEX EXECs need to be downloaded to the SMA2 when the SMA2 is RTSed. Prior to this activity this set of EXECs were not allowed to be provisioned against an SMA2. This is an existing set of EXECs that just needs to be sent to the SMA2.

Note: These EXECs need to be provisioned against the host peripheral for the RMM, which also can now include the LTC and LGC. Although we did not officially support the LTC and LGC prior to this release they were allowed to have the RSMEX EXECs provisioned against them already, so no work was done by this activity to support this.

4.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

4.5.2.3.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	Unchanged by this activity	Unchanged by this activity	Unchanged by this activity.

4.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for LTCINV.

EXECTAB = “RMM_TERM RSMEX”

When adding a subtending RMM on an LTC, LGC, or SMA2 the EXECTAB field needs to include RMM_TERM RSMEX. This can be done either at the time the XPM is first provisioned or can be added at a later date using the CHANGE command.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
EXECTAB	Changed	Unchanged from the existing set of EXECs.	RMM_TERM RSMEX	RSMEX EXECs need to be downloaded to the host peripheral for the RMM. The LTC/ LGC already supported this set of EXECs but the SMA2 did not.

4.5.2.3.5 Datafill example

The following example shows sample datafill for table LTCINV. The example shown below demonstrates the addition of RSMEX EXECs to an SMA2 using the CHANGE command. The changes from the prior allowed SMA2 peripheral datafill is highlighted with **bold** characters.

```
CI:
>
>table ltcinv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
>pos sma2 3
      SMA2   3
           2003    CMVI    1     1      1    F    22 MX85AB  XM219AZ
                           (         POTS   POTSEX) (       KEYSET   KSETEX)$
                (        4  7) (        4  8) (        4  9) (        4 10)$
           (UTR6 ) (MSGMX76 HOST ) (CMR5 CMR10A) (ISP 4) $
     NORTHAM                                                  AX74AA  AX74AA
                                                        0
                              NILLOAD
                                  (EXTDS512 192   2  25  65        GWC   0)$
     6X40FB                                           N
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
ADNUM: 2003
>
FRTYPE: CMVI
>
FRNO: 1
>
SHPOS: 1
>
FLOOR: 1
>
ROW: F
>
```

```
FRPOS: 22
>
EQPEC: MX85AB
>
LOAD: XM219AZ
>
EXECTAB: POTS   POTSEX
>
EXECTAB: KEYSET   KSETEX
>
EXECTAB:
>RMM_TERM RSMEX
EXECTAB:
>$
CSLNKTAB: 4  7
>
CSLNKTAB: 4  8
>
CSLNKTAB: 4  9
>
CSLNKTAB: 4 10
>
CSLNKTAB:
>$
OPTCARD: UTR6
>
OPTCARD: MSGMX76
>
MX76LOC: HOST
>
OPTCARD: CMR5
>
CMRLOAD: CMR10A
>
OPTCARD: ISP
>
SLOT_NUMBER: 4
>
OPTCARD:
>$
TONESET: NORTHAM
>
PROCPEC: AX74AA  AX74AA
>
EXTLINKS: 0
>
E2LOAD: NILLOAD
>
OPT_ATTR: EXTDS512
>
IPADDR: 192   2  25  65
>
GWC_HOST: GWC   0
>
OPT_ATTR:
>$
PEC6X40: 6X40FB
>
EXTSHELF: N
>
TUPLE TO BE CHANGED:
      SMA2   3
           2003    CMVI    1     1      1    F    22 MX85AB  XM219AZ
 (         POTS   POTSEX) (       KEYSET   KSETEX) (     RMM_TERM    RSMEX)$
```

```
(        4  7) (        4  8) (        4  9) (        4 10)$
          (UTR6 ) (MSGMX76 HOST ) (CMR5 CMR10A) (ISP 4) $
     NORTHAM                                                AX74AA  AX74AA
                                                      0
                              NILLOAD
                                  (EXTDS512 192   2  25  65        GWC   0)$
     6X40FB                                             N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

4.5.2.3.6 Table release history update

The following changes have been made to table LTCINV in this release:

1. EXECTAB field for SMA2, LGC, and LTC can now include "RMM_TERM RSMEX"

4.5.2.3.7 Supplementary information

Limitations:

- The RMM is only supported on the LGC, LTC, and SMA2 ABI XPMs, not on the SMS.

4.5.2.3.8 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

4.6 Service Orders (SO) (CM & SESM)

Not Applicable

4.7 Software optionality control (SOC)

Not Applicable

4.8 Element Management

Not Applicable

4.9 Command interface changes

4.9.1 Directory: MAPCI;MTC;PM

4.9.1.1 Directory description

No new commands or parameters have been introduced. However an RMM has been introduced as a subtending peripheral of an LTC, LGC, and SMA2. Existing maintenance actions through the MAP are supported for an RMM subtending these peripherals.

4.9.1.2 Accessing directory: PM

4.9.1.2.1 Access to directory or MAP level and return to CI

The updated displays are accessed through the PM (peripherals) level of the maintenance (MTC) level of the DMS core command interface (MAPCI). The RMM must be posted to perform maintenance actions on the RMM.

4.9.2 Command: TRNSL C

4.9.2.1 Command type: Listed MENU

4.9.2.2 Command target: All

This functionality will only be used in Succession ABI loads, but the software exists in all loads.

4.9.2.3 Command availability: RES

4.9.2.4 Command description

TRNSL C (translate c-side links) is not a new command, however when an RMM subtends an LTC, LGC, or SMA2, a TRNSL C of the RMM will display its c-side link.

Note that the supertending[1] peripheral is an ABI peripheral, and a TRNSL C of that peripheral will provide additional ABI information.

4.9.2.5 Command syntax

Table 8 TRNSL C

Command	Parameters and variables
TRNSL C	unchanged
Parameters and variables	unchanged

4.9.2.6 Example

Usage example for "MAPCI;MTC;PM; POST RMM <X>;TRNSL C" command

[1]The phrase "supertend peripheral" defines the peripheral which is immediately to the Cside of the peripheral being described. The phrase is meant to distinguish it from "host" peripheral, which sometimes implies the peripheral connected to the Network.

```
XAC       MS      IOD      Net       PM     CCS      Lns      Trks     Ext      APPL
 Split     Istb    NO AMA     .       1 RCU  1    RS     .       75CC.    1Crit     .
                     *C*                 *C*      *C*                *C*      *C*
RMM                                     SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit           PM                       9        0        0        0       19       34
 2 Post_          RMM                      0        0        0        0        0        3
 3 ListSet
 4              RMM          0    InSv
 5 TRNSL        TRNSL  c
 6 TST          LINK 52: LTC 0 5;CAP:MS;STATUS: OK       ;MsgCond:OPN
 7 BSY
 8 RTS
 9 OffL
10 LoadPM_
11 Disp_
12 Next_
13
14 QueryPM
15
16
17
18
  SARAH
Time  11:51  >
```

RMM is posted.

Supertending peripheral can be one of LTC, LGC or SMA2.

4.9.3 Command: TRNSL P

4.9.3.1 Command type: Listed MENU

4.9.3.2 Command target: All

But will only be seen in Succession ABI loads.

4.9.3.3 Command availability: RES

4.9.3.4 Command description

TRNSL P (translate p-side links) is not a new command, however when an RMM subtends an LTC, LGC, or SMA2, a TRNSL P of the supertending peripheral will display the p-side links of the peripheral as connecting to a RMM on the applicable port.

Note that the supertending peripheral is an ABI peripheral, and a TRNSL C of that peripheral will provide additional ABI information.

4.9.3.5 Command syntax

Table 9 TRNSL P

Command	Parameters and variables
TRNSL P	unchanged
Parameters and variables	unchanged

4.9.3.6 Example

Usage example **"MAPCI;MTC;PM; POST <XPM>;TRNSL P" command**

```
XAC      MS      IOD      Net      PM      CCS      Lns      Trks     Ext      APPL
 Split    Istb    NO AMA     .      1 RCU   1    RS     .      75CC.    1Crit     .
                   *C*               *C*      *C*               *C*      *C*
 RCC2                                SysB     ManB     OffL     CBsy     ISTb     InSv
  0 Quit          PM                    9        0        0        0       19       34
  2 Post_         LTC 0        0        0        0        2        0
  3 ListSet
  4 BITS       LTC 0 ISTb  Links_OOS: CSide  0 , PSide  8
  5 Trnsl_     Unit0:   Inact ISTb
  6 Tst_       Unit1:   Act   ISTb
  7 Bsy_       Trnsl  p
  8 RTS_       Link  1: Carrier of Class - Trunk ;Status:SBsy
  9 Offl       Link  2: Carrier of Class - Trunk ;Status:SBsy
 10 LoadPM_    Link  3: Carrier of Class - Trunk ;Status:SBsy
 11 Disp_      Link  4: Carrier of Class - Trunk ;Status:SBsy
 12 Next      Link  5: RMM 0              0;Cap MS;Status:OK      ;MsgCond:OPN
13 SwAct     Link  6: Carrier of Class - Trunk ;Status:SBsy
 14 QueryPM   Link  7: Carrier of Class - Trunk ;Status:SBsy
 15 DCH       Link 10: DCH 5;Status:OK
 16 IRLINK    Link 17: DCH 6;Status:OK
 17 Perform
 18 ISG
   SARAH
 Time  11:56  MORE...
```

LTC posted. Could also be LGC or SMA2

RMM is displayed on appropriate link.

4.10 Security

Not Applicable

4.11 Configuration Walkthrough

The following lists the steps to provision and RMM hosted on an existing SMA2 ABI XPM:

1. Upgrade all Succession components (Core, GWC, MG9K, etc.) to SN06.2.
2. Install RMM and Power up.
3. Install DS30A boards (MX74) in slot 13 and 15 of an SMA2 shelf following existing procedure for MX74 installation for RCC2 shelf. One place this procedure is defined is in "DMS-100 Family NA100 Card Replacement Procedure Vol 7 of 7 LEC0015 and up". There is a section within this document entitled "NTMX74 in an RSC-S (DS-1) Model A RCC2".
4. Install the DS30A cable from the SMA2 (port 52) to the RMM.
5. Provision LTCINV for the SMA2 which supertends the RMM with EXECTAB set to "RMM_TERM RSMEX".
6. Table LTCPSINV - Change the new SMA2 tuple to include a DS30A link on the SMA2 in P-side port 52 for the RMM (note the restrictions on where this link may exist are documented earlier in this chapter).

7. Table RMMINV - Add a new RMM to point to the SMA2 as it's CSIDEPM with the CSIDPORT set to the same port number as the DS30A datafilled in step #6 (52).
8. Once this is complete the new SMA2 can be RTSed and brought into service and it should download the RSMEX EXECs..
9. Test the DS30A cable by running a DS30A test from the map with SMA2 XPM posted.
10. RTS the DS30A link.
11. Load and RTS the RMM.

5: Configuration (CN): A00002009

5.1 Data schema (DS)

- Table KSETFEAT: The name up to 24 characters provided by this feature will be stored in this table.
- Table LCCOPTS: The list of compatible LCCs of this feature will be specified here.

5.2 Service Orders (SO)

5.2.1 Summary of service order impact

NAME24 must be added to a set via SERVORD.

5.2.2 Service order change details

- IDENTIFY any NEW LCC introduced by this feature:

  None.
- IDENTIFY any NEW OPTIONS introduced by this feature:

  NAME24.
- FOR EACH OPTION, list other options that must be assigned:

  NAME option must be assigned for NAME24 option to work.

5.2.3 Line class code compatibility

Compatible LCCs in the CCM layer:

- PSET
- P_Phone
- M5008
- M5009
- M5208
- M5209
- M5112
- M5212
- M5312

- M5216
- M5316

Compatible LCCs in the MSL layer

- P_Phone
- PSET
- M5008
- M5009
- M5208
- M5209
- M5112
- M5212
- M5312
- M5216
- M5316
- M2008
- M2616
- M2216A
- M2216B
- M2008
- M2016s
- M2616ct.

5.2.4 Assignability

The following functionalities apply to this option:

- set functionality: <no>
- subset functionality: <no>
- DN functionality: <yes>
- key functionality: <no>

5.2.5 Option prerequisites

NAME24 has the following prerequisites:

NAME.

5.2.6 New Prompts

Table 1 New Prompt

Prompt Text	Valid Input	Description	Areas Affected by Prompt
DISPLAY_NAME	Vector of up to 24 chars	This field is used to enter up to 24 characters to be displayed	OPTION

5.2.7 SERVORD examples

NAME option must be on the line

```
>ado
SONUMBER:    NOW  3  4  9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>yourNameUpto24Characters
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME24 TESTINGTSTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
NAME24 CAN ONLY BE ADDED TO A LINE AFTER
THE NAME OPTION HAS BEEN ADDED.
```

—continued—

```
NAME24 did NOT pass checking.
***  ERROR - INCONSISTENT DATA  ***
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME24 TESTINGTSTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>n
```

Add NAME and NAME24 together

```
>ado
SONUMBER:    NOW   3  4  9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name
NETNAME:
>public
DISPLAYNAME:
>NameForPublic
NETNAME:
>$
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>nameUpto24Characters
OPTKEY:
>$
```

—continued—

```
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME ( PUBLIC TESTING15 ) $ ) ( 1 NAME24
TESTINGTESTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Query the DN

```
>qdn 7502537
--------------------------------------------------------------------------------
DN:     7502537
TYPE: SINGLE PARTY LINE
SNPA: 909   SIG:  N/A    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 18 19
LINE CLASS CODE:  M5209 SET
KEY:  1
CUSTGRP:            CGA  SUBGRP: 0  NCOS: 0  RING: Y
CARDCODE:  6X21AC    GND: N  PADGRP: PPHON  BNV: NL MNO: Y
PM NODE NUMBER     :   67
PM TERMINAL NUMBER :    596
OPTIONS:
NAME PUBLIC NAMEFORPUBLIC 3WC CWI CWO
PIC C541 Y NAME24 NAMEUPTO24CHARACTERS CWT Y Y N 1 CFU N $ I 1 CWD PRL
```

Query table KSETFEAT

```
>table ksetfeat
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: KSETFEAT
>
>pos 0 0 18 19 name24
HOST  0 0 18 19 1   NAME24      NAME24       NAMEUPTO24CHARACTERS
```

Can't delete NAME if NAME24 is on the line

```
>deo
SONUMBER:    NOW   3  4  9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 3 4 9 PM 7502537 ( 1 NAME ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
CANNOT DELETE NAME FROM A LINE IF NAME24 EXISTS.
NAME did NOT pass checking
***  ERROR - INCONSISTENT DATA  ***
COMMAND AS ENTERED:
DEO NOW 3 4 9 PM 7502537 ( 1 NAME ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>n
```

5.3 Software optionality control (SOC)

— Option assignment via SERVORD will not be limited by the SOC states (On or Off).

— Option processing will be performed only when the SOC state is On.

Table 2 SOC

SOC option name:	Enh Name/Num Dis
SOC option title:	00036430
SOC option control type:	state
New SOC option?	Yes
SOC option order code	MDC00075
Option defined in DRU:	CCM
Affected products:	CCM

6: Configuration (CN): A00002012

6.1 Command interface changes

Currently on XA-Core, the CMIC functionality on packlet is provided by a CMIC link. The RTIF functionality on packlet is provided by an RTIF port. With the introduction of the CMIC/RTIF HIOP card, port/link separation will be implemented for the CMIC and RTIF functionalities on HIOP. That is, both services will be maintained by a port and a link. Hence, the CMIC and RTIF MAP levels have to change to reflect the new port/link separation.

> **Note:** this feature does not implement port/link separation on CMIC and RTIF packlets.

Port/link separation has already been done for the ETHR and AMDI functionality on the HIOP card by the Ethernet Maintenance feature (A59019176) and the HIOP ATM Maintenance software feature (A59035251). In order to have consistent MAP representation of ports and links in the XA-Core system, this feature will reuse the OAM design decisions applied for those features.

6.1.1 IO MAP level

Currently on the IO MAP level, the CMIC and RTIF functionality are only represented on packlets in lower and upper positions. No ‘middle’ packlets exist. Please refer to “Figure 1 IO MAP with CMIC and RTIF packlets on IOPs in slots 4R and 15R” on page 2421. With the introduction of the CMIC/RTIF HIOP, these functionalities can be hosted on either packlets or HIOP cards. Please refer to “Figure 2 IO MAP with CMIC/RTIF HIOPs in slots 4R and 15R” on page 2421.

Figure 1 IO MAP with CMIC and RTIF packlets on IOPs in slots 4R and 15R

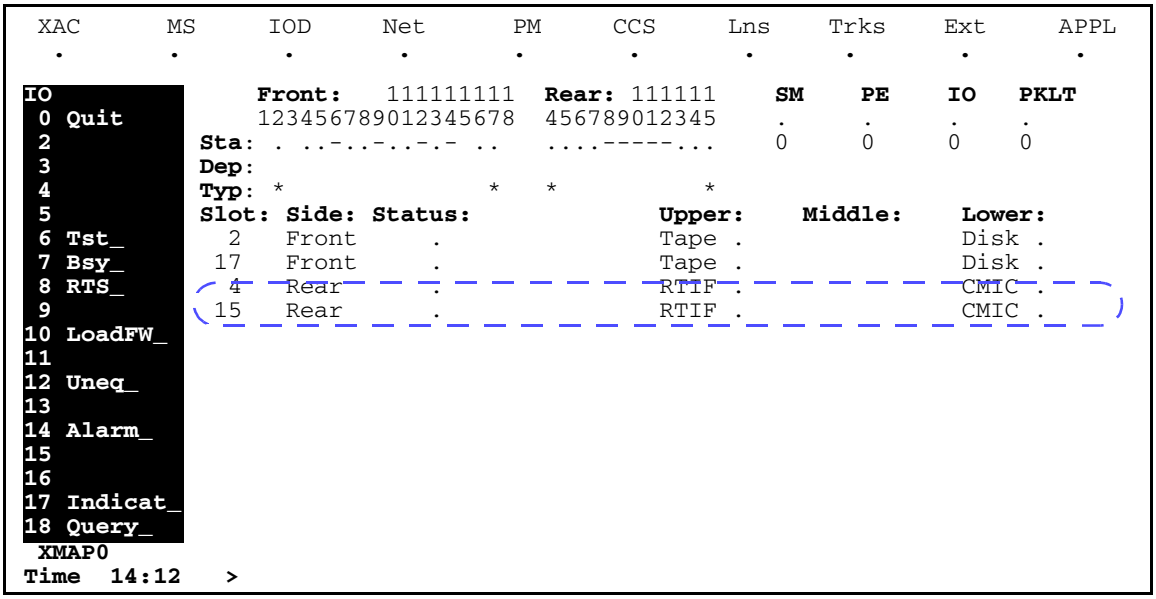
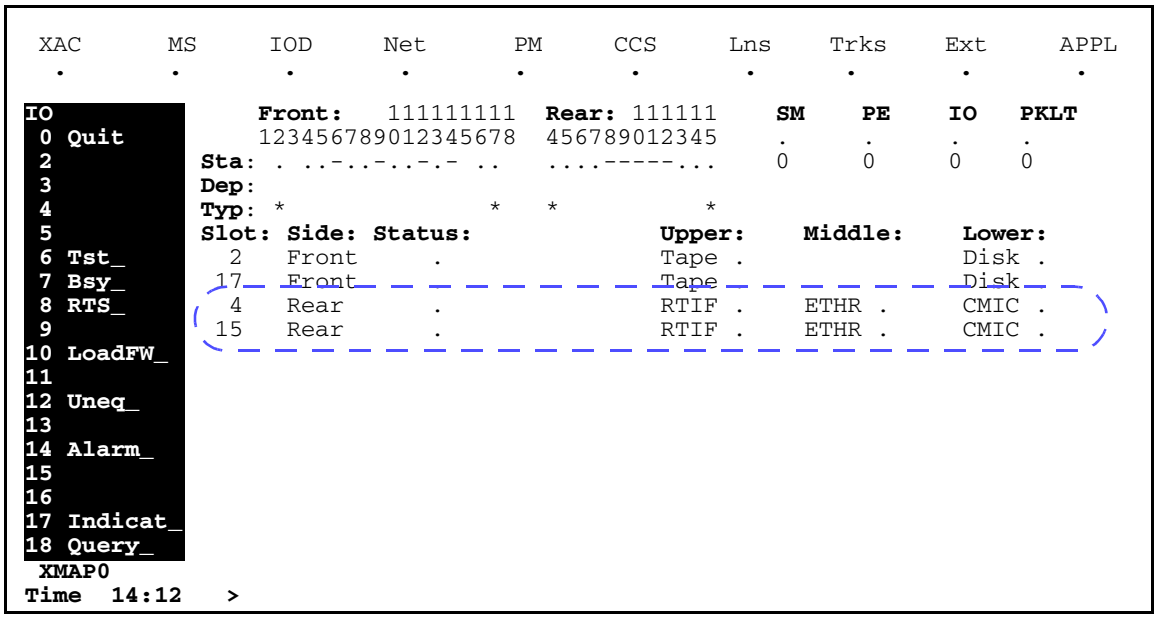


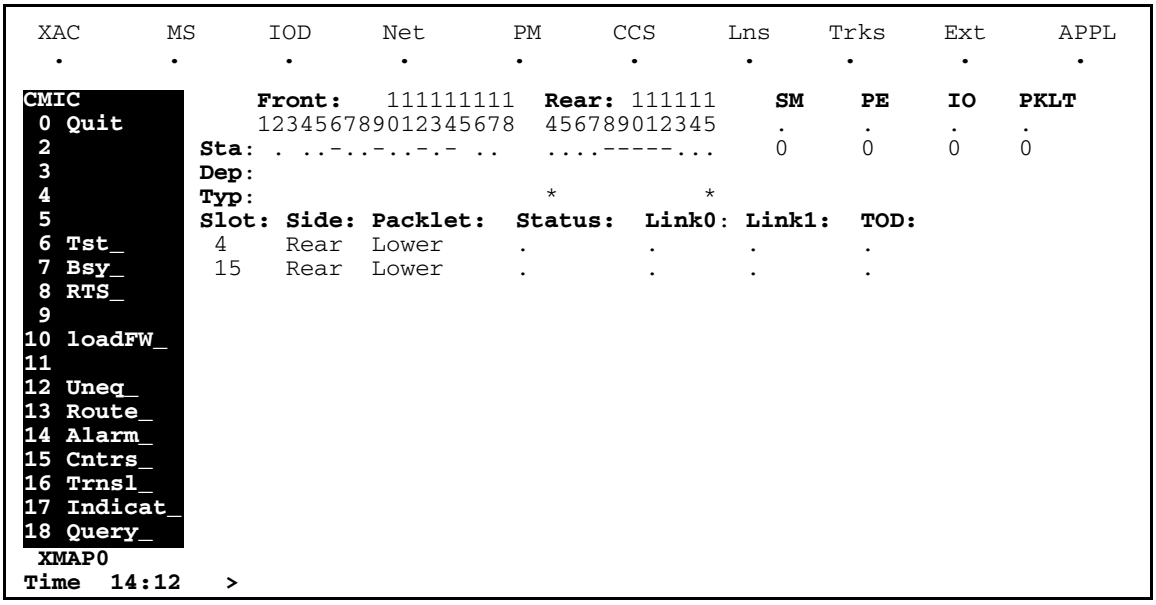
Figure 2 IO MAP with CMIC/RTIF HIOPs in slots 4R and 15R



6.1.2 CMIC MAP level

Currently, the CMIC functionality can only be hosted by a CMIC packlet on an IOP card. Please refer to “Figure 3 Current CMIC MAP level with CMIC packlets in slots 4R and 15R” on page 2422.

Figure 3 Current CMIC MAP level with CMIC packlets in slots 4R and 15R



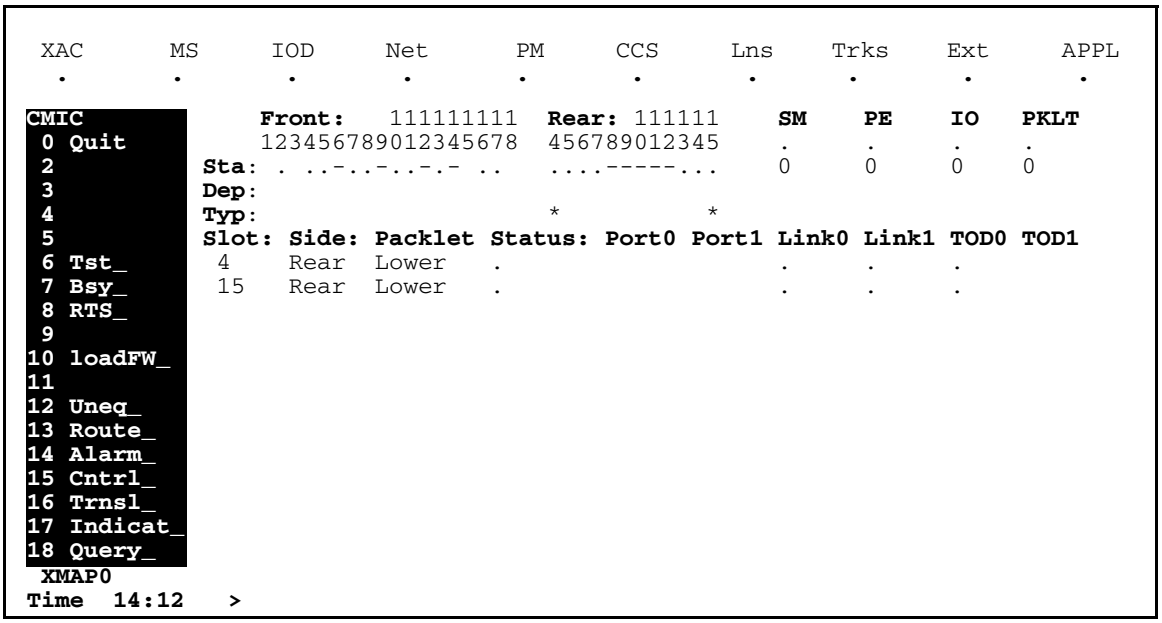
With the introduction of the CMIC/RTIF HIOP, the new CMIC MAP will show the functionality hosted by either a CMIC packlet on an IOP card, or by a CMIC/RTIF HIOP. Also, with CMIC port/link separation on CMIC/RTIF HIOP, new CMIC port0 and CMIC port1 components will be shown on the CMIC MAP level. Furthermore, instead of showing one TOD device component per CMIC packlet, two TOD devices will be shown for each CMIC/RTIF HIOP card: TOD0 and TOD1.

Table 1 Summary of CMIC MAP field changes

Component	Current MAP field	New MAP field	New/Deleted/ Changed
CMIC Port 0	n/a	‘Port0’	new
CMIC Port 1	n/a	‘Port1’	new
CMIC Link TOD	‘TOD’	‘TOD0’	changed
CMIC Link1 TOD	n/a	‘TOD1’	new

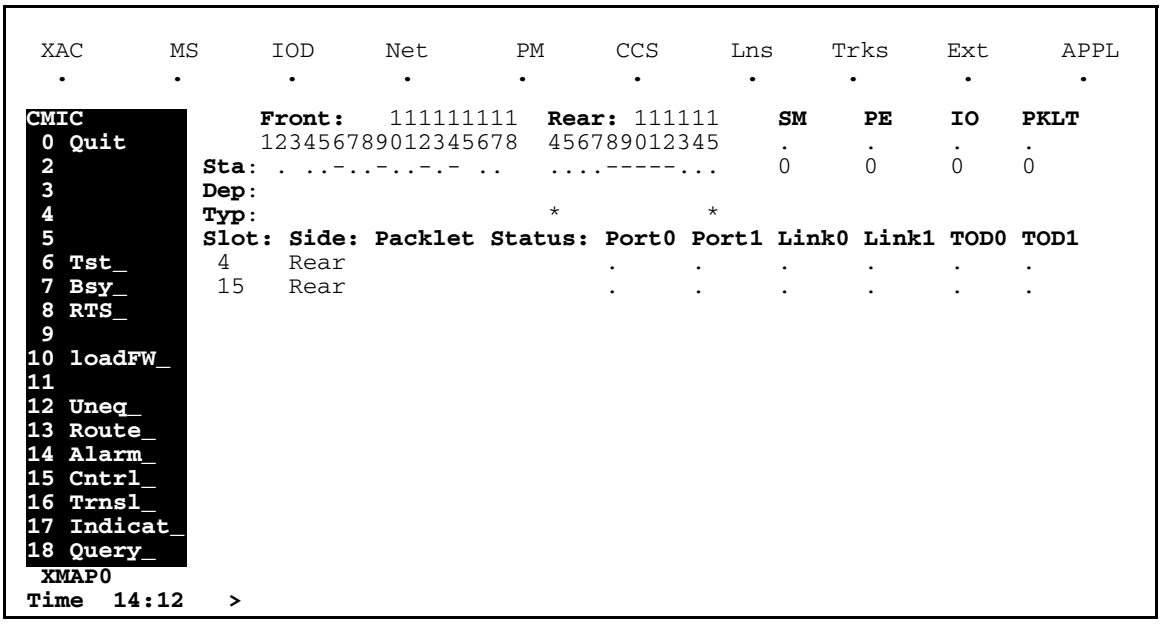
For CMIC packlets represented on the new CMIC MAP level, the following components will be shown as before: Slot, Side, Packlet, Status, link0, and link1. Port0 and port1 components will be left blank. The TOD component will be represented by the new TOD0 component. The TOD1 component will be left blank. Please refer to “Figure 4 New CMIC MAP level with CMIC packlets in slots 4R and 15R” on page 2423.

Figure 4 New CMIC MAP level with CMIC packlets in slots 4R and 15R



For CMIC functionality on CMIC/RTIF HIOP represented on the new CMIC MAP level, since the card does not have packlets, the ‘Packlet’ location field, and the packlet ‘Status’ field will be left blank. Also, in addition to the two CMIC links, there are going to be two new CMIC ports shown (Port0 and Port1), as well as two TOD devices for each CMIC/RTIF HIOP card (TOD0 and TOD1). Please refer to “Figure 5 New CMIC MAP level with CMIC/ RTIF HIOPs in slot 4R and 15R” on page 2424.

Figure 5 New CMIC MAP level with CMIC/RTIF HIOPs in slot 4R and 15R



The new CMIC MAP level will be able to show both, packlet and HIOP, configurations during the migration from one configuration to the other (e.g. CMIC packlet to CMIC/RTIF HIOP).

6.1.2.1 Command: uneq

With the introduction of the new CMIC/RTIF HIOP card, the CMIC packlets will have to be migrated to the new card. Hence, from now on, the XA-Core system will support the provisioning and deprovisioning of CMIC components. The ‘uneq’ command will be used for deprovisioning a CMIC packlet on an IOP card or a CMIC link on a CMIC/RTIF HIOP card. Currently CMIC packlet deprovisioning is not supported.

Table 2 New or modified CMIC MAP commands

Command Name	NEW, CHANGED or DELETED	Directory/MAP level name	MENU/NON-MENU/ HIDDEN
uneq	New	MAPCI;MTC;XAC;CMIC	Menu
trnsl	Changed	MAPCI;MTC;XAC;CMIC	Menu

6.1.2.1.1 Command description

The ‘uneq’ MAP command is used to deprovision a component from the XA-Core system. On the CMIC MAP level, the ‘uneq’ command will be used to deprovision a CMIC packlet residing on an IOP card, or to deprovision a

CMIC link residing on a CMIC/RTIF HIOP card. Until now, deprovisioning of CMIC packlets was not supported since they were part of the ‘fixed’ XA-Core configuration (slots 4R and 15R). From now on, deprovisioning of CMIC components is needed for the migration of CMIC packlets to CMIC/RTIF HIOP cards and back.

Table 3 Summary of the new ‘uneq’ CMIC MAP level command

Command	Menu#	Type	Options	Function
uneq	12	Operational	None	- Deprovision a CMIC packlet on an IOP card - Deprovision a CMIC link on an HIOP card

6.1.2.1.2 Command syntax

The ‘uneq’ command requires parameters. If you do not enter any parameters or you enter invalid parameters, the MAP terminal displays an error message. The MAP terminal prompts you to enter a correct parameter value.

Table 4 ‘uneq’ command parameters and variables

Command	Parameters and variables
uneq	- slot number (0 to 17), - side (front, f or rear, r), - packlet position (upper, u, or lower, l), - link number (link0 or link1).
Parameters and variables	**Description**
slot number	Use the ‘slot number’ parameter value to indicate the number of the physical shelf slot: 0 to 17
side	Use the ‘side’ parameter value to indicate the component location in the physical shelf: front, f or rear, r
packlet position	Use the ‘packlet position’ parameter value to indicate the CMIC packlet location on an IOP card: upper, u or lower, l. This is used only for CMIC packlet deprovisioning and is not used for CMIC link.
link number	Use the ‘link number’ parameter value to indicate the CMIC link position on a CMIC/RTIF HIOP card: link0 or link1. This is used only for CMIC link deprovisioning and is not used for CMIC packlets.

Note: The ‘slot number’ parameter value will usually be ‘4’ or ‘15’. The ‘side’ parameter value will usually be ‘rear’ or ‘r’. The ‘packlet position’ parameter value will usually be ‘lower’ or ‘l’.

6.1.2.1.3 Qualifications and warnings

The ‘uneq’ command should be used with great care since it deprovisions a component from the XA-Core system. There are some general requirements for the successful completion of the ‘uneq’ command. They are (in order):

- first, the component must be brought into a ‘ManB’ state,
- then, the component must be pulled from the shelf,
- finally, the ‘uneq’ command can be issued for the component.

Since the ‘uneq’ command on the CMIC MAP level can be issued for the CMIC packlet residing on an IOP card or for a CMIC link residing on an HIOP card, the command usage will be different depending on the component being deprovisioned. Please refer to Section “6.1.2.1.5 Example” on page 2428.

Note: Deprovisioning of CMIC links on packlets is not supported.

6.1.2.1.4 MAP Responses

Table 5 MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted. Uneq 4 Rear Lower completed. **Meaning:** This response indicates that the ‘uneq’ command has completed successfully. **System or user actions:** none
RESPONSE: Command submitted. Improper state for required action, no action take **Meaning:** this response indicates that the ‘uneq’ command has been issued without bringing the component into the ‘ManB’ state first. **System or user actions:** the craft person has to ‘ManB’ the component

Table 5 MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted H/W must be removed from shelf, no action taken **Meaning:** this response indicates that the ‘uneq’ command has been issued without removing the component from the shelf, or without waiting long enough for the system to recognize the component’s loss of clock. **System or user actions:** the craft person has to remove the component from the shelf. If the component is already removed, the craft person has to wait long enough (e.g. one minute) for the system to recognize the component’s loss of clock.
RESPONSE: Card/device is unadressable...no action taken. **Meaning:** this response indicates that there is no provisioned component in the given location. **System or user actions:** the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters **Meaning:** this response indicates that the ‘uneq’ command was issued without following the correct syntax. For example, the ‘link0’ or ‘link1’ parameter values were entered while deprovisioning a CMIC packlet on an IOP card (CMIC link deprovisioning not supported on packlets). **System or user actions:**
RESPONSE: <slot> <side> is an IOP. Packlet location must be specified **Meaning:** this response indicates that the ‘uneq’ command was issue for a CMIC packlet slot, but the packlet location parameter value (lower, l or upper, u) was not specified. **System or user actions:** re-enter the ‘uneq’ command with correct syntax.
RESPONSE: <slot> <side> is an HIOP. Packlet location does not apply. **Meaning:** this response indicates that the ‘uneq’ command was issued for a CMIC link on an HIOP card, but a packlet location parameter value was entered. **System or user actions:** re-enter the ‘uneq’ command with correct syntax.

6.1.2.1.5 Example

Table 6 Usage examples for 'uneq' command on the CMIC MAP level

Description of task: Command: MAP response:	Deprovision a CMIC packlet on an IOP card Example: uneq 4 rear lower Example: Command submitted. Uneq 4 Rear Lower completed
Description of task: Command: MAP response:	Deprovision a CMIC link 0 on an HIOP card Example: uneq 4 rear link0 Example: Command submitted. Uneq 4 Rear Link0 completed.

6.1.2.2 Command: trnsl

With the introduction of the new CMIC/RTIF HIOP card, the CMIC packlets will have to be migrated to the new card. Hence, from now on, the 'trnsl' command has to support the new HIOP card. This feature does not change the functionality of the command.

6.1.2.2.1 Command description

The 'trnsl' MAP command is used on the MAPCI;MTC;XAC;CMIC MAP level to find out the identity of the MS CMIC paddle board ports connected to a given CMIC link on the XA-Core. Until now, the 'trnsl' command was only used on CMIC packlets. From now on, it can be issued for either a CMIC packlet or CMIC component on the HIOP card.

6.1.2.2.2 Command syntax

This feature does not change the parameter values expected by the 'trnsl' command, its menu number on the CMIC MAP level. It only makes changes to the usage of the command. That is, for CMIC/RTIF HIOP cards, the packlet location parameter value should not be entered. For CMIC packlets, the 'trnsl' command should be issued as before.

6.1.2.2.3 MAP Responses

Table 7 MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted. Trnsl 4 Rear completed. **Meaning:** This response indicates that the 'trnsl' command has completed successfully. **System or user actions:** none

Table 7 MAP outputs with associated meanings and actions

Command
RESPONSE: Card/device is unadressable...no action taken. **Meaning:** this response indicates that there is no provisioned component in the given location. **System or user actions:** the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters **Meaning:** this response indicates that the ‘trsnl’ command was issued without following the correct syntax. For example, the packlet location parameter value was entered for an HIOP. **System or user actions:** re-enter the ‘trnsl’ command with correct syntax.
RESPONSE: <slot> <side> is an IOP. Packlet location must be specified **Meaning:** this response indicates that the ‘trnsl’ command was issued for a CMIC packlet slot, but the packlet location parameter value (lower, l or upper, u) was not specified. **System or user actions:** re-enter the ‘uneq’ command with correct syntax.
RESPONSE: <slot> <side> is an HIOP. Packlet location does not apply. **Meaning:** this response indicates that the ‘trnsl’ command was issued for a CMIC component on an HIOP card, but a packlet location parameter value was entered. **System or user actions:** re-enter the ‘trnsl’ command with correct syntax.

6.1.2.2.4 Example

For CMIC packlets, the ‘trnsl’ command usage will be the same. For CMIC components on an HIOP card, the ‘trnsl’ command will have to be entered without specifying the packlet location (lower or upper). Next table shows some examples.

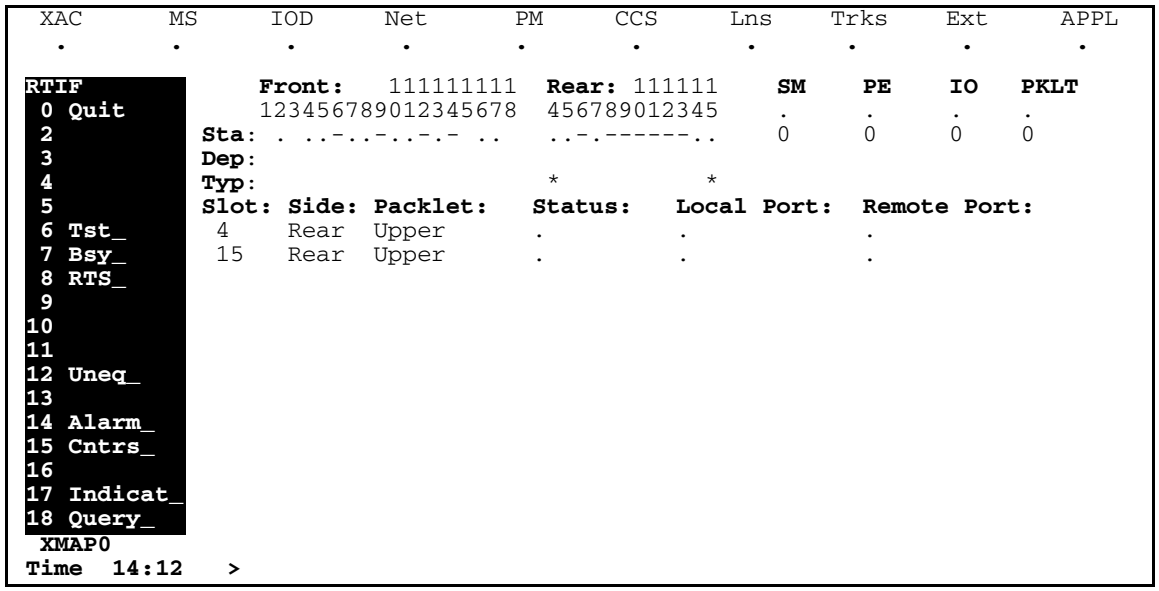
Table 8 Usage examples for ‘trnsl’ command on the CMIC MAP level

Description of task: Command: MAP response:	Trnsl a CMIC packlet on an IOP card Example: trnsl 4 rear lower Example: Command submitted. Trnsl 4 Rear Lower completed
Description of task: Command: MAP response:	Trnsl CMIC on an HIOP card Example: trnsl 4 rear Example: Command submitted. Trnsl 4 Rear completed.

6.1.3 RTIF MAP level

Currently, the RTIF functionality can only be hosted by an RTIF packlet on an IOP card. Please refer to “Figure 6 Current RTIF MAP level with RTIF packlets on IOPs in slots 4R and 15R” on page 2430.

Figure 6 Current RTIF MAP level with RTIF packlets on IOPs in slots 4R and 15R



With the introduction of the new CMIC/RTIF HIOP, the new RTIF MAP will show the functionality hosted by either an RTIF packlet on an IOP card or an CMIC/RTIF HIOP card. Also, with RTIF port/link separation on CMIC/RTIF

HIOP, new RTIF link0 and RTIF link1 components will be shown on the RTIF MAP level.

Table 9 Summary of RTIF MAP field changes

Component	Current MAP Field	New MAP Field	New/Deleted/ Changed
RTIF Local Port on Packlet	'Local Port'	'n/a'	Deleted
RTIF Remote Port on Packlet	'Remote Port'	'n/a'	Deleted
RTIF Local Link on Packlet	n/a	'Link0'	New
RTIF Remote Link on Packlet	n/a	'Link1'	New
RTIF Local Port on HIOP	n/a	'Port0'	New
RTIF Remote Port on HIOP	n/a	'Port1'	New
RTIF Local Link on HIOP	n/a	'Link0'	New
RTIF Remote Link on HIOP	n/a	'Link1'	New

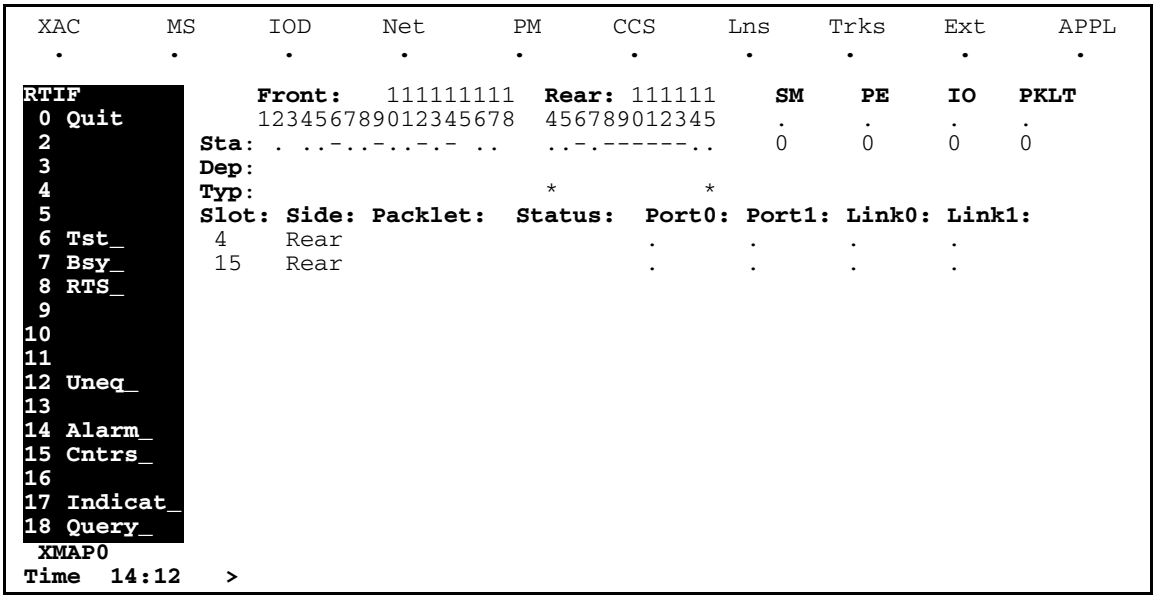
For RTIF packlets on the new RTIF MAP level, the following components will be shown as before: Slot, Side, Packlet, Status. The RTIF local port will be changed to Link0. The RTIF remote port will be changed to Link1. Port0 and Port1 will be left blank. Hence, the RTIF MAP level will be consistent with other packlet MAP levels that have no port/link separation. Please refer to "Figure 7 New RTIF MAP level with RTIF packlets on IOPs in slots 4R and 15R" on page 2431.

Figure 7 New RTIF MAP level with RTIF packlets on IOPs in slots 4R and 15R

```
 XAC      MS      IOD      Net      PM      CCS      Lns     Trks     Ext      APPL
  .       .        .        .       .        .       .       .        .        .

RTIF          Front:   111111111  Rear: 111111     SM     PE     IO    PKLT
 0 Quit       123456789012345678  456789012345     .      .      .     .
 2            Sta: . ..-..-..-.- ..   ..-.------..    0      0      0     0
 3            Dep:
 4            Typ:                    *          *
 5            Slot: Side: Packlet: Status:  Port0: Port1: Link0: Link1:
 6 Tst_        4    Rear  Upper    .                        .      .
 7 Bsy_        15   Rear  Upper    .                        .      .
 8 RTS_
 9
10
11
12 Uneq_
13
14 Alarm_
15 Cntrs_
16
17 Indicat_
18 Query_
 XMAP0
Time  14:12    >
```

For RTIF functionality on CMIC/RTIF HIOP represented on the new RTIF MAP, since the card does not have packlets, the ‘Packlet’ location field, and the packlet ‘Status’ field will be left blank. Also, in addition to the local and remote RTIF ports, there are going to be two new RTIF links shown (link0 and link1). Please refer to “Figure 8 New RTIF MAP level with CMIC/RTIF HIOP cards in slots 4R and 15R” on page 2432.

Figure 8 New RTIF MAP level with CMIC/RTIF HIOP cards in slots 4R and 15R



The new RTIF MAP level will be able to show both, packlet and HIOP, configurations during the migration from one configuration to the other (e.g. RTIF packlet to CMIC/RTIF HIOP).

6.1.3.1 Command: uneq

With the introduction of the new CMIC/RTIF HIOP card, the RTIF packlets will have to be migrated to the new card. Hence, from now on, the XA-Core system will support the provisioning and deprovisioning of RTIF components. The ‘uneq’ command will be used for deprovisioning a RTIF packlet on an IOP card or an RTIF link on a CMIC/RTIF HIOP card. Currently, RTIF packlet deprovisioning is not supported.

Table 10 New or modified CMIC MAP commands

Command Name	NEW, CHANGED or DELETED	Directory/MAP level name	MENU/NON-MENU/ HIDDEN
uneq	changed	MAPCI;MTC;XAC;RTIF	Menu

6.1.3.1.1 Command description

The ‘uneq’ MAP command is used to deprovision a component from the XA-Core system. On the RTIF MAP level, the ‘uneq’ command will be used to deprovision a RTIF packlet residing on an IOP card, or to deprovision a RTIF link residing on a CMIC/RTIF HIOP card. Until now, deprovisioning of RTIF packlets was not supported since they were part of the ‘fixed’ XA-Core configuration (slots 4R and 15R). From now on, deprovisioning of RTIT components is needed for the migration of RTIF packlets to CMIC/RTIF HIOP cards and back.

Table 11 Summary of the new ‘uneq’ CMIC MAP level command

Command	Menu#	Type	Options	Function
uneq	12	Operational	None	- Deprovision a RTIF packlet on an IOP card - Deprovision a RTIF link on an HIOP card

6.1.3.1.2 Command syntax

The ‘uneq’ command requires parameters. If you do not enter any parameters or you enter invalid parameters, the MAP terminal displays an error message. The MAP terminal prompts you to enter a correct parameter value.

Table 12 <’uneq’> command parameters and variables

Command	Parameters and variables
uneq	- slot number (0 to 17), - side (front, f or rear, r), - packlet position (upper, u, or lower, l), - link number (link0 or link1).
Parameters and variables	**Description**
slot number	Use the ‘slot number’ parameter value to indicate the number of the physical shelf slot: 0 to 17
side	Use the ‘side’ parameter value to indicate the component location in the physical shelf: front, f or rear, r
packlet position	Use the ‘packlet position’ parameter value to indicate the RTIF packlet location on an IOP card: upper, u or lower, l. This is used only for RTIF packlet deprovisioning and is not used for RTIF link.

Table 12 <'uneq'> command parameters and variables

Command	Parameters and variables
link number	Use the 'link number' parameter value to indicate the RTIF link position on a CMIC/RTIF HIOP card: link0 or link1. This is used only for RTIF link deprovisioning and is not used for RTIF packlets.

Note: The 'slot number' parameter value will usually be '4' or '15'. The 'side' parameter value will usually be 'upper' or 'u'. The 'packlet position' parameter value will usually be 'upper' or 'u'.

6.1.3.1.3 Qualifications and warnings

The 'uneq' command should be used with great care since it deprovisions a component from the XA-Core system. There are some general requirements for the successful completion of the 'uneq' command. They are (in order):

- first, the component must be brought into a 'ManB' state,
- then, the component must be pulled from the shelf,
- finally, the 'uneq' command can be issued for the component.

Since the 'uneq' command on the RTIF MAP level can be issued for the RTIF packlet residing on an IOP card or for an RTIF link residing on an HIOP card, the command usage will be different depending on the component being deprovisioned. Please refer to Section "6.1.3.1.5 Example" on page 2436.

Note: Deprovisioning of RTIF links on packlets is not supported.

6.1.3.1.4 MAP Responses

Table 13 MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted. Uneq 4 Rear Upper completed. **Meaning:** This response indicates that the 'uneq' command has completed successfully. **System or user actions:** none
RESPONSE: Command submitted. Improper state for required action, no action take **Meaning:** this response indicates that the 'uneq' command has been issued without bringing the component into the 'ManB' state first. **System or user actions:** the craft person has to 'ManB' the component

Table 13 MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted H/W must be removed from shelf, no action taken **Meaning:** this response indicates that the ‘uneq’ command has been issued without removing the component from the shelf, or without waiting long enough for the system to recognize the component’s loss of clock. **System or user actions:** the craft person has to remove the component from the shelf. If the component is already removed, the craft person has to wait long enough (e.g. one minute) for the system to recognize the component’s loss of clock.
RESPONSE: Card/device is unadressable...no action taken. **Meaning:** this response indicates that there is no provisioned component in the given location. **System or user actions:** the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters **Meaning:** this response indicates that the ‘uneq’ command was issued without following the correct syntax. For example, the ‘link0’ or ‘link1’ parameter values were entered while deprovisioning an RTIF packlet on an IOP card (RTIF link deprovisioning not supported on packlets). **System or user actions:**
RESPONSE: <slot> <side> is an IOP. Packlet location must be specified **Meaning:** this response indicates that the ‘uneq’ command was issue for an RTIF packlet, but the packlet location parameter value (lower, l or upper, u) was not specified. **System or user actions:** re-enter the ‘uneq’ command with correct syntax.
RESPONSE: <slot> <side> is an HIOP. Packlet location does not apply. **Meaning:** this response indicates that the ‘uneq’ command was issued for an RTIF link on an HIOP card, but a packlet location parameter value was entered. **System or user actions:** re-enter the ‘uneq’ command with correct syntax.

6.1.3.1.5 Example

Table 14 Usage examples for 'uneq' command on the RTIF MAP level

Description of task: Command: MAP response:	Deprovision a RTIF packlet on an IOP card Example: uneq 4 rear upper Example: Command submitted. Uneq 4 Rear Upper completed
Description of task: Command: MAP response:	Deprovision a RTIF link 0 on an HIOP card Example: uneq 4 rear link0 Example: Command submitted. Uneq 4 Rear Link0 completed.

6.2 Configuration Walkthrough

6.2.1 Provisioning and Deprovisioning

For provisioning and deprovisioning the CMIC, RTIF, IOP, and HIOP components, this feature makes use of the XA-Core provisioning feature. For a more detailed explanation of the provisioning feature please refer to FN-A59009527.

6.2.1.1 CMIC packlet deprovisioning on IOP

Deprovisioning a CMIC packlet on an IOP card follows the general guidelines for deprovisioning any component in XA-Core. In addition, deprovisioning of CMIC packlets also have some particular characteristics:

- first, the CMIC links have to be manually busied from the MS side (links will go 'CBsy'),
- then the CMIC packlet must be brought into a 'ManB' state,
- once the CMIC links are 'CBsy' and the CMIC packlet is 'ManB', the craft person should remove the CMIC packlet from the IOP card,
- once the CMIC packlet is removed from the IOP card, the craft person should issue the 'uneq' command for the CMIC packlet. This deprovisions the CMIC packlet and the CMIC links.

6.2.1.2 CMIC link deprovisioning on HIOP

Deprovisioning a CMIC link on an HIOP card follows the general guidelines for deprovisioning any component in XA-Core. In addition, deprovisioning of CMIC links also have some particular characteristics:

- first, the CMIC link has to be manually busied from the MS side (link will go ‘CBsy’),
- once the CMIC link is ‘CBsy’, the craft person should remove the CMIC link from the HIOP card,
- once the CMIC link is ‘CBsy’ and removed from the HIOP card, the craft person should issue the ‘uneq’ command for the CMIC link. This deprovisions the CMIC link.

6.2.1.3 CMIC packlet provisioning on IOP

Provisioning of CMIC packlets is done as follows:

- have the host IOP card provisioned and in-service, with an empty (unprovisioned) packlet location,
- on the MS side, the craft person must manually busy both MS ports for the CMIC packlet we want to provision,
- after both MS ports are ‘ManB’, the craft person should plug in the CMIC packlet with no links attached,

  Note: when the system provisions the CMIC packlet, the CMIC links are automatically added to the system inventory. They will be ‘CBsy’.
- once the CMIC packlet is provisioned, the craft person should bring the CMIC packlet in-service,
- after the CMIC packlet is in-service, with the CMIC link ‘CBsy’, the craft person should plug the CMIC links into the CMIC packlet,
- on the MS side, once the CMIC links are provisioned and ‘CBsy’, the craft person must test both MS ports connected to the CMIC links,
- after the MS port tests pass, the craft person should bring the MS ports in-service. This will also bring the CMIC links in-service.

6.2.1.4 CMIC link provisioning on HIOP

Provisioning of CMIC links on HIOP is done as follows:

- have the host HIOP card provisioned and in-service, with an empty (unprovisioned) OC3 link location,
- on the MS side, the craft person must manually busy the MS port for the CMIC link we want to provision,

- after the MS port is ‘ManB’, the craft person should plug the CMIC link into the OC3 port of the HIOP card (the CMIC link will be ‘CBsy’),
- on the MS side, once the CMIC link is provisioned and ‘CBsy’, the craft person must test the MS port connected to the CMIC link,
- after the MS port test passes, the craft person should bring the MS port in-service. This will also bring the CMIC link in-service.

6.2.2 Migration procedures

With the introduction of the new CMIC/RTIF HIOP card, the CMIC and RTIF functionality presently hosted by packlets on IOP cards will have to be migrated to the new HIOP card. Also, a ‘back-out’ migration procedure has to be available so that the office can go from the CMIC/RTIF HIOP cards back to packlets.

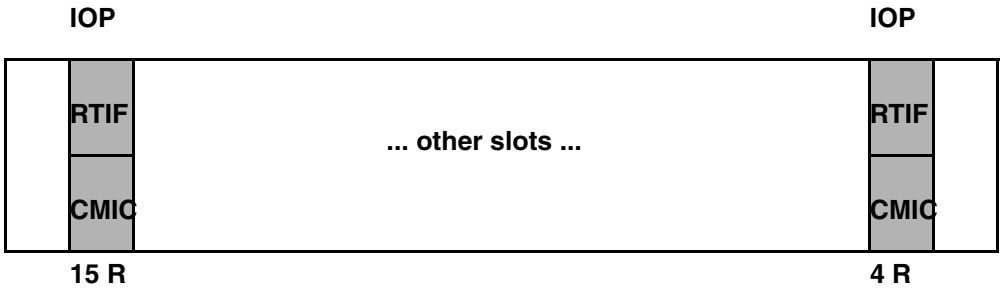
6.2.2.1 Migration from CMIC and RTIF packlets to CMIC/RTIF HIOP for SuperNode (SN)

This section describes the migration procedure from an XA-Core system with CMIC and RTIF functionality provided by packlets on IOP cards to a system with CMIC and RTIF functionality provided by CMIC/RTIF HIOP cards. The recommended approach will provision the new HIOP cards in the *same* slots (4R and 15R) as the deprovisioned IOP cards with packlets. Because of lost redundancy during the migration, there are two E2 conditions during this procedure.

The following sequence of events shows the steps:

- Start with a CMIC and RTIF packlet configuration on IOP cards in slots 4R and 15R (no CMIC/RTIF HIOP cards in the shelf). Please refer to “Figure 9 Initial CMIC and RTIF packlet configuration - XA-Core rear view” on page 2438.

Figure 9 Initial CMIC and RTIF packlet configuration - XA-Core rear view



- set the ‘xa_component_install_state’ office parameter in table OFCENG to ‘manbusy’,

- verify that table XAFWLOAD is datafilled with valid FW (ROM) and DLL (RAM) loads for the new CMIC/RTIF HIOP card,
- issue the ‘trnsl’ command for the CMIC packlet in 4 rear lower: ‘trnsl 4 rear lower’. The MAP response should look like this:

```
trnsl 4 rear lower
Command Submitted.
Trnsl  4 Rear   Lower    completed

Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trnsl’ command for the CMIC packlet in 4 rear lower,
- on the MS MAP level, manually busy the MS ports returned by the ‘trnsl’ command for CMIC packlet in slot 4 rear lower (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- on the CMIC MAP level, manually busy the CMIC packlet in slot 4 rear lower,
- on the RTIF MAP level, manually busy the RTIF packlet in slot 4 rear upper,
- on the IO MAP level, manually busy the IOP card in slot 4 rear,
- pull the CMIC packlet in slot 4 rear lower with links attached,
- pull the RTIF packlet in slot 4 rear upper,
- pull the IOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC packlet: ‘uneq 4 rear lower’.
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF packlet: ‘uneq 4 rear upper’.
- on the IO MAP level, issue the ‘uneq’ command for the IOP card: ‘uneq 4 rear’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              CMIC MBSY  HOST 01 A00 DPCC:00 00 04R L  NTLX05AB/NNTM64422MWV

XAC628 MAR19 14:17:20 5700 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 04R U  NTLX08AA/NNTM64422MWV

XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              IO   MBSY  HOST 01 A00 DPCC:00 00 04R NTLX03AB/NNTM64422MWV
```

- at this stage, the CMIC and RTIF functionality is provided only by the packlets in slot 15 rear. Please refer to “Figure 10 Reduced CMIC and RTIF redundancy (service on packlets) - XA-Core rear view” on page 2440.

Figure 10 Reduced CMIC and RTIF redundancy (service on packlets) - XA-Core rear view

- plug the CMIC/RTIF HIOP card into slot 4 rear with no links attached. The following log should be generated:

  Note: Once the HIOP card is provisioned, all its associated ports will be provisioned as well.

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 04R NTLX04BA/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the HIOP card in slot 4 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        HIOP          4    R             OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the HIOP card in slot 4 rear has been verified, the craft person should manually RTS the card,

  Note: Once the HIOP card is in-service, all its associated ports are automatically brought in-service by the system, provided their OOS test passes.

- plug the CMIC links into the OC3 ports of the HIOP card in slot 4 rear. The system will automatically provision the CMIC links, perform an OOS test on them, and bring them into a ‘CBsy’ state.

  Note: use the same configuration as recorded for the ‘trnsl’ command issued for the CMIC packlet in slot 4 rear lower. The following log should be generated:

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX04BA/NNTM64422MWV
```

```
XAC628 MAR19 14:22:20 7100 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX04BA/NNTM64422MWV
```

- on the MS MAP level, test the MS ports returned by the ‘trnsl’ command for the CMIC packlet in slot 4 rear lower (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25).

- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). On the MS MAP level the MS ports will go from ‘M’ to ‘.’, while on the XAC CMIC MAP level the CMIC links will go from ‘CBsy’ to ‘.’.

- once the CMIC links are in-service, issue the ‘trnsl’ command for the CMIC links on HIOP in 4 rear: ‘trnsl 4 rear’. The MAP response should look like this:

```
trnsl 4 rear
Command Submitted.
Trnsl  4 Rear completed

Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trnsl’ command for the CMIC links on HIOP card in 4 rear. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC packlet in 4 rear lower,

- plug the RTIF local link into the HIOP card’s local RTIF port in slot 4 rear. The system will automatically provision and attempt to bring the local RTIF link in-service. The following log should be generated:

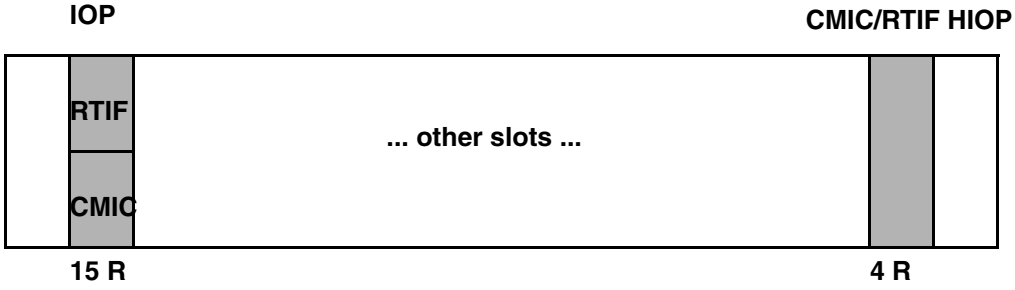
```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX04BA/NNTM64422MWV
```

- plug the RTIF remote link into the HIOP card’s remote RTIF port in slot 4 rear. The system will automatically provision and attempt to bring the remote RTIF link in-service. The following log should be generated:

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX04BA/NNTM64422MWV
```

- at this point, we have a hybrid CMIC and RTIF system: the CMIC and RTIF functionality in slot 15R is still provided by packlets on IOP cards, while the CMIC and RTIF functionality in slot 4R is provided by the new CMIC/RTIF HIOP. Please refer to “Figure 11 Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view” on page 2442.

Figure 11 Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view



- issue the ‘trnsl’ command for the CMIC packlet in 15 rear lower: ‘trnsl 15 rear lower’. The MAP response should look like this:

```
trnsl 15 rear lower
Command Submitted.
Trnsl 15 Rear   Lower    completed

Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trnsl’ command for the CMIC packlet in 15 rear lower,
- on the MS MAP level, manually busy the MS ports returned by the ‘trnsl’ command issued for the CMIC packlet in slot 15 rear lower (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- on the CMIC MAP level, manually busy the CMIC packlet in slot 15 rear lower,
- on the RTIF MAP level, manually busy the RTIF packlet in slot 15 rear upper,
- on the IO MAP level, manually busy the IOP card in slot 15 rear,
- pull the CMIC packlet in slot 15 rear lower, with links attached,
- pull the RTIF packlet in slot 15 rear upper,
- pull the IOP card in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC packlet: ‘uneq 15 rear lower’,
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF packlet: ‘uneq 15 rear upper’,
- on the IO MAP level, issue the ‘uneq’ command for the IOP card: ‘uneq 15 rear’. The following logs should be generated:

```
XAC628 MAR19 14:25:20 7300 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              CMIC MBSY  HOST 01 A00 DPCC:00 00 15R L  NTLX05AB/NNTM64422MWV
```

```
XAC628 MAR19 14:26:20 7400 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 15R U  NTLX08AA/NNTM64422MWV

XAC628 MAR19 14:27:20 7500 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              IO   MBSY  HOST 01 A00 DPCC:00 00 15R NTLX03AB/NNTM64422MWV
```

- Please refer to “Figure 12 Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view” on page 2443.

Figure 12 Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view

- plug the CMIC/RTIF HIOP card into slot 15 rear with no links attached. The following log should be generated:

```
XAC628 MAR19 14:28:20 7600 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 15R NTLX04BA/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the HIOP card in slot 15 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:29:40 7700 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        HIOP          15   R             OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the HIOP card in slot 15 rear has been verified, the craft person should manually RTS the card,

  Note: Once the HIOP card is in-service, all its associated ports are automatically brought in-service by the system, provided their OOS test passes.

- plug the CMIC links into the OC3 ports of the HIOP card in slot 15 rear. The system will automatically provision the CMIC links, perform an OOS test on them, and bring them into a ‘CBsy’ state.

  Note: use the same configuration as recorded for the ‘trnsl’ command issued for the CMIC packlet in slot 15 rear lower.

```
XAC628 MAR19 14:30:20 7800 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
```

```
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 0  NTLX04BA/NNTM64422MWV

XAC628 MAR19 14:31:20 7900 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 1  NTLX04BA/NNTM64422MWV
```

- on the MS MAP level, test the MS ports previously returned by the 'trnsl' command for CMIC packlet in slot 15 rear lower (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25).

- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.

- once the CMIC links are in-service, issue the 'trnsl' command for the CMIC links on HIOP 14 rear: 'trnsl 14 rear'. The MAP response should look like this:

```
trnsl 15 rear
Command Submitted.
Trnsl 15 Rear completed

Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trnsl' command for the CMIC links on HIOP card in 4 rear. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC packlet in 15 rear lower,

- plug the RTIF local link into the HIOP card's local RTIF port in slot 15 rear. The system will automatically provision and attempt to bring the local RTIF link in-service.

```
XAC628 MAR19 14:33:20 8100 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 15R 0  NTLX04BA/NNTM64422MWV
```

- plug the RTIF remote link into the HIOP card's remote RTIF port in slot 15 rear. The system will automatically provision and attempt to bring the remote RTIF link in-service.

```
XAC628 MAR19 14:34:20 8200 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 15R 1  NTLX04BA/NNTM64422MWV
```

- set the 'xa_component_install_state' office parameter in table OFCENG back to 'inservice',

- at this point, the CMIC/RTIF HIOP cards in slots 4R and 15R are all in-service, along with their associated CMIC and RTIF links. No CMIC or RTIF packlets on IOP cards are provisioned in the shelf. This constitutes the end of the migration procedure from CMIC and RTIF packlets to

CMIC/RTIF HIOP. Please refer to “Figure 13 Final CMIC/RTIF HIOP configuration - XA-Core rear view” on page 2445.

Figure 13 Final CMIC/RTIF HIOP configuration - XA-Core rear view

6.2.2.2 Migration from CMIC and RTIF packlets to CMIC/RTIF HIOP for SuperNode SE (SNSE)

The migration procedure from CMIC and RTIF packlets to CMIC/RTIF HIOP cards for SuperNode Shelf Extension (SNSE) is similar to the SuperNode (SN) case. The only exception is the MS port numbers that have to be busied, tested, and enabled during the migration procedure. The ‘trnsl’ command should be used on the CMIC MAP level to get the specific MS port numbers to be busied. Please refer to “Table 15 SN to SNSE port mapping” on page 2445.

Table 15 SN to SNSE port mapping

SN MS port	SNSE MS port	XA-Core CMIC link
MS 0, Card 24, Port 0	MS 0, Card 4, Port 0	Slot 15 rear, link 0
MS 1, Card 25, Port 0	MS 1, Card 4, Port 1	Slot 15 rear, link 1
MS 1, Card 24, Port 0	MS 1, Card 4, Port 0	Slot 4 rear, link 0
MS 0, Card 25, Port 0	MS 0, Card 4, Port 1	Slot 4 rear, link 1

6.2.2.3 Migration from CMIC/RTIF HIOP back to CMIC and RTIF packlets on IOP for SuperNode (SN)

This section describes the migration procedure from an XA-Core system with CMIC and RTIF functionality provided by CMIC/RTIF HIOP cards to a system with CMIC and RTIF funcitionality provided by packlets on IOP cards. The recommended approach will provision the new IOP cards and CMIC and RTIF packlets in the *same* slots (4R and 15R) as the deprovisioned HIOP cards. Hence, because of lost redundancy during the migration, there are two E2 conditions during this procedure.

The following sequence of events shows the steps:

- start with a CMIC/RTIF HIOP configuration in slots 4R and 15R (no IOP cards with CMIC or RTIF packlets provisioned in the shelf). Please refer to “Figure 14 Initial CMIC/RTIF HIOP locations - XA-Core rear view” on page 2446.

Figure 14 Initial CMIC/RTIF HIOP locations - XA-Core rear view

- set the ‘xa_component_install_state’ office parameter in table OFCENG to ‘manbusy’,
- issue the ‘trnsl’ command for the CMIC links on the HIOP card in slot 4 rear: ‘trnsl 4 rear’. The MAP response should look like this:

```
trnsl 4 rear
Command Submitted.
Trnsl  4 Rear completed

Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trnsl’ command for the CMIC links on the HIOP card in slot 4 rear,
- on the MS MAP level, manually busy the MS ports returned by the ‘trnsl’ command for CMIC links on the HIOP card in slot 4 rear (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- pull the CMIC links on the HIOP in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC links on the HIOP in slot 4 rear: ‘uneq 4 rear link0’ and ‘uneq 4 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX17AA/NNTM64422MWV

XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX17AA/NNTM64422MWV
```

- on the RTIF MAP level, manually busy the RTIF links on the HIOP card in slot 4 rear,

- pull the RTIF links from the HIOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF links on the HIOP card: ‘uneq 4 rear link0’ and ‘uneq 4 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX17AA/NNTM64422MWV

XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX17AA/NNTM64422MWV
```

- on the IO MAP level, manually busy the HIOP card in slot 4 rear,
- pull the HIOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the IO MAP level, issue the ‘uneq’ command for the HIOP card: ‘uneq 4 rear’. The following log should be generated:

```
XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 04R NTLX17AA/NNTM64422MWV
```

- at this stage, the CMIC and RTIF funcitionality is provided only by the packlets in slot 15 rear. Please refer to “Figure 15 Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view” on page 2447.

Figure 15 Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view

- plug an IOP card into slot 4 rear with no packlets attached. The following log should be generated:

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              IOP  MBSY  HOST 01 A00 DPCC:00 00 04R NTLX03AB/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the IOP card in slot 4 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
```

```
        IOP           4    R             OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the IOP card in slot 4 rear has been verified, the craft person should manually RTS the card,

- plug the CMIC packlet into the in-service IOP card in slot 4 rear lower with the CMIC links attached. The system will automatically provision the CMIC packlet, perform an OOS test on it, and bring it into a 'ManB' state.

  Note: Once the CMIC packlet is provisioned, both CMIC links will be automatically provisioned as well. They will be 'CBsy'.

  Note: when plugging the CMIC links into the CMIC packlet, use the same configuration as recorded for the 'trnsl' command issued for the CMIC links on the HIOP card in slot 4 rear.

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              CMIC MBSY  HOST 01 A00 DPCC:00 00 04R L  NTLX05AB/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the CMIC packlet in slot 4 rear lower by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        CMIC          4    R    L        OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the CMIC packlet in slot 4 rear lower has been verified, the craft person should manually RTS the CMIC packlet,

- on the MS MAP level, test the MS ports returned by the 'trnsl' command for the CMIC links on the HIOP in slot 4 rear (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25).

- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.

- once the CMIC links are in-service, issue the 'trnsl' command for the CMIC links on the CMIC packlet in slot 4 rear lower: 'trnsl 4 rear lower'. The MAP response should look like this:

```
trnsl 4 rear lower
Command Submitted.
Trnsl  4 Rear lower completed

Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trnsl' command for the CMIC links on the CMIC packlet in 4 rear lower. Verify that they are the same as

the MS port numbers recorded before deprovisioning the CMIC/RTIF HIOP card in 4 rear,

- plug the RTIF packlet into the IOP card in 4 rear upper, with links attached.
- the system will automatically provision the RTIF packlet, perform an OOS test on it, and bring it into a ‘ManB’ state.

  Note: Once the RTIF packlet is provisioned, the system will automatically provision the local and remote RTIF links.

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 04R U  NTLX08AA/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the RTIF packlet in slot 4 rear upper by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        RTIF          4    R    U       OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the RTIF packlet in slot 4 rear upper has been verified, the craft person should manually RTS the packlet,
- once the RTIF packlet is in-service, the system will automatically attempt to bring the local and remote RTIF links in-service.
- at this point, we have a hybrid CMIC and RTIF system: the CMIC and RTIF functionality in slot 15R is still provided by an HIOP card, while the CMIC and RTIF functionality in slot 4R is provided by packlets. Please refer to “Figure 16 Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view” on page 2449.

Figure 16 Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view

- issue the ‘trnsl’ command for the CMIC links on the HIOP card in slot 15 rear: ‘trnsl 15 rear’. The MAP response should look like this:

```
trnsl 15 rear
Command Submitted.
Trnsl  15 Rear completed

Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trnsl’ command for the CMIC links on the HIOP card in slot 15 rear,
- on the MS MAP level, manually busy the MS ports returned by the ‘trnsl’ command for CMIC links on the HIOP card in slot 15 rear (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- pull the CMIC links on the HIOP in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC links on the HIOP in slot 15 rear: ‘uneq 15 rear link0’ and ‘uneq 15 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 0  NTLX17AA/NNTM64422MWV

XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 1  NTLX17AA/NNTM64422MWV
```

- on the RTIF MAP level, manually busy the RTIF links on the HIOP card in slot 15 rear,
- pull the RTIF links from the HIOP card in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF links on the HIOP card: ‘uneq 15 rear link0’ and ‘uneq 15 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 15R 0  NTLX17AA/NNTM64422MWV

XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        LINK: Type State Site FL Row Bay    Shf/Slt/Lk    EqPEC/Serial
              RTIF MBSY  HOST 01 A00 DPCC:00 00 15R 1  NTLX17AA/NNTM64422MWV
```

- on the IO MAP level, manually busy the HIOP card in slot 15 rear,
- pull the HIOP card in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the IO MAP level, issue the ‘uneq’ command for the HIOP card: ‘uneq 15 rear’. The following log should be generated:

```
XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
        DESCRIPTION: Resource has been deprovisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              HIOP MBSY  HOST 01 A00 DPCC:00 00 15R NTLX17AA/NNTM64422MWV
```

- at this stage, the CMIC and RTIF funcitionality is provided only by the packlets in slot 4 rear. Please refer to “Figure 17 Reduced CMIC and RTIF redundancy (service on packlet) - XA-Core rear view” on page 2451.

Figure 17 Reduced CMIC and RTIF redundancy (service on packlet) - XA-Core rear view

- plug an IOP card into slot 15 rear with no packlets attached. The following log should be generated:

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
              IOP  MBSY  HOST 01 A00 DPCC:00 00 15R NTLX03AB/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the IOP card in slot 15 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        IOP           15   R             OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the IOP card in slot 15 rear has been verified, the craft person should manually RTS the card,

- plug the CMIC packlet into the in-service IOP card in slot 15 rear lower with the CMIC links attached. The system will automatically provision the CMIC packlet, perform an OOS test on it, and bring it into a ‘ManB’ state.

  Note: Once the CMIC packlet is provisioned, both CMIC links will be automatically provisioned as well. They will be ‘CBsy’.

  Note: when plugging the CMIC links into the CMIC packlet, use the same configuration as recorded for the ‘trnsl’ command issued for the CMIC links on the HIOP card in slot 15 rear.

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              CMIC MBSY  HOST 01 A00 DPCC:00 00 15R L  NTLX05AB/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the CMIC packlet in slot 15 rear lower by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
```

```
        CMIC          15   R    L        OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the CMIC packlet in slot 15 rear lower has been verified, the craft person should manually RTS the CMIC packlet,
- on the MS MAP level, test the MS ports returned by the 'trnsl' command for the CMIC links on the HIOP in slot 15 rear (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25).
- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.
- once the CMIC links are in-service, issue the 'trnsl' command for the CMIC links on the CMIC packlet in slot 15 rear lower: 'trnsl 15 rear lower'. The MAP response should look like this:

```
trnsl 15 rear lower
Command Submitted.
Trnsl  15 Rear lower completed

Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trnsl' command for the CMIC links on the CMIC packlet in 15 rear lower. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC/RTIF HIOP card in 15 rear,
- plug the RTIF packlet into the IOP card in 15 rear upper, with links attached.
- the system will automatically provision the RTIF packlet, perform an OOS test on it, and bring it into a 'ManB' state.

  Note: Once the RTIF packlet is provisioned, the system will automatically provision the local and remote RTIF links.

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
        DESCRIPTION: New resource has been provisioned
        CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
              RTIF CBSY  HOST 01 A00 DPCC:00 00 15R U  NTLX08AA/NNTM64422MWV
```

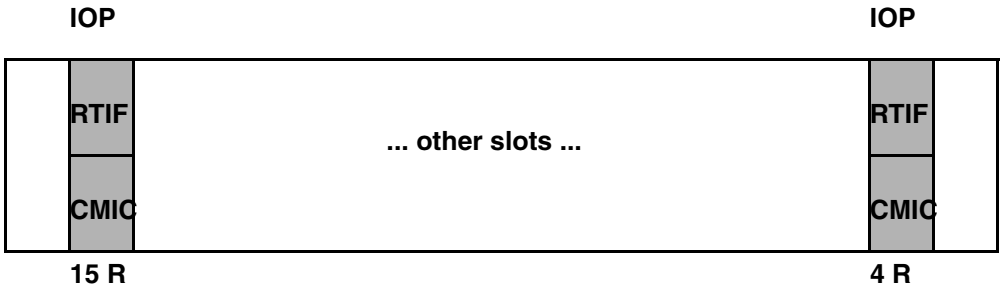
- the craft person should verify the success of the system-initiated provisioning test of the RTIF packlet in slot 15 rear upper by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
        Type Link_Num Slot Side Packlet  Test_Type Result
        RTIF          15    R    U        OOS       Passed
        Initiator: Action initiated by the system
```

- once the integrity of the RTIF packlet in slot 15 rear upper has been verified, the craft person should manually RTS the packlet,

- once the RTIF packlet is in-service, the system will automatically attempt to bring the local and remote RTIF links in-service.
- set the ‘xa_component_install_state’ office parameter in table OFCENG back to ‘inservice’,
- at this point, the CMIC and RTIF packlets on IOP cards in slots 4R and 15R are all in-service, along with their associated CMIC and RTIF links. No CMIC/RTIF HIOP cards are provisioned in the shelf. This constitutes the end of the migration procedure from CMIC/RTIF HIOP to CMIC and RTIF packlets. Please refer to “Figure 18 Final CMIC and RTIF packlet locations - XA-Core rear view” on page 2453.

Figure 18 Final CMIC and RTIF packlet locations - XA-Core rear view



6.2.2.4 Migration from CMIC/RTIF HIOP back to CMIC and RTIF packlets on IOP for SuperNode Shelf Extension (SNSE)

The migration procedure from CMIC/RTIF HIOP cards to CMIC and RTIF packlets on IOP cards for SuperNode Shelf Extension (SNSE) is similar to the SuperNode (SN) case. The only exception is the MS port numbers that have to be busied, tested, and enabled during the migration procedure. The ‘trnsl’ command should be used on the CMIC MAP level to get the specific MS port numbers to be busied. Please refer to “Table 15 SN to SNSE port mapping” on page 2445.

7: Configuration (CN): A00002013

7.1 Hardware and Software Requirements

There are no hardware or software requirements.

7.2 Initial Configuration

During the ONP, if the patch TBF56 is found active on the switch, SOC INW00001 will be switched ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that all 'T1 Timer Expiry' messages should be suppressed.

If the patch TBF56 is found and not active on the switch during ONP, then SOC INW00001 will be switched ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that no 'T1 Timer Expiry' messages should be suppressed.

If the patch TBF56 is not found, then the SOC INW00001 will be switched OFF and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that no 'T1 Timer Expiry' messages should be suppressed.

7.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

7.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	T1_TIMER_EXPIRY_MSG_SUPPRESS	NEW	CM

7.3.2 Parameter information

7.3.2.1 T1_TIMER_EXPIRY_MSG_SUPPRESS

T1_TIMER_EXPIRY_MSG_SUPPRESS

7.3.2.1.1 Functional description

This office parm will be used to provide optionality control for the feature.

7.3.2.1.2 Provisioning rules

There will be four fields in office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION, to switch ‘T1 Timer Expiry’ message suppression ON/OFF, log ON/OFF, alarm ON/OFF and a threshold value.

If SOC INW00001 is switched OFF, the user will not be permitted to provision the office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION.

The user will be able to switch the log or alarm ON/OFF, if the SOC INW00001 is ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION field suppression is switched ON. Additionally, they can only specify a threshold value grater than zero if the alarm creation is ON. If they try to provision incorrectly, then a suitable message will be displayed to indicate the reason for failing the change in SERVORD.

The threshold value is used to determine when to create a GAME102 log entry, which in turn raises an external minor alarm. In order to calculate the value of the threshold, the user should take the highest RSPTMOUT OM count value found within a 24 hour period and multiply this number by 1.25. Calculating the threshold in this way, provides a small amount of padding against the worst situation.

Incidentally, the user will only be permitted to enter a threshold value greater than zero when the alarm option is ON. The threshold value of zero is invalid when the alarm option is ON and if the user attempts to provision it in this way, it will be denied. If denied, a suitable message will be displayed to indicate the problem.

7.3.2.1.3 Range information

The table below provides information about all four fields, as described in 13.3.2.1.2 Provisioning Rules. Fields 1 to 3 are of type BOOLEAN and will only have a value of ‘TRUE’ or ‘FALSE’. It is interpreted that ‘TRUE’ is equivalent to ‘ON’ and ‘FALSE’ is ‘OFF’. Field 4 is an UNSIGNED INTEGER with a value range of 0 to 32,767.

Table 2 Range Information

Field	Minimum	Maximum	Default
1	OFF	ON	OFF
2	OFF	ON	OFF
3	OFF	ON	OFF
4	0	32,767	0

7.3.2.1.4 Activation

In order to suppress ‘T1 Timer Expiry’ messages from being generated, the user will need to switch the SOC INW00001 to ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS field suppression to ON. Once these are ON, the user has the option to activate log or alarm generation when a ‘T1 Timer Expiry’ message is suppressed.

7.3.2.1.5 Dependencies

None.

7.3.2.1.6 Consequences

The following fields, as briefly explained above in section 13.3.2.1.3 Provisioning Rules, represent:

SOC INW00001 needs to be switches ON, before any provisioning of office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION is permitted.

Field 1: Suppression (ON/OFF). When ‘ON’ all ‘T1 Timer Expiry’ messages will be suppressed and permits provisioning of fields 2 to 4.

Field 2: Log (ON/OFF). When ‘ON’, creates an entry in GAME101 during the RSPTMOUT OM transfer period, if the RSPTMOUT OM count is greater than zero.

Field 3: Alarm (ON/OFF): When ‘ON’, creates an entry in GAME102 if the RSPTMOUT OM count equals the office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION threshold value. In turn, when an entry is created, an external minor alarm will be raised.

Field 4: Threshold (0 - 32,767). Used when determining if a entry in the GAME102 log should be created.

For more information on the behavior of these fields, please refer to the relevant customer documentation.

7.3.2.1.7 Verification

During the verification of the four fields the following checks will be done:

Field 1: This can only be equal to ON or OFF. In order for this to be equal to ON, SOC INW00001 should be switched ON.

Field 2: This can only equal to ON or OFF. This can only be set to ON, if field 1 is set to ON.

Field 3: This can only equal to ON or OFF. This can only be set to ON, if field 1 is set to ON.

Field 4: This can only be a number in the range 1 to 32,767. It can only change from a value of 0 if field 3 is set to ON. If field 3 is set to OFF, then the only valid value in this field is 0.

7.3.2.1.8 Memory requirements

Need memory to store data:

Units per memory block = 1

Words per memory block = 3

If the parameter value = 1

words required = (((parameter value - 1)/units per block) + 1) *words per block = 3

7.3.2.1.9 Parameter release history update

New in SN07.

7.4 Upgrade Impact

7.4.1 Dump and Restore

Same details as “7.2 Initial Configuration” on page 2454.

7.4.2 Element Management Upgrade

N/A

7.5 Data schema (DS) (CM, MIBS, RDB)

N/A

7.6 Service Orders (SO) (CM & SESM)

N/A

7.7 Software optionality control (SOC)

Table 3 SOC

SOC option name:	INW00001
SOC option title:	T1 Timer Expiry Msg
SOC option control type:	ON/OFF
New SOC option?	Yes
SOC option order code	INw00001
Option defined in DRU:	SHR
Affected products:	CNA, MMP, MSL, SSR, Succession

7.8 Element Management

N/A

7.9 Command interface changes

N/A

7.10 Security

N/A

7.11 Configuration Walkthrough

8: Configuration (CN): A00002020

8.1 Hardware and Software Requirements

Office has converted to using deterministic LENs for MG9000 as described in SN06 activity “A89009298 - MG9000 Lines Preprovisioning”.

8.2 Initial Configuration

This section describes only the configuration necessary for the core to make ESA data available to the MG9000 EM. It does not describe MG9000 EM or MG9000 operation. Please refer to section “Related Activities” of the FN for this feature for further information.

Table LGRPINV should contain a number of logical groups of lines added by the MG9000 EM. LGRPs with a GRPTYPE of “S” are in one to one correspondence with MG9000 VMGs.

Table ESAPXLA should be provisioned with special dialing codes needed while in ESA. Pretranslator datafill is required for every customer group and LGRP combination. A special entry called ESAPOTS is provided for non-IBN lines

OFCENG parameter ESA_GWDATA_DEVICE specifies the device on the core where the ESA data is generated. The default value is SFDEV but the telco should consider using a disk device for offices with large numbers of MG9000 lines.

Collection of ESA data for LGRPs with GRPTYPE “S” is automatically triggered at 1:00 AM every night.

8.3 Office/Subnet parameters (OP/SP) (CM & SESM)

8.3.1 New/Modified Office parameters

Table 1 New or modified parameters

Parm Table	Parameter Name	New/ Changed/ Deleted/ Relocated	Domain (CM or Subnet Management
OFCENG	ESA_GWDATA_DEVICE	New	CM

8.3.2 Parameter Information

8.3.2.1 ESA_GWDATA_DEVICE

Emergency Stand Alone Gateway Data Device

8.3.2.1.1 Functional Description

Every night at 1:00 AM the CM generates a data file containing ESA data for all MG9000 gateways in the office. The file is called ESA_SYSTEM_SD$XML and is stored on the device indicated by parameter ESA_GWDATA_DEVICE. The file is later retrieved by the MG9000 Element Manager which will erase its existing ESA data only if a valid file is received.

It is highly recommended that a disk device be used even though the default device is SFDEV. Any change to ESA_GWDATA_DEVICE must be also be made on the MG9000 EM.

The file should not be manually modified since it is system generated. It is not normally viewed by the telco but may be transferred to UNIX or PC using FTP and viewed with a text editor. FTP should be used in binary mode.

The DMS PRINT and EDIT/TYPE commands will only partially display the file.

8.3.2.1.2 Provisioning Rules

This parameter can be set to SFDEV or any valid disk volume name.

SFDEV is not recommended due to its limited size and usage by many other applications. The ESA_SYSTEM_SD$XML file can be rather large - approximately 86 KB per 1000 gateway lines. The maximum size of SFDEV (as provisioned in table DSLIMIT) is 5 million words (10 million bytes) and there is no guarantee that all of this will be available for the ESA file.

8.3.2.1.3 Range Information

Table 2 Range Information

Minimum	Maximum	Default
1 character	28 characters	SFDEV

8.3.2.1.4 Activation

If office parameter ESA_GWDATA_DEVICE is changed the following steps are recommended. The data device name property on the MG9000 EM must be updated or the MG9000 will continue to use the ESA data last successfully downloaded from the CM.

1. Change the ESA_GWDATA_DEVICE parameter to its new value.
2. Execute the ESACOLL command in the ESATOOLS CI increment.
3. Verify that an ESA120 log has been generated. This indicates the ESA data file has been successfully generated. It may take several minutes.
4. Verify that file ESA_SYSTEM_SD$XML exists on the new device.

5. ***Important:*** Using the MG9000 EM, Change the ESA.DataDeviceName property to the same device as used in the core. See documentation for activity A00002019.
6. Using the MG9000 EM graphical user interface, manually initiate a download of ESA data. See documentation for activity A00002019.
7. Erase the ESA_SYSTEM_SD$XML file from the OLD device to ensure the MG9000 will not use this file at a later date.

8.3.2.1.5 Dependencies

The MG9000 EM must be manually configured to look for the ESA_SYSTEM_SD$XML file on the new device by using the ESA.DataDeviceName property. Please refer to activity A0002019.

If this parameter is left at its default value of SFDEV, then there is a dependency on table DSLIMIT, where memory is allocated for SFDEV under entry STOREFS. Example:

```
>table dslimit
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DSLIMIT
>list all
TOP
                          DSOWNER   DSMAX  DSUSED
-----------------------------------------------
                          STOREFS 5000000  146592
                          NPOFIMP   45000    3040
                           NTDEVS 3000000  237472
BOTTOM
```

For STOREFS, DSMAX - DSUSED = memory available for the ESA data file

8.3.2.1.6 Consequences

If data collection does not complete successfully using this device, an ESA121 log is output, and the data file will be unusable by the MG9000 EM. The MG9000 will continue to use the ESA data last successfully downloaded.

8.3.2.1.7 Verification

Please refer to section “8.3.2.1.4 Activation” for complete activation and verification instructions.

8.3.2.1.8 Memory Requirements

No memory impact for the parameter itself. See EI section for data file store impact.

8.3.2.1.9 Parameter release history update

This parameter is new for this release.

8.4 Upgrade Impact

8.4.1 Dump and Restore

No additional impact.

8.4.2 Element Management Upgrade

Please refer to A00002019 MG9000 EM Enhancements.

8.5 Data schema (DS) (CM, MIBS, RDB)

8.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ESAPXLA	CHANGED	UNCHANGED

8.5.2 Table Database Schema information

8.5.2.1 Name: ESAPXLA

Emergency Stand Alone Pretranslation Table

8.5.2.1.1 Functional description

Table ESAPXLA lists special dialing codes to be used during emergency stand alone operation and the translation result for these codes. Provisioning is allowed for every IBN customer group and LGRP combination with translator name ESAPOTS being used for non-IBN lines.

Note that 911 lines must be available on each LGRP since individual VMGs can enter ESA without other VMGs on the MG9000. Translations for each LGRP must be provided in table ESAPXLA so 911 will terminate properly.

8.5.2.1.2 Usage sequence and implications (CM Only)

A new table dependency has been added. LGRPINV is a read only table that is filled as the result of MG9000 EM provisioning. It must be provisioned before table ESAPXLA.

Table provisioning order:

- HUNTMEM
- LGRPINV (Read Only table under control of MG9000 EM)
- ESAPXLA

8.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ESAPXLA	0	32 x N x M[a]	No Change. Each new XLANAME/LGRP combination uses 16 bytes for a header. Each tuple uses an additional 16 bytes.

a. N is the number of LGRPs and M is the number of XLANAME entries used including ESAPOTS for POTS lines.

8.5.2.1.4 Fields

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PXLAKEY	CHANGED	NODE	PMTYPE	LGRP selection added. Similar to existing LCM and DLM selectors.

8.5.2.1.5 Datafill example

```
TABLE ESAPXLA
LIST ALL
TOP
                                    PXLAKEY                    RESULT
-------------------------------------------------------------------------
 ESAPOTS  LGRP REM1 00 0              411               T REORDER
 ESAPOTS  LGRP REM1 00 0              611               H 55 1 N
 ESAPOTS  LGRP REM1 00 0              911               L REM1 0 0 2 5 N 0
 IBNXLA   LGRP REM1 00 0              9                 A ESAPOTS Y
```

8.5.2.1.6 Table release history update

Add support for LGRP PMTYPE for MG9000.

8.5.2.1.7 Supplementary information

MG9000 LGRPs do not currently have the capability to support trunks so references to table ESARTE or ESAHNPA are not allowed.

The “L” selector allows terminations to a line with a given line equipment number (LEN). The LEN must be on an MG9000 at the same site as the LGRP in the tuple key.

The “H” selector allows terminations to hunt members given the hunt group number specified in table HUNTGRP and the hunt member number specified in table HUNTMEM. The hunt member must be on the same LGRP as used in the tuple key.

8.5.2.1.8 Translation verification other tools

Please refer to section “8.9.2 Command: ESATRAVER”.

8.6 Service Orders (SO) (CM & SESM)

No change.

8.7 Software optionality control (SOC)

MG9000 ESA supports use of the duplicate office code support SOC (Y78520DO).

8.8 Element Management

Please refer to feature A00002019.

8.9 Command interface changes

8.9.1 Directory: ESATOOLSDIR

8.9.1.1 Directory description

The ESATOOLS CI increment provides a number of customer tools to verify and operate on CS2000 ESA data. This activity will

1. Enhance the ESATRAVER command to work with MG9000 lines.
2. Create a command that will generate an ESA data file for MG9000 lines.

Note that any ESA data must be downloaded to the MG9000 EM and MG9000 before it will affect ESA operation.

8.9.1.2 Accessing directory: ESATOOLSDIR

8.9.1.2.1 Access to directory or MAP level and return to CI

To access the ESATOOLS CI increment, type ESATOOLS from the command prompt. To exit ESATOOLS back to the CI environment, type QUIT.

8.9.2 Command: ESATRAVER

Note: Activity "A00002380 - MG9K ABI ESA" is implemented in CCM20 and enhances MG9K ESA to support ABI as well as non native lines. The ability to support ESATRAVER for ABI has changed some of the messages printed by that command.

8.9.2.1 Command type: NON-MENU

8.9.2.2 Command target: All

8.9.2.3 Command availability: RES

8.9.2.4 Command description

ESATRAVER is a command in the ESATOOLS CI increment which is used to verify ESA translations data in the Call Server.

8.9.2.5 Command syntax

Table 6 ESATRAVER command parameters and variables

Command	Parameters and variables
ESATRAVER	<ORIG> {TR <CLLI> STRING, L <LINE> STRING} <DIGITS> STRING <TRACE> {T, NT, B}
Parameters and variables	**Description**
ORIG	TR <CLLI> : For trunk originations, enter TR and the CLLI name of the trunk group L <LINE> : For line originations, enter L and the 7-digit directory number of the line

Table 6 ESATRAVER command parameters and variables

Command	Parameters and variables
DIGITS	Enter the dialled digits to be verified.
TRACE	T = Trace NT = NoTrace B = Both

8.9.2.6 Qualifications and warnings

The ESATRAVER command syntax has not changed. The software has been enhanced to allow verification of lines originating and terminating on an MG9000 gateway.

Since the MG9000 does not support trunks, the TR <CLLI> parameter does not apply.

8.9.2.6.1 SETRCC command interactions.

SETRCC is an existing command in ESATOOLS that is used to collect trunk group data on an RCC. The SETRCC command must be run for an RCC before the ESATRAVER command can be used on a line or trunk on that RCC.

Since an LGRP does not have trunks, the SETRCC command is not required prior to issuing the ESATRAVER command on a line on an LGRP.

If SETRCC is done on a particular RCC, ESATRAVER on an LGRP line will not use the collected trunk group data and will not affect the data in any way. ESATRAVER on an LGRP line can be followed by ESATRAVER on a line or trunk on that RCC without reissuing the SETRCC command.

8.9.2.7 Responses

8.9.2.7.1 Warning: Cannot verify term LGRP accessible from orig LGRP.

Command: ESATRAVER
Output: Warning: Cannot verify term LGRP accessible from orig LGRP. **Meaning:** The ESATRAVER command has determined that both the originating and terminating lines are in LGRPs with the same site names, but cannot determine which Gateway controls these lines. Both LGRPs must belong to the same Gateway for this call to complete while the Gateway is in ESA mode. It is also possible for one LGRP to be in ESA mode while another on the same MG9000 is not. In this case, the call would not complete. **User actions:** The user must verify at the Element Manager that both LGRPs are controlled by the same Media Gateway.

8.9.2.7.2 Originator and destination are not on the same remote site

Command: ESATRAVER
Output: Originator and destination are not on the same remote site **Meaning:** For an LGRP line originator, this response means that both the originating and terminating line are on LGRPs, but the site names are different, so the termination is not valid**.** **User Actions:** If the user wishes these dialled digits to terminate to a valid LGRP line, then an entry must be made in table ESAPXLA to direct this call to a valid line**.**

8.9.2.7.3 NO MATCH

Command: ESATRAVER
Output: NO MATCH **Meaning**: This is a generic error message that indicates that the digits dialled do not translate to a valid terminator from this originator. For an LGRP line originator, this response indicates that the terminator is not an LGRP line. **User Actions**: If the user wishes these dialled digits to terminate to a valid LGRP line, then an entry must be made in table ESAPXLA to direct this call to a valid line.

8.9.3 Command: ESACOLL

8.9.3.1 Command type: Listed NON-MENU

8.9.3.2 Command target: All

8.9.3.3 Command availability: RES

8.9.3.4 Command description

The ESACOLL command will cause ESA data to be generated for all MG9000 lines in the office. The command will create or replace file ESA_SYSTEM_SD$XML on the device specified by OFCENG parameter ESA_GWDATA_DEVICE.

The file is generated asynchronously and the command prompt will return once file generation has been initiated.

An ESA120 log is output if file generation is initiated successfully and the actual generation is successful. An ESA121 log is output if file generation is initiated but then fails.

8.9.3.5 Command syntax

No command arguments are required.

8.9.3.6 Qualifications and warnings

A failure message will be output if the ESACOLL command was unable to initiate building of the ESA data file.

"ESA static data generation failed to initiate."
"Possible conflict with system or user request."

8.9.3.7 Responses

8.9.3.7.1 ESA Data Generation Initiated

This response is generated if generation of the ESA data file was initiated.

"ESA static data generation initiated."
"See file ESA_SYSTEM_SD$XML on device SFDEV."

8.9.3.8 Example

```
>ESATOOLS
>ESACOLL
Warning: All MG9000 ESA data will be rebuilt.
Please confirm ("YES", "Y", "NO", or "N"):
>Y
ESA static data generation initiated.
See file ESA_SYSTEM_SD$XML on device SFDEV.
```

8.10 Security

The MG9000 EM will have to FTP the ESA data file from the core. Please refer to feature A00002019 for security considerations.

8.11 Configuration Walkthrough

Please refer to feature A00002019 for MG9000 EM operation.

1. Verify tuples with GRPTYPE of "S" have been provisioned in table LGRPINV by the MG9000 EM. Verify that the shelf number (the "0" in "REM1 00 0") for all "S" type LGRPs are 3 or under. If this is not the case the office has not converted to deterministic LENs for MG9000.

```
>table lgrpinv
>lis 2

TOP
      GRPNO          SRVRNAME GRPTYPE                                  LGRPOPTS
-------------------------------------------------------------------------------
REM1  00 0            GWC 110       S                                        $
REM1  00 1            GWC 110       S                                        $
```

2. Provision special dialing codes in table ESAPXLA for POTS (XLANAME = ESAPOTS) as well as for XLANAMEs used by IBN customer groups with members in the LGRP.

```
>table ESAPXLA
>lis all

TOP
                                    PXLAKEY                  RESULT
-----------------------------------------------------------------
 ESAPOTS LGRP REM1  00 0              411               T REORDER
 ESAPOTS LGRP REM1  00 0              911 L REM1  00 2 03 01 N 0
```

3. Set ESA_GWDATA_DEVICE

```
This step is not necessary if SFDEV is being used to hold MG9000 ESA data.

It is recommended that a disk device be used so that SFDEV is available for other
uses. Please refer to "8.3.2.1.4 Activation" for details on how to change the
office parameter.
```

4. Generate ESA data file using ESATOOLS.

```
>ESATOOLS
>ESACOLL
Warning: All MG9000 ESA data will be rebuilt.
Please confirm ("YES", "Y", "NO", or "N"):
>Y
ESA static data generation initiated.
See file ESA_SYSTEM_SD$XML on device D000ESA.

... have prompt back - wait for ESA120/ESA121 log

LOGUTIL ESA
Done.
RTP206BT      ESA120 MAY20 11:12:21 8500 INFO ESA DATA GENERATION


>DISKUT
>LISTFL D000ESA
ESA_SYSTEM_SD$XML

QUIT ALL
```

5. ESA data file will be automatically generated every day at 1:00 AM.

9: Configuration (CN): A00002146

9.1 Hardware and Software Requirements

The commands in this section apply to a fully configured and commissioned XPM with cside connectivity to the ABI cards on an MG9K. The MG9K and Core must contain at least SN06.2 loads.

9.2 Initial Configuration

When moving an existing XPM from the ENET to an MG9K, use the procedures found in Installation Method IM 72-1682: XPM to MG9000 DS512 Rehome.

9.3 Upgrade Impact

9.3.1 Dump and Restore

Not applicable

9.3.2 Element Management Upgrade

Not applicable

9.4 Command interface changes

9.4.1 LGCDIR Directory (changed)

9.4.1.1 Directory description

The LGCDIR directory is associated with the LGC map level. It is available whenever an XPM of node_type LGC is posted. The LGC node_type encompasses a number of pm_types including DTC, LTC, LGC, and SMA2. From this directory/map level, maintenance on the posted XPM can be performed.

The only change to this directory is the addition of the ABILink command to access the ABILink sublevel for performing maintenance on the Cside links of an ABI-hosted XPM. The ABILink command is only available when an ABI-hosted XPM is posted.[1]

9.4.1.2 Accessing directory: LGCDIR

To enter this directory from the CI environment, type:

```
MAPCI;MTC;PM;POST <pm_type> <pm_number>
```

To quit, type:

```
QUIT
```

[1]Due to patching considerations, the ABILink command may not be visible in the MAP menu although the command will still be available.

9.4.1.3 MAP display

```
 XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
  .        .      .       .      1 LGC    .       .        .      .       .

LGC                             SysB    ManB    OffL    CBsy    ISTb    InSv
 0 Quit         PM                 0       0       0       0       1      32
 2 Post_        LGC                0       0       0       0       1       9
 3 ListSet
 4 ABILink   LGC     0 ISTb  Links_OOS: CSide  1 , PSide  0
 5 Trnsl_    Unit0:   Act   InSv
 6 Tst_      Unit1:   Inact InSv
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_
12 Next
13 SwAct
14 QueryPM
15 DCH
16
17 PERFORM
18 ISG
  ADMIN
```

9.4.2 ABILink Command (new)

- **Command type**: Listed MENU (at location 4)
- **Command target**: ALL
- **Command availability**: RES (in Succession loads only)

9.4.2.1 Command description

The ABILink command takes the user to the ABILink sublevel where maintenance can be performed on the CSide links of an ABI-hosted XPM.

9.4.2.2 Command syntax

Table 1 ABILink command parameters and variables

Command	Parameters and variables
ABILink	none

9.4.2.3 Qualifications and warnings

The ABILink command is only available when an ABI-hosted XPM is posted.

9.4.2.4 Examples

```
>ABILink
```

Enters the ABILink level of the MAP.

9.4.3 Trnsl Command (changed)

- **Command type**: Listed MENU (at location 5)
- **Command target**: ALL
- **Command availability**: RES

9.4.3.1 Command description

The Trnsl command translates CSide and PSide link information.

On ABI XPMs, a note appears at the end of the command display when translating CSide links. That note is being changed.

9.4.3.2 Command syntax

Table 2 Trnsl command parameters and variables

Command	Parameters and variables
Trnsl	<FUNCTION> { C [<CSIDE LINK>], P [<PSIDE LINK>], MSG <MESSAGE LINK>, EMSG <EXTENDED MESSAGE LINK> }
Parameters and variables	**Description**
FUNCTION = {C, P, MSG, EMSG}	What kind of link information to display
C	Display C Side link information. The default is to display all CSide links.
CSIDE LINK = {0 TO 31}	Optional parameter to specify a single CSide link
P	Display P Side link information. The default is to display all PSide links.
PSIDE LINK = {0 TO 53}	Optional parameter to specify a single PSide link
MSG	Display only message links
MESSAGE LINK = {C, P}	Specify either CSide or PSide message links
EMSG	Display only Extended Message links
EXTENDED MESSAGE LINK = {C}	Display the CSide Extended message links (required)

9.4.3.3 Qualifications and warnings

The only change to existing behavior is to modify the note at the end of the TRNSL C and TRNSL MSG C commands when issued on an ABI XPM.

9.4.3.4 Examples

```
>trnsl c
Link  0: GWC 16              0;Cap MS;Status:OK      ;MsgCond:OPN,Unrestrict
Link  1: GWC 16              1;Cap MS;Status:OK      ;MsgCond:OPN,Unrestrict
Link  2: GWC 16             **;Cap  S;Status:OK
Link  3: GWC 16             **;Cap  S;Status:OK
. . .
Link 31: GWC 16             **;Cap  S;Status:OK
Please go to the ABILink level for CSide Link Mtc.

>trnsl msg c
Link  0: GWC 16              0;Cap MS;Status:OK      ;MsgCond:OPN,Unrestrict
Link  1: GWC 16              1;Cap MS;Status:OK      ;MsgCond:OPN,Unrestrict
Link  4: GWC 16              2;Cap MS;Status:OK      ;MsgCond:OPN,Restrict
Link  5: GWC 16              3;Cap MS;Status:OK      ;MsgCond:OPN,Restrict
Please go to the ABILink level for CSide Link Mtc.
```

9.4.4 ABILINKDIR Directory (new)

9.4.4.1 Directory description

The ABILINKDIR directory is associated with the ABILINK map level. This directory/map level provides a place for link mtc. on the cside links of an ABI-hosted XPM.

The ABILink level is only available on ABI-hosted XPMs.

9.4.4.2 Accessing directory: ABILINKDIR

To enter this directory from the CI environment, type:

```
MAPCI;MTC;PM;POST <pm_type> <pm_number>;ABILINK
```

To quit, type:

```
QUIT
```

9.4.4.3 MAP display

In the MAP screenshot below, the portions of the MAP which are specific to the ABILink level are shown in boldface type. Dynamic map fields are shown in blue and are described below.

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .      1 LGC     .        .        .       .         .

ABILink                              SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                    0        0        0        0        1       32
 2               LGC                   0        0        0        0        1        9
 3
 4            LGC     0 ISTb  Links_OOS: CSide  1 , PSide  0
 5            Unit0:   Act   InSv
 6 Tst_       Unit1:   Inact InSv
 7 Bsy_
 8 RTS_       CSide host: GWC 16  ABI IP Address: 10.32.133.194
 9                                DS30                 1 1 1 1 1 1
10                         ABI Status 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
11                Plane 0   Master    . . M . . . . . . . . . . . . .
12                Plane 1   Slave     . . . . . . . . . . . . . . . .
13
14
15
16
17
18
  ADMIN
```

Table 3 ABILink MAP display - dynamic fields

Field	Values	Description
CSide host:	<pm_type> <pm_no>	The CSide node which logically hosts the links to the ABI XPM (as datafilled in table LTCINV).
ABI IP Address:	aaa.bbb.ccc.ddd	The IP address of the Master ABI card to which the XPM's DS512 links are attached (as datafilled in table LTCINV). The same IP address follows Mastership of the ABI card pair.
ABI Status	{Master, Slave}	Each ABI card models a network plane. One card is always the Master while the other is Slave.
Link Status fields	'.' = InService 'S' = SysB 'M' = ManB 'C' = CBsy 'P' = PBsy '-' = Unequipped	The current status of each individual link.

9.4.5 Tst Command (new)

- **Command type**: Listed MENU (at location 6)
- **Command target**: ALL
- **Command availability**: RES

9.4.5.1 Command description

The TST command is used to test a CSide link of an ABI XPM. The nature of the test depends on the state of the link and whether the link has message or speech capability. The ALL parameter will test the whole DS512 link. The conversion between link number and plane/port is as follows:

link = 2*port + plane

9.4.5.2 Command syntax

Table 4 Tst command parameters and variables

Command	**Parameters and variables**
TST	<plane> <scope> {ALL, PORT <port_no>} [<type>]
Parameters and variables	**Description**
plane = {0 to 1}	The plane to test. Plane corresponds to ABI card.
scope = {ALL, PORT}	ALL = test the whole DS512 link on the given plane. PORT = test only a single DS30 link on the given port.
port_no = {0 to 15}	The specific DS30 port to test.
type = {MSG, SPC}	MSG = force msg tests and only msg tests to be run SPC = force speech tests and only speech tests to be run

9.4.5.3 Qualifications and warnings

The link must be either InSv or ManB to be tested. If a single link is specified, non-destructive diagnostics are run on the link. If the ALL parameter is given to test the whole plane, all the msg links on that plane which can be tested will be. The Type parameter can be used to force MSG-only or SPC-only diagnostics on links in any state.

Tests on individual speech links are not supported at this time.

9.4.5.4 Examples

1. Port 0 on plane 0 is a message link and is InSv.

```
>tst 0 port 0
Request Passed
```

2. Port 1 on plane 1 is a speech link and is ManB.

```
>tst 1 port 1
Request Invalid - Speech-only links are not supported.
```

3. The entire DS512 on plane 0 is ManB. There is a problem on 1 link.

```
>tst 0 all
```

```
Request Failed
 port 0 on plane 0 - Test Passed
 port 2 on plane 0 - MG9K reports HAL Alarms.
```

4. Port 0 on plane 0 is a message link and is ManB. The ABI card is InSv, but there is a problem with the XPM.

```
>tst 0 port 0
Request Failed - The XPM did not respond to Msg test.
```

5. Port 0 on plane 0 is a message link and is ManB. The ABI card is locked.

```
>tst 0 port 0
Request Failed - The ABI did not respond to Msg test.
```

6. Port 0 on plane 0 is a message link and is CBsy. The hosting GWC is not InSv.

```
>tst 0 port 0
Request Invalid - Link is C-side busy.
```

7. Port 0 on plane 0 is a message link and is CBsy. The hosting GWC is not InSv.

```
>tst 0 port 0 msg
Only MSG tests will be executed.
Request Failed - The GWC did not respond to Msg test.
```

9.4.6 Bsy Command (new)

- **Command type**: Listed MENU (at location 7)
- **Command target**: ALL
- **Command availability**: RES

9.4.6.1 Command description

The BSY command will take the given CSide link of an ABI XPM out of service and mark it as ManB. The ALL parameter will busy the whole DS512 link, i.e. the whole plane. The conversion between link number and plane/port is as follows:

link = 2*port + plane

9.4.6.2 Command syntax

Table 5 Bsy command parameters and variables

Command	Parameters and variables
BSY	<plane> <scope> {ALL, PORT <port_no>}

Table 5 Bsy command parameters and variables

Parameters and variables	Description
plane = {0 to 1}	The plane to busy. Plane corresponds to ABI card.
scope = {ALL, PORT}	ALL = busy the whole DS512 link on the given plane. PORT = busy only a single DS30 link on the given port.
port_no = {0 to 15}	The specific DS30 port to busy.

9.4.6.3 Qualifications and warnings

A link can be manually busied from any state except ManB.

A warning will be output if busying the given link will isolate the XPM unit or take the ABI plane out of service.

Bsying a link may cause call setup failures.

Individual speech links are not supported at this time.

9.4.6.4 Examples

1. Port 0 on plane 0 is a message link and is InSv.

```
>bsy 0 port 0
Request Passed
```

2. Port 0 on plane 1 is a message link and is InSv. Port 0 on plane 0 is already OOS.

```
>bsy 1 port 0
WARNING: Unit 0 of LTC 0 will become isolated.
Please confirm ("YES", "Y", "NO", or "N"):
>y
Request Passed
```

3. Port 1 on plane 0 is a speech link and is InSv.

```
>bsy 0 port 1
Request Invalid - Speech-only links are not supported.
```

4. Port 2 on plane 0 is a message link and is already ManB.

```
>bsy 0 port 2
Request Invalid - link is ManB.
```

5. Port 2 on plane 1 is a message link and is SysB.

```
>bsy 1 port 2
Request Passed
```

6. The entire DS512 on plane 0 is InSv. Plane 0 is the active plane.

```
>bsy 0 all
WARNING: Some calls may be dropped.
WARNING: Bsying the Master plane will cause a Swact of
         the ABI cards.
```

```
Please confirm ("YES", "Y", "NO", or "N"):
>Y
Request Passed
```

9.4.7 RTS Command (new)

- **Command type**: Listed MENU (at location 8)
- **Command target**: ALL
- **Command availability**: RES

9.4.7.1 Command description

The RTS command will return to service the given CSide link of an ABI XPM. The ALL parameter will return to service the whole DS512 link, i.e. the whole plane. The FORCE parameter will skip diagnostics. The conversion between link number and plane/port is as follows:

link = 2*port + plane

9.4.7.2 Command syntax

Table 6 RTS command parameters and variables

Command	Parameters and variables
RTS	<plane> <scope> {ALL, PORT <port_no>} [FORCE]
Parameters and variables	**Description**
plane = {0 to 1}	The plane to RTS. Plane corresponds to ABI card.
scope = {ALL, PORT}	ALL = RTS the whole DS512 link on the given plane. PORT = RTS only a single DS30 link on the given port.
port_no = {0 to 15}	The specific DS30 port to RTS.
FORCE	Skip diagnostics when RTSing the link.

9.4.7.3 Qualifications and warnings

A link must be ManB before it can be RTSed.

Individual speech links are not supported at this time.

9.4.7.4 Examples

1. Port 0 on plane 0 is a message link and is ManB.

```
>rts 0 port 0
Request Passed
```

2. Port 0 on plane 1 is a message link and is SysB.

```
>rts 1 port 0
Request Invalid - SysB link is not ManB.
```

3. Port 1 on plane 0 is a speech link and is ManB.

```
>rts 0 port 1
Request Invalid - Speech-only links are not supported.
```

4. Port 2 on plane 0 is a message link and is ManB.

```
>rts 0 port 2
Request Failed
```

5. Port 2 on plane 0 is a message link and is ManB. Try again without diagnostics.

```
>rts 0 port 2 force
Using the FORCE option will attempt to RTS the link without
running the Speech Tests.
Please confirm ("YES", "Y", "NO", or "N"):
>y
Request Passed
```

6. The entire DS512 on plane 0 is ManB.

```
>rts 0 all
Request Passed
```

9.4.8 ABIREHOME Directory (changed)

9.4.8.1 Directory description

The ABIREHOME directory is the home of the ABI REHOME CI tool. This tool set is intended for use during a controlled rehome of an XPM's c-side from the ENET/JNET to an ABI card on an MG9000 via installation method IM 72-1682: XPM to MG9000 DS512 Rehome. The user must use the TASTOOLCI command SET_ABI_REHOME_STATUS to turn functionality of invasive commands on.

Note: For use by trained and experienced personnel only.

A new command, ADJUST_FRAME_SYNC (or AFS), is being added to the ABIREHOME directory.

9.4.8.2 Accessing directory: ABIREHOME

To enter this directory from the CI environment, type:

```
ABIREHOME
```

To quit, type:

```
QUIT
```

9.4.9 ADJUST_FRAME_SYNC Command (new)

- **Command type**: NON-MENU (part of ABIREHOME directory)
- **Command target**: ALL
- **Command availability**: RES

9.4.9.1 Command description

The Adjust_Frame_Sync command (or AFS for short) is used to tell the ABI interface on an MG9K to adjust its frame sync reference to sync to the inactive XPM unit. This allows the ABI and XPM to achieve proper frame sync when the XPM is connected to both the ENET and ABI during the ABI Rehome installation method.

Note: Because this is an invasive command, the user must first SET_ABI_REHOME_STATUS to ON from within TASTOOLCI.

9.4.9.2 Command syntax

Table 7 AFS command parameters and variables

Command	Parameters and variables
ADJUST_FRAME_SYNC (AFS)	<xpm_node>
Parameters and variables	**Description**
xpm_node = {0 to 4095}	The node number of the XPM

9.4.9.3 Qualifications and warnings

This command should only be used during the process of rehoming an XPM from the ENET to an MG9K. See installation method IM 72-1682: XPM to MG9000 DS512 Rehome

This command is only valid when ABI XPM Rehome Control has been enabled via the SET_ABI_REHOME_STATUS command from within TASTOOLCI.

If the user wishes to reset the frame sync between the ABI and the inactive XPM unit back to its original values, a reset of the Master ABI card is required.

9.4.9.4 Examples

```
>adjust_frame_sync 101
Request Passed

>afs 67
This command must be enabled by TAS via
the TASTOOLCI SET_ABI_REHOME_STATUS command.
Please refer to the installation method.
```

10: Configuration (CN): A00002196

10.1 Hardware and Software Requirements

All hardware and software installation complete and all commissioning activities successful.

10.2 Initial Configuration

N/A

10.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

10.4 Upgrade Impact

10.4.1 Dump and Restore

Lines with the SCA option appear in Table RESFEAT. During the ONP process SCA lines will be restored with the new field DND_ONLY set to its default value of "N."

Lines with DND active as a result of dialing the DNDACT code in table IBNXLA will appear in Table DNDMSB with a status of DNDGA. This ensures that the DND status is preserved over an ONP.

10.4.2 Element Management Upgrade

N/A

10.5 Data schema (DS) (CM, MIBS, RDB)

10.5.1 New/modified tables, MIBs, or Database Schema

IBNXLA, RESFEAT

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IBNXLA	Changed	Unchanged
RESFEAT	Changed	Unchanged

10.5.2 Table Schema information

10.5.2.1 Name: IBNXLA

IBN Translation

10.5.2.1.1 Functional description

Table IBNXLA specifies data for the translation of digits. These digits originate from both an IBN station and a RES station.

10.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

10.5.2.1.3 Size

Unchanged

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNXLA	Unchanged	Unchanged	Unchanged

10.5.2.1.4 Fields/OIDs

The following table lists fields for Table IBNXLA.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Key	Unchanged	XLANAME	Vector up to 8 Chars	Translator Name
Key	Unchanged	DGLIDX	Vector up to 18 digits	Digilator Index
Result	Unchanged	TRSEL	FEAT	Translator Selector
Result	Unchanged	ACR	Y/N	Account Code Entry
Result	Unchanged	SMDR	Y/N	Station Message Detail Recording
Result	New	FEATURE	**DNDACT**	DND Activation
Result	New	FEATURE	**DNDDEACT**	DND Deactivation

10.5.2.1.5 Datafill example

The following example shows sample datafill for table IBNXLA.

Figure 1 Table IBNXLA example datafill

```
TABLE: IBNXLA

        KEY                 RESULT
-------------------------------------------------
RXCFN  77    FEAT  N  N  DNDACT
RXCFN  78    FEAT  N  N  DNDDEACT
```

10.5.2.1.6 Table release history update

DNDACT (DND Activation) and DNDDEACT (DND Deactivation) added as new FEATURE options (type IBN_LOG_FEATURE).

10.5.2.1.7 Supplementary information

A subscriber dials the DNDACT feature access code to activate Do Not Disturb and the DNDDEACT feature access code to deactivate Do Not Disturb.

10.5.2.1.8 Translation verification

The following example shows the output from Traver when it is used to verify Table IBNXLA datafill.

Figure 2 DND Activation Traver

DND Activation:

```
>TRAVER L 6210040 B77 B
TABLE IBNLINES
HOST 00 0 00 21 0 DP STN RES 6210040 0 613_P621_0
L613_LATA1_0 613 (DND) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0
L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE NCOS
RESGRP 2 0 0 RNCOS2 ( XLAS RXCMN2 NXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA RXCFN 0 RES
TABLE DIGCOL
RES specified: RES digit collection
NCOS FEAT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME RXCFN
RXCFN 77 FEAT N N DNDACT
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature  DNDACT   not supported by TRAVER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 3 DND Deactivation Traver

DND Deactivation:

```
>TRAVER L 6210040 B78 B
TABLE IBNLINES
HOST 00 0 00 21 0 DP STN RES 6210040 0 613_P621_0
L613_LATA1_0 613 (DND) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0
L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE NCOS
RESGRP 2 0 0 RNCOS2 ( XLAS RXCMN2 NXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA RXCFN 0 RES
TABLE DIGCOL
RES specified: RES digit collection
NCOS FEAT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME RXCFN
RXCFN 78 FEAT N N DNDDEACT
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature  DNDDEACT   not supported by TRAVER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

10.5.2.2 Name: RESFEAT

RESidential line FEATures

10.5.2.2.1 Functional description

Table RESFEAT contains the assignment of custom local area signaling services (CLASS) for residential lines.

10.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

10.5.2.2.3 Size

Unchanged

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RESFEAT	Unchanged	Unchanged	Unchanged

10.5.2.2.4 Fields/OIDs

The following table lists fields for Table RESFEAT .

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LINE	Unchanged	N/A	EXT_LEN	Line Equipment Number
KEY	Unchanged	N/A	RESFEAT_ KEY_RANGE	0 to 76
FEAT	Unchanged	N/A	SCA	Selective Call Acceptance feature
VAR	Unchanged	DF Subfield	SCA	SCA Data Feature
VAR	Unchanged	AMA Subfield	{AMA, NOAMA}	Automatic Message Accounting
VAR	Unchanged	STATUS Subfield	{INACT, ACT, UNIVI, UNIVA}	Status
DND_ONLY	**NEW**	DF Refinement (DF=SCA)	**{Y, N}**	**Y** if SCA applies only when DND is active **N** for standard SCA

10.5.2.2.5 Datafill example

The following example shows sample datafill for table RESFEAT.

Figure 4 Table RESFEAT example datafill

```
TABLE: RESFEAT

            LINE     KEY     FEAT
                                                    VAR
-----------------------------------------------------------------
HOST 00 1 08 05          0      SCA
                                SCA NOAMA ACT Y
```

10.5.2.2.6 Table release history update

DND_ONLY field added to SCA data feature.

10.5.2.2.7 Supplementary information

None

10.5.2.2.8 Translation verification

Table RESFEAT is not included in TRAVER output.

10.6 Service Orders (SO) (CM & SESM)

This activity does not introduce a new LCC, a new option, or change any existing compatibilities. It does introduce a new field for the SCA option.

10.6.1 Service order change details

A new field DND_ONLY is added to the existing SCA (Selective Call Acceptance) option. Its default value is "N." When DND_ONLY is set to "Y" then this instance of SCA only applies if DND is active. If DND is not active, then SCA screening does not apply to any incoming calls.

10.6.1.1 LCC and options

Unchanged

Table 6 Meridian digital centrex feature assignment requirements

Feature	500/2500	MDC SET	ISDN SET
DND	Y	Y	Y
SCA	Y	Y	Y

10.6.2 New commands

None

10.6.2.1 How service order options are presented

10.6.2.1.1 Description

A new field will be added to the SCA feature. The new field is DND_ONLY (Y/N). When DND_ONLY is set to “Y” it indicates that this instance of SCA should only apply when DND is active on the line. If DND is not active, then this instance of SCA will not screen any incoming calls. If DND_ONLY is set to “N” then the interaction documented prior to this activity between DND & SCA applies.

10.6.2.1.2 ADO Example

The following example shows the SCA option added to a line. The field DND_ONLY is set to Y (Note its default value is N).

Figure 5 Example of the SCA option in prompt mode

```
>ADO $
DN_OR_LEN:
>6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>NOAMA
STATUS:
>ACT
DNS:
>6136210042
VBCOUNT:
>7
DNS:
>$
DND_ONLY: N
>Y
OPTION:
>$
```

Figure 6 Example of the ADO option in no-prompt mode

```
ADO $ 6210040 SCA NOAMA ACT 6136210042 7 $ Y $
```

10.6.2.1.3 Option prompts

Table 7 System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
ADO	N/A	Add Option	Servord Command
DN_OR_LEN:	A DN or a LEN	Enter the DN or LEN	DN or LEN prompt
OPTION	SCA	Selective Call Acceptance	Option Prompt
BILLING_OPTION	NOAMA or AMA	AMA Status	SCA suboption prompt (Existing)
STATUS	INACT, ACT, UNIVI, UNIVA	Activity Status	SCA suboption prompt (Existing)
DNS	TEN DIGIT DN	The DN to add to the SCA list	SCA suboption prompt (Existing)
VBCOUNT	0 TO 10	Ten Digit Count	SCA suboption prompt (Existing)
DND_ONLY	Y/N	Enter Y if this instance of SCA applies only when DND is active. Enter N for standard SCA.	SCA suboption prompt (NEW)

10.6.2.1.4 CHF Example

The following examples show the SCA feature being changed via the CHF command and the new field DND_ONLY bool defaults to N.

Figure 7 Example of the SCA option in prompt mode

```
>CHF $
DN_OR_LEN:
>6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>NOAMA
STATUS:
>ACT
DND_ONLY: N
>Y
OPTION:
>$
```

Figure 8 Example of the ADO option in no-prompt mode

```
CHF $ 6210040 SCA NOAMA ACT Y $
```

10.6.2.1.5 Option prompts

Table 8 System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
CHF	N/A	Change Feature	Servord Command
DN_OR_LEN:	A DN or a LEN	Enter the DN or LEN	DN or LEN prompt
OPTION	SCA	Selective Call Acceptance	Option Prompt
BILLING_OPTION	NOAMA or AMA	AMA Status	SCA suboption prompt (Existing)
STATUS	INACT, ACT, UNIVI, UNIVA	Activity Status	SCA suboption prompt (Existing)

Table 8 System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
DND_ONLY	Y/N	Enter Y if this instance of SCA applies only when DND is active. Enter N for standard SCA.	SCA suboption prompt (NEW)

10.6.2.1.6 Line class code compatibility

Line class code compatibility does not change with this activity.

Table 9 <abbreviated option name> compatibility to LCC

Line class code	Compatible?
RES	Yes
IBN	Yes
PSET	Yes
M5008	Yes
M5009	Yes
M5112	Yes
M5208	Yes
M5209	Yes
M5212	Yes
M5216	Yes
M5312	Yes
M5316	Yes
M6310	Yes
M6320	Yes
ISDNKSET	Yes

10.6.2.1.7 Assignability

Unchanged.

10.6.2.1.8 Option prerequisites

Unchanged

10.6.2.1.9 Notes
None

10.6.2.1.10 Feature identification
Functionality: <functional group>

Feature number: <feature number>

10.6.2.1.11 SERVORD+ Exceptions

10.7 Software optionality control (SOC)

Table 10 SOC

SOC option name:	Enh Do Not Disturb
SOC option title:	No
SOC option control type:	state
New SOC option?	Yes
SOC option order code	RES00102
Option defined in DRU:	CCM
Affected products:	NA100

10.8 Element Management
N/A

10.9 Command interface changes

10.9.1 Directory: N/A

10.9.1.1 Directory description

10.9.1.2 Accessing directory:

10.9.1.2.1 Access to directory or MAP level and return to CI

10.9.2 Command: QSL

10.9.2.1 Command type: NON-MENU

10.9.2.2 Command target: All

10.9.2.3 Command availability: RES

10.9.2.4 Command description

Query Screen List is available from the CI prompt by typing “QSL” and provides the screening lists associated with a line. Command input is not changing as a result of this activity, but the output will be changed to reflect when SCA DND_ONLY is applicable.

10.9.2.5 Command syntax

Table 11 <CommandName> command parameters and variables

Command	Parameters and variables	Description
QSL	DN_OR LEN	7- TO 10-DIGIT DN or LEN
	OPTKEY	1 to 76
	FEATURE	SLE feature name SCA, SCF, or SCRJ , or ALL
	FORMAT	F (Full) or H (Hex)

10.9.2.6 Qualifications and warnings

None

10.9.2.7 Responses

10.9.2.7.1 <response>

Table 12 MAP outputs with associated meanings and actions

Command: QSL 6210040 SCA F
<RESPONSE>: --- DN: 6136210040 LEN: HOST 00 0 00 21 SCA feature is ACTIVE and will not generate AMA records. Do Not Disturb Only: Yes. Contents of SCA list are: 6136210042 --- **Meaning:** 6136210042 is on 6136210040 SCA screening list. The output Do Not Disturb Only indicates the value of the SCA field DND_ONLY. In this example the field DND_ONLY is set to Y. When DND_ONLY is Y then SCA screening applies when DND (Do Not Disturb) is active (provided SCA is active & RES00102 is ON). If DND is active, then caller(s) on the SCA screening list (in this example, 6136210042) will bypass DND and terminate. Callers not on the SCA screening list will receive SCA treatment. If DND is not active, then all callers terminate without going through SCA screening as this iteration of SCA (DND_ONLY = Y) only applies screening when DND is active. **System or user actions:** None.

Table 12 MAP outputs with associated meanings and actions

Command: QSL 6210040 SCA F
<RESPONSE>: --- DN: 6136210042 LEN: HOST 00 0 00 21 SCA feature is ACTIVE and will not generate AMA records. Do Not Disturb Only: No. Contents of SCA list are: 6136210040 --- **Meaning:** 6136210040 is on 6136210042 SCA screening list. The output Do Not Disturb Only indicates the value of the SCA field DND_ONLY. In this example the field DND_ONLY is set to N. When DND_ONLY is N then SCA screening applies to all incoming calls (provided SCA is active) . If DND is active, then caller(s) on the SCA screening list (in this example, 6136210042) will receive DND treatment and not terminate. Callers not on the SCA screening list will receive SCA treatment. If DND is not active or not provisioned, then callers on the SCA screening list will terminate and callers not on the SCA screening list will receive SCA treatment. **System or user actions:** None

10.10 Security

None

10.11 Configuration Walkthrough

11: Configuration (CN): A00002380

11.1 Hardware and Software Requirements

North American office with MG9000 ABI.

11.2 Initial Configuration

MG9000 ABI configured.

11.3 Office/Subnet parameters (OP/SP) (CM & SESM)

11.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	ESA_GWDATA UPD_HOUR	New	CM
OFCENG	ESA_GWDATA UPD_BOOL	New	CM

11.3.2 Parameter Information

11.3.2.1 ESA_GWDATAUPD_HOUR

Emergency Stand Alone Gateway Data Update Hour.

11.3.2.1.1 Functional Description

A file called ESA_SYSTEM_SD$XML is generated every 24 hours for use during MG9000 ESA. ESA_GWDATAUPD_HOUR specifies the time the file should be generated. The time is given in one hour increments using a 24 hour clock.

11.3.2.1.2 Provisioning rules

It is recommended that ESA_GWDATAUPD_HOUR is set in the early morning after bulk provisioning has been applied but several hours before office traffic picks up.

11.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	23	6

11.3.2.1.4 Activation

Immediate with the condition that MG9000 ESA data has not already been collected in the same calendar day. Collection is allowed only once per calendar day except when done manually by the ESACOLL command in the ESATOOLS CI increment.

11.3.2.1.5 Dependencies

File ESA_SYSTEM_SD$XML will not be generated if no MG9000 ABI or ITP (LGRP) lines exist in the office or if table OFCENG parameter ESA_GWDATAUPD_BOOL is set to “N”.

File ESA_SYSTEM_SD$XML will be generated on the device specified by OFCENG parameter ESA_GWDATA_DEVICE.

11.3.2.1.6 Consequences

The MG9000 element manager pulls the ESA data every 24 hours. It is desirable for this to happen shortly after the data has been generated in the CM. Please refer to activity A00002019 - ESA EM Enhancements.

11.3.2.1.7 Verification

An ESA120 log is output upon success generation of the XML data file used during MG9000 ESA. Wait until the time specified in the office parameter either in this calendar day or if ESA data collection has already occurred, the next calendar day. Verify an ESA120 log is generated within 10 minutes of this time.

11.3.2.1.8 Memory requirements

No memory impact.

11.3.2.1.9 Parameter release history update

Initial creation. Default collection time of 6:00 AM ensures release upgrade from the SN06.2 patched version of “A00002020 - ITP ESA” will not change the ESA data collection time.

11.3.2.2 ESA_GWDATAUPD_BOOL

Emergency Stand Alone Gateway Data Update Boolean.

11.3.2.2.1 Functional description

Office parameter ESA_GWDATAUPD_BOOL controls the generation of file ESA_SYSTEM_SD$XML. This file is used during MG9000 ESA for ABI and

ITP (LGRP) lines. Note that the file will not be generated if no MG9000 based lines are present regardless of the setting of this parameter.

11.3.2.2.2 Provisioning rules

This parameter is normally set to "Y" in North American Offices with MG9000 based lines. It is not necessary to set it to "N" if no MG9000 based lines are present.

11.3.2.2.3 Range information

Table 3 Range Information

Values	Default
{Y/N}	Y

11.3.2.2.4 Activation

Immediate. MG9000 ESA data will be generated at the time specified by OFCENG parameter ESA_GWDATAUPD_HOUR.

Follow the steps in "11.11 Configuration Walkthrough" when the parameter is changed to "Y".

11.3.2.2.5 Consequences

ESA_SYSTEM_SD$XML can contain many megabytes of data. Please refer to the engineering information section of A00002020 - ESA Translation download and verify that space is available on the device specified by OFCENG parameter ESA_GWDATA_DEVICE.

The MG9000 EM will attempt to pull the ESA_SYSTEM_SD$XML file if any MG9000s use "enhanced ESA". Stale data may be used if the CM is no longer generating this data. An EM alarm may be generated if the file can not be found on the CM. The craftsperson should ensure that the MG9000 EM has all VMGs using "basic ESA" if this office parm is set to "N".

11.3.2.2.6 Verification

Erase file ESA_SYSTEM_SD$XML from the device specified by ESA_GWDATA_DEVICE and wait until the time specified by ESA_GWDATAUPD_HOUR. Ensure that the file has been generated and an ESA120 log output.

11.3.2.2.7 Memory requirements

Please refer to the EI section of A00002020 - ESA Translation Download.

11.3.2.2.8 Parameter release history update

Initial creation.

11.4 Upgrade Impact

11.4.1 Dump and Restore

ESA_GWDATAUPD_HOUR is new in this release. If a patched version of the ITP ESA activity is used this parameter will be updated automatically during an ONP.

11.4.2 Element Management Upgrade

Addressed in activity A00003567: MG 9000 Element Mgr Support for ABI ESA.

11.5 Data schema (DS) (CM, MIBS, RDB)

11.5.1 New/modified tables, MIBs, or Database Schema

Table 4 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ESAPXLA	Changed	Unchanged

11.5.2 Table/MIB/Remote Database Schema Information

11.5.2.1 Name: ESAPXLA (CM table)

Emergency Stand Alone Pretranslation Table

11.5.2.1.1 Functional description

Table ESAPXLA lists special dialing codes to be used during emergency stand alone operation and the translation results for these codes. Provisioning is allowed for every IBN customer group and ABI XPM combination with translator name ESAPOTS being used for non-IBN lines.

Note that 911 lines must be available for each ABI since individual ABIs can enter ESA while other ABIs and LGRPs on the MG9000 do not. Translations for each ABI must be provided in table ESAPXLA so that 911 will terminate properly.

11.5.2.1.2 Usage sequence and implications (CM Only)

Usage of the “L” selector requires that tables LENLINES, IBNLINEs, and KSETLINES be provisioned before table ESAPXLA. Usage of the “H” selector requires that table HUNTMEM be provisioned before table ESAPXLA. These are existing requirements.

Prior to this activity only RCC and RLCM type peripherals could be used in table ESAPXLA. This activity allows LGC/LTC and SMA type peripherals to be used. These peripherals are provisioned in table LTCINV. This is not

expected to add a new dependency since LENLINES also depends on LTCINV and is already required.

11.5.2.1.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ESAPXLA	0	32 x N x M[a]	No Change. Each new XLANAME/LGRP combination uses 16 bytes for a header. Each tuple uses an additional 16 bytes.

a. N is the number of LGRPs and M is the number of XLANAME entries used including ESAPOTS for POTS lines.

11.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for table ESAPXLA.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PXLAKEY	CHANGED	NODE	PMTYPE	ABI selection added. Allows any XPM supported by ABI ESA as part of an ESAPXLA tuple key. ABI XPMs have the EXTDS512 option in table LTCINV.

11.5.2.1.5 Datafill example

```
ESAPOTS  ABI        LGC   0            201 L REM1  00 0 02 08 N 0
ESAPOTS  ABI        LGC   0            400             T REORDER
ESAPOTS  ABI        LGC   0            402           A ESAPOTS Y
REM1XLA  ABI        LGC   0            202             T SRPDXLA
REM2XLA  ABI        LGC   0            800             T REORDER
REM2XLA  ABI        LGC   0            801         H     3   9 N
```

11.5.2.1.6 Table release history update

Add ESA support for MG9000 ABI XPMs.

11.5.2.1.7 Supplementary information

MG9000 ABIs do not support trunks in ESA so references to table ESARTE or ESAHNPA are not allowed.

The “L” selector allows terminations to a line with a given line equipment number (LEN). The LEN will be screened to ensure it has MG9000 ESA support.

The “H” selector allows terminations to hunt members given the hunt group number specified in table HUNTGRP and the hunt member number specified in table HUNTMEM. The hunt member will be screened to ensure it has MG9000 ESA support.and is served by the same ABI XPM as used in the tuple key.

11.5.2.1.8 Translation verification other tools

Please refer to section “8.9.2 Command: ESATRAVER”.

11.6 Service Orders (SO) (CM & SESM)

No change.

11.7 Software optionality control (SOC)

No change.

11.8 Element Management

Please refer to documentation for activity A00003567: MG 9000 Element Mgr Support for ABI ESA.

11.9 Command Interface Changes

11.9.1 Directory: ESATOOLSDIR

11.9.1.1 Directory description

The ESATOOLS CI increment provides a number of customer tools to verify and operate on CS2000 ESA data. This activity will enhance the ESATRAVER command to work with MG9000 ABI lines.

11.9.1.2 Accessing directory: ESATOOLSDIR

11.9.1.2.1 Access to directory or MAP level and return to CI

To access the ESATOOLS CI increment, type ESATOOLS from the command prompt. To exit ESATOOLS back to the CI environment, type QUIT.

11.9.2 Command: ESATRAVER

Please note that this section includes changes for ESATRAVER related to MG9000 LGRPs and ABI XPMs. It supersedes any prior ESATRAVER

documentation for MG9000. In particular, the ESATRAVER description in activity “A00002020 - ESA Translation Download” is no longer accurate.

11.9.2.1 Command type: NON-MENU

11.9.2.2 Command target: All

11.9.2.3 Command availability: RES

11.9.2.4 Command description

ESATRAVER is a command in the ESATOOLS CI increment which is used to verify ESA translations data in the Call Server.

11.9.2.5 Command syntax

Table 7 ESATRAVER command parameters and variables

Command	Parameters and variables
ESATRAVER	<ORIG> {TR <CLLI> STRING, L <LINE> STRING} <DIGITS> STRING <TRACE> {T, NT, B}
Parameters and variables	**Description**
ORIG	TR <CLLI> : For trunk originations, enter TR and the CLLI name of the trunk group L <LINE> : For line originations, enter L and the 7-digit directory number of the line
DIGITS	Enter the dialled digits to be verified.
TRACE	T = Trace NT = NoTrace B = Both

11.9.2.6 Qualifications and warnings

The ESATRAVER command syntax has not changed. The software has been enhanced to allow verification of lines originating and terminating on MG9000 ABI XPMs. It is already capable of handling MG9000 LGRPs.

Since the MG9000 does not support trunks, the TR <CLLI> parameter does not apply.

11.9.2.6.1 SETRCC command interactions.

SETRCC is an existing command in ESATOOLS that is used to collect trunk group data on an RCC. The SETRCC command must be run for an RCC before the ESATRAVER command can be used on a line or trunk on that RCC.

Since MG9000 does not support trunks in ESA, the SETRCC command is not required prior to issuing the ESATRAVER command on a line on an MG9000.

If SETRCC is done on a particular RCC, an MG9000 ESATRAVER will not use the collected trunk group data and will not affect the data in any way. An MG9000 ESATRAVER can be followed by ESATRAVER on a line or trunk on that RCC without reissuing the SETRCC command.

11.9.2.7 Responses

11.9.2.7.1 Warning: Cannot verify MG9000 Terminator accessible from Originator.

Command: ESATRAVER
Output: Warning: Cannot verify MG9000 Terminator accessible from Originator. **Meaning:** The ESATRAVER command has determined that both the originating and terminating lines are MG9000 based but can not verify that they can call each other during ESA. The main reason for this is that the lines are served by different MG9000s. LGRP to LGRP calls are necessarily on the same site but there is no such restriction with calls involving an ABI line. ESATRAVER between LGRP lines at different sites will not show as completing and will not receive this warning message. **User actions:** The user must verify at the Element Manager that both lines are controlled by the same MG9000.

11.9.2.7.2 NO MATCH

Command: ESATRAVER
Output: NO MATCH **Meaning**: This is a generic error message that indicates that the digits dialled do not translate to a valid terminator from this originator. For an MG9000 line originator this response indicates that the terminator is not on an MG9000. For MG9000 LGRP to LGRP calls it can also mean the two LGRPs are on different sites. **User Actions**: ESATRAVER should be used with originating and terminating lines that can call each other during ESA.

11.9.3 Directory: LGCDIR

11.9.3.1 Directory description

The LGCDIR directory is associated with the LGC level of the MAP. It is available whenever an XPM of node_type LGC is posted. The LGC node_type encompasses a number of PM types including LTC, SMS, SMSR, DTC, SMA2 ... From this directory/map level, maintenance on the posted XPM can be performed.

This activity renames the ABILink directory to ABI. The QUERYPM command is enhanced to query the ABI board for esa capability. This new information of esa enabled/disabled will ONLY exist on ABI-hosted XPMs which not only support ABI ESA funtionality but are capable of esa. The PM types which support ABI ESA functionality are: LGC, LGC with ISP card, or SMA2.

In addition, the maintenance commands (TST, PMRESET, LOADPM, RECOVER, RTS) are enhanced to disallow the maintenance action if the ABI board is in ESA. However the craftsperson is prompted to continue the maintenance action by exitting esa. This new functionality will ONLY exist on ABI-hosted XPMs which support ABI ESA functionality: LGC, LGC with ISP card datafilled, and SMA2.

11.9.3.2 Accessing directory: LGCDIR

11.9.3.2.1 Access to directory or MAP level and return to CI

To enter this directory from the CI evironment, type:

MAPCI;MTC;PM;POST <pm type> <pm number>

To quit, enter:

> QUIT ALL

11.9.3.3 MAP display

The ABILink directory renamed to ABI.

Figure 1 ABILink directory renamed to ABI

```
  XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .         .       .        .        .        .        .
LGC                                   SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit           PM                    12        0        0        0        0        0
 2 Post_          LGC                    1        0        0        0        0        0
 3 ListSet
 4 ABI        LGC      0 ManB  Links_OOS: CSide  0 , PSide  0
 5 Trnsl_      Unit0:   Act   ManB
 6 Tst_        Unit1:   Inact ManB
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_
12 Next
13 SwAct
14 QueryPM
15 DCH
16
17 PERFORM
18 ISG
  ADMIN
```

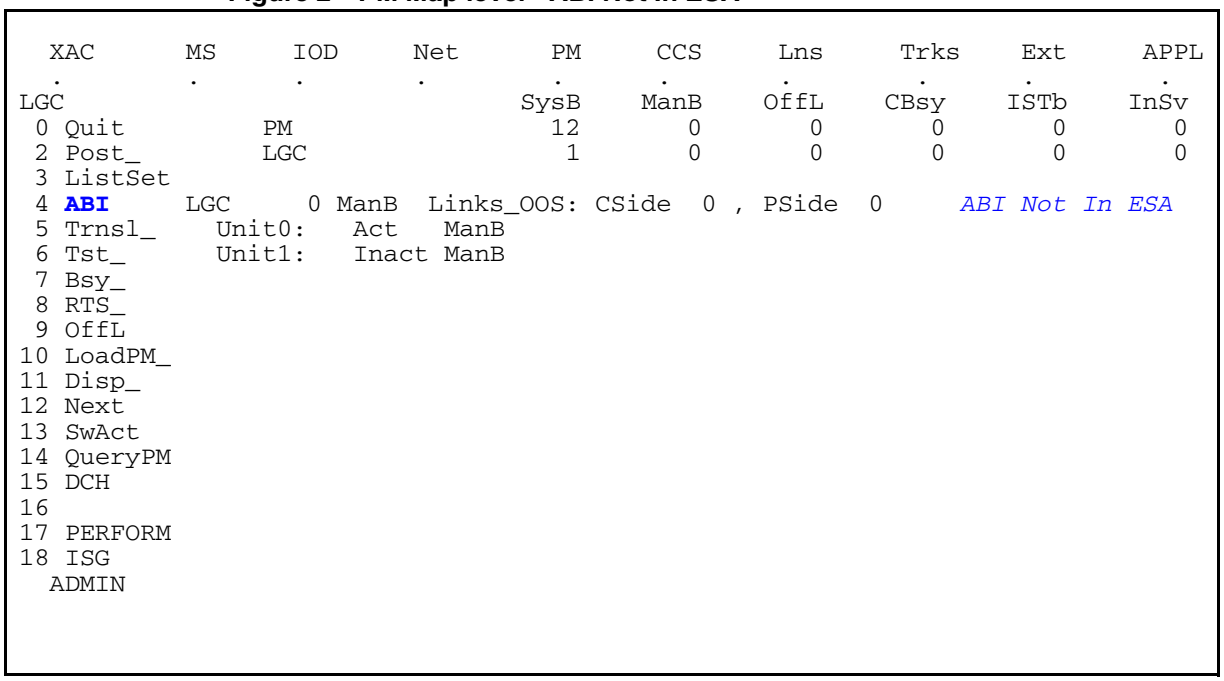
11.9.3.4 ABI ESA MAP status indicator

The new ABI ESA map status indicator is displayed whenever the ABI-hosted XPM has the the following manual maintenance commands initiated (TST, PMRESET, LOADPM, RECOVER, RTS, BSY).

11.9.3.4.1 ABI ESA status MAP indicator - ABI Not in ESA (new)

The ABI ESA status of *ABI Not in ESA* is displayed whenever the ABI board is cabable of ESA and is NOT in ESA.

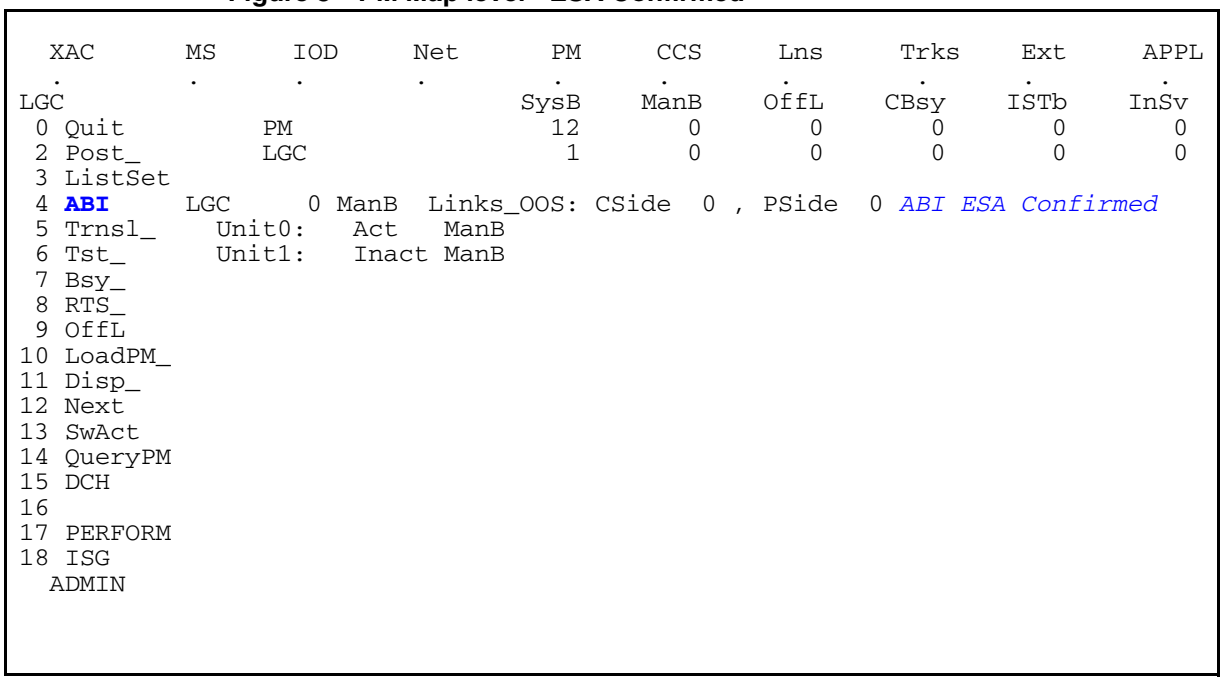
Figure 2 PM Map level - ABI Not In ESA



11.9.3.4.2 ABI ESA status MAP indicator - ABI ESA confirmed (new)

The ABI ESA status of *ABI ESA confirmed* is displayed whenever the ABI board is cabable of ESA and is IN ESA.

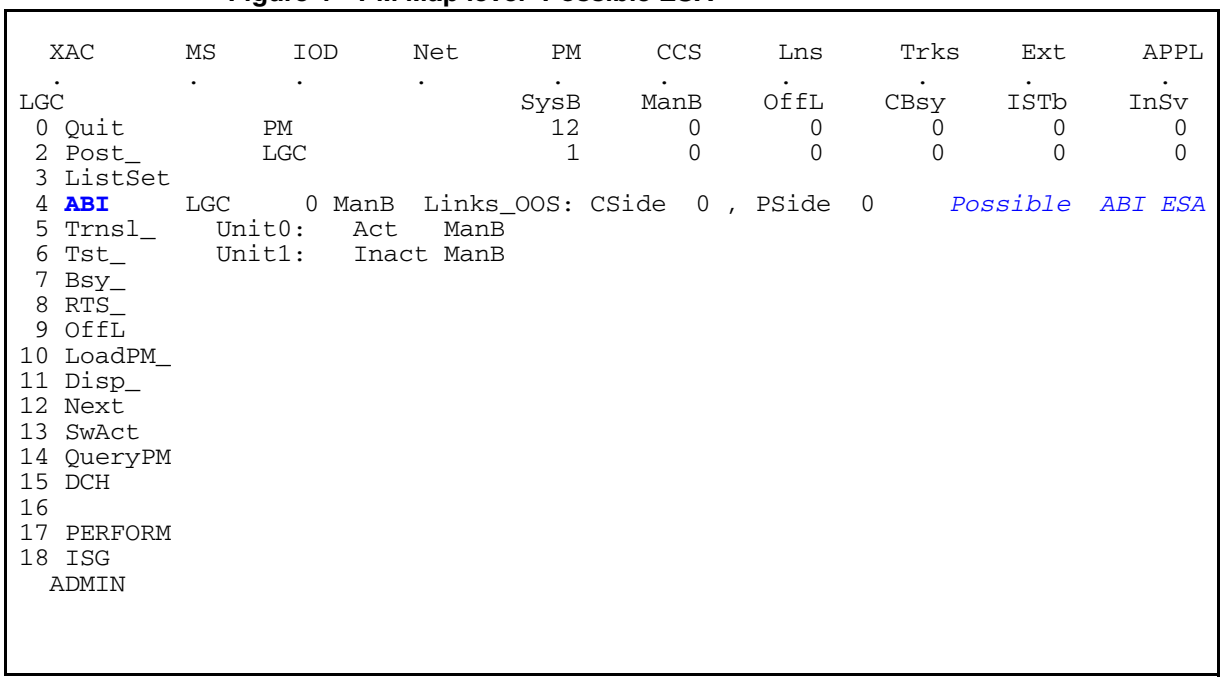
Figure 3 PM Map level - ESA Confirmed



11.9.3.4.3 ABI ESA status MAP indicator - ABI Possible ESA (new)

Possible ABI ESA will be displayed whenever the ABI board is cabable of ESA and communication between the CM and the ABI is down. For example, whenever an InSv ABI-hosted XPM which in capable of ESA goes Cside Busy (CBsy), the ABI ESA map status of Possible ABI ESA will be displayed.

Figure 4 PM Map level -Possible ESA



11.9.4 Command: QUERYPM (existing)

Please note that this section includes additional information for the QUERYPM command for ABI-hosted XPMs which are capable of ESA.

11.9.4.1 Command type: MENU

11.9.4.2 Command target: All

11.9.4.3 Command availability: RES

11.9.4.4 Command description

QUERYPM is a command in the LGCDIR CI increment which is used to query the PM for data. New ABI ESA information is displayed if the ABI board is capable of ESA.

11.9.4.5 Command syntax

Not changed.

11.9.4.6 Qualifications and warnings

none.

11.9.4.7 Responses

11.9.4.7.1 ABI Enhanced ESA enabled - check Element Manager

Command: QUERYPM
Output: ABI Enhanced ESA enabled - check Element Manager **Meaning:** The QUERYPM command queried the ABI board which is capable of ESA and has ESA functionality enabled. The craftsperson can check the Element Manager to verify it's viewpoint of enhanced esa. **User actions:** None. Informational purposes only

11.9.4.7.2 ABI Enhanced ESA disabled - check Element Manager

Command: QUERYPM
Output: ABI Enhanced ESA disabled - check Element Manager **Meaning**: The QUERYPM command queried the ABI board which is capable of ESA and has ESA functionality disabled. The craftsperson can check the Element Manager to verify it's viewpoint of enhanced esa. **User Actions**: None. Informational purposes only

11.9.4.7.3 ABI ESA information not available - no response

Command: QUERYPM
Output: ABI ESA information not available - check Element Manager **Meaning**: The QUERYPM command queried the ABI board and the ABI board did not respond. The craftsperson can check the Element Manager to verify it's viewpoint of enhanced esa. **User Actions**: None. Informational purposes only

11.9.4.7.4 ABI ESA information not available - GWC out of service

Command: QUERYPM
Output: ABI ESA information not available - GWC is out of service **Meaning**: The QUERYPM command attempted to query the ABI board but the host GWC node was out of service. **User Actions**: None. Informational purposes only

11.9.5 Command: TST, PMRESET, LOADPM (existing)

Please note that this section includes changes for TST, PMRESET, and LOADPM only for ABI-hosted XPMs which are capable of ESA. Before performing the initiated maintenance command, the ABI board is queried to determine if it is in ESA. If the ABI board is in ESA or communication is not established between the CM and the ABI board, then the maintenance

command will be rejected. The craftsperson has the option of requesting the ABI board to exit esa and continuing with the maintenance action.

11.9.5.1 Command type: MENU

11.9.5.2 Command target: All

11.9.5.3 Command availability: RES

11.9.5.4 Command description

TST is a command in the LGCDIR CI increment which is used to perform InSv and out-of-service (OOS) diagnostics on the PM. OOS diagnostics occur on a ManB PM/unit. The PM/unit is dropped to ROM at the beginning of the TST command to run ROM diagnostics. PMRESET is a command in the LGCDIR CI increment which is used to drop the ABI-hosted XPM to ROM-level.

LOADPM is a command in the LGCDIR CI increment which is used to load an XPM load into the ABI-hosted XPM. Loading of the XPM is performed only at ROM-level.

Berfore allowing the XPM to be dropped to ROM-level the ABI board is verified if it is in ESA. If so, the craftsperson is informed that the ABI board is in ESA and maybe processing calls. The craftsperson can chose to continue and exit ESA and if exit fails, to force exit the ABI board out of ESA.

11.9.5.5 Command syntax (existing)

The command syntax for the TST, PMRESET, LOADPM, and BSY commands did not change.

11.9.5.6 Qualifications and warnings

The only change to existing behavior is to allow the craftsperson to initiate an ABI esa exit and continue the XPM maintenance command. MAPCI responses are displayed at the MAP for ABI-hosted XPMs which are capable of ESA.

11.9.5.7 Responses (new)

11.9.5.7.1 A COLD ABI ESA Exit will be attempted.

Command: TST
Output: <pmtype> <xpm number> Unit <unit number> A COLD ABI ESA Exit will be attempted **ALL active ESA calls will be ABORTED** **Please confirm ('YES', 'Y', 'NO', or 'N');** **Meaning:** The TST command queried the ABI and determined that the ABI board has esa enabled and is in ESA and out-of-service diagnostics are not permitted. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exitting abi esa.

Command: PMRESET
Output: <pmtype> <xpm number> Unit <unit number> A COLD ABI ESA Exit will be attemped **ALL active ESA calls will be ABORTED** **Please confirm ('YES', 'Y', 'NO', or 'N');** **Meaning:** The PMRESET command queried the ABI and determined that the ABI board has esa enabled and is in ESA and a PMRESET is not permitted. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exitting abi esa.

Command: LOADPM
Output: <pmtype> <xpm number> Unit <unit number> A COLD ABI ESA Exit will be attempted **ALL active ESA calls will be ABORTED** **Please confirm ('YES', 'Y', 'NO', or 'N');** **Meaning:** The LOADPM command queried the ABI and determined that the ABI board has esa enabled and is in ESA and a LOADPM is not permitted. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exitting abi esa.

Figure 5 Mapci response - A Cold ABI ESA Exit will be attempted

```
  XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .         .       .        .        .        .        .
LGC                                   SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                     12        0        0        0        0        0
 2 Post_         LGC                     1        0        0        0        0        0
 3 ListSet
 4 ABI       LGC     0 ManB  Links_OOS: CSide  0 , PSide  0 ABI ESA Confirmed
 5 Trnsl_     Unit0:   Act   ManB
 6 Tst_       Unit1:   Inact ManB
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_    > LGC 0 A Cold ABI ESA Exit will be attempted
12 Next
13 SwAct            ALL active ESA calls will be ABORTED
14 QueryPM    Please confirm ("YES", "Y", "NO", or "N");
15 DCH
16
17 PERFORM
18 ISG
  ADMIN
```

11.9.5.7.2 A Force will allow maintenance actions

Command: TST
Output: <pmtype> <xpm number> Unit <unit number> A Force will allow maintenance actions **This action will result in a CALL PROCESSING OUTAGE** **Please confirm ('YES', 'Y', 'NO', or 'N');** **Meaning:** The TST command queried the ABI and determined that the ABI board has esa enabled and is in ESA and the craftsperson attempted to exit esa, but the abi board can only partially exit esa. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exit forcing esa.

Command: PMRESET
Output: <pmtype> <xpm number> Unit <unit number> A Force will allow maintenance actions **This action will result in a CALL PROCESSING OUTAGE** **Please confirm ('YES', 'Y', 'NO', or 'N');** **Meaning:** The PMRESET command queried the ABI and determined that the ABI board has esa enabled and is in ESA and the craftsperson attempted to exit esa, but the abi board can only partially exit esa. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exit forcing esa.

Command: LOADPM

Output: <pmtype> <xpm number> Unit <unit number> A Force will allow maintenance actions

This action will result in a CALL PROCESSING OUTAGE

Please confirm ('YES', 'Y', 'NO', or 'N');

Meaning: The LOADPM command queried the ABI and determined that the ABI board has esa enabled and is in ESA and the craftsperson attempted to exit esa, but the abi board can only partially exit esa.

User actions: Craftsperson has the option of leaving the ABI in ESA or continuing by exit forcing esa.

Figure 6 Mapci response - A Cold ABI ESA Exit will be attempted

```
  XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .         .       .        .        .        .        .
LGC                                   SysB    ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                     12       0        0        0        0        0
 2 Post_         LGC                     1       0        0        0        0        0
 3 ListSet
 4 ABI       LGC     0 ManB  Links_OOS: CSide  0 , PSide  0 ABI ESA Confirmed
 5 Trnsl_     Unit0:   Act   ManB
 6 Tst_       Unit1:   Inact ManB
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_    > LGC 0 A Force will allow maintenance actions
12 Next
13 SwAct            This action will result in a CALL PROCESSING OUTAGE
14 QueryPM    Please confirm ("YES", "Y", "NO", or "N");
15 DCH
16
17 PERFORM
18 ISG
  ADMIN
```

11.9.5.7.3 ABI communication is NOT possible.

Command: TST
Output: <pmtype> <xpm number> Unit <unit number> ABI communication is NOT possible **Perform ABI maintenance from the Element Manager.** **Meaning:** The TST command tried to query the ABI and received no response, out-of-service diagnostics are not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

Command: PMRESET
Output: <pmtype> <xpm number> Unit <unit number> ABI communication is NOT possible **ABI maintenance may be performed from the Element Manager.** **Meaning:** The PMRESET command tried to query the ABI and received no response, PMRESET is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

Command: LOADPM
Output: <pmtype> <xpm number> Unit <unit number> ABI communication is NOT possible **ABI maintenance may be performed from the Element Manager.** **Meaning:** The LOADPM command tried to query the ABI and received no response, LOADPM is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

Figure 7 PM Map level - ABI Communication NOT possible

```
  XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
  .         .       .        .         .       .        .        .        .        .
LGC                                   SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                     12        0        0        0        0        0
 2 Post_         LGC                     1        0        0        0        0        0
 3 ListSet
 4 ABI      LGC     0 ManB  Links_OOS: CSide  0 , PSide  0     Possible  ABI ESA
 5 Trnsl_     Unit0:   Act   ManB
 6 Tst_       Unit1:   Inact ManB
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_  LGC 2 Unit 0 ABI Communication is NOT possible
12 Next                Perform ABI maintenance from the Element Manager
13 SwAct
14 QueryPM
15 DCH
16
17 PERFORM
18 ISG
   ADMIN
```

11.9.6 Command: RTS, RECOVER (existing)

Please note that this section includes changes for RTS and RECOVER related to ABI-hosted XPMs. These commands will drop the ABI-hosted XPM to ROM before performing the initiated maintenance command. If the ABI is in ESA the craftsperson can chose to continue and exit the ABI board out of ESA but the craftsperson is not allowed to force exit the ABI board out of ESA.

11.9.6.1 Command type: MENU

11.9.6.2 Command target: All

11.9.6.3 Command availability: RES

11.9.6.4 Command description

RTS is a command in the LGCDIR CI increment which is used to recover the ABI-hosted XPM unit(s) from a ManB to an InSv state. RTS can only occur on a ManB PM/unit. If the ABI is in ESA or communication is not established between the CM and the ABI, the RTS command will be rejected. If the ABI is in ESA, then the craftsperson will be prompted to initiate exit esa causing ALL active calls to be aborted.

RECOVER is a command in the LGCDIR CI increment which is used to recover the ABI-hosted XPM from a ManB or SysB to an InSv state.

RECOVER will reload the units if necessary and recover the units to an InSv state.

11.9.6.5 Command syntax (existing)

The command syntax for the RTS and RECOVER commands did not change.

11.9.6.6 Qualifications and warnings

The only change to existing behavior is to display failure responses at the MAP for ABI-hosted XPMs and to initiate ABI esa exit.

11.9.6.7 Responses (new)

11.9.6.7.1 ABI callp is NOT possible.

Command: RTS
Output: <pmtype> <xpm number> Unit <unit number> ABI callp is NOT possible **Perform ABI maintenance from the Element Manager** **Meaning:** The RTS command queried the ABI and determined that the ABI board has esa enabled and is in partially in ESA and the RTS is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

Command: RECOVER
Output: <pmtype> <xpm number> Unit <unit number> ABI callp is NOT possible **Perform ABI maintenance from the Element Manager** **Meaning:** The RECOVER command queried the ABI and determined that the ABI and ABI board has esa enabled and is in partially in ESA and the RECOVER is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

11.9.6.7.2 ABI communication is NOT possible.

Command: RTS
Output: <pmtype> <xpm number> Unit <unit number> ABI communication is NOT possible **ABI maintenance may be performed from the Element Manager.** **Meaning:** The RTS command tried to query the ABI and received no response, RTS is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

Command: RECOVER
Output: <pmtype> <xpm number> Unit <unit number> ABI communication is NOT possible **ABI maintenance may be performed from the Element Manager.** **Meaning:** The RECOVER command tried to query the ABI and received no response, RECOVER is not permitted. **User actions:** Craftsperson has the option of performing ABI maintenance from the Element Manager.

11.9.6.7.3 A Cold ABI ESA Exit will be attempted.

Command: RTS
Output: <pmtype> <xpm number> Unit <unit number> A Cold ABI ESA Exit will be attempted **This will cause ALL active calls to be ABORTED** **Please confirm (“YES”, “Y”, “NO”, “N”):** **Meaning:** The RTS command queried the ABI and determined that the ABI board has esa enabled and is in ESA and a RTS is not permitted. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exitting abi esa.

Command: RECOVER
Output: <pmtype> <xpm number> Unit <unit number> A Cold ABI ESA Exit will be attempted **This will cause ALL active calls to be ABORTED** **Please confirm ("YES", "Y", "NO", "N"):** **Meaning:** The RECOVER command queried the ABI and determined that the ABI board has esa enabled and is in ESA and a RECOVER is not permitted. **User actions:** Craftsperson has the option of leaving the ABI in ESA or continuing by exitting abi esa.

11.9.7 Directory: ABIDIR

11.9.7.1 Directory description

The ABIDIR directory is associated with the ABI level of the MAP. It is available whenever an ABI-hosted XPM is posted. The LGC node_type encompasses a number of pm_types including LTC, SMS, SMSR, DTC, SMA2 ... From this directory/map level, maintenance on the posted ABI-hosted XPM can be performed.

11.9.8 Command: QUERYABI (new)

11.9.8.1 Command type: MENU

11.9.8.2 Command target: All

11.9.8.3 Command availability: RES

11.9.8.4 Command description

QUERYABI is a command in the ABIDIR CI increment which is used to display table GATWYINV information and display the ABI board's esa capability of enabled/disabled if the ABI board has esa functionality.

11.9.8.5 Command syntax

Table 8 ABIEXITESA command parameters and variables

Command	Parameters and variables
QUERYABI	none

11.9.8.6 Qualifications and warnings

The QUERYABI command is only available when an ABI-hosted XPM is posted.

11.9.8.7 Responses

11.9.8.7.1 ABI Enhanced ESA enabled.

Command: QUERYABI
Output: ABI ESA enabled. **Meaning:** The QUERYABI command queried the ABI board for it's ESA capability. The information displayed informs the craftsperson that the abi board has esa enabled. **User actions:** None. Informational purposes only

11.9.8.7.2 ABI Enhanced ESA disabled

Command: QUERYABI
Output: ABI ESA disabled **Meaning**: The QUERYABI command queried the ABI board for it's ESA capability. The information displayed informs the craftsperson that the abi board has esa disabled. **User Actions**: None. Informational purposed only.

11.9.8.7.3 ABI ESA information not available - GWC is out of service

Command: QUERYABI
Output: ABI ESA information not available - GWC is out of service **Meaning**: The QUERYABI command attempted to query the ABI board for it's ESA capability. The information displayed informs the craftsperson that the cside host node (GWC) of the ABI-hosted XPM is out-of-service. **User Actions**: None. Informational purposed only.

11.9.8.7.4 ABI ESA information not available - check Element Manager

Command: QUERYABI
Output: ABI ESA information not available - check Element Manager **Meaning**: The QUERYABI command attempted to query the ABI board for it's ESA capability. The information displayed informs the craftsperson that the ABI board did not respond to the esa query. **User Actions**: None. Informational purposed only.

11.10 Security

The security issue of the FTP transfer of file ESA_SYSTEM_SD$XML from the CM to the MG9000 EM is considered in activity A00002019 - ESA EM Enhancements.

11.11 Configuration Walkthrough

Please refer to activityA00002019 ESA EM Enhancements for information on configuring the MG9000 EM.

1. Verify tuples exist in table LTCINV with the EXTDS512 option. This indicates the XPM has ABI capability.

```
TABLE: LTCINV
>top
       LGC    0
```

```
             10    LTEI    0     4      1    C    31 6X02NA  QLI20AZ
 (          POTS   POTSEX) (       KEYSET   KSETEX) (     RMM_TERM    RSMEX)$
                (         4  0) (         4  1) (         4  2) (         4  3)$
                                (     UTR15 ) (   MSG6X69 ) (       ISP 16)$
     NORTHAM     SX05AA $ SX05AA $
                                                        0
                            SXFWAJ01
                            (EXTDS512 HOST 1 2 192 2 7 65 GWC 3) $
     6X40FB                                             N
```

2. Provision special dialing codes in table ESAPXLA for POTS (XLANAME = ESAPOTS) as well as for XLANAMEs used by IBN customer groups with member lines on the ABI XPM.

```
>table ESAPXLA
>lis all

TOP
                                  PXLAKEY                  RESULT
-----------------------------------------------------------------
 ESAPOTS ABI LGC 0              411 T REORDER
 ESAPOTS ABI LGC 0              911 L HOST 00 2 03 01 N 0
```

3. Set OFCENG parameter ESA_GWDATA_DEVICE

```
This step is not necessary if SFDEV is being used to hold MG9000 ESA data.

It is recommended that a disk device be used so that SFDEV is available for other
uses.
```

4. Set OFCENG parameter ESA_GWDATAUPD_HOUR

```
This step is not necessary if the default generation time of 6:00 AM is acceptable.
```

5. Verify OFCENG parameter ESA_GWDATAUPD_BOOL is set to “Y”.

6. Generate ESA data file using ESATOOLS.

```
>ESATOOLS
>ESACOLL
Warning: All MG9000 ESA data will be rebuilt.
Please confirm ("YES", "Y", "NO", or "N"):
>Y
ESA static data generation initiated.
ESA 120 log will be output upon successful generation of
file ESA_SYSTEM_SD$XML on device D000ESA.

... have prompt back - wait for ESA120/ESA121 log

LOGUTIL ESA
Done.
RTP207BT      ESA120 NOV20 11:12:21 8500 INFO ESA DATA GENERATION


>DISKUT
>LISTFL D000ESA
ESA_SYSTEM_SD$XML

QUIT ALL
```

7. ESA data file will be automatically generated every 24 hours at the time specified by ESA_GWDATAUPD_HOUR. An ESA120 log is output when the data is successfully generated.

12: Configuration (CN): A00002431

12.1 Hardware and Software Requirements

None.

12.2 Initial Configuration

None.

12.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

12.4 Upgrade Impact

12.4.1 Dump and Restore

During an ONP from an earlier release where the capindx field is not present to a release where the capindx field is introduced in table MNNODE, this field is set to ‘Standard’.

12.4.2 Element Management Upgrade

Not Applicable.

12.5 Data schema (DS) (CM)

12.5.1 New/modified tables

Table 1 Modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	CHANGED	NEW
MNCKTPAK	CHANGED	NEW

12.5.2 Table information

12.5.2.1 Name: MNNODE

12.5.2.1.1 Functional description

A new field ‘capindx’ is added in table MNNODE for DMSCP class of SPMs only. This new field can take the values ‘Standard’, ‘Enhanced’ or ‘Premium’ where ‘Standard’ is the default value.

During tuple addition in table MNNODE, for using ‘Enhanced’ or ‘Premium’ values, the respective SOC options must have its RTU set to Y and the Usage count must be less than its Limit. Also for using ‘Enhanced’ capacity, number of DMSCP SPMs provisioned with Enhanced capacity must be less than the limit of SPMS0020 SOC option and for using ‘Premium’ capacity, number of DMSCP SPMs provisioned with Premium capacity must be less than the limit of SPMS0028 SOC option.

While changing the capindx field to ‘Enhanced’ or ‘Premium’ values, the PEC codes of the CEM units provisioned in table MNCKTPAK for this node are also verified for NTLX82BA, in addition to the SOC check. If all the check passes, the appropriate SOC usage value is incremented. For capindx field changes from ‘Enhanced’ or ‘Premium’ values to ‘Standard’, appropriate SOC usage counts are decremented if both the CEM tuples are present in table MNCKTPAK.

Tuple change with No change to the ‘capindx’ field is not validated. For tuple deletion, there are no restrictions enforced on this field. Refer table 2, table 3 and table 4 for the various Error, Warning and Success messages that are introduced in table MNNODE as part of this activity.

Note: All the table control operations in table 2 shall be failed with appropriate error messages and all the table control operation in table 3 and table 4 shall be passed with appropriate messages.

Table 2 New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
1	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity.	SPMS0020 SOC option's RTU set to 'N'
	RTU value not set for SPM Enhanced capacity SOC option SPMS0020.	
2	a. Tuple addition in MNNODE with 'Premium' capacity. b. Tuple change in MNNODE from 'Standard' to 'Premium' capacity. c. Tuple change in MNNODE from 'Enhanced' to 'Premium' capacity.	SPMS0028 SOC option's RTU set to 'N'
	RTU value not set for SPM Premium capacity SOC option SPMS0028.	
3	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity.	SPMS0020 SOC option's Limit is equal to the No. of SPMs provisioned with 'Enhanced' capacity.
	Capindx cannot be provisioned as Enhanced capacity for more SPMs than the limit of SOC option SPMS0020. Check existing tuples using SPMCPCAP tool.	

Table 2 New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
4	a. Tuple addition in MNNODE with ‘Premium’ capacity. b. Tuple change in MNNODE from ‘Standard’ to ‘Premium’ capacity. c. Tuple change in MNNODE from ‘Enhanced’ to ‘Premium’ capacity.	SPMS0028 SOC option's Limit is equal to the No. of SPMs provisioned with ‘Premium’ capacity.
	Capindx cannot be provisioned as Premium capacity for more SPMs than the limit of SOC option SPMS0028. Check existing tuples using SPMCPCAP tool.	
5	a. Tuple change in MNNODE from ‘Standard’ to ‘Enhanced’ capacity.	a. No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or Both the CEM PEC is/are not NTLX82BA.
	Both CEM PEC codes must be NTLX82BA for Enhanced capacity. **Verify MNCKTPAK datafill.**	
6	a. Tuple change in MNNODE from ‘Standard’ to ‘Premium’ capacity.	a. No. of SPMs provisioned with Premium capacity is less than the Limit and b. One or Both the CEM PEC is/are not NTLX82BA.
	Both CEM PEC codes must be NTLX82BA for Premium capacity. **Verify MNCKTPAK datafill.**	

Table 3 New Warning Messages

No.	Table Control operations	Pre - conditions
	Warning Messages	
1	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity	a. SPMS0020 SOC option's RTU set to Y, No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or both the CEM tuples in table MNCKTPAK is/are not provisioned.
	WARNING: Capindx provisioned as Enhanced capacity. **Both CEMs must be provisioned as NTLX82BA.**	
2	a. Tuple addition in MNNODE with 'Premium' capacity. b. Tuple change in MNNODE from 'Standard' to 'Premium' capacity. c. Tuple change in MNNODE from 'Enhanced' to 'Premium' capacity.	a. SPMS0028 SOC option's RTU set to Y, No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or both the CEM tuples in table MNCKTPAK is/are not provisioned.
	WARNING: Capindx provisioned as Premium capacity. **Both CEMs must be provisioned as NTLX82BA.**	

Table 4 New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
1	a. Tuple change in MNNODE from 'Enhanced' to 'Standard' capacity.	Both the CEM tuples are present in table MNCKTPAK.
	Datafill conditions met for de-activation of **SPM Enhanced capacity SOC option SPMS0020.**	
2	a. Tuple change in MNNODE from 'Premium' to 'Standard' capacity.	Both the CEM tuples are present in table MNCKTPAK.
	Datafill conditions met for de-activation of **SPM Premium capacity SOC option SPMS0028.**	

Table 4 New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
3	a. Tuple change in MNNODE from 'Standard' to 'Enhanced'. b. Tuple change in MNNODE from 'Premium' to 'Enhanced'.	a. No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. Both the CEM tuples are present in table MNCKTPAK and both the CEM PEC are NTLX82BA.
	Datafill conditions met for activation of SPM Enhanced capacity SOC option SPMS0020.	
4	a. Tuple change in MNNODE from 'Standard' to 'Premium'. b. Tuple change in MNNODE from 'Enhanced' to 'Premium'.	a. No. of SPMs provisioned with Premium capacity is less than the Limit and b. Both the CEM tuples are present in table MNCKTPAK and both the CEM PEC are NTLX82BA.
	Datafill conditions met for activation of SPM Premium capacity SOC option SPMS0028.	

12.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

12.5.2.1.3 Size

Not impacted.

12.5.2.1.4 Fields/OIDs

The following table lists fields for table MNNODE which are changed as part of this activity.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CAPINDX	New	Not Applicable		This field is introduced for DMSCP class of SPMs only in table MNNODE.

12.5.2.1.5 Datafill example

Datafill examples for each capacity datafilled in table MNNODE are shown below.

Figure 1 Datafill example

```
SPM 1 SPM_1 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) $ (ABTRK SPMEX) $ STANDARD

SPM 2 SPM_2 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) $ (ABTRK SPMEX) $ ENHANCED

SPM 3 SPM_3 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) $ (ABTRK SPMEX) $ PREMIUM
```

12.5.2.1.6 Table release history update

Not Applicable

12.5.2.1.7 Supplementary information

Not Applicable

12.5.2.1.8 Translation verification other tools

Not Applicable

12.5.2.2 Name: MNCKTPAK

12.5.2.2.1 Functional description

The CEM tuples of DMSCP variant of SPM are allowed to be provisioned only with the PECs - NTLX82AA, NTLX82AB and NTLX82BA in table MNCKTPAK. With the introduction of the new field ‘CAPINDX’ in table MNNODE, the provisioning of the PEC is dependent on the capindx value. The capindx can be provisioned with ‘Standard’, ‘Enhanced’ or ‘Premium’.

Incase the capindx in table MNNODE is ‘Standard’, the PEC shall be allowed to be datafilled as NTLX82AA, NTLX82AB or NTLX82BA. In case of ‘Enhanced’ or ‘Premium’ capindx, the PEC must be datafilled as NTLX82BA.

For Non-DMSCP class of SPMs, no validations for CEM PEC are introduced by this activity. The PEC that is datafilled for both the CEMs in table MNCKTPAK automatically determines the capacity for that SPM. If both the CEMs are datafilled with NTLX82BA PEC cards, then capacity is ‘Premium’ and for any other combinations of PEC cards, the capacity is ‘Standard’. Refer table 7 and table 8 for the various Error and Success messages that are introduced in table MNCKTPAK as part of this activity.

Table 6 New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
1	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82AA. b. Updation of a CEM PEC from NTLX82BA to NTLX82AA.	a. The capindx field in table MNNODE is Enhanced or Premium and b. The other CEM tuple may or may not be present.
	Cannot allocate NTLX82AA card for an SPM that has been datafilled with Enhanced or Premium capacity. Check MNNODE datafill.	
2	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82AB. b. Updation of a CEM PEC from NTLX82BA to NTLX82AB.	a. The capindx field in table MNNODE is Enhanced or Premium and b. The other CEM tuple may or may not be present.
	Cannot allocate NTLX82AB card for an SPM that has been datafilled with Enhanced or Premium capacity. Check MNNODE datafill.	

Table 7 New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
1	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Enhanced and b. The other CEM tuple is already present.
	Datafill conditions met for activation of SPM Enhanced capacity SOC option SPMS0020.	
2	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Premium and b. The other CEM tuple is already present.
	Datafill conditions met for activation of SPM Premium capacity SOC option SPMS0028.	
3	a. Deletion of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Enhanced and b. The other CEM tuple is already present.
	Datafill conditions met for de-activation of SPM Enhanced capacity SOC option SPMS0020.	
4	a. Deletion of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Premium and b. The other CEM tuple is already present.
	Datafill conditions met for de-activation of SPM Premium capacity SOC option SPMS0028.	

12.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

12.5.2.2.3 Size

Not impacted.

12.5.2.2.4 Fields/OIDs

The following table lists fields for table MNCKTPAK which are changed as part of this activity.

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

12.5.2.2.5 Datafill example

Not Applicable.

12.5.2.2.6 Table release history update

Not Applicable

12.5.2.2.7 Supplementary information

Not Applicable

12.5.2.2.8 Translation verification other tools

Not Applicable

12.6 Service Orders (SO) (CM & SESM)

Not Applicable

12.7 Software optionality control (SOC)

Two new USAGE SOCs are created under a new group called CAP. These SOCs are used only by DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity and the SOC option SPMS0028 corresponds to the SPMs with Premium capacity.

The hard limit value of SPMS0020 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Enhanced capacity and the hard limit value of SPMS0028 denotes the maximum number of DMSCP

class of SPMs in the office that can be provisioned with Premium capacity. The threshold value of these SOC options are set to 100%.

The value of the USAGE of SPMS0020 and SPMS0028 denotes the number of DMSCP class of SPMs currently running with the Enhanced and Premium capacity respectively from Core's perspective. Refer Appendix A in Section 13.12 for the syntax of some of the SOC commands.

Table 9 Enhanced SOC option

SOC option name:	SPMS Enhanced Call cap
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	SPMS0020
Option defined in DRU:	SHR
Affected products:	SPM

Table 10 Premium SOC option

SOC option name:	SPMS Premium Call cap
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	SPMS0028
Option defined in DRU:	SHR
Affected products:	SPM

12.8 Element Management

Not Applicable.

12.9 Command interface changes

12.9.1 Directory: None

12.9.2 Command: SPMCPCAP

12.9.2.1 Command type: NON-MENU

12.9.2.2 Command target: All

12.9.2.3 Command availability: RES

12.9.2.4 Command description

Command SPMCPCAP is used to display CallP capacity information for SPMs.

12.9.2.5 Command syntax

The command syntax is as shown in Figure 2.

Figure 2 Syntax of SPMCPCAP command

```
>help spmcpcap
SPM Callp Capacity information tool.
SPMCPCAP - Displays Callp Capacity information for SPMs.
           Remarks field displays if CEM(s) are not
           datafilled for the SPM.

Parms: <OPTION> {Class <Class type> {DMSCP,
                                     IW,
                                     MG4K,
                                     ALL},
                Capacity <Capacity type> {Standard,
                                          Enhanced,
                                          Premium,
                                          ALL},
                SPM <SPM Number> {0 TO 85}}
```

```
Syntax  : spmcpcap
Parameter Description:

  CLASS DMSCP      : List CallP capacities of all the DMSCP SPMs provisioned
                     in the office.

  CLASS MG4K       : List CallP capacities of all the MG4K SPMs provisioned in
                     the office.

  CLASS IW         : List CallP capacities of all the IW SPMs provisioned in
                     the office.

  CLASS ALL        : List CallP capacities of all the classes of SPMs
                     provisioned in the office.

  CAPACITY Standard: List all the SPMs in an office that have 'Standard' CallP
                     capacity.

  CAPACITY Enhanced: List all the SPMs in an office that have 'Enhanced' CallP
                     capacity.

  CAPACITY Premium : List all the SPMs in an office that have 'Premium' CallP
                     capacity.

  CAPACITY ALL     : List all the SPMs in an office and their corresponding
                     CallP capacity.

  SPM <SPM NO>     : List CallP capacity for a given SPM node number.
```

12.9.2.6 Qualifications and warnings

If either or both the CEM tuple are not present in table MNCKTPAK for an SPM, then the remarks field against that SPM displays that the CEM datafill is incomplete. If the both the CEM tuples are datafilled, remarks field displays 'None' against that SPM.

CallP capacity information is taken from table MNNODE datafill for DMSCP class of SPMs. Supported capacities for this class are ‘Standard’, ‘Enhanced’ and ‘Premium’.

For other classes (MG4K and IW) this capacity is derived from CEM PEC datafill in table MNCKTPAK. Supported capacities for these classes are ‘Standard’ and ‘Premium’. If the CEM(s) are not datafilled in table MNCKTPAK, then the tool displays ‘Standard’ capacity for MG4Ks and IWs.

12.9.2.7 Responses

12.9.2.7.1 Listing SPMs with Enhanced CallP capacity

Listing of SPMs with Enhanced capacity will not display information of MG4K and IW SPMs as this capacity is invalid for these classes. This option is valid for DMSCP class of SPMs only.

12.9.2.8 Example

Table 13 lists various usage examples for SPMCPCAP command.

Table 11 Usage examples for SPMCPCAP command

Description of task:	Display CallP Capacity information for a SPM node
Command: MAP response:	CI: >spmcpcap class DMSCP --- SPM No Capacity Remarks --- 3 Premium CEM(s) not datafilled. 4 Enhanced CEM(s) not datafilled. 10 Enhanced None. 13 Premium None. 14 Standard None. ---

Table 11 Usage examples for SPMCPCAP command

Command: MAP response:	CI: >spmcpcap class MG4K -- SPM No Capacity Remarks -- 0 Standard None. 1 Standard None. 6 Standard None. 7 Standard None. 8 Premium None. 9 Standard None. 12 Standard None. 27 Standard None. 29 Standard None. 30 Standard None. --
Command: MAP response:	CI: >spmcpcap class IW -- SPM No Capacity Remarks -- 11 Premium None. --

Table 11 Usage examples for SPMCPCAP command

Command:

```
CI:
>spmcpcap class ALL
```

MAP response:

```
DMSCP :
-----------------------------------------------
  SPM No     Capacity         Remarks
-----------------------------------------------
     3       Premium     CEM(s) not datafilled.
     4       Enhanced    CEM(s) not datafilled.
    10       Enhanced          None.
    13       Premium           None.
    14       Standard          None.
-----------------------------------------------


IW :
-----------------------------------------------
  SPM No     Capacity         Remarks
-----------------------------------------------
    11       Premium           None.
-----------------------------------------------


MG4K :
-----------------------------------------------
  SPM No     Capacity         Remarks
-----------------------------------------------
     0       Standard          None.
     1       Standard          None.
     6       Standard          None.
     7       Standard          None.
     8       Premium           None.
     9       Standard          None.
    12       Standard          None.
    27       Standard          None.
    29       Standard          None.
    30       Standard          None.

-----------------------------------------------
```

Command:

```
CI:
>spmcpcap capacity Enhanced
```

MAP response:

```
-----------------------------------------------
  SPM No     Capacity         Remarks
-----------------------------------------------
     4       Enhanced    CEM(s) not datafilled.
    10       Enhanced          None.
-----------------------------------------------
```

Table 11 Usage examples for SPMCPCAP command

Command: MAP response:	CI: >spmcpcap SPM 7 --- SPM No Capacity Remarks --- 7 Standard None. ---

12.10 Security

Not Applicable.

12.11 Configuration Walkthrough

Not Applicable.

12.12 Appendix A: SOC commands

Appendix A lists the syntax for various SOC commands.

- To display information about SOC group and options.

  SOC:

  >SELECT GROUP CAP

  >SELECT OPTION SPMS0020

  >SELECT OPTION SPMS0028

- To assign a limit to the new SOC options, SPMS0020 and SPMS0028.

  SOC:

  >ASSIGN LIMIT <value of limit> <key code> TO SPMS0020

  >ASSIGN LIMIT <value of limit> <key code> TO SPMS0028

- To assign the threshold value(percentage and absolute).

  SOC:

  >ASSIGN THRESHOLD <percentage value> PERCENT TO SPMS0020

  >ASSIGN THRESHOLD <absolute value> ABSOLUTE TO SPMS0020

13: Configuration (CN): A00002433

13.1 Hardware and Software Requirements

This feature is intended to verify that an XA-Core meets baseline HW and FW requirements, that may vary from one SW release to another.

13.2 Initial Configuration

No configuration steps are required to enable this feature in CSP20.
For CSP17/18/19, a patch must be developed which does a “precheck” to alert the user that they are not at HW baseline for CSP20, and that these components will not come into service if they were to continue with the unsplit. Documentation will also indicate the required HW PEC and HW releases required.

13.3 Office parameters

No new or modified office parameters.

13.4 Upgrade Impact

13.4.1 Dump and Restore

No dump and restore impact, as existing table PECINV, and new table FWINV are NOT restored over an ONP.

13.4.2 CSP20 XA-Core Baselines

HW baselines and optoinal exception releases are listed in table PECINV.
FW baselines and optional exception versions are listed in table FWINV.
XA-Core baselines are shown below - these should be added to customer ONP documentation. Used in ONP prechecks weeks prior to ONP, while unsplit: (a) ONPREADY, b) SWUPGRADE READY; START, c) BCSUPDATE; PRECHECK) as well as during ONP pre-swact checks, while split (BCSUPDATE; SWACTCI; PRESWACT):

Figure 1 XA-Core HW Baselines, CSP20 - Table PECINV

```
>TABLE PECINV; FORMAT PACK
>RANGE SSYSBASE
 2 SSYSBASE          SN_SSYS_BASELINE
TYPE IS SN_SSYS_BASELINE VECTOR OF UP TO 11 MULTIPLES WITH
        SUBSYS           SN_SUBSYSTEM_HW
        BASELINE         TABLE OF 2 CHAR'S
        EXCPTN           VECTOR OF UP TO 4 TABLES OF 2 CHAR'S

>LIST ALL (SSYSBASE GE XACHW)
TOP
PEC        SSYSBASE
--------  -------------
NTLX02CA (XACHW 01 $) $
NTLX02DA (XACHW 01 $) $
NTLX03AA (XACHW 28 $) $
NTLX03AB (XACHW 03 $) $
NTLX03BA (XACHW 28 $) $
NTLX03BB (XACHW 03 $) $
NTLX04AA (XACHW 01 $) $
NTLX04BA (XACHW 01 $) $
NTLX04CA (XACHW 01 $) $
NTLX05AB (XACHW 01 $) $
NTLX05BA (XACHW 01 $) $
NTLX06AA (XACHW 01 $) $
NTLX06AB (XACHW 01 $) $
NTLX06AC (XACHW 01 $) $
NTLX07AA (XACHW 01 $) $
NTLX07BA (XACHW 01 $) $
NTLX08AA (XACHW 01 $) $
NTLX08AB (XACHW 01 $) $
NTLX09AA (XACHW 01 $) $
NTLX12AA (XACHW 04 $) $
NTLX14CA (XACHW 01 $) $
NTLX14FA (XACHW 01 $) $
NTLX17AA (XACHW 01 $) $
NTLX22AA (XACHW 07 $) $
NTLX22BA (XACHW 02 $) $
NTLX27AA (XACHW 01 $) $
BOTTOM

>COUNT (SSYSBASE GE XACHW)
BOTTOM
SIZE = 26
```

Figure 2 XA-Core FW Baselines, CSP20 - Table FWINV

```
>TABLE FWINV; FORMAT PACK
>RANGE FWBASE
 2 FWBASE            TFWINV_TUPLE
TYPE IS TFWINV_TUPLE VECTOR OF UP TO 2 MULTIPLES WITH
        FWTYPE       {FW,DLL}
        VERSION      TABLE OF 8 CHAR'S
        EXCEPTIONS   VECTOR OF UP TO 4 TABLES OF 8 CHAR'S

>LIST ALL
TOP
PEC        FWBASE
--------   --------------------------------
NTLX02CA (FW XAPE01AG $) $
NTLX02DA (FW XAPE02AB $) $
NTLX03AA (FW XAIO01AK $) $
NTLX03AB (FW XAIO01AK $) $
NTLX03BA (FW XAIO01AK $) $
NTLX03BB (FW XAIO01AK $) $
NTLX04AA (FW XHIO02AA $)(DLL XHIO02AJ $) $
NTLX04BA (FW XHIO02AA $)(DLL XHIO02AJ $) $
NTLX04CA (FW XHIO02AH $)(DLL XHIO02AJ $) $
NTLX17AA (FW XHIO03AA $)(DLL XHIO03AA $) $
NTLX05AB (FW PK12CE12 $) $
NTLX05BA (FW PK12CE12 $) $
NTLX09AA (FW EP14D003 $) $
BOTTOM

>COUNT
BOTTOM
SIZE = 13
```

13.4.3 Pre-ONP checks (while usnplit)

Existing steps have been enhanced for XA-Core, and to check for non-baseline XA-Core HW/FW/DLL.

1. ONPREADY % Step "DISPLAY_PEC_INFO"
   Step saves MAP output to file, then scans it for baseline failures.
2. BCSUPDATE; PRECHECK % Step "DISPLAY_PEC_INFO"
   Step display MAP output to screen ONLY.
   Step always “fails”, so that user wil manually scan for non-baseline indicators.
   Override the step to continue, once all resources are at baseline.
3. SWUPGRADE READY; START % Step “VERIFY_SN_PECS_INFO”
   Step saves MAP output to file, then scans it for baseline failures.

13.4.4 PRESWACT checks (while split)

A new preswact check is added, and run while the XA-Core is split. Active side queries are sent to inactive side for comparison against NEW PECINV baselines. Incompatible cards/packlets are sent back to active side for display. If list is nil, step passes, else preswact step fails.

Figure 3 PRESWACT - Baseline Check Behaviour

```
ACTIVE SIDE                                          INACTIVE SIDE
-----------                                          --------------
1- Card/pklt query list -> Buf
                                     Buf
2- preswact_transfer(PSEND, INITIAL) --->
   Invokes
                                       3- Compare card/pklts vs NEW PECINV baseli
                                                Non-baseline items->Buf

                                     Buf
4- preswact_transfer(PRECEIVE)       <---
   Pass: Display OK OR
   Fail: list problem card/pklts
```

Sample output, when HW is NOT compatible with NEW side baselines:

Figure 4 Sample PRESWACT output - step XACORE_BASELN_CHECK

```
>BCSUPDATE; SWACTCI; PRESWACT
XACORE_BASELN_CHECK              executing
      16 of 23 cards+packlets compatible with NEW SIDE baselines.

      ******************************************************
      ** XACore resources incompatible with NEW baselines. **
      ** ABORT PRESWACT AND UPDATE RESOURCES TO MEET       **
      ** NEW BASELINES, ONCE SYSTEM IS UNSPLIT.            **
      ******************************************************

      Non-baseline XA-Core Resources vs NEW side:
      -------------------------------------------
                  --HW vs. PECINV--
      Type NT Loc  PEC+Release BL OK  Failure reason on NEW side
      ---- ------  ----------- -- --
      Disk  2 F L  NTLX06AC 00 01 N*  Below PECINV Baseline
      IOP  17 F    NTLX03BB 02 03 N*  Below PECINV Baseline
      IOP   4 R    NTLX03AA 03 28 N*  Below PECINV Baseline
      CMIC  4 R L  NTLX05AB 00 01 N*  Below PECINV Baseline
      HIOP 14 R    NTLX04BA 00 01 N*  Below PECINV Baseline
      IOP  15 R    NTLX03AB 00 03 N*  Below PECINV Baseline
      RTIF 15 R U  NTLX08AB 00 01 N*  Below PECINV Baseline

      XACORE_BASELN_CHECK              not complete

      Investigate and correct if needed.
```

13.5 Data schema (DS)

13.5.1 New/modified tables

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
PECINV	CHANGED	UNCHANGED (NEW)
FWINV	NEW	NEW

13.5.2 Table Data Schema information

13.5.2.1 Name: PECINV

PECINV is changed in the following ways:

1. Maximum number of tuples is increased from 200 to 256.
2. Default datafill (added at loadbuild time using PLS DMSPL module EXTPECHWSUB) is updated:
   a. Added new PECs and their correct baseline releases.
   b. Corrected baseline release on some existing PECs.

13.5.2.1.1 Functional description

PECINV is intended to mainatin the HW baseline PEC, release and exception releases for various subsystems.

Its data is accessed by:

1. CHECKMS CI - MSHW and STDHW subsystems only.
2. CHECKREL CI - all supported subsystems.
3. SREX - through run_hardware_monitor() check.
   Only MSHW subsystem. has a target procedure bound curretnly.

13.5.2.1.2 Usage sequence and implications

No table dependencies. Current datafill order unchanged.

13.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
PECINV	0	256	Store for 256 tuples is pre-allocated in DSPROT. Each tuple approx 20 bytes

13.5.2.1.4 Datafill example

The following example shows sample datafill for table FWINV:

Figure 5 PECINV examples

```
PEC SSYSBASE
------------
1. NTLX02CA (XACHW 01 $) $
```

13.5.2.1.5 Table release history update

1. Extended maximum tuple range from 200 to 256.

2. Added missing PEC/releases to default datafill: (now 211 entries at IPL)
NTLX02DA XACHW 01 % ATLAS PE
NTLX03AB XACHW 03 % single width IOP card
NTLX03BB XACHW 03 % double width IOP card
NTLX04AA XACHW 01 % HIOP card - ETHR
NTLX04BA XACHW 01 % HIOP card - ETHR/AMDI
NTLX04CA XACHW 01 % HIOP card - ETHR/CMIC
NTLX05AB XACHW 01 % CMIC packlet
NTLX05BA XACHW 01 % AMDI packlet
NTLX06AC XACHW 01 % Disk packlet - 34.2 GB
NTLX07BA XACHW 01 % Tape packlet - 20 GB DDS4
NTLX08AB XACHW 01 % RTIF Packlet
NTLX09AA XACHW 01 % ETHR Packlet
NTLX14FA XACHW 01 % 512MB SM Card
NTLX17AA XACHW 01 % HIOP Card - CMIC/RTIF .

3. Corrected baseline releases on existing PECs:
NT9X13DE LIMHW 01 --> 03
NT9X63AA MSHW 01 --> 10
NT9X71AB LIMHW 00 --> 01
NT9X72BA LISHW 00 --> 01
NTLX02AA XACHW 04 --> 01
NTLX03AA XACHW 04 --> 28
NTLX03BA XACHW 04 --> 28
NTLX05AA XACHW 02 --> 01

NTLX06AA XACHW 02 --> 01
NTLX07AA XACHW 02 --> 01
NTLX12AA XACHW 02 --> 04
NTLX14CA XACHW 02 --> 01
NTLX22AA XACHW 02 --> 07
NTLX27AA XACHW 02 --> 01

4. Removed XA-Core PECs - no longer supported
NTLX02AA XACHW % HIPPO based PE
NTLX05AA XACHW % CMIC packlet

13.5.2.1.6 Supplementary information
NONE

13.5.2.1.7 Translation verification other tools

PECINV does not use translation verification tools.

13.5.2.2 Name: FWINV
FWINV is a NEW table.

13.5.2.2.1 Functional description
FWINV is intended to mainatin the FW baseline for a PEC, and allows from 0 up to 4 exception versions.

Its data is accessed by:

1. MAPCI;MTC;XAC;QUERY SHELF/CARD
2. Periodic internal queries
3. SREx
4. Card/Packlet RTS
5. ONP prechecks, prior to ONP
6. ONP preswact, while split, during ONP

13.5.2.2.2 Usage sequence and implications

No table dependencies. Current datafill order unchanged.

13.5.2.2.3 Size

Table 3 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
FWINV	0	64	Store for 64 tuples is pre-allocated in DSPROT. Each tuple is 90 bytes.

13.5.2.2.4 Fields/OIDs

The following table lists fields for table FWINV. Only 2 fields are shown by the RANGE command: PEC (key) and FWBASE. FWBASE is further broken down into FWTYPE/FWBASE/EXCEPTIONS

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	NEW	Subfield	8 chars	Must begin with NTLX
FWBASE	NEW	Subfield	Sum of 3 below	
FWTYPE	NEW	Subfield	FW or DLL	FW for ROM baseline. DLL for DLL baseline.
VERSION	NEW	Subfield	8 chars	ASCII A-Z, 0-9, beginning with: PE: XAPE IOP: XAIO HIOP: XHIO CMIC: PKdd, d=0-9 AMDI: PKdd, d=0-9 ETHR: EPdd, d=0-9 NO FW for: SM, DISK, TAPE, RTIF
EXCEPTIONS	NEW	Subfield	8 chars	Same restrictions as above. This FW/DLL version is bad, and will be alarmed if used.

13.5.2.2.5 Datafill example

The following example shows sample datafill for table FWINV.

Figure 6 FWINV examples

```
PEC FWBASE
------------
1. NTLX02CA (FW XAPE01AG $) $
2. NTLX04CA (FW XHIO02AH $) (DLL XHIO02AI $)

%% Eg. ONLY, to show exception format.
3. NTLX05AB (FW PK12CE12 (PK12CE13) $) $
```

13.5.2.2.6 Table release history update

1. Initial release.

13.5.2.2.7 Supplementary information

NONE

13.5.2.2.8 Translation verification other tools

FWINV does not use translation verification tools.

13.6 Service Orders (SO)

No impact to Service Orders.

13.7 Software optionality control (SOC)

Feature is not SOC controlled.

13.8 Command interface changes

QUERY CARD and QUERY SHELF commands are enhanced to show if FRU is HW and FW/DLL baseline compatible.

13.8.1 Directory: MAPCI; MTC; XAC

13.8.1.1 Directory description

Existing levels are still used - only the display is changed for QUERY SHELF.
QUERY SHELF is available from XAC and its sublevels:
XACMTC, SM, PE, IO, CMIC, RTIF, DISK, TAPE, AMDI, ETHR

13.8.1.2 Accessing directory: XACDIR

13.8.1.2.1 Access to directory or MAP level and return to CI

enter XAC level from CI:
    MAPCI;MTC;XAC
exit to CI:
    QUIT ALL

13.8.2 Command: QUERY SHELF

13.8.2.1 Command type: Listed MENU

13.8.2.2 Command target: XA-Core

13.8.2.3 Command availability: RES

13.8.2.4 Command description

QUERY SHELF lists:

1. Last REX data: time, type, result
2. Information per FRU installed in the shelf.

13.8.2.5 Command syntax

Table 5 QUERY SHELFcommand parameters and variables

Command	Parameters and variables
QUERY SHELF	No additional parameters available.

13.8.2.6 Qualifications and warnings

13.8.2.7 Example

See Figure 7, on page 2551

Figure 7 Query SHELF Example

```
>MAPCI NODISP;MTC;XAC
>QUERY SHELF

LAST REX DATA
-------------
REXtst run at: 1976/01/02 01:56:52
REXtst type  : full
REXtst result: pass

SHELF DATA
----------
Notes:
  FW: ROM version. HIOP adds DLL version on following line.
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
 2 F   IOP  NTLX03BA 30 28 Y    NNTM6441882N XAIO01AK XAIO01AK Y
 2 F L Disk NTLX06AC 01 01 Y    NNTM171W2SKC n/a      n/a      Y
 2 F U Tape NTLX07AA 02 01 Y    NNTM171XLG8W n/a      n/a      Y
 4 F   PE   NTLX02CA 02 01 Y    NNTM64419MYY XAPE01AG XAPE01AG Y
 5 F   PE   NTLX02CA 01 01 Y    NNTM64416MJB XAPE01AG XAPE01AG Y
11 R   SM   NTLX14CA 02 01 Y    NNTM64415KXH n/a      n/a      Y
 7 F   SM   NTLX14CA 09 01 Y    NNTM64429LK2 n/a      n/a      Y
10 R   SM   NTLX14CA 02 01 Y    NNTM1721FG2L n/a      n/a      Y
 8 F   SM   NTLX14CA 09 01 Y    NNTM64429LM1 n/a      n/a      Y
12 F   PE   NTLX02CA 05 01 Y    NNTM171WT19M XAPE01AG XAPE01AG Y
13 F   PE   NTLX02CA 12 01 Y    NNTM64415C78 XAPE01AG XAPE01AG Y
16 F   PE   NTLX02CA 05 01 Y    NNTM171WMXQ9 XAPE01AG XAPE01AG Y
17 F   IOP  NTLX03BB 02 03 N*   NNTM6441VHPX XAIO01AK XAIO01AK Y
17 F L Disk NTLX06AA 02 01 Y    NNTM1721FDZW n/a      n/a      Y
17 F U Tape NTLX07AA 02 01 Y    NNTM171Z17HM n/a      n/a      Y
 4 R   IOP  NTLX03AA 03 28 N*   NNTM17218T79 XAIO01AK XAIO01AK Y
 4 R L CMIC NTLX05AB 01 01 Y    NNTM171VY7C9 PK12CE12 PK12CE12 Y
 4 R U RTIF NTLX08AA 02 01 Y    NNTM171BP2Y0 n/a      n/a      Y
10 F   SM   NTLX14CA 02 01 Y    NNTM64419R6Q n/a      n/a      Y
14 R   HIOP NTLX04BA 01 01 Y    NNTMEM0135GG XHIO02AA XHIO02AA Y
                                            XHIO02AH XHIO02AJ N*
15 R   IOP  NTLX03AB 01 03 N*   NNTM6441DSGW XAIO01AK XAIO01AK Y
15 R L CMIC NTLX05AB 03 01 Y    NNTM171Z1GWG PK12CE12 PK12CE12 Y
15 R U RTIF NTLX08AB 01 01 Y    NNTM171ZQ2DS n/a      n/a      Y
```

13.8.3 Command: QUERY CARD

13.8.3.1 Command type: Listed MENU

13.8.3.2 Command target: XA-Core

13.8.3.3 Command availability: RES

13.8.3.4 Command description

QUERY CARD output varies per FRU type. Common to all is:

1. Information per FRU installed in the shelf.

13.8.3.5 Command syntax

Table 6 QUERY SHELFcommand parameters and variables

Command	Parameters and variables
QUERY CARD <position>	position = <slot> <front | rear> [<upper | lower>]

13.8.3.6 Qualifications and warnings

13.8.3.7 Example

See Figure 8, on page 2553

Figure 8 Query CARD Examples

```
>MAPCI NODISP;MTC;XAC
>QUERY CARD 2 F
Notes:
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                 ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
 2 F   IOP  NTLX03BA 30 28 Y    NNTM6441882N XAIO01AK XAIO01AK Y
HW/SW Vintage   : 01

>QUERY CARD 17 F L
Notes:
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                 ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
17 F L Disk NTLX06AA 02 01 Y    NNTM1721FDZW n/a      n/a      Y
HW/SW Vintage   : 01
Vendor          : SEAGATE
Product ID      : ST39216W
Revision        : 0004
Nom Capacity(MB): 8602
Block Size   (B): 512

>QUERY CARD 4 R L
Notes:
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                 ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
 4 R L CMIC NTLX05AB 00 01 N*   NNTM171VY7C9 PK12CE12 PK12CE12 Y
HW/SW Vintage   : 01

>QUERY CARD 4 R U
Notes:
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                 ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
 4 R U RTIF NTLX08AA 02 01 Y    NNTM171BP2Y0                     Y
HW/SW Vintage   : 01

>QUERY CARD 14 R
Notes:
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
            --HW vs. PECINV--                 ----FW vs. FWINV----
Pos    Type PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
------ ---- ---------- -- -- -------------- -------- -------- --
14 R   HIOP NTLX04BA 00 01 N*   NNTMEM0135GG XHIO02AA XHIO02AA Y
                                            XHIO02AH XHIO02AI N*
HW/SW Vintage   : 01
Ethernet MAC Address : 00603887A969
Port     IP Address  : n/a  % Actual IP addresses, if provsioned
Assigned IP Address 1: n/a
Assigned IP Address 2: n/a
```

13.9 Security

No impact to switch security.

13.10 Configuration Walkthrough

14: Configuration (CN): A00002510

14.1 Hardware and Software Requirements

14.2 Initial Configuration

14.3 Office/Subnet parameters (OP/SP) (CM & SESM)

14.4 Upgrade Impact

14.5 Data schema (DS) (CM, MIBS, RDB)

14.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPNETWRK	changed	old

14.5.2 Table/MIB/Remote Database Schema information

Table schema for IPNETWRK has been modified as follow.

Field name PARM in table IPNETWRK has been refined, a new value IRM_INTERFACE is introduced, to replace existing IOP_INTERFACE.

As well a new dependency is introduced which has an impact to the dump and restore table transfer order. Table CMIPADDR need to be transferred before IPNETWRK.

14.5.2.1 Name:

IP Network Table

14.5.2.1.1 Functional description

A new value under PARM, called IRM_INTERFACE, has been introduced in CSP20 to replace an existing IOP_INTERFACE.

The IP address specified under the IRM_INTERFACE must conform with one of the CMHOST IP addresses assigned for the XA-Core IOP (IRM) or the Ethernet interface for the XA-Core, and this IP address must have been datafilled in table CMIPADDR.

14.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Transfer order must be changed such that CMIPADDR is transferred before IPNETWRK.

CMIPADDR

IPNETWRK

14.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DDPACDEV	0	8 000 000	Memory is automatically allocated for 16 DPC devices.

14.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IPNETWRK.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

14.5.2.1.5 Datafill example

The following example shows sample datafill for table IPNETWRK using parm IRM_INTERFACE:

```
TABLE: IPNETWRK

KEYREF CMIPADDR SUBNET OPTION PARMAREA
-------------------------------------
1 10 101 8 100 16 $ (IRM_INTERFACE )$
```

and note that the CMIPADDR value used above must already been assigned as one of the CMHOST IP addresses, such as shown in the following example of CMIPADDR table:

```
TABLE: CMIPADDR:
KEY DATA
--------
GATEWAY 0 GW (10 101 8 1) 0
CMHOST 0 HOST (10 101 8 100) 24 0
CMHOST 1 HOST (10 101 8 101) 24 0
ETHRLNK 0 ETHR 5 REAR NONE (10 101 8 102) 24 (10 101 8 103) 24 (10 101 8 10) 0
ETHRLNK 1 ETHR 14 REAR NONE (10 101 8 104) 24 (10 101 8 105) 24
(10 101 8 10) 0
```

14.5.2.1.6 Table release history update

14.5.2.1.7 Supplementary information

14.5.2.1.8 Translation verification other tools

IPNETWRK does not use translation verification tools.

14.6 Service Orders (SO) (CM & SESM)

14.7 Software optionality control (SOC)

14.8 Element Management

14.9 Command interface changes

14.10 Security

14.11 Configuration Walkthrough

15: Configuration (CN): A00002555

This feature allows the ADO, DEO and CLN Servord commands to manipulate the GND Bool in table LNINV for certain adaptive line cards. See the Servord section, starting at paragraph 13.6

15.1 Hardware and Software Requirements

SN07

15.2 Initial Configuration

n/a

15.3 Office/Subnet parameters (OP/SP) (CM & SESM)

15.4 Upgrade Impact

15.5 Data schema (DS) (CM, MIBS, RDB)

15.6 Service Orders (SO) (CM & SESM)

This feature allows the ADO, DEO and CLN Servord commands to manipulate the GND Bool in table LNINV for the below list of the supported line cards.

- 3A06BA
- 7A25AA
- SCD271
- RDTCON
- RDTLSG

The above line cards are refered in this document as the supported line cards.

There are other line cards that support GND but they are not supported by this feature. Other Servord commands are not effected. Commands that establish new service such as NEW and EST will function as before.

If table OFCVAR parm SO_ALLOW_REDUNDANT_FEATURE is set to Y, then the redundant feature is turned on. Redundant feautre is now supported for GND for the ADO, DEO and CLN commands. This means for example, if the ADO of GND is attempted to a line that already has the GND option, the command will not be rejected and no journal file update will occur.

15.6.1 Service order change details

15.6.1.1 LCC and options

There are no new options introduced by this feature. The behavior of the ADO, DEO and CLN Servord commands is changed for the GND option for the supported line cards only. The GND option is not applicable to key sets or ISDNSETs. The option pretains mostly to COIN and PBX lines.

15.6.2 New commands

There are no new commands introduced by this feature.

15.6.2.0.1 Command prompts

There are no additional or changes to prompts for this feature.

15.6.2.1 How service order options are presented

15.6.2.1.1 Description

The GND option is used to specify that the line will be a GROUND START line. It is determined by the value of GND in table LNINV for the tuple assoicated with the line. Only certain line cards can be ground start lines and only the supported line cards apply to this feature. Prior to this feature, the ADO, DEO and CLN Servord commands could not change the GND Bool for any line.. This value was set when the tuple was datafulled in table LNINV. This feature doesn't add the GND option or additional prompts as the option already exists. It allows the Servord commands ADO, DEO and CLN to change the value fo GND for the supported line cards. Prior to this feature, an error message was given when GND was attempted to be ADO-ed or DEO-ed.. The error message is still given for lines that do not have a supported line card. Use QLEN or QDN to determine the line card and GND value. Positioning on the LEN in table LNINV can also be used

Perhaps the biggest enhancement of this feature is with the CLN command. If the NEW_LEN has a supported line card, the value of GND will be set to that of the OLD_LEN. If the value will change, a warning message is output. If the NEW_LEN does not have a supported line card, the value of GND on the NEW_LEN will be the same as it was prior to execution of the CLN command. If the value of GND is different between the OLD_LEN and the NEW_LEN, a warning message will be output.

QLEN or QDN can be used to determine the line card and the value of GND. GND will also appear in the option list if it set to Y in table LNINV. The below example shows a line with a RDTLSG line card with GND set to Y.

```
>qlen rdt0 1 0 1 2
------------------------------------------------------------------------------
LEN:     RDT0  01 0 01 02
TYPE: SINGLE PARTY LINE
SNPA: 908
DIRECTORY NUMBER:     9451104
LINE CLASS CODE:      1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     400
CARDCODE:  RDTLSG    GND: Y  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    221
PM TERMINAL NUMBER :    2
OPTIONS:
DGT GND NAME PUBLIC C1FR1RGB
OFFICE OPTIONS:
AIN TIID
------------------------------------------------------------------------------
>
```

15.6.2.1.2 Example

Figure 1 Example of ADO of GND in NO PROMPT mode

Example of ADO of the GND option in prompt mode

```
>ado
SONUMBER:      NOW    3    12   1 PM
>
DN_OR_LEN:
>RDT0 1 0 1 2
OPTION:
>GND
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 12 1 PM RDT0 1 0 1 2 ( GND ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

Figure 2 Example of DEO of GND in No Prompt mode

```
>deo
SONUMBER:       NOW    3    12   1 PM
>
DN_OR_LEN:
>RDT0 1 0 1 2
OPTION:
>GND
OPTION:
>$
COMMAND AS ENTERED:
DEO  NOW 3 12 1 PM RDT0 1 0 1 2 ( GND ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

The below example shows a CLN from a OLD_LEN that has GND set to a NEW_LEN that has a supported line card. NOTE: The warning is output only if the GND values are different between the OLD_LEN and NEW_LEN prior to the execution of the command.

Figure 3 Example of CLN command to a NEW_LEN with Supported Line Card

```
>CLN
SONUMBER:       NOW    3    12   1 PM
>
OLD_LEN:
>RSC0 0 0 3 0
NEW_LEN:
>RSC0 0 0 0 7
COMMAND AS ENTERED:
CLN NOW 3 12 1 PM RSC0 00 0 03 00 RSC0 00 0 00 07
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
y
WARNING: GND will be changed to TRUE in table LNNIV
              on the NEW_LEN, same setting as the OLD_LEN
```

The below example shows a CLN from a OLD_LEN that has GND set to a NEW_LEN that doesn't have a supported line card. NOTE: The warning is output only if the GND values are different between the OLD_LEN and NEW_LEN prior to the execution of the command.

Figure 4 Example of CLN, NEWLEN is not a Supported Line Card

```
>CLN
SCLNUMBER:       NOW    3    12   1 PM
>
OLD_LEN:
>RSC0 0 0 3 0
NEW_LEN:
>0 0 0 3
COMMAND AS ENTERED:
CLN NOW 3 12 1 PM RSC0 00 0 03 00 HOST 00 0 00 03
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
y
WARNING: GND is FALSE in table LNNIV on the NEW_LEN
              The setting was TRUE on the OLD_LEN
```

Figure 5 Example of ADO and DEO of the GND option in no-prompt mode for SERVORD+

```
ADO $ RDT0 1 0 1 2 GND $ Y Y

DEO $ RDT0 1 0 1 2 GND $ Y Y
```

15.6.2.1.3 Option prompts

There are no changes to prompts. The GND option already exists.

15.6.2.1.4 Line class code compatibility

There are no changes to LCC compatibilty for GND

15.6.2.1.5 Assignability

The following functionalities apply to this option:

- set functionality: NO
- subset functionality: NO
- DN functionality: NO
- key functionality: NO

The GND option is not a typical line option in that it gives added functions to the line or set. It determines how the line card detects when the subscriber goes off hook. It is a hardware function of the line card, transparent to the subscriber.

15.6.2.1.6 Option prerequisites

GND has the following prerequisites:

None

15.6.2.1.7 Notes

The following notes apply to GND:

This feature applies only to the supported line cards. It may be necessary to post the line at the MAP and BSY and RTS the line in order for the change to take effect

15.6.2.1.8 Feature identification

Feature number: A00002555

15.6.2.1.9 SERVORD+ Exceptions

none known.

15.7 Software optionality control (SOC)

15.8 Element Management

15.9 Command interface changes

15.10 Security

15.11 Configuration Walkthrough

16: Configuration (CN): A00002558

16.1 Hardware and Software Requirements

None

16.2 Initial Configuration

None

16.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None

16.4 Upgrade Impact

None

16.5 Data schema (DS) (CM, MIBS, RDB)

16.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TOLLTRKS	NEW	NEW

16.5.2 Table/MIB/Remote Database Schema information

16.5.2.1 Name: <TOLLTRKS>

16.5.2.1.1 Functional description

Table TOLLTRKS stores the common language location identifiers (CLLI) of all trunk groups carrying incoming toll completing traffic, and LDI evaluates the CLLI name to determine the long distance status.

16.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

TRKGRP

TOLLTRKS

16.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOLLTRKS	0	8192	Memory is automatically allocated.

16.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for TOLLTRKS.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CLLI	New	N/A	alphanumeric (1 to 16 characters)	Common language location identifier. This field specifies the trunk over which long distance calls can come into an office. Enter a CLLI from table TRKGRP (1 to 16 characters)

16.5.2.1.5 Datafill example

The following example shows sample datafill for table TOLLTRKS:

```
CLLI
-----------------------------------

ANSIISUP
ETSIISUP
HKISUP
CTUP
```

16.5.2.1.6 Table release history update
Table TOLLTRKS is created for trunks.

16.5.2.1.7 Supplementary information
None

16.5.2.1.8 Translation verification other tools
None

16.6 Service Orders (SO) (CM & SESM)
None

16.7 Software optionality control (SOC)
None

16.8 Element Management
None

16.9 Command interface changes
None

16.10 Security
None

16.11 Configuration Walkthrough
None

17: Configuration (CN): A00002585

Purpose:

XML Commands Responses and Errors for Feature A00002585 - TMM Support For PTS Trunk, POST by Carrier.

This document described the examples about commands responses and errors with XML format. These new commands responses and errors are introduced by the A00002585 “TMM Support for PTS trunk, Post ByCarrier”.

Reference: None.

17.1 Introduction

This document describes the changes being made to the interface via OSSGate by activity A00002585 in SN07. This section is not meant to be a complete description of the interface via OSSGate.

17.2 Mtc By Carrier

The example input from OSSGate are as following:

17.2.1 Get Carriers

```
**************** INPUT XML STRING ******************
<CommandList>
  <Command>
               <Interface>TrunkMtc</Interface>
               <Methods Version="2.0">
                       <GetCarriers/>
               </Methods>
  </Command>
  <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierAction.xsl</Stylesheet>
  </Options>
</CommandList>

**************** OUTPUT XML STRING ******************
<CommandList>
   <Response>
      <Interface>TrunkMtc</Interface>
      <Methods>
   <GetCarriers>
      <Carriers GatewayName="ZLYGW" GWCName="GWC-6"
CarrierNames="DS3_20.0,DS3_20.1,DS3_20.10,DS3_20.11,DS3_20.12
,DS3_20.13,DS3_20.14,DS3_20.15,DS3_20.16,DS3_20.17,DS3_20.18,DS3_20.19,DS3_20.2,
DS3_20.20,DS3_20.21,DS3_20.22,DS3
_20.23,DS3_20.24,DS3_20.25,DS3_20.26,DS3_20.27,DS3_20.28,DS3_20.29,DS3_20.3,DS3_
20.30,DS3_20.31,DS3_20.32,DS3_20.
33,DS3_20.34,DS3_20.35,DS3_20.36,DS3_20.37,DS3_20.38,DS3_20.39,DS3_20.4,DS3_20.4
0,DS3_20.41,DS3_20.42,DS3_20.43,D
```

```
S3_20.44,DS3_20.45,DS3_20.5,DS3_20.6,DS3_20.7,DS3_20.8,DS3_20.9"/>
   </GetCarriers>
      </Methods>
   </Response>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierAction.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.2.2 Query Carriers States

```
*************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <QESByCarrier
         GatewayName="ZLYGW"
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="0-"
         ShowDetails="true"
         FilterState="ALL"
       />
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>

*************** OUTPUT XML STRING FOR ERROR CASE******************
<CommandList>
   <Response>
      <Interface>TrunkMtc</Interface>
      <Methods>
        <QESByCarrier>
          <Header
            GatewayName="ZLYGW" EndpointRange="1-25"
            NodeNumber="74"
            FilterState="ALL"
          >
            <Summary>
              <State Value="UNKNOWN" Count="25"/>
            </Summary>
          </Header>
          <Members>
            <Member TerminalNumber="1">
              <Error
               Number="137"
               Message="The trunk member is not data filled"
               Severity="MAJOR"
              />
            ......
            <Member TerminalNumber="25">
              <Error
               Number="137"
               Message="The trunk member is not data filled"
               Severity="MAJOR"
              />
            </Member>
          </Members>
```

```
        </QESByCarrier>
      </Methods>
   </Response>
  <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>

*************** OUTPUT XML STRING FOR SUCCESS CASE******************
<CommandList>
  <Response>
    <Interface>TrunkMtc</Interface>
    <Methods>
      <QESByCarrier>
        <Header
          GatewayName="ZLYGW"
          EndpointRange="1-25"
          NodeNumber="68"
          FilterState="ALL"
        >
          <Summary>
            <State Value="INB " Count="25"/>
          </Summary>
        </Header>
        <Members>
          <Member TerminalNumber="1" State="INB " />
          .....
        </Members>
      </QESByCarrier>
    </Methods>
  </Response>
  <Options>
    <UseStyleSheet>true</UseStyleSheet>
    <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
  </Options>
</CommandList>
```

17.2.3 Post Carriers

```
*************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <PostByCarrier
         GatewayName="ZLYGW"
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="0-"
         ShowDetails="true"
         FilterState="ALL"
       />
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>

*************** OUTPUT XML STRING ******************
<CommandList>
   <Response>
```

```
      <Interface>TrunkMtc</Interface>
      <Methods>
        <PostByCarrier>
          <Header
            GatewayName="ZLYGW"
            EndpointRange="1-25"
            NodeNumber="68"
            FilterState="ALL"
          >
            <Summary>
              <State Value="UNKNOWN" Count="1"/>
              <State Value="INB " Count="24"/>
            </Summary>
          </Header>
          <Members>
            <Member
              TerminalNumber="1"
              State="INB "
              ConnectedTo="                    "
              TrunkDirection="2W"
              TrunkSignaling="ISD ISD "
              PMType="GWC_NODE"
              PMNumber="6"
              EndpointName="DS3_20.0.1"
              TrunkCLLI="T0              "
              TrunkMember="1"
              TrunkType="PRI"
              PMCarrier="0"
              PMTimeSlot="1"
            />
            ......
            <Member TerminalNumber="24">
              <Error
               Number="139"
               Message="The trunk member is invalid"
               Severity="MAJOR"
              />
            </Member>
            ......
          </Members>
         </PostByCarrier>
      </Methods>
    </Response>
    <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
    </Options>
</CommandList>
```

17.2.4 Busy Carriers

```
**************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <BSYByCarrier
         GatewayName="ZLYGW"
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="0-"
         ShowDetails="true"
         FilterState="ALL"
       />
```

```
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.2.5 Return Carriers to Service

```
**************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <RTSByCarrier
         GatewayName="ZLYGW"
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="0-"
         ShowDetails="true"
         FilterState="ALL"
       />
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.2.6 Force Release Carriers

```
**************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <FRLSByCarrier
         GatewayName="ZLYGW"
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="1,2,3,4,5"
         ShowDetails="true"
         FilterState="ALL"
       />
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.2.7 Installation Busy Carriers

```
**************** INPUT XML STRING ******************
<CommandList>
  <Command>
    <Interface>TrunkMtc</Interface>
    <Methods Version="2.0">
       <FRLSByCarrier
         GatewayName="ZLYGW"
```

```
         GWCName="GWC-6"
         CarrierNames="DS3_20.0"
         EndpointRange="1,2,3,4,5"
         ShowDetails="true"
         FilterState="ALL"
        />
   </Methods>
   </Command>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByCarrierResults.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.3 Show trunk types in post result set

If the command “PostByGatewayName” with the option “ShowDetails” to be set from OSSGate, the corresponding response is as following:

```
*************** OUTPUT XML STRING ******************
<CommandList>
   <Response>
      <Interface>TrunkMtc</Interface>
      <Methods>
        <PostByGatewayName>
          <Header
            GatewayName="ZLYGW"
            EndpointRange="0-2"
            NodeNumber="68"
            FilterState="ALL"
          >
            <Summary>
              <State Value="INB " Count="2"/>
            </Summary>
          </Header>
        <Members>
         <Member
            TerminalNumber="1"
            State="INB "
            ConnectedTo="                    "
            TrunkDirection="2W"
            TrunkSignaling="ISD ISD "
            PMType="GWC_NODE"
            PMNumber="6"
            EndpointName="DS3_20.0.1"
            TrunkCLLI="T0              "
            TrunkMember="1"
            TrunkType="PRI"
            PMCarrier="0"
            PMTimeSlot="1"
          />
          <Member
            TerminalNumber="2"
            State="INB "
            ConnectedTo="                    "
            TrunkDirection="2W"
            TrunkSignaling="ISD ISD "
            PMType="GWC_NODE"
            PMNumber="6"
            EndpointName="DS3_20.0.2"
            TrunkCLLI="T0              "
            TrunkMember="2"
```

```
            TrunkType="PRI"
            PMCarrier="0"
            PMTimeSlot="1"
          />
        </Members>
      </PostByGatewayName>
    </Methods>
   </Response>
   <Options>
      <UseStyleSheet>true</UseStyleSheet>
      <Stylesheet>tmm/MtcByGatewayNameResults.xsl</Stylesheet>
   </Options>
</CommandList>
```

17.4 Keep Return Codes Compliance

New return codes are as following:

```
<?xml version="1.0"?>
<TMM>
   <Errors
      ERR_5100="The command: %1 is being processed by request of: %2"
      ERR_5101="Unable to communicate with the TMM Server"
      ERR_5102="The error '%1' occurred processing the request"
      ERR_5103="Unable to connect to the CORBA ORB"
      ERR_5104="Unable to connect to the TMM Server"
      ERR_5105="Insufficient Security Privileges to perform this action"
      ERR_5201="The requested command '%1' is not supported"
      ERR_5202="An error occurred communicating with the SDM"
      ERR_5203="The error '%1' occurred while initializing the server"
      ERR_5204="The error '%1' occurred while connecting to '%2'"
      ERR_5205="Unable to connect to the network databases%1"
      ERR_5206="Unable to connect to the gateway controller element manager
databases%1"
     ERR_5301="Invalid parameters passed in. Either the CM CLLI or the Trunk CLLI
is missing"
      ERR_5302="Invalid parameters passed in. The trunk range '%1' is invalid"
      ERR_5303="This requested trunk member is not valid"
      ERR_5304="None of the trunk members in the range '%1' was valid for this
Trunk CLLI"
      ERR_5305="Invalid parameters passed in. NodeNumber and TerminalNumber are
required and must be numeric"
      ERR_5401="Invalid parameters passed in. The gateway name is missing"
      ERR_5402="Invalid parameters passed in. The endpoint range '%1' is invalid"
      ERR_5403="No CM CLLI exists for gateway '%1'"
     ERR_5404="None of the endpoints in the range '%1' was valid for this gateway"
      ERR_5405="No response was received from the CM CLLI '%1'"
    ERR_5406="The error '%1' occurred while getting endpoint data from the gateway
controller element manager"
      ERR_5407="The gateway '%1' is not a trunk gateway"
      ERR_5408="The gateway information for the gateway '%1' was not found or
contained invalid information. Please enter a different gateway name"
      ERR_5409="The error '%1' occurred while retrieving gateway information"
      ERR_5410="The error '%1' occurred while retrieving gateway controller
information"
      ERR_5411="Some of the requested endpoints are not valid"
      ERR_5412="SDM failed to send the endpoint data, but gave a success status.
Check the DMA logs for further information"
      ERR_5413="NO trunk CLLIs are assigned to gateway: %1"
      ERR_5501="The error '%1' occurred while retrieving the gateway names"
      ERR_5502="The error '%1' occurred while retrieving the gateway controller
names"
      ERR_5503="The error '%1' occurred while retrieving the call server names"
```

```
    ERR_5504="Unable to retrive carriers data from the gateway controller element
manager"
      ERR_5505="Invalid parameters passed in. The GWC name is missing"
      ERR_5506="No Carrier is associated to gateway: %1"
      ERR_5507="Invalid parameters passed in. The Carrier is missing"
     ERR_5508="Invalid endpoint range for selected carriers. The valid endpoint
range should be: %1"


      ERR_131="The trunk member is in deload%1"
      ERR_132="The state could not be retrieved for the trunk member%1"
      ERR_133="The trunk member could not be put into deload%1"
      ERR_134="The trunk member could not be selected%1"
      ERR_135="The request has been delayed%1"
      ERR_136="The request failed%1"
      ERR_137="The trunk member is not data filled%1"
      ERR_138="The trunk CLLI was invalid%1"
      ERR_139="The trunk member is invalid%1"
      ERR_1310="The request has already been completed%1"
      ERR_1311="Unable to transition the endpoint to the requested state%1"
      ERR_1312="An unknown error occurred%1"
      ERR_1313="The request is invalid%1"
      ERR_1314="The message length of the request is invalid%1"
      ERR_1315="The message's TID format was invalid%1"
      ERR_1316="The message's TID range was invalid%1"
      ERR_1317="The message's node was invalid%1"
      ERR_1318="The specified CLLI is not supported%1"
      ERR_1319="Specified Message Type is not valid%1"
      ERR_1320="The TMM version is not supported%1"
      ERR_1321="Specified Request Handler is not valid%1"
      ERR_1322="The range specified in the request message is invalid%1"
      ERR_1323="The maintenance action specified in the request message is
invalid%1"
      ERR_1324="The Specified Request Handler is not available%1"
      ERR_1325="The circuit is not valid for the specified request handler %1"
      ERR_1326="The circuit is already handling a maintenance action%1"

      ERR_71="Command successful%1"
      ERR_72="Unable to synchronize all tables%1"
      ERR_73="Requested entity is empty%1"
      ERR_710="Audit Failed. Data is not in sync%1"
      ERR_711="Data integrity problems were found that could not be corrected%1"
     ERR_712="System is partially operational. Check logs to determine available
functionality%1"
      ERR_713="Command partially successful%1"
      ERR_714="DMOPRO input partially successful%1"
     ERR_715="Data subscription failed due to prior higher-level subscription%1"
      ERR_716="Data subscription canceled due to higher-level subscription%1"
      ERR_717="Data checkout failed due to prior higher-level checkout%1"
      ERR_718="Data checkout canceled due to higher-level checkout%1"
     ERR_719="Data checkout canceled due to higher-priority checkout by another
client%1"
      ERR_720="Failed. Check logs for detailed failure information%1"
      ERR_721="Transaction failed due to command failure%1"
      ERR_731="Add failed. A maximum of one NE may exist in the database%1"
      ERR_732="Add failed. The NE has not been registered with DCE%1"
      ERR_733="Failed. This action will remove client logon information. Before
allowing this operation, you must remove the client from other client groups%1"
      ERR_7100="Command syntax error%1"
      ERR_7101="Input parameter is invalid in this context%1"
      ERR_7102="Input parameters are not consistent with each other%1"
      ERR_7103="Required input parameter is missing from this command%1"
      ERR_7104="A parameter is repeated or illegally used in this command%1"
```

```
     ERR_7105="Input data is not valid even though it may be within the allowable
range%1"
      ERR_7106="Input data is not consistent%1"
      ERR_7107="Input data is out of range or violates data type%1"
      ERR_7108="Input command is invalid in this context%1"
      ERR_7109="Input command is not consistent in this context%1"
      ERR_7110="The input target does not exist%1"
      ERR_7111="The target input entity already exists%1"
     ERR_7112="Permissions violation. User does not have access to an operations
group which includes the command%1"
      ERR_7113="Permissions violation. User may not perform operations on the
target group%1"
      ERR_7114="System problem%1"
      ERR_7115="The member name specified is not a member of the group%1"
      ERR_7116="The input target is not active%1"
     ERR_7117="The group name specified as the accessed group is not defined as
an operation group, an NE group, or a table group%1"
      ERR_7118="The access type specified is invalid%1"
      ERR_7119="The group type specified is invalid%1"
      ERR_7120="The member name specified is already a member of the group%1"
      ERR_7121="Command not supported by DDMS%1"
      ERR_7122="A MessageID has been provided which does not correspond to the
referenced action%1"
      ERR_7123="DMOPRO input unsuccessful%1"
      ERR_7124="Operation in progress%1"
      ERR_7125="Permissions violation. Tuple locked at a higher priority%1"
      ERR_7126="The TCRS is currently in use by the network element%1"
      ERR_7127="Command aborted manually%1"
      ERR_7128="Command not processed due to timeout%1"
      ERR_7129="Command not processed due to DDMS system shutdown%1"
      ERR_7130="Command failed due to a DCE error%1"
      ERR_7131="Specified group does not contain any members%1"
      ERR_7132="Cannot assign permissions to a subgroup%1"
      ERR_7133="Failed to allocate memory for the group%1"
      ERR_7134="Server out of disk space%1"
      ERR_7135="Write error. Database opened in read-only mode%1"
     ERR_7136="The system is down or an invalid version and release has been used
for the category%1"
      ERR_7137="Command not processed. DDMS is not ready (i.e. Initialization in
progress)%1"
      ERR_7138="Command not processed due to DDMS system suspend%1"
      ERR_7139="Invalid OSSDI message header%1"
      ERR_7140="Internal inter-subsystem communications error%1"
      ERR_7141="Invalid argument passed to RPC call%1"
      ERR_7142="Login failed (invalid principal/password combination)%1"
      ERR_7143="Session not logged in%1"
      ERR_7144="DDMS unavailable or off-line%1"
      ERR_7145="Communications with DDMS failed%1"
      ERR_7146="Failure to access DDMS due to a failed binding attempt%1"
      ERR_7147="DCE error. DCE function call failed%1"
      ERR_7148="Entry not found%1"
      ERR_7149="Duplicate entry found%1"
      ERR_7153="Command in progress. Cannot process request%1"
      ERR_7154="Invalid state change for the package%1"
      ERR_7155="Package already in requested state%1"
      ERR_7156="Exceeded the maximum number of ClientGroups limit%1"
      ERR_7157="Command partially completed%1"
      ERR_7158="Command not processed due to an earlier failure in the atomic
transaction%1"
      ERR_7159="Rollback failure%1"
      ERR_7160="More than one tuple specified in the command%1"
      ERR_7161="The group cannot be added as a member of itself%1"
      ERR_7162="System busy. Please try again later%1"
      ERR_7163="Exceeded the limit for maximum number of Clients%1"
```

```
      ERR_7164="Exceeded the limit for maximum number of NEGroups%1"
     ERR_7170="System error has occurred. The system is in an invalid state. Retry
operation. If problem persists, contact system administrator%1"
      ERR_7171="The message data file cannot be opened. Contact system
administrator%1"
     ERR_7172="Could not locate the TxtIdx in message data file. Contact system
administrator%1"
      ERR_7173="An error occurred while parsing the message data file. Contact
system administrator%1"
      ERR_7174="Mandatory information is missing from message data file entry%1"
      ERR_7175="Invalid CGI name value pair received by GUIDE application%1"
      ERR_7176="Mandatory CGI name value pair missing from input stream%1"
      ERR_7178="No message or message data was returned for the executed OSSDI
command%1"
      ERR_7179="Invalid argument passed to CGI interface%1"
      ERR_7180="DCE function call failed within the CGI interface%1"
      ERR_7181="GuideD unavailable or off-line%1"
     ERR_7182="Perform FINDREF? Be aware that operation can take several minutes
to perform%1"
      ERR_7183="The delete operation has failed. FINDREF must be performed
manually%1"
      ERR_7184="FINDREF is being performed now. Please wait%1"
      ERR_7185="Command has been sent successfully. No response message will be
displayed due to command execution duration. To determine command success or
failure, refer to the command Usage Notes in the OSSDI Technical Reference Manual
(297-5051-915)%1"
     ERR_7186="OSSDI command acknowledgement. An OSSDI command has been received
by the OTG (OSS Telnet Gateway) and sent to the DDMS for processing%1"
      ERR_7255="A timeout occurred communicating with the SDM%1"
   />
</TMM>
```

18: Configuration (CN): A00002607

18.1 Hardware and Software Requirements

The changes provided by this feature will allow the customer to physically identify ABI configured hardware components as well as MG9K frames/ shelves hosting only native lines when trouble shooting their network therefore allowing for quick problem resolutions. These Core changes provide:

- ABI XPM Site information and MG9K hosting data
- limited MG9K Frame/Shelf location data for MG9Ks hosting only native lines
- changes to the Mapci, Logs and OM applications to make use of this data

Therefore the following hardware needs to be in place prior to exercising the software provided by this feature. The software is exercised by provisioning the physical location data of these hardware components:

- A typical ABI configuration
- A typical MG9K Gateway configuration

Software Requirements:

- SN06 Succession Core load with this feature patched back

-OR-

- SN07 Succession Core load or later

18.2 Initial Configuration

As a provisioning component of the Succession program, much of this functionality performs as designed without the hardware being in place. However, to provision actual physical location data, the provisioning of the configurations mentioned in “18.1 Hardware and Software Requirements” should be installed.

Once the hardware is installed and the software is available, provisioning of the physical location data can begin. The ABI location data is provisioned in table LTCINV. The MG9K Frame/Shelf location data for MG9Ks hosting native lines only is provisioned in table LGRPINV. The steps to perform the provisioning are described in section “18.5 Data schema (DS) (CM, MIBS, RDB)” on page 2580.

18.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

18.4 Upgrade Impact

18.4.1 Dump and Restore

No impact to Dump and Restore mechanisms. This data is preserved via the existing TabXfr mechanism available to all Table Control tables.

18.4.2 Element Management Upgrade

Not applicable.

18.5 Data schema (DS) (CM, MIBS, RDB)

18.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	Changed	Unchanged
LGRPINV	Changed	Unchanged

18.5.2 Table LTCINV Database Schema information

18.5.2.1 Name: LTCINV

Long Table Name: Line Trunk Controller INVentory

18.5.2.1.1 Functional description

Table LTCINV contains the inventory data, except P-side link assignments, for various host peripheral module (XPM) types. This feature will only impact ABI XPM tuples. The impact does not change existing datafilled but extends the optional data associated with the ABI (EXTDS512) option. This new optional data will allow the provisioning of the physical XPM location data. Please refer to “Table 3 Table LTCINV changed field descriptions” on page 2581.

18.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- No change to current datafill order.

18.5.2.1.3 Size

No change in the maximum number of tuples for table LTCINV.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	0	210	Memory is automatically allocated in increments of 10 XPMs at a time up to 210

18.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for Table LTCINV.

Table 3 Table LTCINV changed field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTATTR	Changed	Modified the EXTDS512 refinement, add 3 new subfields	SITE - 4 alpha numerics	SITE_NAME - This is the Site name as datafilled in table Site. There is an existing data dictionary type for SITE. Valid values are verified against entries in table SITE. Example data fill CARY.
			NE_NBR - 0 TO 999	NETWORK_ELEMENT_NO - This is the network element number assigned when the MG9K gateway is added via the MG9K-EM. This requires a new dictionary type. Value of 0 is the NIL value.
			ABI_SLOT - 1 TO 21	SLOT_NO - new dictionary type. Valid values are 2-9 and 14-21, even numbers only. Because the range is 1 TO 21, verification of this value is enforced outside the data dictionary via format aspects.

18.5.2.1.5 Datafill example

The following example illustrates the prompting sequence for the new Location data associated with the EXTDS512 option in table LTCINV.

Figure 1 Prompting sequence for new Location fields for option EXTDS512

```
>add lgc 1 7 lgci 0 32 1 D 33 6x02na qli16at pots potsex keyset ksetex $ $ msg6x69 isp +
16 $ northaa sx05aa $ sx05aa $ 0 sxfwaj01
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y

OPT_ATTR:
>asdfd
 ***  ERROR  ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
OPT_ATTR:
>asdfd
 ***  ERROR  ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
TYPE                                    IS                                  LTCINV_OPT_ATTR
{CCS7,STRBBF,STRDTRE,STRN5,FSTR2,PCM30,NX64,METER,
                FLS,OC,FDCP,EXTDS512}
OPT_ATTR:
>extds512
SITE:
>cary
NE_NBR:
>12
ABI_SLOT:
>8
IPADDR:
>47 122 133 44
GWC_HOST:
>gwc 99
... << continue with normal datafill for LTCINV >>
```

Figure 2 on page 2582 shows the changes to the OPTATTR field with the new Location field ranges for the optional refinement EXTDS512.

Figure 2 Range Values for new Location datafill in option EXTDS512

```
>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
>range optattr
18 OPTATTR          LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
      OPT_ATTR              LTCINV_OPT_ATTR REFINEMENTS:
      {EXTDS512}            MULTIPLE WITH
         SITE               CHAR_VECTOR VECTOR OF UP TO 16 CHAR'S
         NE_NBR             {0 TO 999}
         ABI_SLOT_NBR   ABI_SLOT_RANGE:EVEN NUMBERS {2 TO 8,14 TO 20}
         IPADDR          TABLE OF 4 {0 TO 255}'S
         GWC_HOST          MULTIPLE WITH
            PMTYPE       PM_TYPE
            PMNO         {0 TO 255}
      OTHERWISE             LTCINV_OPT_ATTR_NIL_DATA
```

Figure 3, on page 2583 provides a view of the successfully added tuple with the new Location data fields for option EXTDS512.

Figure 3 Sample LTCINV Tuples with new Location fields for option EXTDS512

```
>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB
CSLNKTAB OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
-----------------------------------------------------------------------------------------------------------------------
LGC 1 1002 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) $ (4 0)(4 1)(4 2)(4 3) $ (MSG6X69)
$ NORTHAM SX05AA $ SX05AA $ 0 SXFWAE08 (EXTDS512 CARY 12 8 47 122 133 44 GWC 99) $
6X40FA N

SMA2 2 1009 LTE 1 51 2 E 31 MX85AB QLI17AY1 (POTS POTSEX) $ (4 4) (4 5)(4 6) (4 7) $ (UTR6)
(MSGMX76 HOST ) (ISP 4) $ NORTHAM AX74AA AX74AA 0 SXFWAE08
(EXTDS512 GRNR 10 14 47 202 34 22 GWC 50) $ 6X40AC N
```

18.5.2.1.6 Table release history update

SN07 Feature A00002607:

Modified field: OPTATTR:

— adding 3 new subfields for the EXTDS512 refinement. For more information see “Table LTCINV changed field descriptions” on page 2581.

18.5.2.1.7 Supplementary information

Limitations:

- LTCINV - since these new fields apply to the EXTDS512 option, they can only be datafilled on tuples with the EXTDS512 option.

18.5.2.1.8 Translation verification other tools

Table LTCINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table LTCINV. The following Figure 4 on page 2584 shows the output from TABAUDIT when it is used to verify LTCINV.

Figure 4 Sample Tabaudit output for Verifying Table LTCINV Datafill

```
>tabaudit
TABAUDIT:
>include ltcinv

>execute
-------------------------------------------------------------------------------
|            TABAUDIT STATUS
-------------------------------------------------------------------------------

The following tables are included:
      table LTCINV (91)

The following tables are excluded:
  From table VERSIONS (0)              to table SERVRINV (90).
  From table MGCINV (92)               to table IPINV (299).
  From table X75INFO (301)             to table INWATNPA (1426).

Please confirm ("YES", "Y", "NO", or "N"):
>yes
Creating TABAUDIT summaryfile: SUMMARY$MAP on SFDEV.
Starting DMS data verification ...
Table LTCINV: New table control.
     Completed tuple checking.
     SUMMARY: Tbl LTCINV: tuples checked 2, passed 2, failed 0.
Data verification is completed.
```

18.5.3 Table LGRPINV Database Scheme information

18.5.3.1 Name: LGRPINV

Long Table Name: Logical GRouP INVentory

18.5.3.1.1 Functional description

Table LGRPINV is where Logical Groups (Lgrps) are provisioned. Generally speaking Logical Groups (one or more) are the Cores representation of Gateways. Specifically, for MG9K Gateways, one Lgrp represents one shelf in a specific MG9K Frame. MG9K Lgrps are Logical Groups with a GroupType of “S”.

This feature will only impact MG9K Lgrps. The impact is to provide a new optional field called LGRPLOC. The optional Location field will contain the physical location of a specific MG9K shelf. Please refer to “Table 5 Table LGRPINV Changed field descriptions” on page 2585.

18.5.3.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- No change to current datafill order.

18.5.3.1.3 Size

No change in the maximum number of tuples for table LGRPINV.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LGRPINV	0	1000	Memory is automatically allocated in increments of 20 LCDs at a time up to 1000.

18.5.3.1.4 Fields/OIDs

The following table lists fields/OIDs for Table LGRPINV.

Table 5 Table LGRPINV Changed field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LGRPOPTS	Changed	Added new refinement, LGRPLOC with 6 fields.	FRAME_TYPE	FRAME_NAME - existing data dictionary type. The unique frame type. MG9Ks have a frame type of 'MG9F'.
			FLOOR_POSITION {0 TO 99}	FLOOR_POS - existing data dictionary type. The unique floor with a unique Site (generally a building).
			ROW_POSITION {A,B,C...X,Y,Z,AA, BB,CC...XX,YY,ZZ}	ROW_POS - existing data dictionary type. The unique row within a floor.
			FRAME_POSITION {0 TO 99}	FRAME_POS - existing data dictionary type. The unique frame position within a row.
			SHELF_POSITION {0 TO 77}	SHELF_POS - existing data dictionary type. Traditionally, this is the bolt hole position as measured in inches from the floor up. For MG9K shelves, it will be equal to the Shelf Number as specified in the Lgrp Key. The unique shelf position within a specific frame.

18.5.3.1.5 Datafill example

The following example illustrates the prompting sequence for the new optional Location data in table LGRPINV.

Figure 5 Prompting sequence for new option Location datafill

```
>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
>add cary 1 0 gwc 1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYPE:
>S
LGRPOPTS:
>lgrploc
FRAME_TYPE:
>MG9F
FLOOR_POSITION:
>2
ROW_POSITION:
>C
FRAME_POSITION:
>5
SHELF_POSITION:
>0
LGRPOPTS:
>$
```

Figure 6 on page 2586 shows the changes to the LGRPOPTS field with the new optional Location fields ranges.

Figure 6 Range Values for new optional Location datafill

```
>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
>ran LGRPOPTS
 4 LGRPOPTS        LGRPINV_OPT_ATTR_VECTOR
TYPE IS LGRPINV_OPT_ATTR_VECTOR VECTOR OF UP TO 2 MULTIPLES WITH
      LGRPOPTS             {MTSTAPT,LGRPLOC} REFINEMENTS:
      {MTSTAPT}            MULTIPLE WITH
          SITE_NAME         TABLE OF 4 CHAR'S
          VERT_INFO         VECTOR OF UP TO 8 MULTIPLES WITH
              VERT_NO      {0 TO 1023}
              MTAPTNO      {0 TO 48}
      {LGRPLOC}            MULTIPLE WITH
         FRAME_TYPE           FRAME_NAME
          FLOOR_POSITION     {0 TO 99}
          ROW_POSITION       ROW_POS
          FRAME_POSITION     {0 TO 99}
          SHELF_POSITION     {0 TO 77}
```

Figure 7 on page 2587 provides a view of a successfully added tuple with the new optional Location data fields.

Figure 7 Sample LGRPINV Tuples with new optional Location datafill

```
>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
pos lg 1 0
GRPNO SRVRNAME GRPTYPE LGRPOPTS
-------------------------------------------------------------
CARY 01 0 GWC 1 S  LGRPLOC MG9F 2 C 5 0 $
```

18.5.3.1.6 Table release history update

SN07 Feature A00002607:

Modified field: LGRPOPTS

— adding a new LGRPLOC refinement. For more information see “Table LGRPINV Changed field descriptions” on page 2585.

18.5.3.1.7 Supplementary information

Limitations:

- LGRPINV - the new LGRPLOC optional data should be datafilled against MG9K LGRPs, LGRPs with a GRPTYPE of S and shelf number < 4. This requirement will be enforced by the table control software and if not provided a warning will be issued. For other LGRP types, datafilling of this data is optional.

18.5.3.1.8 Translation verification other tools

Table LGRPINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table LGRPINV. The following Figure 4 on page 2584 shows the output from TABAUDIT when it is used to verify Table LGRPINV.

Figure 8 Sample Tabaudit output for Verifying LGRPINV Table Datafill

```
>tabaudit
TABAUDIT:
>include lgrpinv

>execute
-------------------------------------------------------------------------------
|             TABAUDIT STATUS
-------------------------------------------------------------------------------

The following tables are included:
table LGRPINV (300)

The following tables are excluded:
  From table VERSIONS (0)              to table SERVRINV (90).
  From table MGCINV (92)               to table IPINV (299).
  From table X75INFO (301)             to table INWATNPA (1426).

Please confirm ("YES", "Y", "NO", or "N"):
>yes
Creating TABAUDIT summaryfile: SUMMARY$MAP on SFDEV.
Starting DMS data verification ...
Table LGRPINV: New table control.
      Completed tuple checking.
      SUMMARY: Tbl LGRPINV: tuples checked 26, passed 26, failed 0.
Data verification is completed.
```

18.6 Service Orders (SO) (CM & SESM)

Not Applicable.

18.7 Software optionality control (SOC)

Not Applicable.

18.8 Element Management

Not Applicable.

18.9 Command interface changes

Not Applicable.

18.10 Security

Not Applicable.

18.11 Configuration Walkthrough

As indicated earlier, there is no change to the provisioning sequence of the tables. There are changes to the prompting sequence within the LTCINV and LGRPINV tables for the new data. Examples of these prompting sequences for each table are provided in “18.5 Data schema (DS) (CM, MIBS, RDB)” on page 2580.

19: Configuration (CN): A00002858

19.1 Hardware and Software Requirements

The spectrum load tape should contain an EXT file with correct information about all the spectrum load releases which is used to datafill the table SPMLDVAL.

19.2 Initial Configuration

None.

19.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

19.4 Upgrade Impact

19.4.1 Dump and Restore

In SN06, table SPMLDVAL contains both the INTL and NA DMSCP loads in the same tuple. i.e. One tuple contains CST, CEM, STM and OC3 loads. Here, CEM and OC3 loads are specific to DMSCP NA product whereas CST and STM loads are specific to DMSCP INTL product of SPM.

In SN07, since a new field is introduced to identify the product type of each tuple, such a combination of loads becomes invalid.

During the dump and restore of table SPMLDVAL from release SN06 to SN07, a single tuple with both DMSCP NA and INTL loads is splitted up into two tuples. The product type of the first tuple is written as SPMNA and contains CEM and OC3 loads. On the other hand, the product type of the second tuple is written as SPMIN and contains CST and STM loads.

19.5 Data schema (DS) (CM, MIBS, RDB)

19.5.1 Modified table

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SPMLDVAL	CHANGED	NEW

19.5.2 Table/MIB/Remote Database Schema information

19.5.2.1 Name: SPMLDVAL

Spectrum Load Name Validation.

19.5.2.1.1 Functional description

Table SPMLDVAL is enhanced to store the device load lineups for both TDM and Succession spectrum load releases.

Table SPMLDVAL has a 5 part key. The 5 parts of the key are

- Spectrum family load type indicator.
- General release number.
- Maintenance release number.
- Emergency release number.
- Spectrum family product line type indicator.

Figure 1 shows some example tuples in table SPMLDVAL.

Figure 1 : Example tuples in table SPMLDVAL

```
SP 17 0 0 SPMNA (CEM17BU) (DLC17BV) (DL217BT) (DSP17BU) $
SP 17 0 0 SPMIN (CST17BS) (DLC17BV) (DL217BT) (DSP17BU) $
SN 06 0 0 MG4AT (MG419BR) (ATC19BO) (IED19BO) (OC419BN) $
SN 06 0 0 MG4IP (MG419BR) (GEM19BN) $
SN 06 0 0 IWSAT (IWS19BP) (ATC19BO) (SYN19BN) $
SN 06 0 0 IWSIP (IWS19BP) (GEM19BN) $
SN 06 0 1 DPTAT (IWS19BP) (ATC19BO) (DSP19BN (COH0019) $
SN 07 0 1 DPTIP (IWS20BA) $
```

For a general release, the key subfields ‘maintenance release’ and ‘emergency release’ are datafilled as 0. Similarly for a maintenance release, the key subfield ‘emergency release’ is datafilled as 0.

Note 1: The PPSL loads are considered under the current maintenance release name only. No new tuple is added in the table whenever a PPSL load is released.

Note 2: Whenever a coherant load changes the version in a release the first seven characters remains same and so this change will not be reflected in the table SPMLDVAL. However, a new tuple shall be added in the table with the same coherant load name.

Table SPMLDVAL can be datafilled in the following ways.

- During panther execution, filecopy command copies the EXT file from the tape to the disk volume and run the EXT file to get the table datafilled.

- If tuples need to be added manually, then ADMIN can use RWOK ON option and get write permission for the table.

The following applications retrieve data from table SPMLDVAL.

- CI tool SPMLDINFO gets the load lineup information for different spectrum load releases from table SPMLDVAL.
- QueryPM files command compares the device loads in a SPM with the load lineup of different spectrum load releases datafilled in table SPMLDVAL to find out the running release load for that SPM.

19.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

19.5.2.1.3 Size

The Size of this table is increased from 255 to 2048.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SPMLDVAL	0	2048	Protected Memory

19.5.2.1.4 Fields/OIDs

The following table lists fields for SPMLDVAL.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PRODUCT_TYPE	New	T_SPMLDVAL_KEY	SPMNA, SPMIN, MG4AT, MG4IP, IWSAT, IWSIP, DPTAT, DPTIP	A new subfield is introduced which defines the product line of the SPM.
LOAD_TYPE	Changed	T_SPMLDVAL_KEY	SP, SN	This subfield supports both SP and SN.

19.5.2.1.5 Datafill example

The following example shows sample datafill for table SPMLDVAL.

>lis all

TOP
KEY LOAD_LIST

SP 17 0 0 **SPMNA** (CEM17BU) (DLC17BV) (DL217BT) (DSP17BU) $
SP 17 0 0 **SPMIN** (CST17BS) (DLC17BV) (DL217BT) (DSP17BU) $
SN 06 0 0 **MG4AT** (MG419BR) (ATC19BO) (IED19BO) (OC419BN) $
SN 06 0 0 **MG4IP** (MG419BR) (GEM19BN) $
SN 06 0 0 **IWSAT** (IWS19BP) (ATC19BO) (SYN19BN) $
SN 06 0 0 **IWSIP** (IWS19BP) (GEM19BN) $
SN 06 0 1 **DPTAT** (IWS19BP) (ATC19BO) (DSP19BN (COH0019) $
SN 07 0 1 **DPTIP** (IWS20BA) $
BOTTOM

19.5.2.1.6 Table release history update

Table SPMLDVAL was introduced in CSP release 19.

19.5.2.1.7 Supplementary information

The protection level of the table is SYSPROT which prevents the user from add / delete / modify tuples in this table directly. The user needs to enter 'RWOK ON' to get write permission to the table.

19.5.2.1.8 Translation verification other tools

Table SPMLDVAL does not use translation verification tools.

19.6 Service Orders (SO) (CM & SESM)

Not Applicable.

19.7 Software optionality control (SOC)

Not Applicable.

19.8 Element Management

Not Applicable.

19.9 Command interface changes

19.9.1 Directory: SPMLDINFO

19.9.1.1 Directory description

- The CI directory was used to display the spectrum load release information for DMSCP class of SPMs only. It is enhanced to enable the craftsperson to display the load release information for all the following product lines of SPMs:
  - — DMSCP - NA
  - — DMSCP - INTL
  - — SMG4 - ATM
  - — SMG4 - IP
  - — IW - ATM
  - — IW - IP
  - — DPT - ATM and
  - — DPT - IP

19.9.1.2 Accessing directory: SPMLDINFO

19.9.1.2.1 Access to directory or MAP level and return to CI

To access SPMLDINFO from the CI environment, enter **SPMLDINFO**.

To return to the CI environment, enter **quit**.

19.9.2 Command: LISTLOAD

19.9.2.1 Command type: Non-Menu

19.9.2.2 Command target: All

19.9.2.3 Command availability: Res

19.9.2.4 Command description

This command **listload** was used for displaying the load lineup information for a given spectrum load release name. Now, it can be used for displaying the load lineup information for a given SN load release name also. In case of many tuples(many product lineup) with the same release present in the table, then all the load lineups are displayed along with the product line information. See Table 4 for more information.

19.9.2.5 Command syntax

The command syntax is as shown in Figure 2.

Figure 2 : LISTLOAD command syntax

```
SYNTAX : LISTLOAD <load_type> <general_release> <maintenance_release>
                        <emergency_release>
Parms: <load_type> { SP, SN}
       <general_release> {1 TO 99}
       <maintenance_release> {0 TO 9}
       <emergency_release> {0 TO 9}

Parameter Description:
```

load_type :
Enter the type of load. It can take values - SP or SN

general_release :
Enter the milestone release number. It takes values in the range 1 to 99.

maintenance_release :
Enter the maintenance release number. Enter 0 if it is a milestone release. It takes values in the range 0 to 9.

emergency_release :
Enter the emergency release number. Enter 0 if it is a milestone release or maintenance release. It takes values in the range 0 to 9.

19.9.2.6 Qualifications and warnings

None.

19.9.2.7 Responses

If the load release name entered is not datafilled in table SPMLDVAL, then the following message is displayed.
This load release is not datafilled in table SPMLDVAL.

19.9.2.8 Example

Table 4 shows the output of listload command.

Table 4 Usage examples for listload command

Description of task:	Display the list of device loads belonging to a particular spectrum load release.
Command: MAP response:	SPMLDINFO; listload SN 07 3 1 CI: >**SPMLDINFO** SPMLDINFO: >**listload SN 07 3 1** Circuit Pack Load Lineup for MG4K ATM Load Release SN07.3.1: CEM Load : MG420AL DSP Load : DSP20AL DLC Load : DLC20AL ..... Circuit Pack Load Lineup for MG4K IP Load Release SN07.3.1: CEM Load : MG420AL DSP Load : DSP20AL DLC Load : DLC20AL ..... Circuit Pack Load Lineup for IW ATM Load Release SN07.3.1: IWS Load : IWS20AL DSP Load : DSP20AL DLC Load : DLC20AL .....
Command: MAP response:	SPMLDINFO; listload SN 03 1 1 CI: >**SPMLDINFO** SPMLDINFO: >**listload SN 03 1 1** This load release is not datafilled in table SPMLDVAL.

Note: It uses the first 3 characters of the loadname to identify a load type. For example, OC3 for OC315DF, DL2 for DL215AH etc..

19.9.3 Command: LISTRELEASE

19.9.3.1 Command type: Non-Menu

19.9.3.2 Command target: All

19.9.3.3 Command availability: Res

19.9.3.4 Command description

This command **listrelease** was used only for displaying the spectrum(SP) load releases in which a given device load is included. Now, it is used for displaying the SN load releases also.

19.9.3.5 Command syntax

The command syntax is as shown in Figure 3.

Figure 3 : LISTRELEASE command syntax

```
SYNTAX : listrelease <loadname> STRING
Parms: <load_name>

Parameter Description:


    load_name :
                Enter the device load name. It is a string which can take up to 7 characters.
                Ex: MG420CQ, DSP20DO
```

19.9.3.6 Qualifications and warnings

None.

19.9.3.7 Responses

If the circuit pack loadname entered is not 7 character long, then the following warning message is displayed.

***** Warning : Loadname must be 7 characters in length.**

If the circuit pack loadname entered is not datafilled in table SPMLDVAL, then the following message is displayed.
Circuit pack load <load name> is not datafilled in table SPMLDVAL.

19.9.3.8 Example

Table 5 shows the output of listrelease command.

Table 5 Usage examples for listrelease command

Description of task:	Display the list of spectrum load releases in which the given device load is included.
Command: MAP response:	SPMLDINFO; listrelease DLC20AB CI: **>SPMLDINFO** SPMLDINFO: **>listrelease DLC20AB** Circuit pack load DLC20AB is valid in the following load releases. MG4K ATM Load Release SN07.2.1
Command: MAP response:	SPMLDINFO; listrelease MG420 CI: **>SPMLDINFO** SPMLDINFO: **>listrelease MG420** *** Warning : Loadname must be 7 characters in length.
Command: MAP response:	SPMLDINFO; listrelease IWS15CZ CI: **>SPMLDINFO** SPMLDINFO: **>listrelease IWS15CZ** Circuit pack load IWS15CZ is not datafilled in table SPMLDVAL.

19.9.4 Command: LISTSPMLOAD

19.9.4.1 Command type: Non-Menu

19.9.4.2 Command target: All

19.9.4.3 Command availability: Res

19.9.4.4 Command description

This command **listspmload** is used for displaying the running release load name for all the SPMs in the office. This command has 3 options. Option ‘all’ can be used to list the load release names for all SPMs. In the second option, the user can specify a range, say SPM 1 4, in which case, the load release

names of all SPMs in the given range is displayed. In the third option, the user can specify one SPM, in which case, the load release names of that SPM is displayed.

19.9.4.5 Command syntax

The command syntax is as shown in Figure 4.

Figure 4 LISTSPMLOAD command syntax

```
SYNTAX : listspmload
Parms: { All }
        { spm <spm no> <spm no>}

Parameter Description:
```

All:

This option lists the running release loads for all the SPMs.

SPM <spm no> <spm no>:

Specify the range of SPM numbers for which the running load release information is required.

19.9.4.6 Qualifications and warnings

None.

19.9.4.7 Responses

If the running device loads in an SPM do not match with any of the load release lineups datafilled in table SPMLDVAL, then a warning is displayed as follows.

SPM <spm no> : Load lineup does not match with any of the load releases datafilled in table SPMLDVAL.

If the CEMs/RMs in the SPM are out of service, then the tool will not be able to get the running loads in the SPM's devices. In that case, the following warning message is displayed.

SPM <spm no> : Unable to contact the devices. The requested data cannot be retrieved.

When option 'all' is specified, then it will check whether at least 1 SPM is datafilled. If not, then it will give the following message and stop execution.

No SPMs are datafilled in the office.

When spm number range is specified, if one of the spm numbers within the range is not datafilled in table MNNODE, then the following warning message is displayed.

SPM <spm no> is not datafilled.

Non-datafilled SPMs will not be displayed in the case of '**all**' option.

19.9.4.8 Example

Table 6 shows the output of listspmload command.

Table 6 Usage examples for listspmload command

Description of task:	Display the list of spectrum load releases running in each of the SPMs in the office.
Command: MAP response:	SPMLDINFO; listspmload all CI: >**SPMLDINFO** SPMLDINFO: >**listspmload all** SPM 1 : MG4K ATM Load Release SN07.3.1 SPM 3 : DMSCP NA Load Release SP20.3.1 SPM 5 : IW ATM Load Release SN07.3.1 SPM 6 : Unable to contact the devices. The requested data cannot be retrieved. SPM 7 : Load lineup does not match with any of the load releases datafilled in table SPMLDVAL
Command: MAP response:	SPMLDINFO; listspmload spm 1 4 >**SPMLDINFO** SPMLDINFO: >**listspmload spm 1 4** SPM 1 : MG4K ATM Load Release SN07.3.1 SPM 2 is not datafilled. SPM 3 : DMSCP NA Load Release SN07.3.1 SPM 4 is not datafilled.
Command: MAP response:	SPMLDINFO; listspmload spm 1 >**SPMLDINFO** SPMLDINFO: >**listspmload spm 1** SPM 1 : MG4K ATM Load Release SN07.3.1

Table 7 shows the output of listspmload all command, when no SPMs are datafilled in the office.

Table 7 : Usage Examples for listspmload command.

Description of task:	Display the list of spectrum load releases running in each of the SPMs in the office.
Command: MAP response:	SPMLDINFO; listspmload all CI: **>SPMLDINFO** SPMLDINFO: **>listspmload all** No SPMs are datafilled in the office.

19.9.5 Command: QUIT

19.9.5.1 Command type: Non-Menu

19.9.5.2 Command target: All

19.9.5.3 Command availability: Res

19.9.5.4 Command description

QUIT command is used to quit from SPMLDINFO directory**.**

19.9.5.5 Command syntax

The command syntax is as shown in Figure 5.

Figure 5 : QUIT command syntax

```
SYNTAX : QUIT (from within SPMLDINFO directory)
Parms: None.

Parameter Description:

               : Not Applicable.
```

19.9.5.6 Qualifications and warnings

None.

19.9.5.7 Responses

When quit command is issued, SPMLDINFO directory is being exited. No warnings or messages are displayed.

19.9.5.8 Example

Table 8 shows the output of quit command.

Table 8 Usage examples for quit command

Description of task:	Quit from SPMLDINFO directory
Command: MAP response:	quit **>SPMLDINFO** SPMLDINFO: **>quit** CI: >

19.9.6 Command: mapci;mtc;pm;post spm <n>; querypm <option>

19.9.6.1 Command type: Menu

19.9.6.2 Command target: All

19.9.6.3 Command availability: Res

19.9.6.4 Command description

The command **querypm** is used to list information about loads running in the devices of a SPM and to list the faults present in the devices. It has 2 optional parameters ‘files’ and ‘flt’ to list different information as mentioned above. Querypm files displays the spectrum load release running on DMSCP class of SPMs only. This feature enhances ‘**querypm files**’ to display the spectrum load release running on a any class of SPM.

19.9.6.5 Command syntax

The command syntax is as shown in Figure 6.

Figure 6 : QueryPM files command syntax

```
SYNTAX : mapci;mtc;pm;post spm <n>;querypm {<files> or <flt>}
Parms: <files> or <flt>

Parameter Description:

              : Enter <files> to get information about the load files
                running on the SPM.
                Enter <flt> to get the faults in the devices.
```

The following sections explain only the ‘files’ option of querypm since this feature does not change ‘flt’ option.

19.9.6.6 Qualifications and warnings

No new warnings or qualifications.

19.9.6.7 Responses

With the new enhancement, ‘querypm files’ command displays the running spectrum load release name for the posted SPM irrespective of the variant type. If the posted SPM is MG4K ATM product and the device loads of that SPM do not match with any of the load release lineups datafilled for which the product type is MG4AT in table SPMLDVAL, then the following message is displayed.

Running MG4K ATM Load Release : Load Lineup of this SPM does not match with any of the load releases datafilled in table SPMLDVAL.

If the CEMs/RMs of an SPM are out of service such that the running loads in each of the devices cannot be determined, then it will display the following warning message.

Running MG4K ATM Load Release : Unable to contact the devices. The requested data cannot be retrieved.

19.9.6.8 Example

Table 9 shows the changed output of querypm files command.

Table 9 Usage examples for querypm files command

Description of task:	Display the spectrum load release name running in the SPM in context.

Table 9 Usage examples for querypm files command

Command: MAP response:	mapci; mtc; pm; post spm 1; querypm files **>mapci nodisp; mtc; pm; post spm 1** SPM: SPM 1 ISTb ATM 0 InSv Act Default Loadname: ATC20AJ Default Filename: ATC20AJ_010009 Running Load: ATC20AJ_010009 Load in Flash: ATC20AJ_010009 ... ... DSP 3 InSv Act Default Loadname: DSP20AJ Default Filename: DSP20AJ_010009 Running Load: DSP20AJ_010009 Load in Flash: DSP20AJ_010009 Running MG4K ATM Load Release : SN07.3.1
Command: MAP response:	mapci;mtc;pm;post spm 4;querypm files **>mapci nodisp; mtc; pm; post spm 4** SPM: **>querypm files** SPM 4 ISTb ATM 0 InSv Act Default Loadname: ATC20AJ Default Filename: ATC20AJ_010009 Running Load: ATC20AJ_010009 Load in Flash: ATC20AJ_010009 ... ... DSP 3 InSv Act Default Loadname: DSP20AJ Default Filename: DSP20AJ_010009 Running Load: DSP20AJ_010009 Load in Flash: DSP20AJ_010009 Running MG4K ATM Load Release : Load Lineup of this SPM does not match with any of the load releases datafilled in table SPMLDVAL.

If the CEMs/RMs of an SPM are out of service such that the running loads in each of the devices cannot be determined, then it will display a warning message. Table 10 shows the output of QueryPM Files command when all the CEMs/RMs are out of service.

Table 10 : Usage examples for QueryPM files command.

Command:	mapci;mtc;pm;post spm 5; querypm files
MAP response:	**>mapci nodisp; mtc; pm; post spm 5** SPM: **>querypm files** SPM 5 SysB CEM 0 SysB Act Default Loadname: CEM17BC Default Filename: CEM17BC_010028 Running Load: Unable to contact CEM Load in Flash: Unable to contact CEM CEM 1 SysB InAct Default Loadname: CEM17BC Default Filename: CEM17BC_010028 Running Load: Unable to contact CEM Load in Flash: Unable to contact CEM .... DSP 0 CBsy Act Default Loadname: DSP17BC Default Filename: DSP17BC_010028 Running Load: Invalid host node status Load in Flash: Invalid host node status DSP 1 CBsy InAct Default Loadname: DSP17BC Default Filename: DSP17BC_010028 Running Load: Invalid host node status Load in Flash: Invalid host node status Running DMSCP NA Load Release : Unable to contact the devices. The requested data cannot be retrieved.

19.10 Security

Not Applicable.

19.11 Configuration Walkthrough

Not Applicable.

20: Configuration (CN): A00002858

20.1 Hardware and Software Requirements

This feature requires the following features to function:

- A00002607 - ABI XPM SITE and MG9K Location support.
- A00002146 - MAPCI ABI Link Test & Legacy Comparison.

20.2 Initial Configuration

An ABI XPM must be datafilled to observe the new functionality provided via the QUERYPM command at the PM level(s) of the MAP.

20.3 Command interface changes

20.3.1 QUERYPM MAPCI command

The QUERYPM command is used to query miscellaneous information about the currently posted XPM at the PM level of the MAP. This feature modifies the legacy QUERYPM command as follows:

1. Add additional screen output to the default QUERYPM command (without arguments) which reflects SITE, ABI slot, and network element number information. New output only occurs if the posted XPM is an ABI XPM.
2. Add an additional option to the QUERYPM command, ABICONN, which is used to trigger a looparound message at the ABI XPM for verifying connectivity between the CM and XPM.

20.3.1.1 Legacy QUERYPM

Figure 1 on page 2607 displays the legacy version of the QUERYPM command and options.

Figure 2 on page 2607 displays the legacy output of the QUERYPM command without arguments.

Figure 1 Legacy MAPCI help QUERYPM command.

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 ETHR     .       .      LOAD    1 SPM  1   RS    .      10C.R    .       .
   M                             *C*     *C*             *C*
                                 SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit          PM               2       2      11       1      10      20
  2 Post_         LGC              0       0       1       0       1       1
  3 ListSet
  4            LGC     0 InSv  Links_OOS: CSide  0 , PSide  0
  5 Trnsl_     Unit0:   Act   InSv
  6 Tst_       Unit1:   Inact InSv
  7 Bsy_       help querypm
  8 RTS_       QUERYPM: QUERY MISC INFO ABOUT THE PM
  9 OffL       Parms: [<OPTION> {FLT,
 10 LoadPM_                     CNTRS,
 11 Disp_                       FILES,
 12 Next                        CONFIG,
 13 SwAct                       DIAGHIST [<OPTHIST> {DIAG,
 14 QueryPM                                          CARD,
 15 DCH                                              RESET}]}]
 16
 17 PERFORM
 18 ISG
   Nortel
```

Figure 2 Legacy MAPCI QUERYPM command.

```
 XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
ETHR      .       .      LOAD    1 SPM  1   RS    .      10C.R    .       .
  M                             *C*     *C*             *C*
                                SysB    ManB    OffL    CBsy    ISTb    InSv
 0 Quit          PM               2       2      11       1      10      20
 2 Post_         LGC              0       0       1       0       1       1
 3 ListSet
 4            LGC     0 InSv  Links_OOS: CSide  0 , PSide  0
 5 Trnsl_     Unit0:   Act   InSv
 6 Tst_       Unit1:   Inact InSv
 7 Bsy_       querypm
 8 RTS_       PM Type: LGC  PM No.: 0  PM Int. No.: 0  Node_No.: 67
 9 OffL       PMs Equipped: 46  Loadname: QLI19BE  EEPRom Load: SXFWAJ01
10 LoadPM_    Warning! Unit 0 is missing patches
11 Disp_      Warning! Unit 1 is missing patches
12 Next       WARM SWACT is supported and available.
13 SwAct      LGC 0 is included in the REX schedule.
14 QueryPM    REX on LGC 0 has not been performed.
15 DCH        Node Status: {OK, FALSE}
16            Unit 0   Act, Status: {OK, FALSE}  ,MtcArb functional
17 PERFORM    Unit 1 Inact, Status: {OK, FALSE}  ,MtcArb functional
18 ISG         Site Flr RPos  Bay_id   Shf  Description    Slot     EqPEC
  Nortel       HOST  01  C31  LTEI 000  04  LGC : 000              6X02NA
```

20.3.1.2 New QUERYPM

20.3.1.2.1 New QUERYPM - HELP OUTPUT

Figure 4 on page 2608 reflects the new ouput when a “help querypm” is input at the MAP. Note the new ABICONN option.

Figure 3 New QUERYPM Help Output

```
help querypm
QUERYPM: QUERY MISC INFO ABOUT THE PM
Parms: [<OPTION> {FLT,
                  CNTRS,
                  FILES,
                  CONFIG,
                  DIAGHIST [<OPTHIST> {DIAG,
                                       CARD,
                                       RESET}],
                  ABICONN}]
```

20.3.1.2.2 New QUERYPM without options - INPUT

No additional input will be required by the craftsperson. The system will determine the output based on provisioning and display the information accordingly.

20.3.1.2.3 New QUERYPM without options - OUTPUT

Figure 4 on page 2608 illustrates the additional information output for an ABI XPM when no additional options are provided at the command prompt.

Figure 4 QueryPM (no options) output for ABI XPM

```
>querypm
PM Type: LGC  PM No.: 0  PM Int. No.: 0  Node_No.: 67
PMs Equipped: 47  Loadname: QLI19BE  EEPRom Load: SXFWAJ01
Unit 0 is patched
Unit 1 is patched
WARM SWACT is supported and available.
LGC 0 is included in the REX schedule.
Last REX date was SAT. 2003/06/21 at 02:20:34; PASSED.
Node Status: {OK, FALSE}
Unit 0   Act, Status: {OK, FALSE}  ,MtcArb functional
Unit 1 Inact, Status: {OK, FALSE}  ,MtcArb functional
 Site Flr RPos  Bay_id   Shf  Description   EqPEC
 CARY 01  CC02  LTEI 002 19   LGC : 001     6X02NA
 SITE ABISlots NE
 CARY 4:5      12
```

20.3.1.2.4 QUERYPM with ABICONN option - INPUT

Entering “QUERYPM ABICONN” at the MAP will attempt a looparound test at the ABI XPM. Information regarding the results will be displayed at the MAP. Please refer to “20.3.1.2.5 QUERYPM with ABICONN option - OUTPUT” on page 2609 for an overview of the possible results which are output at the MAP.

20.3.1.2.5 QUERYPM with ABICONN option - OUTPUT

There are a number of nodes in the path between the CM and ABI XPM which are necessary to perform the link looparound. If a failure occurs, the link looparound test will attempt to isolate the issue. Based on success or the point of failure, various messages will be output informing the end user of the status.

Table 1, “QUERYPM with ABICONN MAP outputs,” on page 2609 lists the possible messages output at the MAP when the QUERYPM command using the ABICONN option is input at the MAP. There should be a separate output for each of the messaging paths to the XPM.

Table 1 QUERYPM with ABICONN MAP outputs

QUERYPM ABICONN
Response: “Connectivity to XPM has been confirmed.” **Meaning:** A successful link looparound test was completed. The CM is communicating with the XPM. **System or user actions:** No actions are required.
Response: “Connectivity check via link # PASSED.” **Meaning:** Connectivity was verified over the specified link. **System or user actions:** None.

Table 1 QUERYPM with ABICONN MAP outputs

QUERYPM ABICONN
Response: “Connectivity check via link # FAILED.” **Meaning:** Connectivity over the specified link could not be verified, or the verification failed. **System or user actions:** Refer to the extra output when this occurs for troubleshooting steps if any.
Response: “Invalid link state for test.” **Meaning:** The connectivity tests were not run because of the state of the link. **System or user actions:** Retry the test when the links are in a valid state for test.
Response: “Querypm ABICONN has been aborted by higher priority mtc.” **Meaning:** The connectivity test was aborted because the resources were needed by higher priority maintenance. **System or user actions:** Retry the command later.
Response: ’Failed to maintenance open link.’ **Meaning:** The Mtc system was unable to open the link for test purposes. **System or user actions:** Retry the command later.

Table 1 QUERYPM with ABICONN MAP outputs

QUERYPM ABICONN
Response: 'Failed XPM messaging test.' **Meaning:** The XPM is not messaging properly. **System or user actions:** Troubleshoot the XPM for resolution of the issue.
Response: 'Check connectivity between the ABI and XPM.' **Meaning:** Communication between the ABI and XPM could not be verified. **System or user actions:** Troubleshoot communications between the ABI and XPM.
Response: 'Check connectivity between the GWC and ABI.' **Meaning:** Communication between the GWC and ABI could not be verified. **System or user actions:** Troubleshoot communications between the GWC and ABI.
Response: 'Check connectivity between the CM and GWC. ' **Meaning:** Communication between the CM and GWC could not be verified. **System or user actions:** Troubleshoot communications between the CM and GWC.
Response: 'Invalid response - spch #' **Meaning:** This is an invalid response to this test. **System or user actions:** Contact next level of support.

Table 1 QUERYPM with ABICONN MAP outputs

QUERYPM ABICONN
Response: 'MG9K reports VMG is OOS.' **Meaning:** The ABI is reporting the VMG is not INSV. **System or user actions:** Verify VMG status at the Element Manager.
Response: 'MG9K reports Node Mtc is not ready.' **Meaning:** The MG9K is not in a proper state to support the connectivity test. **System or user actions:** Verify the MG9K and ABI status at the Element Manager.
Response: 'MG9K reports HAL Alarms.' **Meaning:** The test is failing because of faults which are alarmed. **System or user actions:** Verify the ABI status at the Element Manager and clear any critical alarms.
Response: 'MG9K reports no Sync with XPM.' **Meaning:** Clock sync between the XPM and ABI has not been achieved. **System or user actions:** Verify physical connectivity between the ABI and XPM.

21: Configuration (CN): A00002858

21.1 Hardware and Software Requirements

Just need SN07/20 release or later in the Core and SPMs.

21.2 Initial Configuration

At the CI prompt:

ENGWRITE ON

TABLE OFCENG

POS SPM_NODE_ISTB_FOR_CARRIER_OUTAGE

21.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Introducing OFCENG office parameter SPM_NODE_ISTB_FOR_CARRIER_OUTAGE in the CM.

21.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	SPM_NODE_ISTB_FOR_CARRIER_OUTAGE	NEW	CM

21.3.2 Parameter information

21.3.2.1 SPM_NODE_ISTB_FOR_CARRIER_OUTAGE

SPM Node ISTb under PM Map banner for carrier outage

21.3.2.1.1 Functional description

This parameter controls taking a SPM or STM-1 node ISTb under the PM Map banner whenever one of its carriers has an outage. The carrier outage can be 1) whenever any of the SPM's carriers goes SysB, or 2) whenever one of the SPM's line carriers (STS3L or STM1M) has a RFI (Remote Failure Indicator) alarm.

When the parameter is enabled (“Y”), any SPM carrier outage will cause an indicator under the PM banner that a SPM node has gone ISTb. When the parameter is disabled (“N”), carrier outages will never cause a SPM node to go ISTb.

The parameter is only supported on TDM Legacy nodes (SPM and STM-1), and has no impact on Succession nodes (MG4K, LSA, IW, STS-1).

21.3.2.1.2 Provisioning rules

21.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
N	Y	N It is strongly recommended that this parameter be enabled (“Y”) so the telco craftperson will be alerted at the Map to any carrier outages that can disrupt service.

21.3.2.1.4 Activation

Activation is immediate; no restart or manual action is required.

When the parameter is changed to “Y” to enable the feature, these warning messages will be seen:

WARNING: If pre-20 Local loads are running on Legacy SPM/STM

while this parm is YES, then carrier outages may occur.

WARNING: Activation takes up to 45 minutes to complete.

The first warning insures that user does not enable the feature when the local software to support it is not available. For the feature to work when enabled, the Core and Local must be running version 20 or later. If the Local is running 19 or earlier, then carrier outages can occur when the feature is enabled.

The second warning indicates that it can take up to 45 minutes for the change to be propagated to every SPM node, and the current SPM carrier outage status reflected under the Map PM banner.

21.3.2.1.5 Dependencies

None

21.3.2.1.6 Consequences

N/A

21.3.2.1.7 Verification

The only way to test this parameter is working is to turn it on, cause an outage, and confirm the Map reflects the outage. Since service would be disrupted, this is not recommended.

21.3.2.1.8 Memory requirements

No memory impact.

21.3.2.1.9 Parameter release history update

Added SPM_NODE_ISTB_FOR_CARRIER_OUTAGE parameter to Table OFCENG to control taking SPM node ISTb in the MAP whenever one of the SPM carriers has an outage.

21.4 Upgrade Impact

21.4.1 Dump and Restore

No impact.

21.4.2 Element Management Upgrade

No impact.

21.5 Data schema (DS) (CM, MIBS, RDB)

No impact.

21.6 Service Orders (SO) (CM & SESM)

No impact.

21.7 Element Management

No impact.

21.8 Command interface changes

Two new ISTb reasons were added to the output of the existing QUERYPM FLT REASON command.

See the OPTFN section of this feature for good examples of how this command is used.

21.8.1 Directory: MAPCI;MTC;PM;POST SPM [spm#]

21.8.1.1 Directory description

PM is an existing MAP level.

21.8.1.2 Accessing directory: MAPCI;MTC;PM;POST SPM [spm#]

21.8.1.2.1 Access to directory or MAP level and return to CI

Example of how to access and quit the PM Map level for SPM 10:

mapci;mtc;pm;post spm 10

quit mapci

21.8.2 Command: QUERYPM FLT REASON

21.8.2.1 Command type: Listed MENU

21.8.2.2 Command target: All

21.8.2.3 Command availability: RES

21.8.2.4 Command description

The QUERYPM FLT REASON will show the reason an SPM is in the ISTb or SysB state. This feature adds the following new ISTb reasons:

Check SysB Carrier - non-critical fault that indicates the OC3 (or STM) RM has a carrier in the SysB state.

Check RFI Alarm on STS3L Carrier - non-critical fault that indicates the STS3L carrier on the OC3 (which OC3 specified below) has a RFI alarm.

Check Carrier on OC3 RM - non-critical fault that indicates a carrier on this OC3 has one of the two faults listed above.

21.8.2.5 Command syntax

Table 3 QUERYPM command parameters and variables

Command	Parameters and variables
QUERYPM	existing
Parameters and variables	Description
FLT REASON	existing

21.8.2.6 Qualifications and warnings

None

21.8.2.7 Responses

There are two possible new responses for the QUERYPM FLT REASON command. Each is a status message visible on “All” systems.

21.8.2.7.1 Check SysB Carrier

>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check SysB Carrier
CEM 0 ISTb NonCritical faults:
Check Carrier on OC3 RM

If this is the international STM-1 product, substitute “OC3” above with “STM”.

This ISTb status output indicates that one of the carriers on the OC3 (or STM) is in a SysB state.

21.8.2.7.2 Check RFI Alarm on STS3L Carrier

>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check RFI Alarm on STS3L Carrier
CEM 0 ISTb NonCritical faults:
Check Carrier on OC3 RM

If this is the international STM-1 product, substitute “OC3” above with “STM” and “STS3L” with “STM1M”.

This ISTb status output indicates that one of the STS3L (or STM1M) carriers on the OC3 (or STM) has an RFI (Remote Fault Indicator) alarm.

Table 4 MAP outputs with associated meanings and actions

Command: QUERYPM FLT REASON
RESPONSE: Check SysB Carrier **Meaning:** one of the carriers on the OC3 has gone SysB. **System or user actions:** see Troubleshooting chapter of the OPTFN section.
RESPONSE: Check RFI Alarm on STS3L Carrier **Meaning:** one of the STS3L carriers on the OC3 has an RFI alarm. **System or user actions:** see Troubleshooting chapter of the OPTFN section.

21.8.2.8 Example

See OPTFN section of this feature for examples of each scenario when these new responses can occur, and what the telco response should be in each case.

21.9 Security

No impact.

21.10 Configuration Walkthrough

Other than upgrading to the new SN07/20 release, no further action is required to provision this feature. The new SPM_NODE_ISTB_FOR_CARRIER_OUTAGE office parameter will be “on” by default, so this feature will start working right away.

22: Configuration (CN): A00002900

22.1 Hardware and Software Requirements

N/A.

22.2 Initial Configuration

N/A.

22.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

22.4 Upgrade Impact

N/A.

22.5 Data schema (DS) (CM, MIBS, RDB)

22.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	Unchanged

22.5.2 Table/MIB/Remote Database Schema information

22.5.2.1 Name: SERVINFO

22.5.2.1.1 Functional description

Option INITDP_PARMS of table SERVINFO is extended to add two new fields **IP_AVA** and **IPSSP_CAP** to indicate whether parameters IPAvailable and IPSSPCapabilities will be carried in IDP. These two fields should be datafilled at the same time.

Meanwhile, option SRF_INFO is extended to add new filed **IP_INFO** to provide detailed information of the IP capability within SSP.

If IP_AVA and IPSSP_CAP are datafilled and IP_INFO is not datafilled, parameters iPAvailable and iPSSPCapabilities are set to default value according to China INAP, the default value of iPAvailable is ‘01’H (which indicates that the IP is available), the default value of iPSSPCapabilities is ‘#0C00’ (which indicates that DTMF digit collection and tone & announcement is supported). If IP_INFO is datafilled, then iPAvailable and iPSSPCapabilities are set according to this datafill. That means IP_INFO will take effect only if IP_AVA and IPSSP_CAP are datafilled, otherwise, the information of this datafill will not be carried in IDP.

IP_INFO contains two subfields: **IP_AVA** and **IP_SSP_CAPABILITIES**, which are for parameter IPAvailable and IPSSPCapabilities respectively.

22.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

22.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	no change	no change	N/A

22.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INITDP_PARMS	Changed	refinement	Boolean Value	Add new selections: IP_AVA and IPSSP_CAP.
SRF_INFO	Changed	refinement	Boolean Value	Add new sub-option: IP_INFO
IP_INFO	New	Subfield	Boolean Value	Add new sub-options: IP_AVA and IP_SSP_CAPABILITIES
IP_AVA	New	Subfield	Boolean Value	Indicate whether the IP is available.
IP_SSP_CAPABILITIES	New	Subfiled	Boolean	Provide the detailed information of IP capabilities. (See table 4 for details)

According to China INAP, there are 14 kinds of IP capabilities which are indicated by parameter iPSSPCapabilities. These capabilities can be datafilled in IP_SSP_CAPABILITIES as shown in table 4:

Table 4 IP Capabilities defined in China INAP

IPSSPCapabilites parameter	Value	Meaning	IPSSP_CAPABILITIES selections
1st byte, bit 0	0/1	Not support/Support IPRoutingAddress	IPRA
1st byte, bit 1	0/1	Not support/Support VoiceBack	VOICE_BACK
1st byte, bit 2	0/1	Not support/Support VoiceInformation, recognize through voice, speech.	VOICE_INFO_SPEECH
1st byte, bit 3	0/1	Not support/Support VoiceInformation, recognize through voice, voice.	VOICE_INFO_VOICE
1st byte, bit 4	0/1	Not support /SupportText to Voice conversion.	TEXT_TO_VOICE
1st byte, bit 5	0/1	Not support/Support fax.	FAX
1st byte, bit 6	0/1	Not support/Support recorder.	RECORDER
1st byte, bit 7	0/1	Not support/Support script.	SCRIPT
2nd byte, bit 0	0/1	Not support/Support manual operator.	MAN_OPERATOR
2nd byte, bit 1	0/1	Not support/Support conference.	CONFERENCE
2nd byte, bit 2	0/1	Not support/Support tone & announcement.	TONE_ANNC
2nd byte, bit 3	0/1	Not support/Support DTMF digit collection.	DTMF_DIGCOL
2nd byte, bit 4	0/1	Not support/Support sending DTMF signal.	SEND_DTMF_SIG
2nd byte, bit 5	0/1	Not support/Support sending FSK signal.	SEND_FSK_SIG
2nd byte, bit 6,7	To be defined.		
3rd, 4th bytes	To be defined.		

22.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVINFO:

Example of datafill:
TABLE SERVINFO
200 (INITDP_PARMS (SERVKEY) (CDPA)(**IP_AVA**) (**IPSSP_CAP**) $)
(SRF_INFO (EARLY_ANS ANS_ON_ANNS)
(**IP_INFO Y** (**IPRA**) (**VOICE_INFO_SPEECH**)
(**TONE_ANNC**)(**DTMF_DIGCOL**)$)$)$

22.5.2.1.6 Table release history update

New sub-option IP_AVA, IPSSP_CAP are added to option INITDP_PARMS. New sub-option IP_INFO is added to SRF_INFO and new option IP_INFO has 2 sub-options: IP_AVA and IP_SSP_CAPABILITIES.

22.5.2.1.7 Supplementary information

N/A.

22.5.2.1.8 Translation verification other tools

N/A.

22.6 Service Orders (SO) (CM & SESM)

N/A.

22.7 Software optionality control (SOC)

N/A.

22.8 Element Management

N/A.

22.9 Command interface changes

N/A.

22.10 Security

N/A.

22.11 Configuration Walkthrough

N/A.

23: Configuration (CN): A00002901

23.1 Hardware and Software Requirements

23.2 Initial Configuration

23.3 Office/Subnet parameters (OP/SP) (CM & SESM)

23.4 Upgrade Impact

23.5 Data schema (DS) (CM, MIBS, RDB)

23.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
EMMCDATA	NEW	NEW

23.5.2 Table/MIB/Remote Database Schema information

23.5.2.1 Name: EMMCDATA

23.5.2.1.1 Functional description

This table is used for Enhanced Meet-Me Conference provisioning.

23.5.2.1.2 Usage sequence and implications (CM Only)

N/A.

23.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
EMMCDATA	0	8192	

23.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for EMMCDATA.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LKEY	New		see subfields	EMMC table Key, this field consists of subfields SNPA, OFCCODE and STNCODE
		SNPA	serving_numbering_plan_area	area code of a DN
		OFCCODE	ofccode_digit_register	office code of a DN
		STNCODE	stncode_digit_register	station code of a DN
RESERVE	New		see subfields	The reservation type of the conference: timeless or schedule.
		RESERVED	SCHEDULE or TIMELESS	Selector. If the conference is reserved for the user to have a conference at any time, then enter TIMELESS and datafill no refinement is this field. If the conference is reserved for the user to have conference only at specific time, then enter SCHEDULE and datafill refinements SCHEDULE, STARTDAT, STARTTIM and ELAPSED.
SIZE	New	N/A.	numeric {3 TO 30}	Conference size. Specify the maximum allowed conferees in this confernece.
CHAIPSWD	New	N/A.	6 digits code	Chair-person's password. Enter the 6 digit length password.
PARTPSWD	New	N/A.	6 digits code	Invited Participant's password. Enter the 6 digit length password. This password can not be the same as the one of chair-person's.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
QUICKST	New	N/A.	Y or N (boolean)	Quick Start option. If the conference can start without the chair-person, enter Y. With this datafill, all participants enter before the chair-person will be placed on hold. If the conference must start with the chair-person entering, then enter N.
GREETING	New	N/A.	alphanumeric {a maximum of 16 characters}	Enter the CLLI name of the announcement defined for the greeting of this conference.
AUDIOGRP	New	N/A.	audio group	Enter the audio group name of the music which will be played while an invited participant is to be held.
ENDALARM	New	N/A.	{1 TO 10}	numeric range
CONTINUE	New	N/A.	Y or N (boolean)	Continue option. Enter Y if the confernece can continue after the chair-person leaves. If the conference should drop after the chair-person leaves, Enter N.
BILLING	New	N/A.	Y or N (boolean)	Billing option. Enter Y for generating conference specific AMA log. Enter N for no specific AMA log generation.

RESERVED = SCHEDULE

If the entry in subfield is SCHEDULE, datafill refinement as described below.

Table 4 Table field descriptionswhen RESERVED = SCHEDULE

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
		SCHEDULE	DAILY, WEEKLY, MONTHLY or NONPERIOD	Scheduled type of the conference. This field denotes the scheduled type of the conference being reserved. If the conference is reserved to be used during a specific time for each day, enter DAILY. If the conference is reserved to be used during a specific time and is able to be used on one day of each week, enter WEEKLY. If the conference is reserved to be used during a specific time and and is able to be used on one day of each month, enter MONTHLY. If the conference is reserved to be used during a specific time and is only for once, enter NONPERIOD.
		STARTDAT	yyyymmdd	Conference start date. Enter the start date of this conference (year, month and day).
		STARTTIM	hhmm	Conference start time. Enter the start time of this conference (hours and minutes).
		ELAPSED	1 to 9999	Conference elasped time. Enter the predefined elasped time of this conference (in minutes).

23.5.2.1.5 Datafill example

The following example shows sample datafill for table EMMCDATA.

```
TABLE: EMMCDATA
LKEY RESERVE SIZE CHRPSWD PARTPSWD QUICK GREETING AUDIOGRP ENDALARM CONTINUE
BILLING
---------------------------------------------------------------------
131 830 1000 SCHEDULE NONPERIOD 20030810 0930 60 6 111111 222222 Y EMMCOMPA AUDIO10 5
Y N
131 801 5555 TIMELESS 10 111111 222222 N EMMCOMPB AUDIO10 0 Y Y
131 830 2000 SCHEDULE DAILY 20030810 1130 60 6 111111 222222 Y EMMCOMPA AUDIO10 5 Y Y
```

23.5.2.1.6 Table release history update

New table EMMCDATA is added.

23.5.2.1.7 Supplementary information

N/A.

23.5.2.1.8 Translation verification other tools

N/A.

24: Configuration (CN): A00002960

24.1 Hardware and Software Requirements

In order to perform originator identification screening SOC UTRS0011 must be ON and the terminating ISUP EANT trunk must have ORIGIDSCR assigned in Table TRKOPTS.

24.2 Initial Configuration

This feature only impacts calls that terminate on ISUP EANT trunk.

24.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

24.4 Upgrade Impact

24.4.1 Dump and Restore

No special steps are required.

24.4.2 Element Management Upgrade

N/A

24.5 Data schema (DS) (CM, MIBS, RDB)

24.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	Changed	New

24.5.2 Table/MIB/Remote Database Schema information

24.5.2.1 Name: TRKOPTS

TRunK OPTionS

24.5.2.1.1 Functional description

A new trunk group option, ORIGIDSCR, is introduced in Table TRKOPTS for ISUP EANT trunks only. This allows the customer to specify which ISUP EANT trunks perform originator identification screening introduced by this feature.

24.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

24.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	0	131072	Dynamically Allocated

24.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for TRKOPTS impacted by this feature.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	Refinement	ORIGIDSCR refinement is added	New option is ORIGinator IDentificaton SCreening.

24.5.2.1.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

Figure 1 Table TRKOPTS Examples

TABLE: TRKOPTS

TRK1 ORIGIDSCR ORIGIDSCR

When an attempt to add ORIGIDSCR to a trunk other than EANT type or an MF EANT trunk the following error message is generated by table control:
TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can only be assigned to EANT ISUP trunks.

When an attempt to add ORIGIDSCR to an incoming trunk the following error message is generated by table control:
TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can not be assigned to Incoming trunks.

24.5.2.1.6 Table release history update

Added option ORIIDSCR option for ISUP EANT trunks. This allows the customer to specify which ISUP EANT trunks perform originator identification screening.

24.5.2.1.7 Supplementary information

None

24.5.2.1.8 Translation verification other tools

Table TRKOPTS is not diplayed in TRAVER.

24.6 Service Orders (SO) (CM & SESM)

N/A

24.7 Software optionality control (SOC)

Table 4 SOC

SOC option name:	UCS ORIG ID SCREEN
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes

Table 4 SOC

SOC option order code	UTRS0011
Option defined in DRU:	UCS
Affected products:	SN07

24.8 Element Management

N/A

24.9 Command interface changes

N/A

24.10 Security

N/A

24.11 Configuration Walkthrough

In order to perform originator identification screening SOC UTRS0011 must be ON and the terminating ISUP EANT trunk must have ORIGIDSCR assigned in Table TRKOPTS.

25: Configuration (CN): A00002970

25.1 Hardware and Software Requirements

25.1.1 Hardware Requirements

None.

25.1.2 Software Requirements

None.

25.2 Initial Configuration

None.

25.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

25.4 Upgrade Impact

25.4.1 Dump and Restore

Over ONP from SN06 and previous releases, the new field ‘SITE’ in Table MNNODE(for SMG4s only), is defaulted to 'HOST'.

25.4.2 Element Management Upgrade

Not Applicable.

25.5 Data schema (DS) (CM, MIBS, RDB)

25.5.1 New/modified tables, MIBs, or Database Schema

Table 1 lists the Tables being modified as a result of this feature:

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Table MNNODE	CHANGED	UNCHANGED

25.5.2 Table Information

25.5.2.1 Name: MNNODE

25.5.2.1.1 Functional description

The Table control changes in the Table ‘MNNODE’ would consist of introducing a new inservice editable field, ‘*site’*.

25.5.2.1.2 Fields

Table 2 lists the fields for table MNNODE which are added/changed as part of this activity:

Table 2 Table field description

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SITE	New	Not Applicable	Not Applicable	This field is used to indicate the site location where the SMG4 is located. This is introduced only for SMG4 class of SPM nodes and can be datafilled only by the site names that are provisioned in Table SITE.

25.5.2.1.3 Datafill example

Figure 1 shows the sample datafill for table MNNODE, depicting that the ‘site’ field has been referenced from Table SITE :

Figure 1 Table MNNODE tuple - Existing and Desired.

MNNODE Tuple prior to this feature:-

```
SPM 4 SPM_4 SMG4 0  SYNC LINE 50 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60) (MF
60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)  (MANBNA MJ
RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (TONESLOW MN RPT) (MFLOW
MN RPT) (CMRLOW MN RPT) (SMG4CN MJ RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT)
(ST3EHLD MJ RPT) (ST3EHLD24 CR RPT) (SMCHLD MJ RPT) (SMCHLD24 CR RPT)
(SPMSRMNTD MN RPT) (LOCUR MJ RPT) (TMCFAIL CR RPT) $ $ N 0 $ N
```

MNNODE Tuple after the feature:-

```
SPM 4 SPM_4 SMG4 REM1 0  SYNC LINE 50 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)  (MANBNA MJ
RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (TONESLOW MN RPT) (MFLOW
MN RPT) (CMRLOW MN RPT) (SMG4CN MJ RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT)
(ST3EHLD MJ RPT) (ST3EHLD24 CR RPT) (SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMSRMNTD
MN RPT) (LOCUR MJ RPT) (TMCFAIL CR RPT) $ $ N 0 $ N
```

```
Table SITE tuples:

NAME LTDSN MODCOUNT OPVRCLLI ALMDATA
---------------------------------
HOST   0      1          VER90      $
REM1   1      0          RMMVER90   $
REM2   2      0          RMMVER90   $
REM3   3      0          RMMVER90   $
REM4   4      0          RMMVER90   $
```

25.5.2.1.4 New Error Messages

As a result of the feature enhancements, some new error messages are introduced which are described in Table 3.

Table 3 New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
1.	a. Tuple addition in Table MNNODE. b.Tuple modification('SITE' field) in Table MNNODE.	'SITE' field value not present in Table SITE. (Note : This is an error message already present in Table Control Command Interface.)
	TYPE OF SITE IS SITE_INDEX. **TYPE IS SITE_INDEX {<SITE VALUE 1>,<SITE VALUE2>,<SITE VALUE3>,...}**	

No.	Table Control operations	Pre - conditions
	Error Messages	
2	a. Change SITE name value for a particular tuple.	An SMG4 already provisioned at the changed site location and at the same floor, row, frame position and shelf position.
	The specified site, floor and shelf is already occupied. **See tuple SPM <no.>.**	
3	a. Deleting tuple from Table SITE.	The corresponding site is being referred to in Table MNNODE. (Note : This error message already exists in the Table Control Command Interface.)
	Error : Table MNNODE still references this tuple.	

25.5.2.1.5 Usage sequence and implications (CM Only)

The datafill order remains unchanged.

However, the addition of an SMG4 in a new site requires the data to be provisioned in Table SITE first (See FN-Section 2.9 for more details.)

25.5.2.1.6 Size
Not impacted

25.5.2.1.7 Table release history update
Not Applicable

25.5.2.1.8 Supplementary information
Not Applicable

25.5.2.1.9 Translation verification other tools
Not Applicable

25.6 Service Orders (SO) (CM & SESM)

Not Applicable.

25.7 Software optionality control (SOC)

Not Applicable.

25.8 Element Management

Not Applicable.

25.9 Command interface changes

Prior to this feature, the value for site was hardcoded to 'HOST' in the MAPs that displayed site name. This feature now picks up the site value from the corresponding data in Table MNNODE and displays it in the existing MAPs.

A snapshot of all the affected MAPs is shown in this section with modified displays. Also shown in Figure 2 is the related SMG4 tuple from the Table MNNODE.

Figure 2 An MNNODE tuple with SITE data

MNNODE Tuple for SMG4

```
SPM 60 SPM_60 SMG4 REM1 1 SYNC LINE 50 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)  (MANBNA MJ
RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (TONESLOW MN RPT) (MFLOW
MN RPT) (CMRLOW MN RPT) (SMG4CN MJ RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT)
(ST3EHLD MJ RPT) (ST3EHLD24 CR RPT) (SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMSRMNTD
MN RPT) (LOCUR MJ RPT) (TMCFAIL CR RPT) $ $ N 0 $ N
```

25.9.1 SPERFORM Level MAP display

Figure 3 SPERFORM Level MAP display

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
   .        .      DLOG E   16PSLk    4 SPM     .        .         ...      .     ATM_65
                                      *C*                                        *C*
 SPERFORM                             SysB     ManB     OffL     CBsy     ISTb     InSv
  0 Quit           PM                    0        0        1        0        6       24
  2 SPMAct         SPM                   0        0        0        0        5        9
  3 SPUSAGE
  4              SPM   60  ISTb  Loc: Site REM1 Floor  1 Row B  FrPos 14
  5              LOAD NAME : MG419BR
  6              STATUS:              REASON:               LOGS:     TIME:
  7
  8
  9 PFQuery
 10              SPERFORM:
 11
 12
 13
 14
 15 OMInfo
 16
 17
 18
   USER1
 Time  05:27  >
```

25.9.2 Carrier Level Map Display

Figure 4 Carrier Level MAP Display.

```
C      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
  .       .     DLOG E  16PSLk   4 SPM     .       .       ...     .    ATM_65
                                 *C*                                    *C*
 POST         CLASS    ML   OS ALRM  SYSB  MANB UNEQ OFFL  CBSY PBSY  INSV
 0 Quit       TRUNKS   84    0    0     0     0    0    8     0    0   840
 2 Post_      HSCARR    6    0    0     0     0    0   16     0    0   872
 3             OC3S
 4            N  CLASS  SITE SPM RM OC3S CKT STATE  TR MA
 5 Loop_      0  HSCARR REM1 60  0    0   1 INSV   .. ..
 6 Tst_       1  HSCARR REM1 60  1    0   2 INSV   .S ..
 7 Bsy_       2  HSCARR REM1 60  0    0 176 INSV   .. ..
 8 RTS_       3  HSCARR REM1 60  1    0 177 INSV   .S C.
 9 Offl_
10            SIZE OF POSTED SET  :  180                    MORE...
11 Disp_      POST:
12 Next
13
14 Detail_
15 ListAlm_
16
17 Perfmon_
18
   USER1
Time 05:50 >
```

25.9.3 Querypm Command Output

Figure 5 Query PM Command output display

```
C      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
  .       .     DLOG E  16PSLk   4 SPM     .       .       1E..    .    ATM_65
                                 *C*                                    *C*
 SPM                             SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit        PM                 0       0       1       0       6      24
  2 Post_       SPM                0       0       0       0       5       9
  3 ListSet
  4 ListRes   SPM   60  ISTb  Class: SMG4
  5 Trnsl
  6          Shlf0 SL A Stat  Shlf0 SL A Stat  Shlf1 SL A Stat  Shlf1 SL A Stat
  7 ATMConn ATM 0  1 A InSv  CEM 1  8 A ISTb  DLC 0  1 I InSv  -----  8 - ----
  8          ATM 1  2 I InSv  OC3 0  9 A InSv  -----  2 - ----  DSP 3  9 A InSv
  9 OfClk     VSP0  3 A InSv  OC3 1 10 I InSv  DSP 1  3 A InSv  DSP 4 10 I InSv
 10           VSP 1  4 A InSv  VSP 2 11 A InSv  DSP 2  4 A InSv  DSP 0 11 A InSv
 11 Disp_     ----- 5 - ----  VSP 3 12 A InSv  VSP 6  5 A InSv  ----- 12 - ----
 12 Next      ----- 6 - ----  VSP 4 13 A InSv  VSP 7  6 A InSv  ----- 13 - ----
 13 Select_   CEM 0 7 I ISTb  VSP 5 14 A InSv  DLC 1  7 A InSv  VSP 8 14 I InSv
 14 QueryPM   QueryPM
 15 ListAlm   SPM 60 ISTb        Location: Site REM1 Floor  1
 16 Clock     ATM  0 InSv Act    Loc: Row B  FrPos 13 ShPos  7 ShId 0 Slot  1
 17 SPERFORM ATM  1 InSv InAct  Loc: Row B  FrPos 13 ShPos  7 ShId 0 Slot  2
 18 Upgrade_ VSP  0 InSv Act    Loc: Row B  FrPos 13 ShPos  7 ShId 0 Slot  3
    USER1    VSP  1 InSv Act    Loc: Row B  FrPos 13 ShPos  7 ShId 0 Slot  4
 Time  06:00  MORE...
```

25.9.4 CktLoc Command Output

Figure 6 CktLoc Command Output

```
C       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
   .        .      DLOG E  16PSLk    4 SPM      .       .        1E..      .     ATM_65
                                      *C*                                        *C*
 TTP
  0 QUIT       POST  1511  DELQ             BSYQ          DIG
  2 Post_      TTP  6-0007
  3 SEIZE      CKT TYPE      PM NO.          COM LANG      STA S R  DOT TE  RESULT
  4            2W S7 S7 SPM  60   9  1 MG4K60SS7IT2W   1 IDL
  5 BSY                                                        R
  6 RTS
  7 TST
  8
  9 CktInfo
 10 CktLoc
 11 Hold       CktLoc
 12 NEXT        Site Flr RPos  Bay_id   Shf  Description    Slot     EqPEC
 13 RLS         REM1 01  B13   SMGE  1    00  SPM :  60      09       DS1SIG
 14 Ckt_       CKT   RPAD    TPAD     MNL   IANL    EML     PBAL     LOOP   CRES
 15 TrnslVf_         (DB)    (DB)    (DBRM) (DBRM)  (DB)
 16 StkSdr_    9     0.00    0.00     50     50     0.0      --       --     --
 17 Pads
 18 Level_
    USER1
 Time  06:57  >
```

25.9.5 SPMREG CI Tool

Figure 7 SPMREG CI Tool Output

```
CI:
>spmreg
SPMREG:
>dispnode spm 60
 Node record for SPM 60:
-----------------------------------------------------
Alias:  SPM_60
Location: Site - REM1
          Floor- 1

-----------------------------------------------------
NNT Node Name   : SPM60U0
IOUI Node Number: 60
GRID:             SPM 60
Load name given:  N
Loc. info given:  N
Service FTA:     4268 1000

            Unit 0                    Unit 1
            ------                    ------
CPID:    125 60 1 0                125 60 1 1
FTS PC:       0022                    0023
FTA:     4266 1000                 4267 1000
DDM Index:    0012
```

25.10 Security

Not Applicable.

25.11 Configuration Walkthrough

Not Applicable.

25.12 Glossary

Term	Description
SPM	Spectrum Peripheral Module
SMG4	Succession Multiservice Gateway 4000
CS2K	Call server 2000

25.13 Appendix

25.13.1 Table SITE Description

```
Table SITE tuples:

NAME LTDSN MODCOUNT OPVRCLLI ALMDATA
-------------------------------------
HOST    0      1          VER90      $
REM1    1      0          RMMVER90   $
REM2    2      0          RMMVER90   $
REM3    3      0          RMMVER90   $
REM4    4      0          RMMVER90   $
```

Table 26 Table SITE field description

S.No.	Field Name	Description
1.	Name	Site Name
2.	LTDSN	Site Index(Unique integer representing SITE.)
3.	MODCOUNT	A count of the number of modules on that site.
4.	OPVRCLLI	CLLI (Common Language Location Identifier) for operator verification at that site.

Table 26 Table SITE field description

S.No.	Field Name	Description
5.	ALMDATA	Descriptions of the alarm points at that site.

26: Configuration (CN): A00002979

26.1 Hardware and Software Requirements

N/A

26.2 Initial Configuration

N/A

26.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

26.4 Upgrade Impact

N/A

26.5 Data schema (DS) (CM, MIBS, RDB)

N/A

26.6 Service Orders (SO) (CM & SESM)

N/A

26.7 Software optionality control (SOC)

N/A

26.8 Element Management

N/A

26.9 Command interface changes

26.9.1 Directory: PMUPGDIR

26.9.1.1 Directory description

The PMUPGRADE CI allows users to prepare and plan for the upgrade of peripherals in the office.

26.9.1.2 Accessing directory: PMUPGDIR

26.9.1.2.1 Access to directory or MAP level and return to CI

To access PMUPGDIR from the CI environment, enter >PMUPGRADE

To return to the CI environment, enter >quit

26.9.2 Command: SET

26.9.2.1 Command type: NON-MENU

26.9.2.2 Command target: All

26.9.2.3 Command availability: RES

26.9.2.4 Command description

The LOADDISTRIB and PATCHDISTRIB options of the SET command are extended to support electronic software delivery via FTP as described below.

A complete description of the SET command can be found in the "Commands" subsection of the "Overview of automated update process" section of the following NTP:

North American DMS-100 Peripheral Module Software Release Document, NTP 297-2663-599

26.9.2.5 Command syntax

Table 1 SET command parameters and variables

Command	**Parameters and variables**
SET	<Set options> <new values>
Parameters and variables	**Description**
<Set options>	LOADDISTRIB: The source of the load files to be copied. PATCHDISTRIB: The source of the patch files to be copied.
<new values>	ftp://<SDM_IP_address><directory_location>

26.9.2.6 Qualifications and warnings

None.

26.9.2.7 Responses

The LOADDISTRIB and PATCHDISTRIB options of the SET command will allow the crafts person to specify remote FTP volumes as PM load and patch distribution volumes.

The name of a **remote FTP volume** looks like:

```
ftp://<SDM_IP_address><directory_location>
```

where **<SDM_IP_address>** designates the IP address of the SDM containing the PM upgrade files to be copied, and **<directory_location>** designates where on the SDM the PM upgrade files are stored.

26.9.2.7.1 SET LOADDISTRIB and PATCHDISTRIB

Table 2 MAP outputs with associated meanings and actions

Command
>SET LOADDISTRIB 'ftp://<SDM_IP_address_1><directory_location_1>' The current PMUPGRADE settings are: **Load File Distribution: ftp://<SDM_IP_address_1><directory_location_1>** Load File Destination: S00DPMLOADS **Patch File Distribution: S00T** ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads: **>SET PATCHDISTRIB 'ftp://<SDM_IP_address_2><directory_location_2>'** The current PMUPGRADE settings are: **Load File Distribution: ftp://<SDM_IP_address_1><directory_location_1>** Load File Destination: S00DPMLOADS **Patch File Distribution: ftp://<SDM_IP_address_2><directory_location_2>** ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads: **Meaning:** The crafts person has requested PMUPGRADE to set the load distribution volume and patch distribution volume to be remote FTP volumes. **System or user actions:** PMUPGRADE sets the load distribution volume and patch distribution volume as requested, and displays the new settings. **Note**: Because of DMS command interpreter restrictions, the remote FTP volumes must be enclosed in single quotes as shown in the example above.

26.9.2.8 Example

Table 3 Usage examples for SET command

Description of task	The crafts person request PMUPGRADE to set the load distribution volume and patch distribution volume to be remote FTP volumes.

Table 3 Usage examples for SET command

Command: MAP response:	>**SET LOADDISTRIB 'ftp://10.1.2.3/NA08/pm-loads'** The current PMUPGRADE settings are: **Load File Distribution: ftp://10.1.2.3/NA08/pm-loads** Load File Destination: S00DPMLOADS **Patch File Distribution: S00T** ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads: >**SET PATCHDISTRIB 'ftp://10.1.2.3/NA08/pm-patches'** The current PMUPGRADE settings are: **Load File Distribution: ftp://10.1.2.3/NA08/pm-loads** Load File Destination: S00DPMLOADS **Patch File Distribution: ftp://10.1.2.3/NA08/pm-patches** ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads

26.9.3 Command: START

26.9.3.1 Command type: NON-MENU

26.9.3.2 Command target: All

26.9.3.3 Command availability: RES

26.9.3.4 Command description

The FILECOPY phase of the START command is extended to support electronic software delivery via FTP as described below.

A complete description of the START command can be found in the "Commands" subsection of the "Overview of automated update process" section of the following NTP:
North American DMS-100 Peripheral Module Software Release Document, NTP 297-2663-599

26.9.3.5 Command syntax

Table 4 START command parameters and variables

Command	Parameters and variables
START	<Start phases>
Parameters and variables	**Description**
<Start phases>	FILECOPY: Will copy load files and patches required to upgrade the peripherals on the switch.

26.9.3.6 Qualifications and warnings

None.

26.9.3.7 Responses

26.9.3.7.1 Remote FTP volume login

Table 5 MAP outputs with associated meanings and actions

Command
>START FILECOPY **Please enter the username and password for the remote FTP volume:** **ftp://<IP_address_1><directory_location_1>** **Username? <username_1>** **Password? <password_1>** **Please enter the username and password for the remote FTP volume:** **ftp://<IP_address_2><directory_location_2>** **Username? <username_2>** **Password? <password_2>** **Meaning:** The crafts person has requested PMUPGRADE to begin the FILECOPY phase of the PM upgrade process. The FILECOPY phase of the START command will allow the crafts person to copy PM load and patch files from remote FTP volumes to the destination volumes on the DMS switch. **System or user actions:** Because the load distribution volume and patch distribution volume are remote FTP volumes, PMUPGRADE prompts the crafts person to supply usernames and passwords. The crafts person enters the usernames and passwords for the remote FTP volumes. **Notes:** Up to two retries will be provided by PMUPGRADE for the username and password prompts in case the original supplied values are not valid.

26.9.3.8 Example

Table 6 Usage examples for START command

Description of task:	

Table 6 Usage examples for START command

Command: MAP response:	>START FILECOPY **Please enter the username and password for the remote FTP volume:** **ftp://10.1.2.3/NA08/pm-loads** **Username? nortel-esd** **Password? <password>** **Please enter the username and password for the remote FTP volume:** **ftp://10.1.2.3/NA08/pm-patches** **Username? nortel-esd** **Password? <password>**

26.10 Security

N/A

26.11 Configuration Walkthrough

N/A

27: Configuration (CN): A00003073

27.1 Hardware and Software Requirements

SimRing Deny Redirection feature requires Redirection Framework.

No new hardware is required.

27.2 Initial Configuration

Set existing redirection_framework office parm to Y.

```
TABLE: OFCVAR
PARMNAME PARMVAL
----------------
REDIRECTION_FRAMEWORK Y
```

27.3 Office/Subnet parameters (OP/SP) (CM & SESM)

No office parameter is added or modified by this feature.

27.4 Upgrade Impact

27.4.1 Dump and Restore

Reformat Procs will be written to deal with table KSETFEAT and IBNFEAT changes during ONP. The new added field (REDIRECTION) will have the default value of “ALLOWED”. This will ensure that the existing SimRing feature in the switch will work the same as before.

27.4.2 Element Management Upgrade

N/A

27.5 Data schema (DS) (CM, MIBS, RDB)

27.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IBNFEAT	changed	unchanged
KSETFEAT	changed	unchanged

27.5.2 Table/MIB/Remote Database Schema information

27.5.2.1 Name: IBNFEAT

27.5.2.1.1 Functional description

This feature adds a Redirection subfield to the SimRing line option datafilled in table IBNFEAT. When this option has a value of Not_allowed on a SimRing pilot DN then the resultant NPMDN legs are not allowed to call forward.

27.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

27.5.2.1.3 Size

Current table size is unchanged.

27.5.2.1.4 Fields/OIDs

The following table lists the new subfield for SimRing line option in IBNFEAT.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Redirection	NEW	none	allowed / not_allowed	SimRing Deny Redirection Allowed assigned to this subfield of simring group option indicates that NPMDN terminators with active call forwarding are allowed to redirect calls. Not_Allowed assigned to this subfield of simring group option indicates that NPMDN terminators are not allowed to call forward.

27.5.2.1.5 Datafill example

The following example shows sample datafill for table IBNFEAT line option SimRing.

```
TABLE: IBNFEAT
>
>list
LEN DNNO DF FEATURE DATA
------------------------
HOST 01 0 00 00 0 SIMRING SIMRING 0 ACT FALSE $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
FEATURE: SIMRING
>
GRPKEY: 0
>
STATE: ACT
>
REDIRECTION: ALLOWED
>not_allowed
PIN: $
>
TUPLE TO BE CHANGED:
HOST 01 0 00 00 0 SIMRING SIMRING 0 ACT NOT_ALLOWED $
```

27.5.2.1.6 Table release history update

A subfield, Redirection, added to the SimRing group option.

27.5.2.1.7 Supplementary information

None.

27.5.2.1.8 Translation verification other tools

Not applicable.

27.5.2.2 Name: KSETFEAT

27.5.2.2.1 Functional description

This feature adds an Redirection subfield to the SimRing line option datafilled in table KSETFEAT. When this option has a value of Not_allowed on a

SimRing pilot DN then the resultant NPMDN legs are not allowed to call forward.

27.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

27.5.2.2.3 Size

There is no change to the table size.

27.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for KSETFEAT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Redirection	NEW	none	allowed / not_allowed	SimRing Deny Redirection Allowed assigned to this subfield of simring group option indicates that NPMDN terminators with active call forwarding are allowed to redirect calls. Not_Allowed assigned to this subfield of simring group option indicates that NPMDN terminators are not allowed to call forward.

27.5.2.2.5 Datafill example

The following example shows sample datafill for table KSETFEAT line option SimRing.

```
TABLE: KSETFEAT
>list
FEATKEY FEATURE KVAR
--------------------
ISDN 1 1 SIMRING SIMRING 1 ACT ALLOWED $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
FEATURE: SIMRING
>
GRPKEY: 1
>
STATE: ACT
>
REDIRECTION: ALLOWED
>not_allowed
PIN: $
>
TUPLE TO BE CHANGED:
ISDN 1 1 SIMRING SIMRING 1 ACT NOT_ALLOWED $
```

27.5.2.2.6 Table release history update

A subfield, SRDR, added to the SimRing group option.

27.5.2.2.7 Supplementary information

None.

27.5.2.2.8 Translation verification other tools

Not applicable.

27.6 Service Orders (SO) (CM & SESM)

27.6.1 Service order change details

27.6.1.1 LCC and options

27.6.2 New commands

This activity adds a new option “REDIRECTION” to the existing SimRing group commands. The commands that can be used to datafill SimRing the standard ADO, DEO, CHF, EST, ADD, and DEL commands. The following table describes what the new prompt is for each of the ServOrd commands.

Command	Prompting
ADO	• **Redirection** • PIN
DEO	• No new prompt
CHF	• state • **Redirection** • PIN
EST	• NPMDNs • State • **Redirection** • PIN
ADD	• No new prompt
DEL	• No new prompt

27.6.2.1 How service order commands are presented

No new commands added

27.6.2.1.1 Command prompts

The system prompts for EST and CHF commands are shown in order of their appearance.

27.6.2.2 How service order options are presented

27.6.2.2.1 Description

For SimRing, EST and CHF commands are changed in order to have the new "REDIRECTION" option. Other than that crafts person will not see any other changes.

27.6.2.2.2 Example

Figure 1 Example of the EST command in prompt mode

```
>est
SONUMBER:    NOW   3  7 16 AM
>
GROUPTYPE:
>simring
SIMRING_PILOT_LEN_OR_DN:
>6213510
SIMRING_MEMBER_DN:
>6213511
SIMRING_MEMBER_DN:
>$
SIMR_STATE: INACT
>act
REDIRECTION:
>allowed
SIMR_PIN:
>123
COMMAND AS ENTERED:
EST NOW 3 7 16 AM SIMRING 6213510 ( 6213511 ) $ ACT ALLOWED 123
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 2 Example of the EST command in no-prompt mode

```
est $ simring 6213510 6213511 $ act allowed 123 y y
```

Figure 3 Example of the CHF command in prompt mode

```
>chf
SONUMBER:    NOW   3  7 16 AM
>
DN_OR_LEN:
>6213510
OPTION:
>simring
SIMR_STATE: INACT
>act
REDIRECTION:
>allowed
SIMR_PIN:
>123
OPTION:
>$
COMMAND AS ENTERED:
CHF NOW 3 7 16 AM 6213510 ( SIMRING ACT ALLOWED 123 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
COMMAND AS ENTERED:
EST NOW 3 7 16 AM SIMRING 6213510 ( 6213511 ) $ ACT ALLOWED 123
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 4 Example of the CHF command in prompt mode

```
chf $ 6213510 simring allowed 123 $ yy
```

27.6.2.2.3 Option prompts

Table 4 System prompts for Redirection field of SimRing option

Prompt	Valid input	Description	Areas affected by prompt
REDIRECTION	ALLOWED	NPMDN with active call forwarding are allowed to redirect calls.	This change only affect NPMDNs with active call forwarding (CFA, CFD, CFB)
	NOT_ALLOWED	NPMDN with active call forwarding are not allowed to forward calls.	

27.6.2.2.4 Line class code compatibility

No change to SimRing option / LCC compatibility.

Table 5 Redirection compatibility to LCC

Line class code	Compatible?
N/A	
1FR-1MR	Yes/No

27.6.2.2.5 Assignability

Redirection option is SimRing group option.

27.6.2.2.6 Option prerequisites

Redirection option is part of the SimRing group option and can not be added to any lines.

27.6.2.2.7 Notes

n/a

27.6.2.2.8 Feature identification

n/a

27.6.2.2.9 SERVORD+ Exceptions

n/a

27.7 Software optionality control (SOC)

No new SOC is introduced by this feature.

27.8 Element Management

Not applicable.

27.9 Command interface changes

27.9.1 Command: QSIMR

This feature modifies the display of QSIMR. It adds an indication that Redirection is allowed/not allowed on the SimRing group.

27.10 Security

This feature does not impact security.

27.11 Configuration Walkthrough

See “27.6 Service Orders (SO) (CM & SESM)” on page 2654 for configuration details.

28: Configuration (CN): A00003074

28.1 Hardware and Software Requirements

Not Required

28.2 Initial Configuration

Not Required

28.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Required

28.4 Upgrade Impact

28.4.1 Upgrade Impact

28.4.1.1 Dump and Restore

In order to upgrade to SN07.0, the customer must currently be running the SN06.2 release.

In order to bring the data from SN06.2 to SN07 during an SN06.2 to SN07 upgrade, the customer must export the SN06.2 data in the SN06.2 Subnet View for the individual gateway node and then import the gateway node into SN07. The export files from SN06.2 must be saved on another device if rollback of a gateway is anticipated. The SN06.2 export data is used to repopulate the node in the SN07 Mg9k Element Manager.

Prior to performing a maintenance release (MR) upgrade (i.e. SN07 to SN07MR), the customer should backup the Oracle database on the CS2M machine. This is a normal backup of the oracle database on the CS2M machine.

28.4.1.2 Element Management Major Release Upgrade

Changes to the SN06.2 to SN07 upgrade are

- After upgrading to SN07, new hardware for SCO, SCI, ITX, ITP, and ABI can be upgraded.
- If attempting to rollback to SN06.2, the new SN07 boards have to be removed and replaced with the old hardware boards prior to downgrading the loads on the cards. Failure to do so could damage the hardware.
- During the time when the DCC cards have been upgraded to SN07 but the NE resides in the SN06.X Subnet View, the SN06.X OM Collector will not collect any OMs due to security features added in the SN07 MG9k card software. The NE should be removed from the SN06.X OM Collector collection list.

- When the user installs the MG9000 Master server software, the “pkgadd” command now performs an additional check. If two releases of the MG9000 server software are already installed, the installation fails and the user sees the following message:

  The package cannot be installed. The following releases of the MG9000 EM Master server are already installed:

  NTmg9ks_6_45.pkg

  NTmg9ks_6_221_0.pkg

  At most two releases of the MG9K EM Master server software should be installed on a given SSPFS at any time. Before installing the new package, you must remove one of the packages listed above. Please remove the package that is no longer being used. To remove a package, use the “pkgadd” command.

- When the user installs the MG9000 mid-tier server software, the “pkgadd” command now performs the same check. If two releases of the MG9000 mid-tier software are already installed, the installation fails and the user sees the following message:

  The package cannot be installed. The following releases of the MG9000 EM mid-tier server are already installed:

  NTmg9km_6_45.pkg

  NTmg9km_6_221_0.pkg

  At most two releases of the MG9K EM mid-tier server software should be installed on a given SSPFS at any time. Before installing the new package, you must remove one of the packages listed above. Please remove the package that is no longer being used. To remove a package, use the “pkgadd” command.

28.4.1.3 Element Management Maintenance Release (MR) Upgrade

Compared to previous releases, the SN07 maintenance release (MR) upgrade process has the following differences:

- Prior to the MR upgrade, the user should backup the entire Oracle database.
- The user does not export each NE prior to the upgrade.

The SN06.2 MR upgrade process is documented in section “Upgrading the MG 9000 Manager software to a maintenance release” of document NN10048-461 entitled “Upgrading the MG9000” (version SN07). Below is a summary of the MR upgrade process for SN07.

- Backup the entire Oracle database.
- Upgrade the hardware, if necessary. Ensure the connection from the MG 9000 Manager to the MG 9000 is up.

- Stop the GUI clients.
- Stop the mid-tier server.
- Stop the Performance Collector and Formatter (PCF) OM collection application.
- Stop the master server.
- Remove the old master server package.
- If required, perform an MR upgrade on the SSPFS software.
- Install, configure, and start the MR release master server. When you configure the master server, typically you should use the same settings from the previous installation of the master server. You will NOT be prompted with the questions “Is this an MR upgrade?” and “Do you want to initialize the database?”. The software knows the correct actions to take.
- Remove the old midtier server package.
- Install, configure, and start the MR release midtier server. When you configure the midtier server, typically you should use the same settings from the previous installation of the midtier server.
- Launch the new client. The client will display any NEs that were provisioned prior to the MR upgrade.
- Reconnect any third party application that retrieves alarms for delivery to Operations Support System (OSS) fault management systems.
- Install and start the MR release OM collection application.

28.4.2 OSS Changes

28.4.2.1 Prefix Changes

With SN07 the northbound interfaces need to change the prefix for event channel, and fault manager entries. In SN06.2, the prefix was Subnet_62. With the SN07 release the prefix for applicable CORBA Naming Service entries should be changed to Subnet_7.

Example ORB entry changes:

SN06.2

EventChannel = “Subnet_62.ec.Oss”

FaultServiceManager = “Subnet_62.Services.FaultServiceManager”

SN07

EventChannel = “Subnet_7.ec.Oss”

FaultServiceManager = “Subnet_7.Services.FaultServiceManager”

28.4.2.2 Customer Log Changes

New customer logs are added to inform users when data has not been saved in the database. These are cases where the data is provisioned successfully in all appropriate places except for the database. The logs indicate when this situation occurs for termination data, when an attempt to correct the database fails, and when the database is corrected. The MGEM logs apply to all components on the MG9K EM except for terminations and the VMG logs apply to termination data. The logs and examples are below:

- MGEM 704 - An attempt to correct the database has failed.

```
MGEM 704 Warning INFO

Database unavailable, correction failed

Failed database correction on VMG.  The database will
be corrected when it is available.  Check the
database for problems.
```

```
MGEM 704 Warning INFO

Database unavailable, correction failed

Failed database correction to MODIFY TERM ESA DATA on
VMG LCE023-0-3, termination tp/04/01 with DN
9192234567.  The database will be corrected when it
is available.  Check the database for problems.
```

- MGEM 705 - An attempt to correct the database has passed.

```
MGEM 705 Warning INFO

Database corrected

Data is corrected on VMG.
```

- VMG 600 - Termination data was successfully provisioned in all appropriate areas except for the database.

```
VMG 600 Warning INFO

Database unavailable, update failure
```

```
Failed database update to MODIFY TERM DN on VMG
LCE023-0-3, termination tp/04/01 with DN 9192234567
and gateway ESA flag value of 0. The database will be
corrected when it is available.  Check the database
for problems.
```

- VMG 601 - An attempt to correct termination data in the database has passed.

```
VMG 601 Warning INFO

Database corrected

Data is corrected for MODIFY TERM DN on VMG LCE023-
0-3, termination tp/04/01 with DN 9192234567.
```

28.4.3 External Interface Changes

With SN07 the TL1 Adaptor for SN07 connects to 2363 port. Thus third party equipment should connect to port 2363 for SN07.

In SN07, the EM's SNMP listening port is 8002.

28.5 Element Management

28.5.1 New/modified GUIs

28.5.1.1 MG9000 Menu changes

In SN06.2 and earlier releases, the MG9000 menu tab in the subnet view has a menu item for ExportNE. However, as of SN07, the menu item for ExportNE no longer exists. When upgrading from SN07 to a later release, the user no longer exports the NE data.

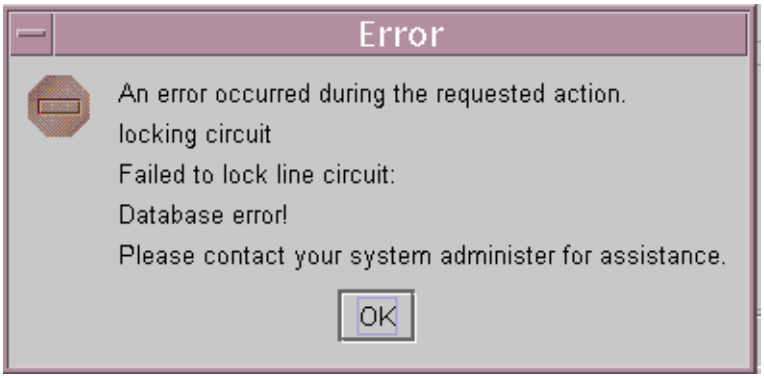
28.5.1.2 New Status Icon

Consider a scenario in which an MG9K is upgraded from an EM running version SN06.2 to an EM running version SN07. After the upgrade, the SN06.2 version of the EM notices that the MG9K is reporting its traps to an IP address and port that is different from its own SNMP listening port. Essentially, the SN06.2 EM is no longer managing that MG9K.

When an EM has an MG9K provisioned but is no longer managing that MG9K, the EM's GUI should provide an indication to the user regrading the status of that MG9K. More specifically, in the GUI's subnet view, the following status icon will appear on top of the NE icon:

28.5.1.3 New database error

With this feature, some data that used to reside in memory will now be persisted in the database. If a database error is encountered during MG9000 EM GUI actions, an error message will be displayed to inform the user that the operation has failed due to a database error. The following GUI is an example of such an error message:



29: Configuration (CN): A00003454

29.1 Hardware and Software Requirements

There are no special hardware or software requirements.

29.2 Configuration

The initial configuration of this package is completed as part of the installation.

Following is an example of getting to the SOCKS configuration using *cli*. All following examples will presume the SOCKS configuration was successfully navigated to.

29.2.0.1 Starting the SOCKS configuration

```
>/opt/nortel/NTsocks/cli

Command Line Interface

 1 - View

 2 - Configuration

 3 - Other


 X - exit


select - 2




Configuration

 1 - NTP Configuration

 2 - Apache Proxy Configuration

 3 - DCE Configuration

 4 - OAMP Application Configuration

 5 - CORBA Configuration

 6 - IP Configuration

 7 - DNS Configuration
```

```
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Succession Element Configuration
14 - chg_tz (Change Timezone)
15 - login_session_timeout (Login Session Timeout
Configuration)
16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select - 13



Succession Element Configuration
1 - SAM21EM Application Configuration
2 - NPM Application Configuration
3 - PSE Application Configuration
4 - OMPUSH Application Configuration
5 - SOCKS Configuration

 X - exit

select - 5


SOCKS Configuration
1 - SOCKS configuration tool
```

```
select - 1



Socks Configuration
 1 - config_socks (Modify Socks Security Service)
 2 - list_socks (List Socks Security Service)

 X - exit

select - 1
```

The changes of the server side port is a disruptive action. If the server side port is changed, the SOCKS server and all dependant applications must be restarted.

SOCKS ports in all offices must be configured the same. Misconfiguration will cause EMS clients to not function.

Proceed with caution.

29.2.0.2 Successful configuration of the SOCKS ports using default values.

```
Enter the port the Server side SOCKS Proxy will
listen on. Value must be
within [1025 - 65535]. default value 10080.
Current value 10080[?,q]



Is port 10080 acceptable? [y] [y,n,?,q] y



Enter the port the Client side SOCKS Proxy will
listen on. Value must be
```

```
within [1025 - 65535]. Current Value - 10090 [?,q]
Leaving CLIENT port at 10090.
Leaving both ports at configured values:
           Server side SOCKS Proxy port: 10080
           Client side SOCKS Proxy port: 10090


=== "config_socks" completed successfully
```

29.2.0.3 Entering a non-default value for both the server and client ports.

WARNING: Configuring the SOCKS server side port requires a restart of the SOCKS server and all dependent applications, are you sure you want to change the configuration? [y] [y,n,?,q] y

Enter the port the Client side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10090 [?,q] 3445

Warning: Clients already running Succession GUI's must be restarted to use this new port, are you sure you want to change the configuration?
[y] [y,n,?,q] y
Configuring ports:
Server side SOCKS Proxy port to 2334
Client side SOCKS Proxy port to 3445

WARNING: Configuring the Server Side socks port. This will cause disruption of
service. Do you want to continue? [y] [y,n,?,q] y
Stopping NTSocks on Thu Jan 29 05:32:41 EST 2004
Socket creation to 2334 failed
Socket creation to 2334 failed
Socket creation to 2334 failed
Socket creation to 2334 failed
Socket creation to 2334 failed
both sockets listening
in checkSocks 10081
streams created
readSocksReply ... calling read
read returned count 2
readSocksReply 2
local port correctly working. Attempting again
in checkSocks 10081
streams created
readSocksReply ... calling read

```
read returned count 2
readSocksReply 2
Socks Server is running
The SOCKS ports have been successfully configured to:
        Server side SOCKS Proxy port to 2334
        Client side SOCKS Proxy port to 3445

=== "config_socks" completed successfully
```

29.2.0.4 Entering invalid port ranges for both server and client ports

```
The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all
dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port.
Misconfiguration will cause EMS clients to not function.

Proceed with caution.

Enter the port the Server side SOCKS Proxy will listen on. Value must be
within [1025 - 65535]. Current Value - 10080 [?,q]
Leaving SERVER port at 10080
The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all
dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port.
Misconfiguration will cause EMS clients to not function.

Proceed with caution.

The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all
dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port.
The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all
dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port.
Misconfiguration will cause EMS clients to not function.

Proceed with caution.
```

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10080 [?,q] 111
ERROR: Invalid entry: Enter the SOCKS Proxy Port..

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10080 [?,q] 65555

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10080 [?,q] 1098

WARNING: Configuring the SOCKS server side port requires a restart of the SOCKS server and all dependent applications, are you sure you want to change the configuration? [y] [y,n,?,q] y

Enter the port the Client side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10090 [?,q] 1
ERROR: Invalid entry: Enter the SOCKS Proxy Port..

Enter the port the Client side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10090 [?,q] 70000

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Client side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. Current Value - 10090 [?,q] 10098

Warning: Clients already running Succession GUI's must be restarted to use this new port, are you sure you want to change the configuration?
[y] [y,n,?,q] y
Configuring ports:
Server side SOCKS Proxy port to 1098
Client side SOCKS Proxy port to 10098

WARNING: Configuring the Server Side socks port. This will cause disruption of
service. Do you want to continue? [y] [y,n,?,q]
Stopping NTSocks on Thu Jan 29 05:40:54 EST 2004
Socket creation to 1098 failed
Socket creation to 1098 failed
Socket creation to 1098 failed
Socket creation to 1098 failed
Socket creation to 1098 failed
both sockets listening

```
in checkSocks 10081
streams created
readSocksReply ... calling read
read returned count 2
readSocksReply 2
local port correctly working. Attempting again
in checkSocks 10081
streams created
readSocksReply ... calling read
read returned count 2
readSocksReply 2
Socks Server is running
The SOCKS ports have been successfully configured to:
        Server side SOCKS Proxy port to 1098
        Client side SOCKS Proxy port to 10098

=== "config_socks" completed successfully
```

29.2.0.5 Configuring only the server side port

```
WARNING: Configuring the SOCKS server side port requires a restart of the
SOCKS server and all dependent applications, are you sure you want to change
the configuration?  [y] [y,n,?,q] y

Enter the port the Client side SOCKS Proxy will listen on. Value must be
The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all
dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port.
Misconfiguration will cause EMS clients to not function.

Proceed with caution.

Enter the port the Server side SOCKS Proxy will listen on. Value must be
within [1025 - 65535]. Current Value - 1098 [?,q] 10080


WARNING: Configuring the SOCKS server side port requires a restart of the
SOCKS server and all dependent applications, are you sure you want to change
the configuration?  [y] [y,n,?,q] y

Enter the port the Client side SOCKS Proxy will listen on. Value must be
within [1025 - 65535]. Current Value - 10098 [?,q]
Leaving CLIENT port at 10098.
Configuring ports:
```

```
        Server side SOCKS Proxy port to 10080
        Client side SOCKS Proxy port to 10098

WARNING: Configuring the Server Side socks port. This will cause
disruption of
service. Do you want to continue? [y] [y,n,?,q] y
Stopping NTSocks on Thu Jan 29 05:44:47 EST 2004
Socket creation to 10080 failed
Socket creation to 10080 failed
Socket creation to 10080 failed
Socket creation to 10080 failed
Socket creation to 10080 failed
both sockets listening
in checkSocks 10081
streams created
readSocksReply ... calling read
read returned count 2
readSocksReply 2
local port correctly working. Attempting again
in checkSocks 10081
streams created
readSocksReply ... calling read
read returned count 2
readSocksReply 2
Socks Server is running
The SOCKS ports have been successfully configured to:
        Server side SOCKS Proxy port to 10080
        Client side SOCKS Proxy port to 10098

=== "config_socks" completed successfully
```

29.2.0.6 Configuring only the client side port

The changes of the server side port is a disruptive action.
If the server side port is changed, the SOCKS server and all dependant applications must be restarted.

SOCKS ports in all offices must be configured to the same port. Misconfiguration will cause EMS clients to not function.

Proceed with caution.

```
Enter the port the Server side SOCKS Proxy will listen on. Value must be
within [1025 - 65535]. Current Value - 10080 [?,q]
Leaving SERVER port at 10080
```

Enter the port the Client side SOCKS Proxy will listen on. Value must be

within [1025 - 65535]. Current Value - 10098 [?,q] 10090

Warning: Clients already running Succession GUI's must be restarted to use this new port, are you sure you want to change the configuration?
[y] [y,n,?,q] y
Configuring ports:
Server side SOCKS Proxy port to 10080
Client side SOCKS Proxy port to 10090
The SOCKS ports have been successfully configured to:
Server side SOCKS Proxy port to 10080
Client side SOCKS Proxy port to 10090

=== "config_socks" completed successfully

29.2.0.7 Running the list command

Socks Configuration

1 - config_socks (Modify Socks Security Service)

2 - list_socks (List Socks Security Service)

X - exit

select -2

The ports configured for use by socks are:

The Client side SOCKS Proxy will listen on port 10090

The Server side SOCKS Proxy will listen on 10080

=== "list_socks" completed successfully

30: Configuration (CN): A00003487

30.1 Hardware and Software Requirements

30.1.1 Hardware

No additional hardware is required in order to upgrade to a load capable of supporting multiple packet networks (support limited to IP interworking with AAL2 for SN07). All exisiting TDM/Packet configurations will continue to be supported, including:

- UA-AAL1
- PT-AAL1
- Ultralite AAL1
- UA-IP
- PT-IP
- PT-IP Compact (includes AAL2 via the PVG)
- AAL2 Wireless

In addition, the following new office configuration are supported:

- UA-AAL1/IP
- New hardware will be required for the addition of the second packet network.

30.1.2 Software

The software reconfiguration to use the new networking tables (BEARNETS, NETBRDGE, NETPATH, NET2NET) will occur automatically to include default datafill dictated by the value of a new office parameter. This parameter, PRE_SN07_DUMPSIDE_PACKET_FABRIC, must be set by the engineering team and applied to the office prior to the table transfer.

SESM will align with the standard SESM requirements.

In order to provision a second packet network, the customer will have to provision the new network, any bridging resources for that network, and the connectivity supported between the networks via the bridging resource paths.

30.2 Initial Configuration.

30.2.1 Office parameters

30.2.1.1 NETWORK_ACTIVE

The network_active office parameter will be set to EXTENET when upgraded to the SN07 Succession load, even if it had been previously set to ENET.

If it had been set to JNET, the value will remain as JNET. In these offices, there will be no default network datafill in the new network tables.

> ***Note:*** If the value of the network_active office parameter is set to JNET, the packet connectivity function is not available.

30.2.1.2 PRE_SN07_DUMPSIDE_PACKET_FABRIC

Will be set to one of {UNDEF[1], NONE, AAL1, AAL2, IP}. Once the ONP is complete, there is no need to change this office parameter.

30.2.1.3 MULTINET_DISPLAY_ACTIVE = 'N'

The display control for the new OMs and Logs introduced by this activity is initially off.

30.2.2 New Network Tables - initial datafill

The examples that follow are the default tuples that will be in the new network tables after the ONP is complete. Note that the initial value of the NET 1 FABRIC field will be determined by the new office parameter PRE_SN07_DUMPSIDE_PACKET_FABRIC.

The following examples show the post TABXFER views of the new table data for the various "from" office network configurations.

[1]Should be set to something other than UNDEF by the engineering team prior to table transfer. UNDEF will be an error condition if the network_active = EXTENET.

Figure 1 JNET only on from side (JNET)

```
TABLE BEARNETS:
NETIDX  BNETNAME          DISPLAY          FABRIC           OPTIONS
-----------------------------------------------------------------

TABLE CLLI:
CLLI             ADNUM            TRKGRSIZ                  ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI         BRDGTYPE         DISPLAY                   ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                  NETPATH
-------------------------------------

TABLE NET2NET
BNETNAME                 CONNNETS
-------------------------------------

Note: If JNET, then the network_active = JNET, and packet networks are not supported
at all.
```

Figure 2 ENET only on from side (ENET)

```
TABLE BEARNETS:
NETIDX  BNETNAME          DISPLAY          FABRIC           OPTIONS
-----------------------------------------------------------------
NET 0   TDM_ENET         ENET             ENET         $

TABLE CLLI:
CLLI             ADNUM            TRKGRSIZ                  ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI         BRDGTYPE         DISPLAY                   ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                  NETPATH
-------------------------------------
0                        $

TABLE NET2NET
BNETNAME                 CONNNETS
-------------------------------------
TDM_ENET              $
```

Figure 3 ENET & AAL1 on from side (UA-AAL1 & PT-AAL1)

```
TABLE BEARNETS:
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET         $
NET 1   NET_AAL1        ATM             AAL1            (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    725             0                       ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    CORE_BRDG       E-A1                    (TDM_ENET NET_AAL1) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $
1                       (ENET_TO_AAL1) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_AQAL1 1) $
NET_AAL1                (TDM_ENET 1) $
```

Figure 4 AAL1 on from side (Ultralite-AAL1)

```
TABLE BEARNETS:
NETIDX  BNETNAME       DISPLAY         FABRIC          OPTIONS
-----------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET         $
NET 1   NET_AAL1       ATM            AAL1          (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                $
NET_AAL1                $
```

Figure 5 ENET & IP on from side (UA-IP and PT-IP)

```
TABLE BEARNETS
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET       $
NET 1    NET_IP          IP              IP        (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_IP      725             0                       ENET_TO_IP_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_IP      CORE_BRDG       E-IP                    (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $
1                       (ENET_TO_IP) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_IP 1) $
NET_IP                  (TDM_ENET 1) $
```

Figure 6 IP on from side (PT-IP Compact)

```
TABLE BEARNETS
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 1   NET_IP          IP              IP              (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
NET_IP                  $
```

30.2.3 New fields in existing tables

30.2.3.1 MNNODE

- IW SPM: will include new field BRDGCLLI set to key of only entry in table NETBRDGE.
- IW DPT: will include a new field BEARNETS set to (<name of NET 1> Y) $.
- MG4K: will include a new field BEARNETS set to (NET_AAL1 Y) $

30.2.3.2 TRKOPTS

- DPT tuples will be pulled out of the DYNAMIC option as an application type and moved into it's own option area.
- DPT tuples will contain a new BEARNETS field, that will contain (<name of NET 1> Y) $
- SIPT DPT tuples contain a new selector named NGSS. This selector indicates if the trunk group uses the new Next Generaion Session Server (NGSS) for SIP architecture implemented by activities A00003933. The values of this field is either 'Y' or 'N'.

30.2.3.3 SERVRINV

- Will contain a new BEARNETS field, which will be set to:

— (<name of NET 1> Y) $ if GWC is not a DPT GWC

— $ if a DPT GWC

30.2.3.4 Routing tables: CND PKT selector

The existing CND PKT routing selector will be converted to CND FABRIC in all of the applicable routing tables.

30.2.4 SESM

Each non DPT GWC provisioned will have a network codec profile associated with it, using the existing network codec profile that is configured for the office.

DPT GWC's will not have a network codec profile associated with them.

30.3 Office/Subnet parameters (OP/SP) (CM & SESM)

30.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCOPT	network_active	Unchanged	CM
OFCVAR	multinet_display_active	New	CM
OFCSTD	pre_sn07_dumpside_packet_fabric	New	CM

30.3.2 Parameter information

30.3.2.1 OFCOPT::NETWORK_ACTIVE

- The parameter itself is not really changing in SN07. It will simply be used to aid in the detection of an upgrade to a Succession call server capable of supporting multiple packet networks.
- As of SN04, any ENET offices upgrading to a packet capable Succession load will have this office parameter converted to EXTENET automatically during the upgrade.
- The value EXTENET is now expanded to include the ability to support mutiple packet networks.

- The use of the network tables (BEARNETS, NETBRDGE, NETPATH, and NET2NET) is enforced in connectivity for interworking the various networks, even when only a single packet network exists.

30.3.2.1.1 Functional description
This parameter controls various aspects of call processing, most importantly the network connectivity capabilities that are supported by the system.

30.3.2.1.2 Provisioning rules
For JNET call processing, set the value of this parameter to JNET.

For Succession (single or multiple packet networks), the value should be set to EXTENET. “Succession” includes all cases where the load is packet capable, such that it includes the MSH DRU. This includes offices that currently only have an ENET provisioned.

30.3.2.1.3 Range information
Unchanged.

30.3.2.1.4 Activation
Unchanged.

30.3.2.1.5 Dependencies
No additional dependencies.

30.3.2.1.6 Consequences
Unchanged.

Note: The update mentioned under activation was put in place because this office parameter requires a restart for activation, and packet network connectivity is not available unless the office parm is set to EXTENET for Succession loads.

30.3.2.1.7 Verification
Not applicable.

30.3.2.1.8 Memory requirements
No memory impact.

30.3.2.1.9 Parameter release history update
Office parm value EXTENET now implies that the software can support multiple packet networks.

Note: The current SN06 NTP documentation does not reflect that this parameter will be changed on an ONP to EXTENET, if the from side is currently set at “ENET” and the to load contains the MSH DRU. The update that does this was submitted in TL16.

30.3.2.2 OFCVAR::MULTINET_DISPLAY_ACTIVE

Multiple Networks Display Active

30.3.2.2.1 Functional description

This is a new office parameter associated with Succession Call Server that activates the new and changed OMs and logs. This allows the customer the flexibility of enabling multiple packet networks (likely for testing purposes only) prior to having the back-office system (i.e., OSS systems) ready to support the new OMs and log fields. This is an Y/N type parameter. This parameter would be part of OFCVAR table. The default would be set to 'N'.

This parameter does not control the display of the IWBM per bridge pool OMs.

30.3.2.2.2 Provisioning rules

This office parameter cannot be turned on unless NETWORK_ACTIVE = EXTENET.

There are no restrictions for setting it to 'N'.

30.3.2.2.2.1 Behavior when the parameter is set to 'Y'

- Change from 'N' to 'Y' using table control.
  - — The tuples in the new OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are created/ (if non-existant) displayed.
  - — Pegging of the OM group registers in TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group is displayed. The bearer network is also displayed for DPTNODE OMs if the DPT node is SPM based. The bearer network will not be displayed for GWC hosted DPT.
  - — The display of the bridge pool in IWBM 800 series of LOGS is enabled.

30.3.2.2.2.2 Behavior when the parameter is set to 'N'

- Change from 'Y' to 'N' using table control
  - — A warning message would be displayed "All OM and LOGs data pertaining to multiple bearer networks on this call server will be lost.".
  - — The tuples in the new OM groups would not be displayed.
  - — The signaling type and bearer network for the DPT node tuple in the DPTNODE OM group would not be displayed.
  - — All the counters for the registers of the new OM groups would be set to zero.

— The counters of the registers of the new OM groups would not be pegged.

— The display of bridge pool in IWBM 800 series of LOGS would be disabled.

— The OMSHOW command would display the OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

30.3.2.2.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
Y/N	Y/N	N

30.3.2.2.4 Activation
Immediate

30.3.2.2.5 Dependencies

This parameter cannot be set to Y unless NETWORK_ACTIVE = EXTENET.

30.3.2.2.6 Consequences

Setting this parameter to Y will result in new OM tuples and log fields to be displayed. This could adversely affect downsteam OOS systems that have not yet been upgraded to handle this additional data.

30.3.2.2.7 Verification
To verify that the MULTINET Display is active and OM groups are created, use the CI command OMSHOW DPTOFCP. This command should display the OM group files and its tuples.

30.3.2.2.8 Memory requirements
Refer to the EI section for final details.

The new OM groups will be created at IPL time, but the tuples will not be created/displayed until the office parameter is set to Y.

- For the OM groups DPTOFCP, OFZ2NET1 and OFZ2NET2 the tuples would be created but not displayed.
- For the OM TRK2NET1 and TRK2NET2, the tuples would not be created and would be created when the office parameter "MULTINET_DISPLAY_ACTIVE" is set to Y for the first time.

30.3.2.2.9 Parameter release history update

New in SN07.

30.3.2.3 OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC

SN07 Dumpside Packet Fabric prior to Succession MULTINET upgrade.

30.3.2.3.1 Functional description

This office parameter is set by the Nortel engineering team in an office parm changes flat file prior to the night of ONP. It is to be applied after the transfer of the office parameters and prior to the TABXFER.

The purpose of the parameter is to identify the FABRIC type of the single packet fabric supported on the from side prior to the upgrade, in order for the proper network tuples to be created in tables BEARNETS, CLLI, NETBRDGE, NETPATH, and NET2NET, as well as allow the new network related fields in tables MNNODE, TRKOPTS, and SERVRINV to be assigned the proper default values.

It is very important that this parameter be set correctly.

30.3.2.3.2 Provisioning rules

This parameter has the following range: {UNDEF, NONE, AAL1, AAL2, IP}. It will be defaulted to UNDEF at IPL in a Succession load, and NONE if in a non-Succession load. It should be set to one of the other values (not UNDEF) on all upgrades to Succession loads. Although present in non Succession loads, it does not need to be set for these loads. Once an office is already on an SN07 or later load, it does not need to be set again.

A warning will be output on all changes except “UNDEF” to one of the other values that this parameter impacts the automatic creation of the network data on ONP, and should be changed with care.

Once a packet tuple is provisioned in table BEARNETS, changes will not be allowed.

In order to properly set the value, datafill will be required from the dump side from the following tables: MNNODE, MNCKTPAK, SERVRINV, TRKOPTS, LGRPINV.

Explanation of parameter values:

- UNDEF: Default value at IPL. Indicates that the engineering team has not looked at the data.
- NONE: The engineering team has analyzed the from side data and detected that no packet nodes are provisioned. Indications that a packet node existed would include:

— MNNODE: IW SPM, DPM SPM, or MG4K SPMs are provisioned.

— SERVRINV: any tuple provisioned.

— Although one could argue that datafill in tables SERVSINV or LGRPINV also indicates a packet node, it cannot be added without a GWC first.

- AAL1: The from side packet datafill contained one of the following:
  — MNNODE contained an SMG4 (MG4K). Prior to SN07.1, MG4K IP did not exist.
  — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is ATM RM.
- AAL2:
  — Cannot be detected based on table datafill. Hopefully the engineering team knows if the PVG is using AAL2 or IP/AAL5.
- IP:
  — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is GEM RM.
  — Table LGRPINV contains tuples whose GRPTYPE field is ‘M’ or ‘C’. indicating IAD devices or CICM.
  — The parm should also be set to IP if dumpside was using IP/AAL5. This will not be distinguished as a seperate bearer network.

30.3.2.3.3 Range information

Table 3 Range Information

Minimum	Maximum	Default
{UNDEF, NONE, AAL1, AAL2, IP}	{UNDEF, NONE, AAL1, AAL2, IP}	ENET - if load does not contain the MSH DRU UNDEF - if load contains MSH DRU.

30.3.2.3.4 Activation

Not applicable. This office parameter is only used during the TABXFER of data to a new load. It should be set to the correct fabric PRIOR to the night of ONP, and not changed thereafter. It is not used by call processing.

30.3.2.3.5 Dependencies

The following tables rely on the proper provisioning of this parameter:

- BEARNETS
- NETBRDGE

- NETPATH
- NET2NET
- MNNODE
- TRKOPTS
- SERVRINV

30.3.2.3.6 Consequences

- There are no consequences of incorrect provisioning if there are no packet nodes currently supported at the site. If the parameter is set to a packet fabric in a site that does not have a packet network, then network tuples will automatically be created in tables BEARNETS, NETBRDGE, NETPATH, NET2NET.
- If a packet network was supported, and the parameter is provisioned incorrectly, tuple transfer errors could occur in the following tables:
  - TABXFER data errors in MNNODE, TRKOPTS, SERVRINV.
- For an SN07 to SN07 lab upgrade, where the new tables suddenly appear in the load:
  - The ONP will not detect this scenario as a multinet upgrade. Instead, the network tables will appear in the load first, and the lab primes will be notified of the change. They will be required to go to a website and download/apply a DMOPRO file for the type of lab they are working in that contains the default data. In a following load, the dependent fields will be added to the existing tables, and type reformats will pick up the default datafill.

30.3.2.3.7 Verification

Not applicable.

30.3.2.3.8 Memory requirements

Minimal. Just need to store the fabric type in a protected variable. Does not control the allocation of any additional memory.

30.3.2.3.9 Parameter release history update

New in SN07.

30.4 Upgrade Impact

30.4.1 Dump and Restore

Callp functionality should not be affected over an upgrade from pre-SN07 to post-SN07. In order to maintain this, the new/changed tables need to be datafilled over the ONP. It is required that this upgrade has minimum impact to the customer. Aside from the traditional issues with type specific reformats,

we have the additional issue of determining what the FABRIC type was on the from side, in order to properly create default tuples in the new network tables. Since call processing will start depending on this data to make inter-network connections, it is vital that this data is correct after the transfer is ONP.

Given the importance of a proper transfer, the need for user input, and the complexity of the data involved, the design team held a meeting with the upgrade team. This chosen alternative was suggested during this meeting, and was unanimously agreed upon by all who were present.

Once the data transfer is complete, the goal is to have the correct network representation for the currently configured networks, such that only new network information is required for when the customer wishes to add additional networks.

The ONP strategy must handle the following information:

30.4.1.1 Office Parameters

- OFCOPT::NETWORK_ACTIVE - If ENET, convert to EXTENET, and ensure that appropriate datafill is created to handle the existing networks.
- OFCVAR::MULTINET_DISPLAY_ACTIVE - Ensure the new office parameter is defaulted to ‘N’.
- OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC: the new office parameter *must be set by the upgrade engineering team* to indicate the default packet fabric on the from side network. This is set in a flat file that is applied after the office parameters have been transferred and before the tables are transferred. The engineering team is responsible for setting the correct values, and the application team is responsible for applying the changes at the proper point. Note that this is simply a new parameter included in the existing office parameter process. No changes are required to the process. This parameter applies only to alternative 1.

30.4.1.2 ONP Creation of Default Network Tuples

Tuples will be created automatically during the TABXFER via post data move procedures for the following tables. For more information see “New Network Tables - initial datafill” on page 2769.

- BEARNETS
  - — Create a NET 0 tuple representing the ENET if ENET is present.
  - — Create an appropriate NET 1 tuple representing the existing packet network. The FABRIC should be set to either AAL1, AAL2, or IP as appropriate.
- CLLI
  - — Create the appropriate CLLI used as the index to table NETBRDGE.

- NETBRDGE
  - — If there is both an ENET and a packet network defined, a bridge pool will be automatically created in table NETBRDGE for it.
- NETPATH
  - — Path 0 will be created as $. This is the nilpath, indicating that 2 networks can be interconnected without a bridge.
  - — If there are two networks defined, create a path using the bridge pool from NETBRDGE, assuming that bridges exist and that the bridgepool can connect them.
- NET2NET
  - — For each network in table BEARNETS, create a tuple in NET2NET.
  - — If there are multiple networks (both an ENET and a packet network), assume that both the ENET and the packet network can be connected to the other using the path index containing the bridge pool defined in table NETPATH.
  - — Ensure that the NET 1 packet network detected is assigned the PACKET_NETWORK_DEFAULT option.

  Note: It is possible that an upgrade can occur in offices that have both an ENET and a packet network, but no interworking bridge nodes defined. In this case, the default datafill will still be created, but there will be no IW SPM nodes assigned to the bridge pool, so the interconnections defined in table NET2NET will not work. It is assumed that since this is an upgrade from a working office, that translations would prevent such attempts from occuring.

30.4.1.3 Initialization of new fields in existing tables

- MNNODE:
  - — IW SPM: Initialize the new BRDGCLLI field to the single bridge group defined in table NETBRDGE.
  - — DPT SPM: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
  - — MG4K: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
- TRKOPTS:
  - — Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the DPT trunk group.
  - — Initialize the new NGSS field, on SIPT trunks, to ‘N’.
- SERVRINV:

— If not a DPT GWC, initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the GWC.

— If this is a DPT GWC, initialize the new BEARNETS field to $.

30.4.1.4 Type reformats on existing tables

- TRKOPTS: Remove DPT trunk groups as an application under the DYNAMIC trunk option, and create a DPT trunk option.
- OFRn, IBNRTn, HNPACONT::RTEREF, FNPACONT::RTEREF:
  — Convert the CND PKT conditional selector to CND FABRIC in all of the applicable routing tables.

30.4.2 Element Management Upgrade

30.5 Data schema (DS) (CM, MIBS, RDB)

30.5.1 New/modified tables, MIBs, or Database Schema

Table 4 New or modified tables

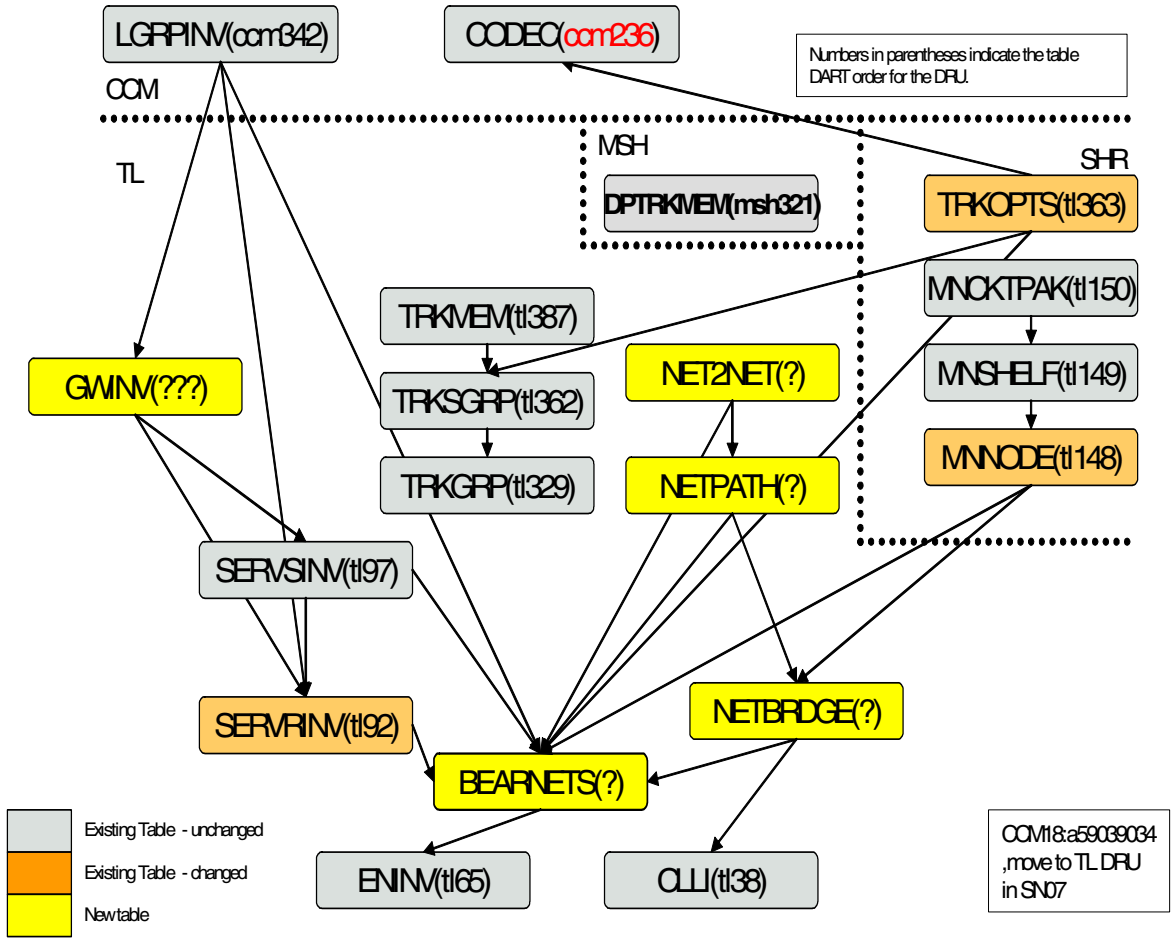
Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Core Tables:		
BEARNETS	NEW	NEW
NETBRDGE	NEW	NEW
NETPATH	NEW	NEW
NET2NET	NEW	NEW
MNNODE	Changed	Unchanged
SERVRINV	Changed	Unchanged
SERVSINV	Changed	Unchanged.
TRKOPTS	Changed	Unchanged
MNCKTPAK	n/a	Unchanged
OFRn	Changed	Unchanged
IBNRTn	Changed	Unchanged
HNPACONT:RTEREF	Changed	Unchanged
FNPACONT:RTEREF	Changed	Unchanged

Table 4 New or modified tables

Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SESM/GWCEM		
GWC_NETWORK_CODEC_PROFILE	New	New
GWC_NETWORK_RECOMMENDED_CODEC_SETTING	New	Old
GWCNode	Changed	New
GATEWAYPROFILE	Changed	Old

30.5.2 Table/MIB/Remote Database Schema information

30.5.2.1 Core Table Dependencies



30.5.2.2 Core Table BEARNETS

Bearer networks

30.5.2.2.1 Functional description

On a Succession Call Server, this table identifies the bearer networks supported by the server and the network options that apply to the packet networks.

The overall default packet network for the office is determined by the assignment of the packet_network_default option to a single tuple in the table. If no packet network is detected in the provisioning hierarchy for a packet agent, this default packet network will be used.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

30.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

ENINV

BEARNETS

NETBRDGE, NET2NET, MNNODE, SERVRINV, TRKOPTS

30.5.2.2.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
BEARNETS	0	8	Memory not allocated unless tuples are provisoned. (Required if NETWORK_ACTIVE = EXTENET).

30.5.2.2.4 Fields/OIDs

The following table lists fields for BEARNETS.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETIDX	New	No	0-7	Key to the table. Will be displayed as “NET 0” - “NET 7”.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	Vector of up to 32 characters.	Identifies the name of the bearer network.This will be used in other tables to reference the associated bearer network and its characteristics. Making the name a field of the tuple rather than the index allows the customer to make name changes to the networks defined. The 32 character name of the network must be unique across the table.
DISPLAY	New	No	Vector of up to 4 characters.	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control.
FABRIC	New	No	ENET, AAL1, AAL2, IP	Identifies the bearer network fabric type.
OPTIONS	New	Refinements	Vector of {pkt_network_default}	Vector of options against the bearer network.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
pkt_network_default	New	OPTIONS refinement (not a field)	n/a	Indicates that this tuple is the packet bearer network default for the office. Primarily used in initializing dependant tables during an ONP. Restrictions: Only one tuple in the table can have this option.

30.5.2.2.5 Datafill example

The following example shows sample datafill for table BEARNETS.

```
TABLE: BEARNETS
NETIDX NETNAME      DISPLAY FABRIC OPTIONS
-----------------------------------------
NET 0  TDM_ENET     ENET    ENET   $
NET 1  NET_AAL1     ATM     AAL1   (PKT_NETWORK_DEFAULT)$
NET 2  NET_IP       IP      IP     $
NET 3  NET_AAL2     AAL2    AAL2   $
```

30.5.2.2.6 Table release history update

New in SN07.

30.5.2.2.7 Supplementary information

Table BEARNETS, along with tables NETBRDGE, NETPATH, and NET2NET) is required to be provisioned in all Succession sites supporting bridged calls from a TDM network to a packet network.

When using the FINDREF tool on table BEARNETS, it is necessary to encapsulate the key field within single parentheses. For example:

FINDREF BEARNETS ‘NET 1’

On an ONP, this table will be automatically provisioned with both TDM and packet networks tuples where they exist.

— If the from side datafill contained an ENET, the NET 0 tuple from the datafill example will be automatically provisioned.

— If the from side supported packet nodes (as indicated by the setting of the PRE_SN07_DUMPSIDE_NETWORK_FABRIC), the NET 1 tuple will be provisioned and marked as the PKT_NETWORK_DEFAULT.

Table 7 BEARNETS Provisioning Restrctions

Field	Provisioning Restrictions
NETIDX	• Additions of packet networks to the table will not be allowed unless the NETWORK_ACTIVE = EXTENET. • Adding a tuple in table BEARNETS will automatically create a tuple in table NET2NET with $. • Cannot delete a BEARNETS tuple unless the NET2NET entry contains a $ and that tuple is the only reference. It is a counted tuple type.
BNETNAME	• Must be unique in table. • Changes to the BNETNAME will be reflected immediately in logs, OMs, etc. • Should only contain alphanumeric and underscore characters.
DISPLAY	• No restrictions, but recommend that this field be unique in the table.
FABRIC	• Only 1 ENET tuple is allowed. • ENET tuple can only be added if ENET exists. • ENET tuple cannot be deleted if ENET exists. • Adds of UNDEF tuples are not allowed. • Changes are not allowed.
OPTION pkt_network_default	• The first packet network added must be the default. • Only one tuple may have this option assigned. If the option is added to another tuple, it will be removed from the first. • Cannot be added if FABRIC = ENET. • Cannot be deleted from a tuple, except by adding to another tuple. • Can only delete the network default tuple if it is the only remaining packet network tuple.

Refer to the supplementary information for table NET2NET for additional information.

30.5.2.2.8 Translation verification other tools

BEARNETS does not use translation verification tools.

30.5.2.3 Core Table NETBRDGE

Network bridging resources.

30.5.2.3.1 Functional description

This table defines the network bridging resources for interconnecting networks. Bridges provide the ability to connect one network to another without regard to the call type. Bridges typically have two connectivity endpoints, one for each of the networks that it inter-connects.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

30.5.2.3.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

CLLI, BEARNETS

NETBRDGE

NETPATH, NET2NET, MNNODE

30.5.2.3.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	64	Refer to the EI section after DSUM.

30.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BRDGCLLI	New	No	CLLI common_language_name	Identifies the name of the bridge resource group.
BRDGTYPE	New	No	CORE_BRDG	The type of the bridging resource. For SN07, this is limited to core bridges, but could be expanded in the future.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DISPLAY	New	No	Vector of up to 4 characters	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control.
BEARNETS	New	Structure	BNETNAME, BNETNAME	Identifies the two networks that can be bridged with this bridging resource group.

30.5.2.3.5 Datafill example

The following example shows sample datafill for table NETBRDGE.

```
TABLE: NETBRDGE
BRDGCLLI      TYPE         DISPLAY BEARNETS
-----------------------------------------
ENET_TO_AAL1  CORE_BRDG   E-A1    TDM_ENET NET_AAL1
ENET_TO_IP    CORE_BRDG   E-IP    TDM_ENET NET_IP
```

30.5.2.3.6 Table release history update

New in SN07.

30.5.2.3.7 Supplementary information

Table 10 NETBRDGE Provisioning Restrctions

Field	Provisioning Restrictions
BRDGCLLI	• Common_language_name provisioned in table CLLI. • Counted tuple type. Deletions are not allowed if referenced by another table.
BRDGTYPE	• Only allowable value in SN07 is {CORE_BRDG}. • Cannot change.

Table 10 NETBRDGE Provisioning Restrctions

Field	Provisioning Restrictions
DISPLAY	• Recommended, but not enforced, to be unique. • No change restrictions.
BEARNETS	• The two network names provided must be provisioned in table BEARNETS. • The two network names must be different. • Changes to the BEARNETS field is allowed only if the tuple is not referenced by another table.

Since the BRDGCLLI is the key to this table, it cannot be changed through the table control interfaces. BRDGCLLI names can be changed for this table using the CI command RENAMECLLI. The name change will then be reflected in all tables, OM, and logs that reference the particular bridge CLLI.

30.5.2.3.8 Translation verification other tools

NETBRDGE does not use translation verification tools.

30.5.2.4 Core Table NETPATH

Interconnecting network path.

30.5.2.4.1 Functional description

Tuples in this table identify the list of bridging resource groups (the bridge path) that can be used to interconnect two networks. In SN07, two bridges are required to connect an AAL1 agent and an IP agent, so the path consists of a bridge resource from each of those NETBRDGE's.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

30.5.2.4.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

NETBRDGE

NETPATH

NET2NET

30.5.2.4.3 Size

Table 11 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETPATH	0	256	Refer to the EI section of this document following the DSUM.

30.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for NETPATH.

Table 12 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PATHIDX	New	New	0 to 255	The key to the table.
NETBRDGE	New	New	Vector of BRDGCLLI	A list of the bridge pools that are required to go from one network to another. Bridge CLLIs must be listed in the order of the traversal required, without regard to the direction of the traversal (forward or backward).

30.5.2.4.5 Datafill example

The following example shows sample datafill for table NETPATH

```
TABLE: NETPATH
PATHIDX       NETBRDGE
----------------------------------------
0              $
1            (ENET_TO_AAL1)  $
2            (ENET_TO_IP)    $
3            (ENET_TO_AAL1), (ENET_TO_IP)$
4            (AAL1_TO_IP)    $

NOTE: PATHIDX 4 is not supported in SN07.
```

30.5.2.4.6 Table release history update

New table in SN07.

30.5.2.4.7 Supplementary information

The following tuple will be created automatically for all Succession offices:

0 $

This will indicate the “nil path” that can be used in table NET2NET to indicate that two networks can be directed connected without the use of bridging resources.

Table 13 NETPATH Provisioning Restrctions

Field	Provisioning Restrictions
PATHIDX	• Counted tuple. Deletions not allowed if refenced by another table.
NETBRDGE	• The same bridge pool should not be in the list more than once. • Limit of 2 bridge pools in SN07. • Order of the bridge pools should be maintained. • Changes are allowed, and take effect immediately for all NET2NET tuples provisioned with this path. • The bridge pools must be listed in the order they will be traversed to go from one network to the other. The pools can be listed in either the forward or reverse direction.

Note: Allowing the NETBRDGE field to be changed allows this user to deload a particular IW SPM by creating another PATH with another NETBRDGE pool of the same type and assigning the desired SPMs to it. The CI tool IWBMCI:DBL can be used to validate when the deloaded SPM is no longer in use.

30.5.2.4.8 Translation verification other tools

NETPATH does not use translation verification tools.

30.5.2.5 Core Table NET2NET

Network interconnection.

30.5.2.5.1 Functional description

Tuples in this table define the allowable interconnections between networks, and the network path used to interconnect them.

Call processing will assume that any agents on the same network can be connected with one another.

Once the normal translations have occurred, a request will be made to connectivity to connect the agents.

- If the agents are on the same network, the connection request will proceed.
- If the agents are provisioned on seperate networks, connectivity will check table NET2NET to see if the connection is allowed.
  - — If the two networks are provisioned as connecting in the table, the NETPATH and associated bridge resources will be retrieved and the connection request will continue. If there are no idle members in the bridge groups, the connection request will then fail.
  - — If the two networks are not provisioned as connecting in the table, the connection request will fail immediately.
- In SN07, no mechansim is provided for choosing an alternate bridging path if the bridging resources are unavailable in the provisioned path.

30.5.2.5.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS, NETPATH

NET2NET

30.5.2.5.3 Size

Table 14 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NET2NET	0	7	Allocated upon first tuple entry.

30.5.2.5.4 Fields/OIDs

The following table lists fields/OIDs for NET2NET.

Each CONNNETS vector entry consists of:

- NET2NET - the interconnecting network
- NETPATH - reference to tuple in table NETPATH definining the path by which the two networks interconnect.

Table 15 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	BNETNAME defined in table BEARNETS	Identifies the name of the bearer network. Must be datafilled in Table BEARNETS first.
CONNNETS	New	No	Vector of connecting_network	Identifies a list of other bearer networks that are allowed to interconnect to this bearer network.
NET2NET	New	Field of connecting_network	BNETNAME provisioned in table BEARNETS	The interworking bearer network. Must be provisioned in Table BEARNETS first.
NETPATH	New	Field of connecting_network	Key to table NETPATH 0 - 255	Index into Table NETPATH.

30.5.2.5.5 Datafill example

The following example shows sample datafill for table NET2NET.

Figure 7 ENET/AAL1/IP NET2NET DatafillI

```
TABLE BEARNETS
NETIDX  BNETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $

TABLE CLLI
CLLI         ADNUM   TRKGRPSIZ    ADMININF
-----------------------------------------------
ENET_TO_IP   725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724     0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
-----------------------------------------------
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP           (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX          NETPATH
-----------------------------------------------
0               $
1               (ENET_TO_AAL1) $
2               (ENET_TO_IP) $
3               (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
BNETNAME        CONNNETS
-----------------------------------------------
TDM_ENET        (NET_ATM 1) (NET_IP 2) $
NET_ATM         (TDM_ENET 1) (NET_IP 3) $
NET_IP          (TDM_ENET 2) (NET_ATM 3) $
```

Figure 8 Enterprise/Carrier DatafilII

```
TABLE BEARNETS
NETIDX BNETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
CLLI         ADNUM   TRKGRPSIZ    ADMININF
-----------------------------------------------
ENET_TO_IP   725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724     0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
-----------------------------------------------
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX          NETPATH
-----------------------------------------------
0               $
1               (ENET_TO_AAL1) $
2               (ENET_TO_IP) $
3               (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
BNETNAME        CONNNETS
-----------------------------------------------
TDM_ENET        (NET_ATM 1) (NET_IP 2) $
NET_ATM         (TDM_ENET 1) (NET_IP 3) $
NET_IP          (TDM_ENET 2) (NET_ATM 3) $
NET_IPE         $
```

Note taht NET_IPE does not connect to NET_IP, even though they have the same FABRIC.

This is the SN07 configuration example to support Carrier Hosted Services (i.e. H.323 and Media Call Server 5200) via PVG looparounds.

Figure 9 Differet Networks, same Fabric

```
TABLE BEARNETS
NETIDX  BNETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
CLLI         ADNUM   TRKGRPSIZ    ADMININF
-----------------------------------------------
ENET_TO_IP   725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724     0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
-----------------------------------------------
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX          NETPATH
-----------------------------------------------
0               $
1               (ENET_TO_AAL1) $
2               (ENET_TO_IP) $
3               (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
BNETNAME        CONNNETS
-----------------------------------------------
TDM_ENET        (NET_ATM 1) (NET_IP 2) $
NET_ATM         (TDM_ENET 1) (NET_IP 3) $
NET_IP          (TDM_ENET 2) (NET_ATM 3) (NET_IPE 0)$
NET_IPE         (NET_IP 0) $
```

To interconnect two different networks on the same fabric, define a NETPATH that requires no bridges, and put entries in NET2NET using that path.

30.5.2.5.6 Table release history update

New in SN07.

30.5.2.5.7 Supplementary information

- NET2NET tuples will automatically be created with CONNNETS = $ whenever new networks are added to table BEARNETS.
- On an ONP, the interconnecting networks should be provisioned with the appropriate bridges automatically.

Table 16 NET2NET Provisioning Restrctions

Field	Provisioning Restrictions
BNETNAME	• Deletions are not allowed from this table. • User may change the tuple to the point that CONNNETS = $. Tuple deletions will be handled via table BEARNETS, and allowed only if CONNNETS = $.
CONNNETS	• Networks that connect only with themselves will have CONNNETS = $. All provisioned networks in table BEARNETS will be represented in this table. • The order of the entries is used during trunk member selection as the network preference order for trunk members when a member that is on the originating agent's network is not avaiable. The most efficient path is recommended to be provisioned first. • Adding a connecting network to a tuple should also add the connection to the tuple for the other network. This addition will be added to the end of the CONNNETS list of that tuple. • Deleting a connecting network from a tuple will also delete the interconnection from the connecting network's tuple. • Changes to NET2NET tuples will take effect immediately upon the change for all new connection requests. Used should be warned when removing an existing interconnection ability.
CONNNETS: NET2NET	• Valid BNETNAME from table BEARNETS. • Should not be the same as the key for the tuple. It is understood that a network can connect to itself. • A given network should appear in the connecting network list only once. • Changing the order will change the order of trunk member selection based on the network of the originating agent.
CONNNETS: NETPATH	• A valid PATHIDX from table NETPATH. • Path changes take effect immediately for new connection requests. Existing connections will continue with the old path until the connection has been released. • If NETPATH = 0 is specified, verify that the network FABRIC for both the BNETNAME network and the NET2NET network are on the same fabric. • Verify that once the starting end of the path is chosen based on the BNETNAME network, the path can then be traced in the appropriate direction to reach the CONNNETS network.

30.5.2.5.8 Translation verification other tools

NET2NET does not use translation verification tools.

30.5.2.6 Core Table MNNODE

Maintenance node table used to provision Spectrum nodes.

30.5.2.6.1 Functional description

Unchanged.

30.5.2.6.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

All existing dependencies, plus BEARNETS, NETBRDGE

MNNODE

All existing dependant tables.

30.5.2.6.3 Size

Table 17 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNNODE	Unchanged	Unchanged	Refer to the EI section of this document after DSUM complete.

30.5.2.6.4 Fields/OIDs

The following table lists fields/OIDs for MNNODE.

The following nodes provisioned in table MNNODE are impacted by these changes:

- Interworking bridges (NODEKEY=IW, DPT_INFO = BRDG_ONLY)
- DPT SPM (NODEKEY = IW, DPT_INFO = DPT_ONLY)
- MG4K (NODEKEY = SMG4)

Each of the applicable node type change is broken into it's own table below.

Table 18 Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged

Table 18 Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	**IW**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	**BRDG_ONLY**	Refinements created based on this field.
BRDGCLLI	**New**	**New subfield when DPT_INFO = BRDG_ONLY**	**List of BRDGCLLI (common_language_identifier) provisioned in table NETBRDGE**	**List of the supported bridge groups the bridges belong to.**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 19 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	**IW**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged

Table 19 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	**DPT_ONLY**	Refinements created based on this field.
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEINFO	Changed	IW refinement	**SMG4**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
EXECTAB	Unchanged	Unchanged	Unchanged	Unchanged
DPT	Unchanged	Unchanged	Unchanged	Unchanged
DPT_NUM_REQ	Unchanged	Unchanged	Unchanged	Unchanged
SLINK_THRESHOLD_DATA	Unchanged	Unchanged	Unchanged	Unchanged
BOOTP_SUPPRESS	Unchanged	Unchanged	Unchanged	Unchanged
REMOTE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**

30.5.2.6.5 Datafill example

The following examples show sample datafill for the affected nodetypes in table MNNODE.

Figure 10 Example Datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-------------------------------------------------
SPM  1 SPM_1  IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $(SYSB CR RPT)  (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT)(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

Figure 11 Example Datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM 1   SPM_1   IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $ (SYSB CR RPT)  (MANB MJ RPT)  (ISTB MN RPT)
(SYSBNA CR RPT)(MANBNA MJ RPT)  (DTMFLOW MN RPT)  (ECANLOW MN RPT)
(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN CR RPT)(SMCHLD MF
RPT)  (SMCHLD24 CR RPT)  $DPT_ONLY  (NET_AAL1 Y) $
(SPMECIDX 0)$
```

Figure 12 Example Datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM  1             SPM_1          SMG4   0   SYNC   LINE   50
(COT 60)  (DTMF 60)  (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT)  (MANB MJ RPT)  (ISTB MN RPT)  (SYSBNA CR RPT)(MANBNA MJ
RPT)  (COTLOW MN RPT)  (DTMFLOW MN RPT)(ECANLOW MN RPT)  (MFLOW
MN RPT)  (CMRLOW MN RPT)(TONESLOW MN RPT)  (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT)(ATMBCN CR RPT)  (STE3HLD MJ RPT)  (STE3HLD24
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  (SPMSRMNTD MN RPT)
(LOCUR MJ RPT)  (TMCFAIL CR RPT)  $ $  N  0  $  N  N  (NET_AAL1 Y) $
```

30.5.2.6.6 Table release history update

In SN07, The following mandatory fields were added:

- BEARNETS field added to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node.
- BRDGCLLI field added to IW BRDG_ONLY nodes to indicate the list of bridge groups the particular SPM node contributes to.

30.5.2.6.7 Supplementary information

- As of SN07, in order for interworking bridges to be utilized, the BRDGCLLI for the IW must be included in a NETPATH used to interconnect two networks in table BEARNETS.
- Terminations to DPT will dynamically match the network of the DPT SPM to the network provsioned against the terminating trunk group in table TRKOPTS to properly select a DPT "terminal" on the correct network.

Table 21 MNNODE IW bridg_only Provisioning Restrctions

Field	Provisioning Restrictions
BRDGCLLI	• Must be provisioned as a single entry in SN07. Cannot have either a nil vector or more than one provisioned. • Ensure the CLLI entered is a bridge clli. • Do not allow BRDGCLLI's where the NETBRDGE packet network fabric is not IP or AAL1. AAL2 is currently not supported by SPM nodes. • Changes are allowed only if the IW is OOS (MANB or OFFL). • On changes, compare the packet fabrics for the networks bridged by the BRDGCLLI. If the fabrics are different, then this means the network cards must be changed as well. Network cards should be removed prior to changing the BRDGCLLI, so a check is made that no network cards are provisioned if the packet fabrics that are bridged are different.

Table 22 MNNODE IW dpt_only Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT}	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network with an IP or AAL1 fabric. • For changes, the SPM must be OFFL and all DPT carriers must be INB. (from DPTTRM, pos spm no, bsy, bsy inb). • If the network fabric is changing, then the network cards must be removed before the change is allowed.

Table 23 MNNODE SMG4 Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network. • For changes, the SPM must be OFFL and all carriers must be INB. If DPT, then from DPTTRM, post spm no, bsy, bsy inb. If not DPT, then from TTP, post d <pm no>, bsy all, bsy inb all. • If the network fabric is changing, then the network cards must be removed before the change is allowed.

Generally, if the packet fabric for the IW is changing (whether a bridge or trunk members), then the following process must be followed to change the BEARNETS or BRDGCLLI provisioned:

- OFFL the SPM and bsy INB all carriers.
- Remove the network cards via table MNCKTPAK.
- Change the MNNODE BEARNETS or BRDGCLLI information.
- Add the correct circuit packs to MNCKTPAK (will be verified against the MNNODE datafill).
- RTS the SPM node.

30.5.2.6.8 Translation verification other tools

MNNODE does not use translation verification tools.

30.5.2.7 Core Table MNCKTPAK

Management Network Node Table

No sematice changes have been made to this table.

Additional validation checking has been added for when the GWM RM and ATM RM card provisioning, to ensure that the network implies by the card agrees with the bearer network provisioned against the node.

30.5.2.7.1 Supplementary information

Table 24 MNCKTPAK Provisioning Restrctions

Field	Provisioning Restrictions
CPKINFO - GEM card	• If SPM is IW brdg_only, ensure that at least one IP network is supported by the BRDGCLLI assigned. • If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is IP.
CPKINFO - ATM card	• If SPM is IW brdg_only, ensure that at least one AAL1 network is supported by the BRDGCLLI assigned. • If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is AAL1.

30.5.2.8 Core Table SERVRINV

Server Inventory

30.5.2.8.1 Functional description

A new field, BEARNETS is added to the SERVRINV table to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default.

In addition, DPT GWCs should not be provisioned with a bearer network, as it is a signalling only network element.

30.5.2.8.2 Usage sequence and implications (CM Only)

The following provisioning dependencies is added :

BEARNETS

SERVRINV

30.5.2.8.3 Size

Table 25 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	Unchanged	Unchanged	tbd

30.5.2.8.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 26 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SERVRNAME	Unchanged	Unchanged	Unchanged	Unchanged
SERVRADDR	Unchanged	Unchanged	Unchanged	Unchanged
SERVREXEC	Unchanged	Unchanged	Unchanged	Unchanged
SERVRTONE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.** **DPT GWC's should not be provisioned with a bearer network.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**

Table 26 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SERVROPTS	Unchanged	Unchanged	Unchanged	Unchanged

30.5.2.8.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Figure 13 Example Datafill

```
TABLE: MNNODE
SERVRNAME SERVRADDR SERVREXEC SERVRTONE BEARNETS SERVROPTS
-----------------------------------------------------------
GWC 0     IP  47 192 48 24 (POTS POTSEX)  (KEYSET  KSETEX)  $
NORTHAA (PACKET_DEFAULT Y) $ $
```

30.5.2.8.6 Table release history update

Added BEARNETS field in SN07.

30.5.2.8.7 Supplementary information

- SERVRINV is the bearer network provisioning point for the following nodes, if the BEARNETS field contains a default network. If the GWC does not have a BEARNETS entry, the office default (the tuple in table BEARNETS with the default_packet_network option assigned) will be taken as the bearer network for the following agents.
  - — IP trunking gateways (PVG, Audiocodes)
  - — Logical groups
  - — ABI lines and trunks
  - — H.323 & Media Call Server 5200
  - — UAS (for CALEA)
- DPT GWCs do not have a bearer network provisioning against them, as the DPT TIDs against the GWC do not have associated hardware. If a network is provisioned against DPT GWC, it will have no effect on call processing. DPT trunk groups get their bearer network from table TRKOPTS.
- It is assumed that SERVRINV will be provisioned via SESM, which will ensure that a default bearer network is added for non-DPT GWCs, and that no bearer network will be added to DPT GWCs. A warning message is output to the user when provisioning changes are made to SERVRINV warning of potential data corruption. This warning message already exists.

Table 27 SERVRINV Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT{	• BEARNETS does not apply if the GWC is a DPT GWC. • If a nil entry is added for a non-DPT GWC, the bearere network will be taken from the office default provisoned in table BEARNETS as the pkt_default_network. • Entry must either be assigned a “$” or a single BNETNAME marked as the default. • Changes require that the GWC be OOS (MANB or OFFL). • Non-DPT trunks must be BSY INB prior to change. • Allow changes to a non-nil BEARNETS field only if not DPT in SERVSINV. Allow deletion of BEARNETS entry only if DPT.

30.5.2.8.8 Translation verification other tools

SERVRINV does not use translation verification tools.

30.5.2.9 Core Table SERVSINV

Server Subtending Inventory

Table unchanged by this activity. Only additional provsioning consistency checks are added for use during an ONP.

30.5.2.9.1 Supplementary information

DPT terminal groups are signalling only, and do not have any physical hardware associated. The DPT trunk group, via provisioning in table TRKOPTS, contains the bearer network information, and DPT “terminals” can be associated with any bearer network provisioned against the trunk group, as long as the signalling type matches.

When transferring table data during an ONP for table SERVRINV, it is not known if the GWC is a DPT GWC, so the BEARNETS will be automatically set to the bearer network default. Therefore, the write procedure for table SERVSINV will be hooked to check whether or not a multinet upgrade is in progress for DPT GWCs (SIPT or BICC) and if it is, it will delete the BEARNETS entry for it’s host GWC.

30.5.2.10 Core Table TRKOPTS

Trunk Options.

30.5.2.10.1 Functional description

Unchanged.

30.5.2.10.2 Usage sequence and implications (CM Only)

The following dependency is added to the existing provisioning order:

BEARNETS

TRKOPTS

30.5.2.10.3 Size

Table 28 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	Unchanged	Unchanged	Refer to EI section after DSUM.

30.5.2.10.4 Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

```
>range
 1 OPTKEY            TRKOPTS_KEY
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
LOGICAL TUPLE TYPE: TRKOPTS_LOGICAL_TUPLE
>range 2
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
TYPE IS TRKOPTS_OPTINFO_VAR_AREA      MULTIPLE WITH
        OPTION                        TRKOPTS_OPTION REFINEMENTS:
{DYNAMIC}                             MULTIPLE WITH
      SIGNALING                       {ISUP,BICC,SIPT}
      SIGNALING_NETWORK               {IP,SS7,STRK}
      BEARER_NETWORK                  {IP,ATM,STRK}
      APPLICATION                     {OC,POS,DPT,RAS,SIPBCPT,STRK}
{DPT}                                 MULTIPLE WITH
      PROTOCOL                        {BICC,SIPT}
      BEARNETS                        {NETNAMES}
      PROTOCOL                        REFINEMENTS:
      {SIPT}                          MULTIPLE WITH
            NGSS                      MULTIPLE WITH
                NGSS_SELECTOR         {N,Y} REFINEMENTS:
                {Y}                   MULTIPLE WITH
                                      INTER_DOMAIN     {N,Y}
                {N}                   MULTIPLE WITH
                    DEST_MGCNAME      MGCINV_KEY
                    TPROFILE          TPROFILE_KEY
                    ALT_HOST_MGCNAME  VECTOR OF UP TO 32 CHAR'S
                    INTER_DOMAIN      {N,Y}
      {BICC}                          MULTIPLE WITH
            CAPABILITY_SET            {1 TO 2}
```

Table 29 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Unchanged	No	Unchanged	Unchanged
OPTINFO	**Changed**	**No**	**Add DPT to list of valid OPTIONs**	**Add DPT to list of valid OPTIONs**
OPTION	**Changed**	**Selector subfield of OPTINFO**	**DYNAMIC**	**Added new DPT option and refinement.**
SIGNALING	**Changed**	**Subfiled of DYNAMIC option**	**Changed**	**ISUPPLUS renamed to BICC**

Table 29 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SIGNALING_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
BEARER_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
APPLICATION	**Changed**	**Subfiled of DYNAMIC option**	**{OC, POS, RAS, SPBCPT, STRK}**	**DPT Removed from valid entry range. Should now be provisioned as a DPT option.**
OPTION	**Changed**	**Selector subfield of OPTINFO**	**DPT**	**Remove DPT from list of valid APPLICATIONs**
PROTOCOL	**New**	**Subfiled of DPT option**	**{BICC, SIPT}**	**The DPT signalling protocol.**
BEARER_NETWORK	**New**	**Subfiled of DPT option**	**BNETNAME from table BEARNETS**	**The BNETNAME of a bearer network provisioned in table BEARNETS.**
PROTOCOL	**New**	**Subfiled of DPT option**	**SIPT**	**Subfields when protocol = SIPT.**
NGSS	**NEW**	**Subfield of SIPT protocol**	**{N,Y}**	**Identifies if the new NGSS SIP architecture is being used**
INTER_DOMAIN	**New**	**Subfield of NGSS 'Y' selector**	**N, Y**	**Refer to activity a89007980.** **Indicates if the SIP-T trunks are inter-domain or intra-domain (between Nortel Networks equipment in the same addressable range).**
DEST_MGCNAME	**New**	**Subfield of NGSS 'N' selector**	**MGCINV_KEY**	**Enter the Media Gateway Controller (MGC) name from table MGCINV.**

Table 29 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TPROFILE	New	Subfield of NGSS 'N' selector	TPROFILE _NAME	Enter the telephony profile name from table TELEPROF.
ALT_HOST_MGCNAME	New	Subfield of NGSS 'N' selector	Vector of up to 32 chars.	Enter an alternative Media Gateway Controller (MGC) name.
INTER_DOMAIN	New	Subfield of NGSS 'N' selector	N, Y	Refer to activity a89007980. Indicates if the SIP-T trunks are inter-domain or intra-domain (between Nortel Networks equipment in the same addressable range).
PROTOCOL	New	Subfiled of DPT option	BICC	Subfields when protocol = BICC (old ISUPPLUS)
CAPABILITY_SET	New	Subfield of BICC protocol	{1 to 2}	This represents the BICC capability set (CS). If the remote switch (other side of the DPT trunk) is unable to supoort CS2 then datafill the CAPABILITY_SET as 1. If the remote switch can support CS2 then datafill CAPABILITY_SET as 2.

30.5.2.10.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

Figure 14 Example Datafill

```
TABLE: TRKOPTS
OPTKEY          OPTINFO
----------------------------------------
DPTTRK DPT      DPT BICC NET_AAL1 1 (100 200) (300 400) $ 200
SIPTRK DPT      DPT SIPT NET_IP N MGC2 PROF MGCTWO Y
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC $
```

30.5.2.10.6 Table release history update

- DPT is removed from APPLICATION field under the DYNAMIC option.
- DPT is added as a new OPTION.
- NGSS is added as a new selector field under the SIPT protocol

30.5.2.10.7 Supplementary information

The signaling network field is not required for DPT. The signaling protocol implies the signaling network: BICC implies SS7, and SIPT implies IP.

The bearer_fabric provisioned for DPT in table TRKOPTS indicates the bearer fabric for a specific DPT trunk group, and a given DPT trunk group can only have one bearer fabric.

GWC DPT trunk “agents” (provisioned in table SERVSINV) will be associated with the DPT trunk group during call processing based on the signaling protocol only. Bearer fabric is not provisioned against DPT GWCs in table SERVRINV.

SPM DPT trunk “agents” (provisioned in table MNNODE) will be associated with the DPT trunk group during call processing based on both the signaling protocol and the bearer network provisioned in table MNNODE.

The new NGSS (New Generation Session Server) selector identifies the SIP architecture used by the trunk group. When the new NGSS architecture is selected only INTER_DOMAIN data is necessary. However, when NGSS is not selected, the fields previously under the Dynamic tuple are required.

Table 30 TRKOPTS Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS	• BNETNAME must be provisioned in table BEARNETS. • Ensure compatibility of the signalling type with the fabric type of the bearer network. • Changes are allowed without restriction and will take effect immediately. Trunk members that are currently call processing will retain their existing network until the call is terminated.

Table 30 TRKOPTS Provisioning Restrctions

Field	Provisioning Restrictions
PROTOCOL	• Changes to the protocol field are not allowed for DPT.

30.5.2.10.8 Translation verification other tools

The following example shows the output from <ToolName> when it is used to verify <abbreviated name of table>.

<abbreviated name of table> does not use translation verification tools.

30.5.2.11 Core Tables OFRT, OFR2, OFR3, OFR4

Office Routing Tables

Same change applies to each

30.5.2.11.1 Functional description

Unchanged.

New CND/NOT selector condition of BEARNET, to allow conditional routing based on the originator's bearer network.

Changed the name of the PKT conditional selector to FABRIC, and increased the allowable FABRIC range from {ENET} to {ENET, AAL1, AAL2, IP}.

30.5.2.11.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

OFRT

30.5.2.11.3 Size

Not Changed

Table 31 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFRT	unchanged	unchanged	unchanged
OFR2	unchanged	unchanged	unchanged
OFR3	unchanged	unchanged	unchanged
OFR4	unchanged	unchanged	unchanged

30.5.2.11.4 Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for FABSEL.

If CND/NOT condition is BEARNET, will be prompted for NETSEL.

Table 32 OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT**~~, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT**~~, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
FABSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS

Table 32 OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

30.5.2.11.5 Datafill example

The following examples shows sample datafill for table OFRT.

Figure 15 CND BEARNET

```
TABLE OFRT
POS 99
100 (CND BEARNET DFLTTDM ST 901)
(CND BEARNET DFLTIP ST 902)
(CND BEARNET DFLTATM ST 903) $ $
```

Figure 16 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901)
   (CND FABRIC IP ST 902)
   (CND FABRIC AAL1 ST 903)
   (CND FABRIC AAL2 ST 904) $ $
```

30.5.2.11.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

30.5.2.11.7 Supplementary information

The above mentioned changes are applicable to all the routing tables OFR2, OFR3, OFR4, IBNRTE, IBNRT2, IBNRT3, IBNRT4 and HNPACONT$RTEREF that have CND and NOT bound in as the route selector.

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

30.5.2.11.8 Translation verification other tools

The following example shows the output from Traver when it is used to verify OFRT.

Figure 17 Traver example: with BEARNET Option

```
traver tr isupicitt 7211001 BEARNET MyAAL1NW b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
.  .  . SAME TABLE
 .  .  . 1002 S D ISUPITOG
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

30.5.2.12 Core Tables IBNRTn (IBNRTE, IBNRT2, IBNRT3, IBNRT4)

IBN Routing Table

30.5.2.12.1 Functional description

Unchanged

30.5.2.12.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

IBNRTE, IBNRT2, IBNRT3, IBNRT4

30.5.2.12.3 Size

Table 33 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNRTE	Unchanged	Unchanged	Unchanged
IBNRT2	Unchanged	Unchanged	Unchanged
IBNRT3	Unchanged	Unchanged	Unchanged
IBNRT4	Unchanged	Unchanged	Unchanged

30.5.2.12.4 Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for PKTSEL.

If CND/NOT condition is BEARNET, will be prompted for NETSEL.

Table 34 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			

Table 34 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~,** TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~**, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
NETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

30.5.2.12.5 Datafill example

Similar to the above examples.

30.5.2.12.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

30.5.2.12.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

30.5.2.12.8 Translation verification other tools

Refer to TRAVER information under table OFRT.

30.5.2.13 Core Tables HNPACONT::RTEREF and FNPACONT::RTEREF

Subtable Route Reference from the Home Numbering Plan Area

Subtable Route Reference from the Foreign Numbering Plan Area

Changes are the same as for OFRn and IBNRTn.

30.5.2.13.1 Functional description

Refer to OFRn.

30.5.2.13.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

HNPACONT::RTEREF & FNPACONT::RTEREF (order between these is unchanged)

30.5.2.13.3 Size

Table 35 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
HNPACONT::RTEREF	Unchanged	Unchanged	Unchanged
FNPACONT::RTEREF	Unchanged	Unchanged	Unchanged

30.5.2.13.4 Fields/OIDs

Same changes as table OFRn.

30.5.2.13.5 Datafill example

Refer to table OFRn.

30.5.2.13.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

30.5.2.13.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

30.5.2.13.8 Translation verification other tools

Refer to OFRn.

30.5.2.14 GWC_NETWORK_CODEC_PROFILE

30.5.2.14.1 Functional description

This new table is used to store network codec profiles that created by customer. The profiles will be used when customer add GWC node. Please refer to DID document for details.

30.5.2.14.2 Fields

The following table lists fields of this table.

Table 36 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
profilename	New	VARCHAR2 (32)	The name of the profile. It is not allow to be NULL. This field is the primary key of this table.
bearerpath	New	NUMBER	Indicates the bearer network fabric type. Refer to table “BEARERPATH_MAP“. The default value is “0”.
defaultcodec	New	NUMBER	Indicate the default codec. Refer to table “CODEC_MAP“. The default value is “0”.
preferredcodec	New	NUMBER	Indicate the preferred codec. Refer to table “CODEC_MAP“. The default value is “0”.
alternativecodec	New	NUMBER	Indicate the alternative codec. Refer to table “CODEC_MAP“. The default value is “0”.
packetizationinteger	New	NUMBER	Indicate the packetization rate. Refer to table “PACKETIZATION_MAP“. The default value is “0”.
t38	New	NUMBER(1)	Indicate whether the T38 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.

Field	New/ Changed	Entry	Explanation and action
rfc2833	New	NUMBER(1)	Indicate whether the RFC2833 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
comfortnoise	New	NUMBER(1)	Indicate whether the comfort noise setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
bearertypedefault	New	CHAR(1)	Indicate whether this profile is a default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is default profile for this bearer network type, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 default profile every bearer network fabric type.
networkdefault	New	CHAR(1)	Indicate whether this profile is network default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is the default profile in network, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 network default profile totally.

30.5.2.15 GWCPROFILE

30.5.2.15.1 Functional description

This table is used to store attributes of Gateway Controller profile. One new field will be added into this table, which is used to indicate whether network instance is needed to be associated to this GWC or not.

30.5.2.15.2 Fields

The following table lists the new field of this table.

Table 37 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_INSTANCE_REQUIRED	New	CHAR(1)	Indicate whether network instance is needed to be associated to this GWC or not. Available values are “Y” and “N”. Char “Y” indicates need, char “N” indicates not need. The default value is “Y”. This field can not be NULL.

30.5.2.16 GATEWAYPROFILE

30.5.2.16.1 Functional description

This table is used to store attributes of Gateway profile. One new field will be added into this table, which is used to enhance the fabric type check when customer associate gateway to GWC node. Please refer to DID document for details.

30.5.2.16.2 Fields

The following table lists fields of this table.

Table 38 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_FABRIC_RESTRICTION_LIST	New	Embedded table of "RestrictList_NT" type	The Name of this field is: Bearer fabric restriction list. This field can be NULL. This field would list the bearer fabrics to which the gateway is restricted. In most cases, this list will be empty and there will be no restriction. But for some special gateway (e.g. MG9000IP and ATM versions), the values would be provided.

30.6 Service Orders (SO) (CM & SESM)

Not applicable.

30.7 Software optionality control (SOC)

Not applicable.

30.8 Element Management

Prior to SN07, the SESM server could support only one bearer network fabric type (IP/AAL1/AAL2) at one time. As of SN07, each GWC will be associated with a beaer network instance, which defines the associated bearer network fabric type. This information will be provided by the customer as they add the GWC through the GWC-EM. In addition to the beaer fabric instance, GWC-EM will allow the cutomer to define multiple network codec "profiles" in the system and will allow the customer to select the desired profile as they add the GWC to the network.

30.8.1 New/modified GUIs

Table 39 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC-EM	Changed

30.8.2 GUI information

30.8.2.1 GWC-EM GUI

Gateway Controller Element Manager Graphical User Interface

30.8.2.1.1 Functional description

The GWC-EM database will be changed to include a new MIB table: GET_NETWORK_CODEC_PROFILE.

The following functionality is added to the GWC-EM:

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
   - — Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
   - — Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
   - — Change the associated network codec profile of one GWC node from GWC-EM GUI.

30.8.2.1.2 GUI usage and implications

GUIs must be used in the following sequence:

Current datafill order unchanged.

30.8.2.1.3 GUI size

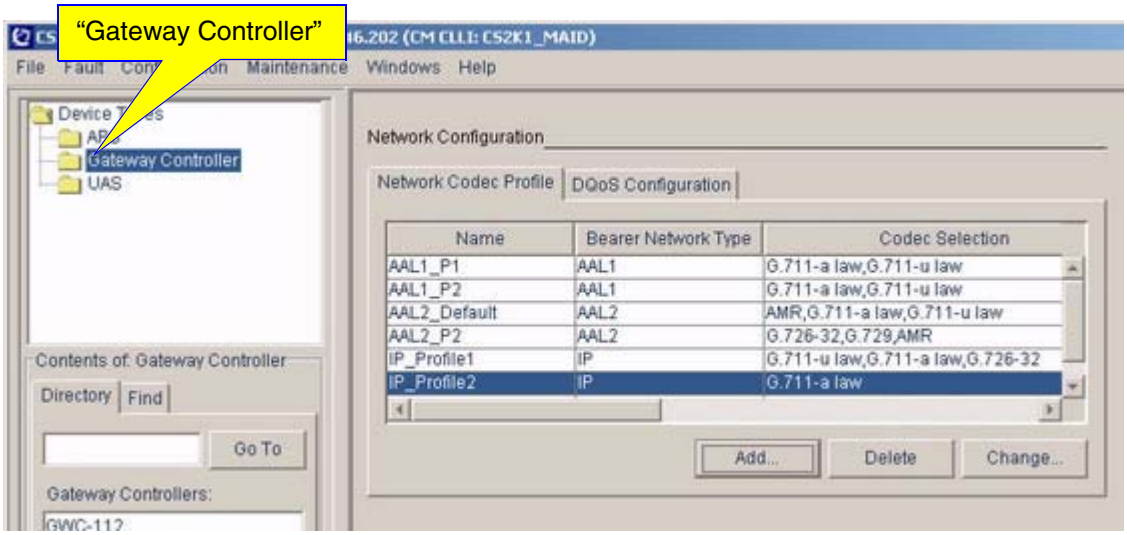
Table 40 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWC-EM	Unchanged	Unchanged	Unchanged

30.8.2.1.4 Usage Example: Display network codec profile

When customer click the “Gateway Controller” type from the device type tree at the left side, all network codec profiles will be displayed on the right side. (Please refer to “Figure 13 Network codec profile display panel”)

Figure 1 Network codec profile display panel



All existing codec profiles will be displayed in a table, each profile includes following parameters:

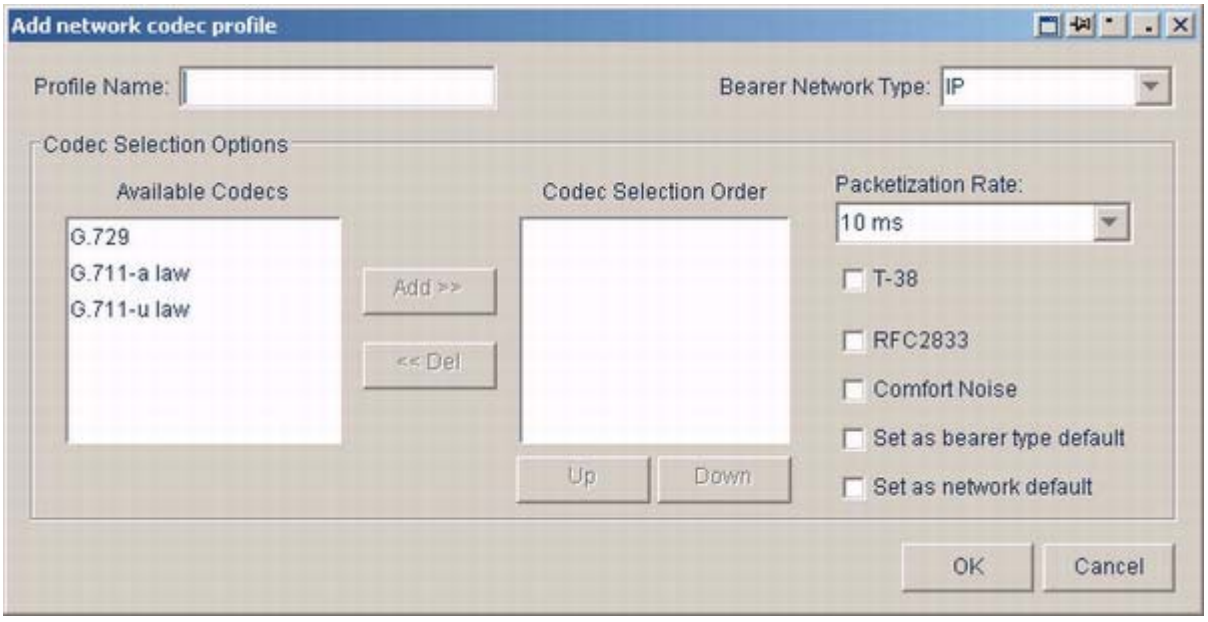
Table 1 Parameters of network codec profile

Parameter name	Description	Notes
Name	The name of the profile.	
Bearer Network Type	Indicates the bearer network fabric type.	
Codec Selection	Indicate the codecs used in this profile.	
Packetization rate	Indicate the packetization rate.	For IP bearer type only.
T-38	Indicate whether the T38 setting is enabled.	For IP bearer type only.
RFC2833	Indicate whether the RFC2833 setting is enabled.	For IP bearer type only.
Comfort noise	Indicate whether the comfort noise setting is enabled.	For IP bearer type only.
Default Profile	Indicate whether this profile is a default profile. Please note that there will be up to 1 default profile every bear network fabric type.	

30.8.2.1.5 Usage Example: Add network codec profile

Customer will be able to add one new network codec profile just by clicking the “Add” button, then a dialog “Add network codec profile” will be popped up. (Please refer to “Figure 14 Add network codec profile dialog”)

Figure 2 Add network codec profile dialog

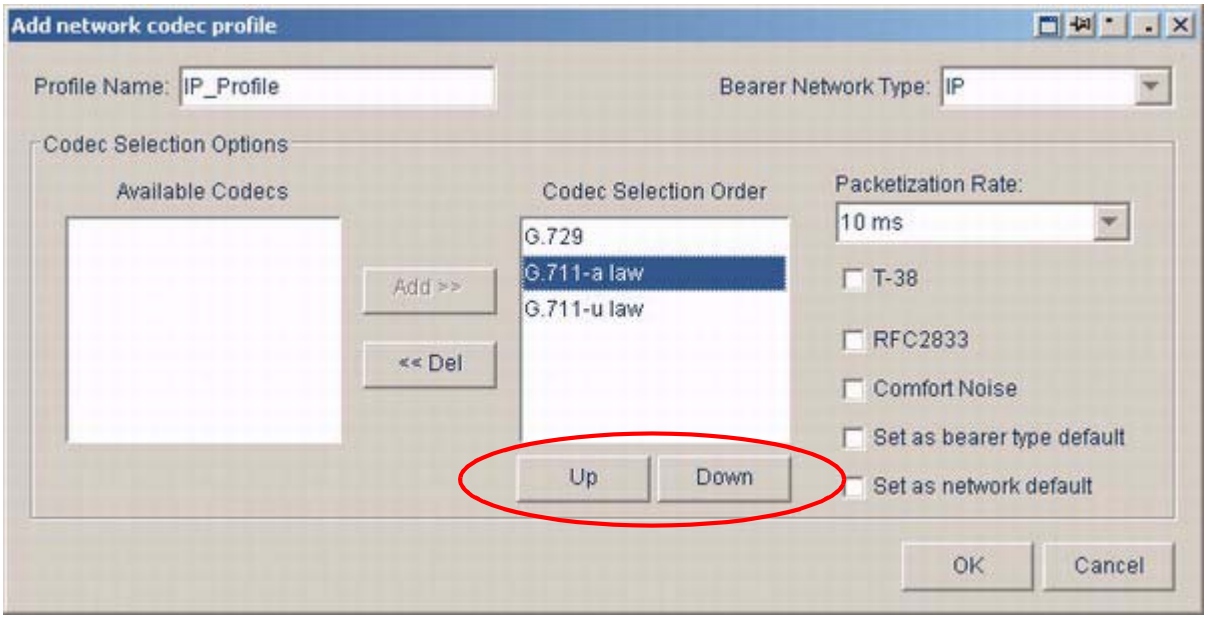


When customer select a bearer network type from the droplist box, the corresponding available codecs will be displayed below in the left list box. The available codec list may be different for different bearer network type.

Please note that the codec selecting is different from SN06 version. Customer won't select different codec for “Compression codec”, “Default codec” and “Alternative Codec” one by one. The available codecs will be listed at left side, customer should be able to select them just by highlighting codec item and clicking the “Add >>” button. Then the selected codec will be added into codec selection. Contrarily, customer could delete some codec from the selection by highlighting the codec item and clicking the button “<< Del”.

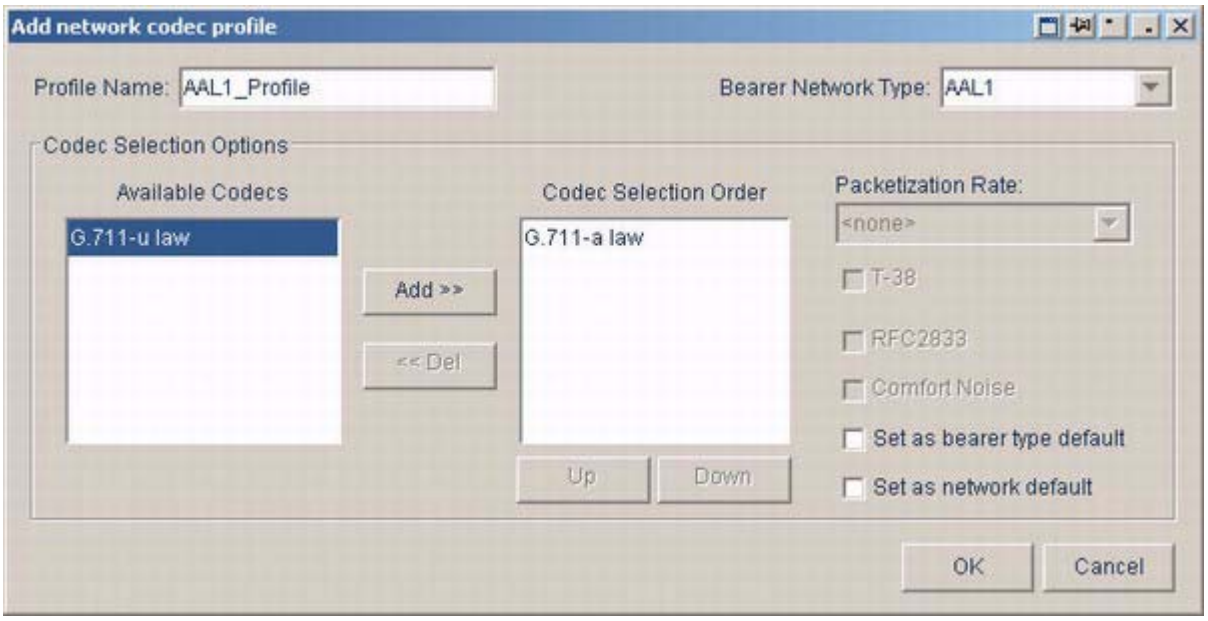
In the codec selection, the order of the codec determines how the device will treat them. For example, the first one will be mapped to “Compression codec”, the second one will be mapped to “Default Codec”, and the last one will be mapped to “Alternative Codec”. Additional, customer could change the order of codecs by highlighting the codec item and clicking the “Up” and “Down” buttons.

Figure 3 Change the order of codecs in the selection



Please note that parameters “Packetization Rate” and LCO options (T38, RFC2833, and Comfort Noise) are settings for IP bearer type only. If customer select “AAL1” or “AAL2” as the bearer network fabric type, these settings will be disabled.

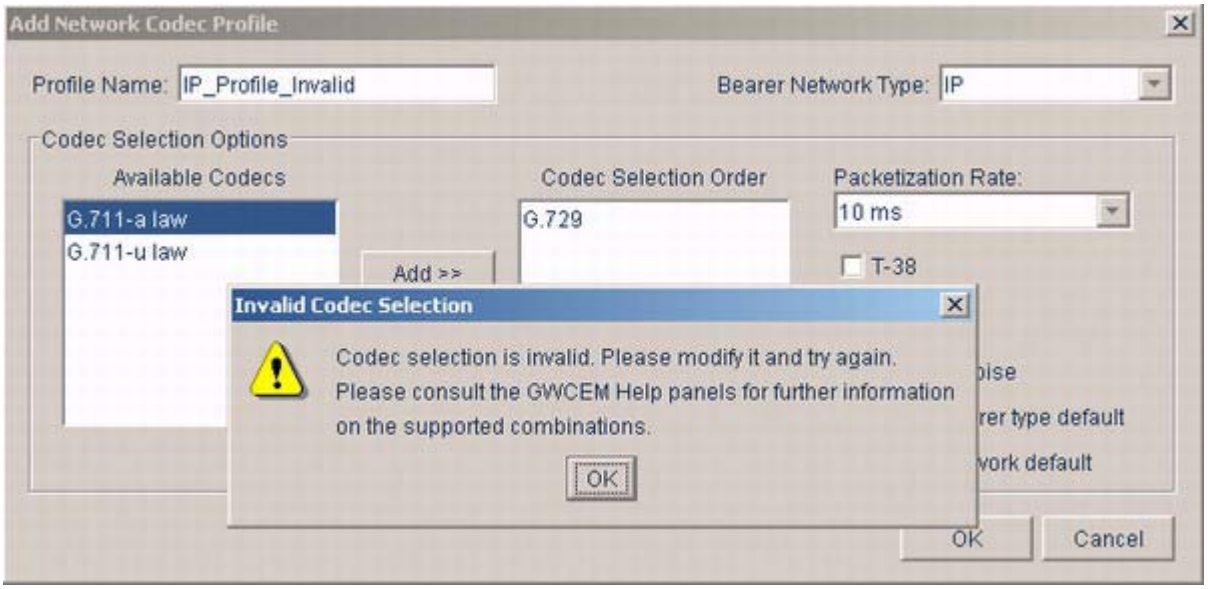
Figure 4 Select “AAL1” as the bearer network fabric type



Customer will be able to use the recommended codec setting by clicking the button “Recommended Codec Setting”, then the recommended setting will be restored into the dialog. Note that the recommended codec setting will be different for different bearer network type.

If customer select an invalid codec selection, alert dialog will be popped up. (Please refer to “Figure 17 Alert dialog for invalid codec selection”)

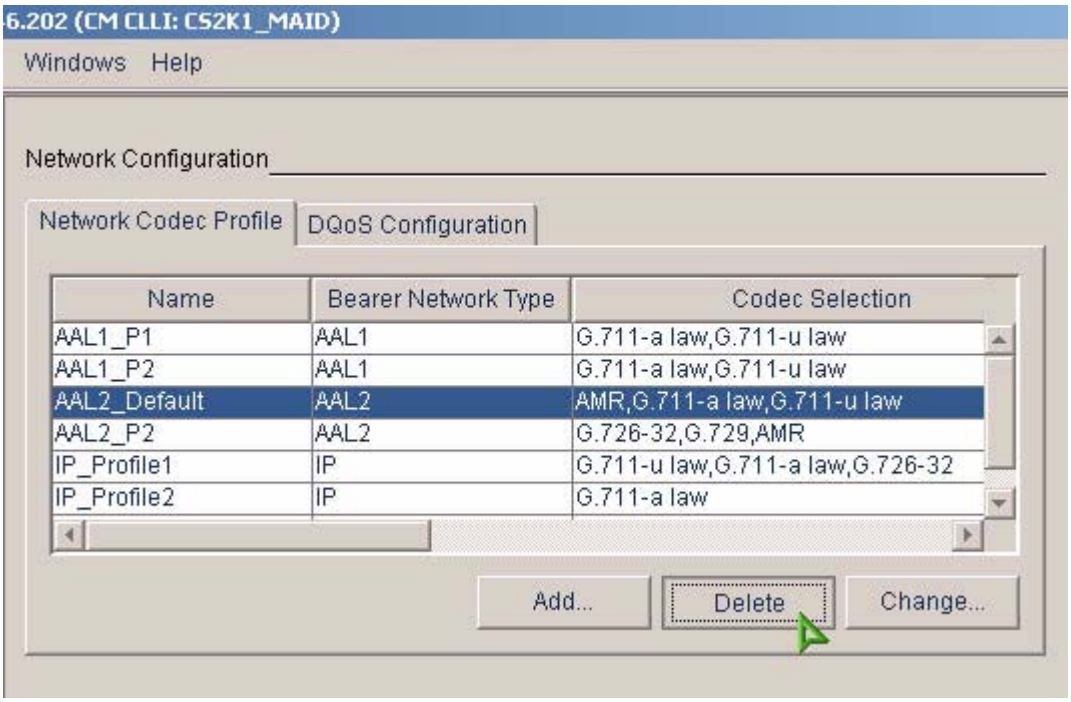
Figure 5 Alert dialog for invalid codec selection



30.8.2.1.6 Usage Example: Delete network codec profile

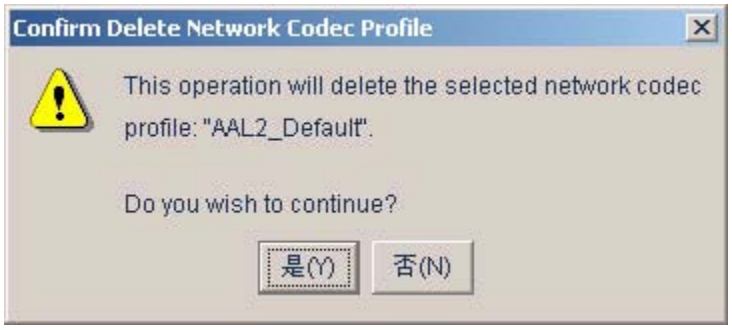
Customer will be able to delete one existing network codec profile just by highlighting the profile row from the table, and click the “Delete” button. (Please refer to “Figure 18 Delete existing network codec profile”)

Figure 6 Delete existing network codec profile



Once customer click the “Delete” button, one confirmation dialog will be popped up.

Figure 7 Delete network codec profile confirmation dialog

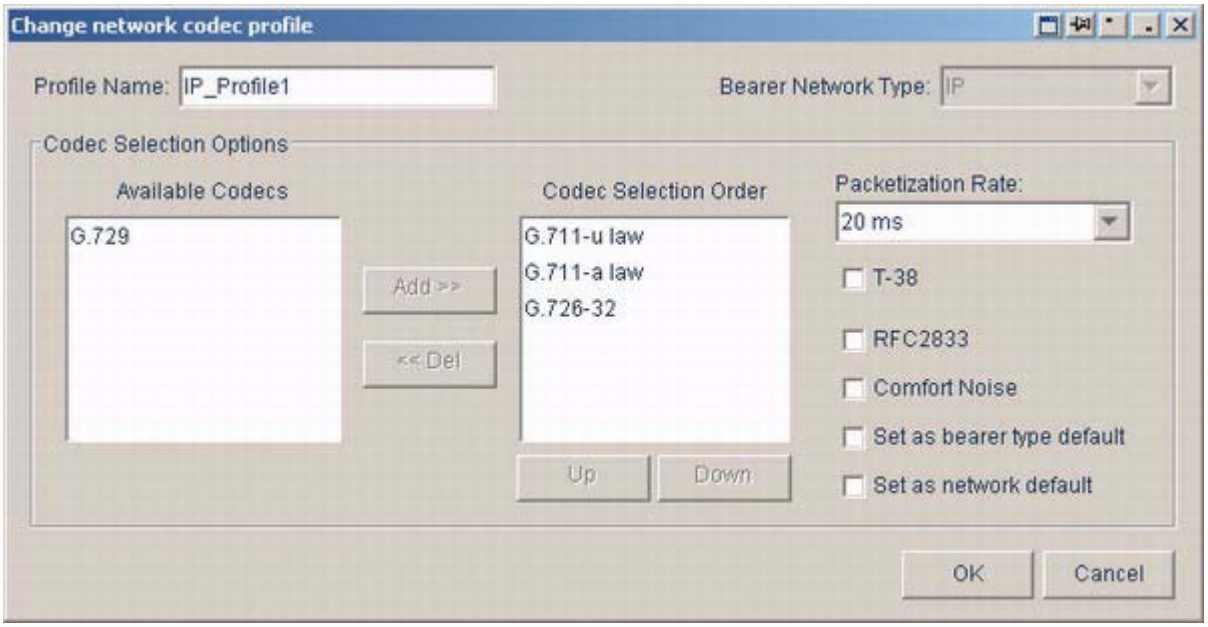


The operation result will be displayed in a pop-up dialog, and the codec profile table will be updated according to the result. Please note that if any GWC using this profile, the delete operation will be failed.

30.8.2.1.7 Usage Example: Change network codec profile

Customer will be able to change one existing network codec profile just by highlighting the profile row from the table, and click the “Change” button. Then the dialog “Change network codec profile” will be popped up. All parameters of the profile will be filled in the dialog. (Please refer to “Figure 20 Change existing network codec profile”)

Figure 8 Change existing network codec profile

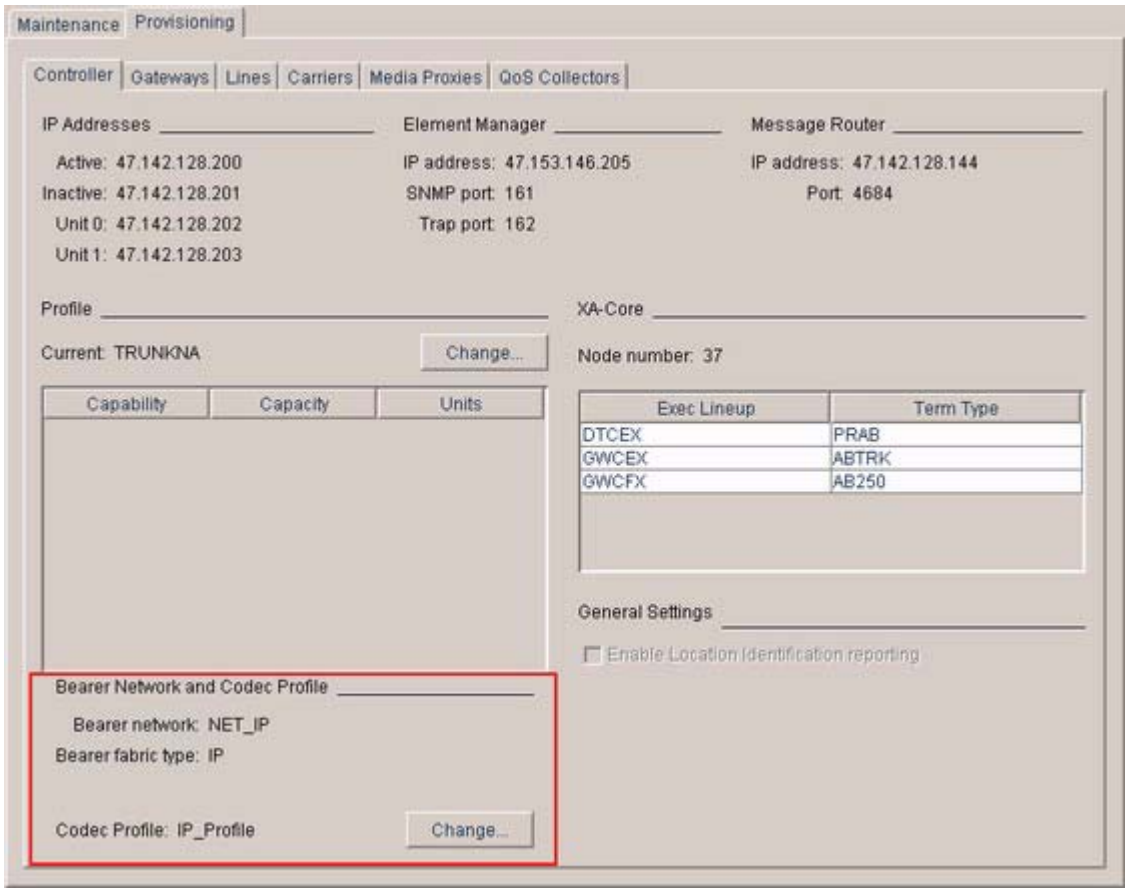


Note that the bearer network type of the profile is not allowed to be changed. Please refer to "32.8.2.1.5 Usage Example: Add network codec profile" section for how to change other parameters. Once the profile was updated successfully, these parameters will be updated into all GWCs using this profile.

30.8.2.1.8 Usage Example: Display GWC node

A new section will be added to the GWC provisioning panel to indicate the bearer network and codec profile configuration for the selected GWC.

Figure 9 Display GWC node



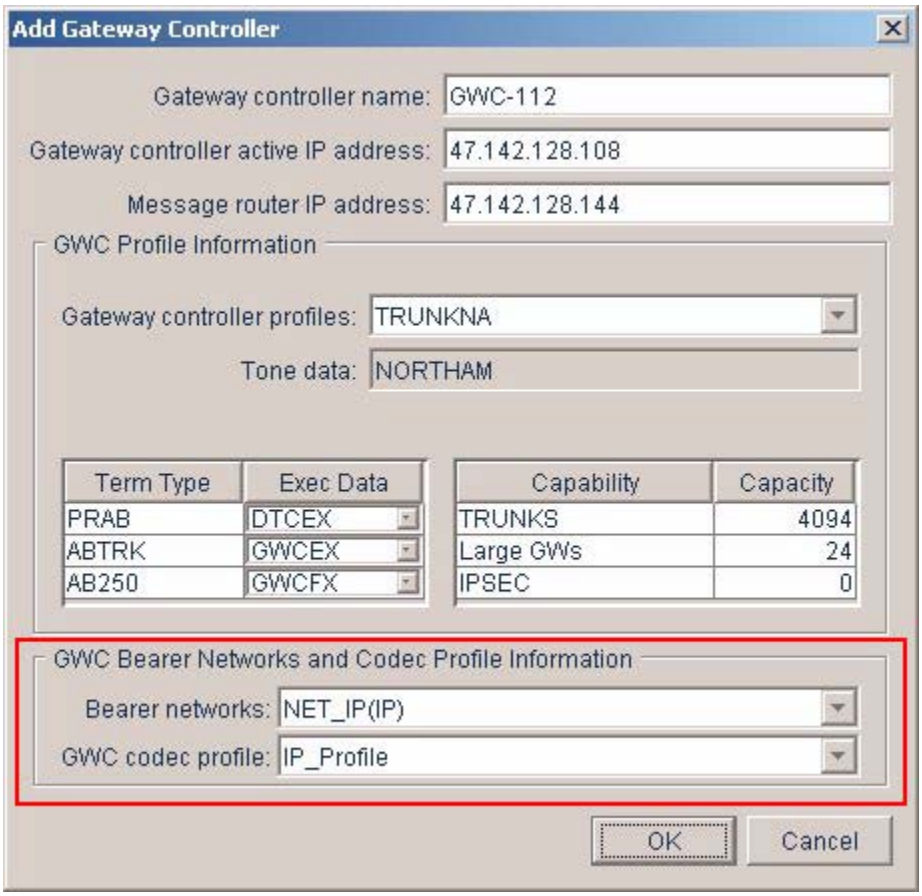
The new section includes two part, one is bearer network area and another is codec profile area. A “Change...” button will be added to the right of the codec profile fields to allow customer to change the codec configuration for the GWC.

This information will be displayed on the GUI with other GWC’s informations together while customer select a GWC from the GWC device list tree.

30.8.2.1.9 Usage Example: Add GWC node

Two new list boxes will be added to the “Add GWC Node” dialog to allow customers to select a specific bearer network instance and codec profile while a GWC is adding to the system.

Figure 10 Add GWC node



One of these two new box contains the bearer network list, another contains the codec profile list. The codec profile list must match the bearer network, that means, if customers select a bearer network instance belonging to “IP” bearer type, then the codec profile box will only contain the names of “IP” codec profiles; if customer select a “AAL1” bearer network instance, the codec profile box will be changed to only contain the “AAL1” codec profile names.

And if customers leave the codec profile box not selected, a default codec profile based on the bearer network type will be selected automatically.

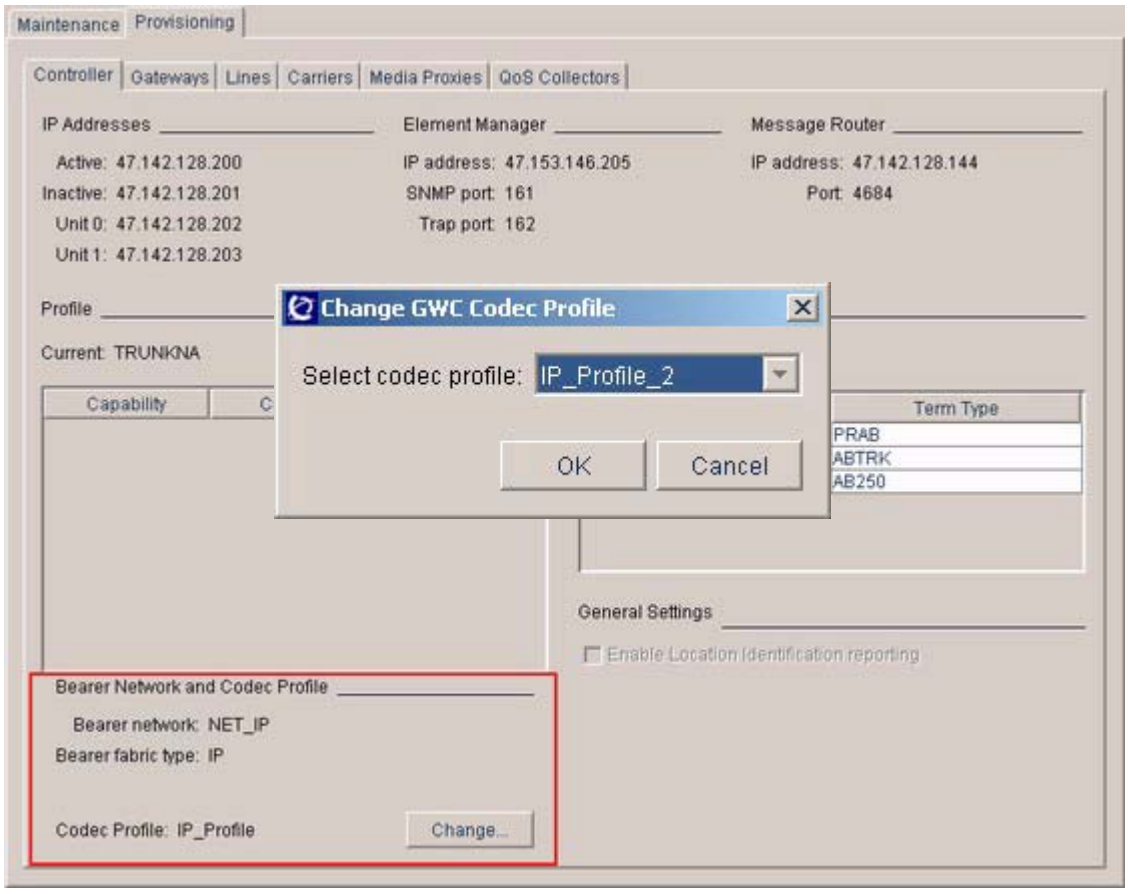
Once the addition operation has been performed successfully, a dialog like following will be pushed to the customer to indicate that the GWC was added to the system without errors.

Figure 11 Add GWC node result dialog

30.8.2.1.10 Usage Example: Change GWC network codec profile

When customers click the “Change...” button on the right of the codec profile fields on the GWC provisioning panel, a “Change Codec Configuration” dialog will be created like the following figure.

Figure 12 Change GWC's network codec profile



From this dialog, customers can select a different codec profile for the specific GWC even after the GWC has been provisioned already and a dialog with successful information will be displayed for customers if the operation has been performed without errors. Otherwise, a error message will be returned to the customers.

30.8.2.1.11 GUI release history update

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.

2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
   - — Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
   - — Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
   - — Change the associated network codec profile of one GWC node from GWC-EM GUI.

30.8.2.1.12 Supplementary information

30.9 Command interface changes

30.9.1 Directory: TRAVER

30.9.1.1 Directory description

TRAnslations VERification.

30.9.1.2 Accessing directory: TRAVER

30.9.1.2.1 Access to directory or MAP level and return to CI

CI> TRAVER <traver options>

Traver is a single command interface rather than an envirnment that is entered. You are automatically returned to the CI level after execution of the command.

30.9.2 Command: TRAVER TR

30.9.2.1 Command type: unchanged

30.9.2.2 Command target: unchanged

30.9.2.3 Command availability: unchanged

30.9.2.4 Command description

Traver an originating trunk based with the digits provided. The originating trunk (TRAVER TR) command is changed as follows:

When encountering a CND FABRIC or CND BEARNET selector in the translations route, three options are created for determining the originator's bearer fabric or network in order to determine how to interprete the CND route selection.

- TRKMEM option: The fabric or network of the member specified will be used.
- NEW BEARNET option: Allows the user to specify the bearer network (32 char vector identifying a BNETNAME provisioned in table BEARNETS) of the specifified trunk group.
- If none of the above options is specified, the TDM network will be assumed for the specified trunk group for non-DPT trunk groups.
- For DPT trunk groups, where none of the above options is specified, the bearer fabric or network will be obtained from table TRKOPTS.

30.9.2.5 Command syntax

Table 41 <CommandName> command parameters and variables

Command	Parameters and variables
TRAVER **TR**	Next par is: <CLLI> STRING Enter: <CLLI> [<CLLIOPT>] [<MBGOPTS>] [<TRIGOPT>] **[<TRKMEM>] [<BEARNET>]** <DIGITS OR N FOR NO DIGITS> [<CDNIE>] [<NSF>] [<TNSIE>] [<OSAIE>] [<BC>] [<SR>] [<PI>] [<TRI>] [<NETINFO>] [<FINFO>] [<RPOAP>] [<RPOAS>] [<NOA>] [<AIN_OPTIONS>] [<AIN_INFO>] [<SCAIIN>]
Parameters and variables	Description
[<TRKMEM>}	Existing option. Input is unchanged. Will now be used to obtain the bearer network and bearer fabric to be used when making conditional translations decisions CND FABRIC or CND BEARNET.
[<BEARNET>]	New option. Allows user to specify the bearer network (up to 32 character BNETNAME provisioned in table BEARNETS) to use as the originating bearer network. This will also imply the FABRIC, since the FABRIC is a field in table BEARNETS. Both of these will be used when making conditional routing decsions based on FABRIC or BEARNET (CND selectors). The network specified will be used, even if the trunk group does not have members on that network.

30.9.2.6 Qualifications and warnings

- Non-DPT trunk groups can have members that are spread across the varioius networks. During call processing, an effort will be made to match the originator’s network to a trunk member of a like network. Traver will not be enhanced to show this selection process.

- Line group originations (eg: HUNT, MDN, ACD) will use the network fabric of the originating member of the group to determine the network fabric.
- If the FABRIC or BEARNET option is used to specify the bearer network information of a trunk group, this information will be used in TRAVER to determine the routing, even if the trunk group does not have members in that network. This allows users to test the translations before adding members, but also allows for verification to pass when during call processing it could actually fail.

30.9.2.7 Responses

30.9.2.7.1 Undefined BEARNET specified

Since the user will be prompted for a 32 character string rather than a list of tuples provisioned in table BEARNET, an invalid entry should be met with a response indicating where to look for the valid information.

Table 42 MAP outputs with associated meanings and actions

Command TRAVER TR <trunk group CLLI> <digits> BEARNET <BNETNAME>
<RESPONSE>: <description> **Meaning:** The BEARNET name entered does not exist in table BEARNETS. **System or user actions:** Choose a BNETNAME of out table BEARNETS.
<RESPONSE>: <description> **Meaning:** **System or user actions:**

30.9.2.8 Example of TRKMEM option

Table 43 Usage examples for TRAVER TR command with TRKMEM option

Description of task:	`traver tr isupicitt 7211001` **`TRKMEM 1001`** `b`
Description of task	`Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the trunk member data.`

Table 43 Usage examples for TRAVER TR command with TRKMEM option

Command: MAP response:	WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 $. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 **. . CND BEARNET MYAAL1NW ST 1003** **. . . SAME TABLE** **. . . 1003 S D ATMTRK1** **. . . EXIT SAME TABLE** . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT ... ... AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++

Table 44 Usage examples for TRAVER TR command with BEARNET option

Description of task:	traver tr isupicitt 7211001 **BEARNET MyAAL1NW** b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing ‘7211001’ where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the BEARNETS MyAAL1NW tuple entry.

Table 44 Usage examples for TRAVER TR command with BEARNET option

Command: MAP response:	WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 $. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 **. . CND BEARNET MYAAL1NW ST 1003** **. . . SAME TABLE** **. . . 1002 S D ISUPITOG** **. . . EXIT SAME TABLE** . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT ... ... AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++

Table 45 Usage examples for TRAVER TR command with FABRIC option

Description of task:	traver tr isupicitt 7211001 **FABRIC AAL1** b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing ‘7211001’ where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be the TDM BEARNET and the AAL1 FABRIC.

Table 45 Usage examples for TRAVER TR command with FABRIC option

Command:
MAP response:

```
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN
N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND FABRIC AAL1 ST 1002
 .  .      CND FABRIC ENET ST 1003
.  .  . SAME TABLE
 .  .  . 1002 S D ISUPITOG
 .  .  . EXIT SAME TABLE
 .  .      CND FABRIC IP ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

30.10 Security

30.11 Configuration Walkthrough

31: Configuration (CN): A00003486

31.1 Hardware and Software Requirements

The changes provided by this feature will allow the customer to physically identify ABI configured hardware components hosting ABI lines from the Core when trouble shooting their network. This enables quick problem resolutions. These Core changes provide:

- MG9K Frame/Shelf physical location data for MG9Ks hosting ABI lines
- Changes to the Mapci QueryPM application to make use of this data

Therefore the following hardware needs to be in place prior to exercising the software provided by this feature. The software is exercised by provisioning the physical location data of these hardware components:

- A typical ABI configuration

Software Requirements:

- SN07 Succession Core load or later

31.2 Initial Configuration

As a provisioning component of the Succession program, much of this functionality performs as designed without the hardware being in place. However, to provision actual physical location data, the provisioning of the configurations mentioned in “31.1 Hardware and Software Requirements” on page 2752 should be installed.

Once the hardware is installed and the software is available, provisioning of the physical location data can begin. The ABI Gateway and its location data is provisioned in table GATWYINV. This is a new table as of SN07. The steps to perform the provisioning are described in section “31.5 Data schema (DS) (CM, MIBS, RDB)” on page 2753.

31.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

31.4 Upgrade Impact

31.4.1 Dump and Restore

Table GATWYINV will use the existing data transfer “TabXfr” mechanism available to all Table Control tables to preserve its data during an upgrade. Because this is a new table as of SN07, there will be no data to preserve.

Due to the changes to table LTCINV for the ABI XPM tuples, data preservation for these tuples will occur when upgrading from any prior release which could contain ABI XPM datafill (SN05 or later) to the SN07 release. This means entries will be created in table GATWYINV when processing table LTCINV to preserve the ABI XPM datafill. Because the new GATWYINV table has much more configuration information available than what is provisioned against the ABI XPMs, much of the data will be defaulted. Therefore, once the upgrade is complete, the customer is expected to modify the newly created data in table GATWYINV to provide more accurate information than could possibly be provided during the upgrade.

31.4.2 Element Management Upgrade

Not applicable.

31.5 Data schema (DS) (CM, MIBS, RDB)

31.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	Changed	Unchanged
GATWYINV	New	New Table Control

31.5.2 Table LTCINV Database Schema information

31.5.2.1 Name: LTCINV

Long Table Name: Line Trunk Controller INVentory

31.5.2.1.1 Functional description

Table LTCINV contains the inventory data, except P-side link assignments, for various host peripheral module (XPM) types. This feature will only impact ABI XPM tuples. The change impacts the datafill associated with the ABI (EXTDS512) option. The change is to move most of the option datafill to table GATWYINV and replace the data with a key to the ABI gateway. Please refer to “Table 3 Table LTCINV changed field descriptions” on page 2755.

31.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table SERVRINV - GWC datafill, no change

2. Table SERVSINV - AUD datafill, no change
3. Table GATWYINV - New table, Gateway datafill. Dependencies on both SERVRINV and SERVSINV.
4. Table LTCINV - Dependency on GATWYINV for ABI XPM tuples
5. Table SERVCONN - ATM server connection datafill, no change

31.5.2.1.3 Size

No change in the maximum number of tuples for table LTCINV.

Table 2 Table LTCINV size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	0	210	Memory is automatically allocated in increments of 10 XPMs at a time up to a maximum of 210 tuples.

31.5.2.1.4 Fields

The following table lists impacted fields for Table LTCINV.

Table 3 Table LTCINV changed field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTATTR	Changed	Modified the EXTDS512 refinement, add 1 new subfield and deleted 4 existing subfields	GTWY_HOST (added)	New field, This field contains the data which points to an entry in the new GATWYINV table. Made up of two sub-fields: GWTYPE GW_TYPE GWNO {0 TO 1023}
			NE_NBR (deleted)	GW_NETWORK_ELEMENT _NUMBER_RANGE - This field is deleted. The data is now available in table GATWYINV.
			ABI_SLOT_NBR (deleted)	ABI_SLOT_RANGE - This field is deleted. The data is now available in table GATWYINV.
			IPADDR (deleted)	TABLE OF 4 {0 TO 255}'s - This field is deleted. The data is now available in table GATWYINV.
			GWC_HOST (deleted)	Made up of two sub-fields: PMTYPE PM_TYPE PMNO {0 TO 255} - This field is deleted. The data is now available in table GATWYINV.

31.5.2.1.5 Datafill example

The following example illustrates the changed prompting sequence for the EXTDS512 option in table LTCINV.

Figure 1 Prompting sequence for the modified option EXTDS512

```
>add lgc 1 7 lgci 0 32 1 D 33 6x02na qli16at pots potsex keyset ksetex $ $ msg6x69 isp +
16 $ northaa sx05aa $ sx05aa $ 0 sxfwaj01
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y

OPT_ATTR:
>asdfd
 ***  ERROR  ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
OPT_ATTR:
>asdfd
 ***  ERROR  ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
TYPE                                IS                                LTCINV_OPT_ATTR
{CCS7,STRBBF,STRDTRE,STRN5,FSTR2,PCM30,NX64,METER,
                FLS,OC,FDCP,EXTDS512}
OPT_ATTR:
>extds512
SITE:
>cary
>GTWY_HOST
>ABI 5
>$
PEC6X40:
>6X40FA

... << continue with normal datafill for LTCINV >>
```

Figure 2 on page 2582 shows the changes to the OPTATTR field with the new gateway field ranges for the optional refinement EXTDS512.

Figure 2 Range Values for new Gateway PM datafill in option EXTDS512

```
>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
>range optattr
18 OPTATTR          LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
      OPT_ATTR            LTCINV_OPT_ATTR REFINEMENTS:
      {EXTDS512}          MULTIPLE WITH
         SITE             CHAR_VECTOR VECTOR OF UP TO 16 CHAR'S
         GTWY_HOST        GW_KEY  MULTIPLE WITH
            GWTYPE        GW_TYPE
            GWNO          {0 TO 1023}
      OTHERWISE           LTCINV_OPT_ATTR_NIL_DATA
```

Figure 3, on page 2583 provides a view of the successfully added tuple with the new Gateway data fields for option EXTDS512.

Figure 3 Sample LTCINV Tuples with new Gateway fields for option EXTDS512

```
>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB
CSLNKTAB OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
-----------------------------------------------------------------------------------------------------------------------
LGC 1 1002 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) $ (4 0)(4 1)(4 2)(4 3) $ (MSG6X69)
$ NORTHAM SX05AA $ SX05AA $ 0 SXFWAE08 (EXTDS512 CARY ABI 5) $ 6X40FA N

SMA2 2 1009 LTE 1 51 2 E 31 MX85AB QLI17AY1 (POTS POTSEX) $ (4 4) (4 5)(4 6) (4 7) $ (UTR6)
(MSGMX76 HOST ) (ISP 4) $ NORTHAM AX74AA AX74AA 0 SXFWAE08
(EXTDS512 GRNR ABI 120) $ 6X40AC N
```

31.5.2.1.6 Table release history update

- SN07 Feature A00003486: Available in the Core with the SN07 or later release.

Modified field: OPTATTR:

— add 1 new subfield for the EXTDS512 refinement and deleted 4 existing subfields for the EXTDS512 refinement. For more information see “Table LTCINV changed field descriptions” on page 2755.

31.5.2.1.7 Supplementary information

Limitations:

- LTCINV - since the impacted fields apply to ABI XPMs, they can only be datafilled on tuples with the EXTDS512 option.

ONP Upgrade to SN07:

— During the upgrade to SN07, tuples will be auto populated in table GWCINV. This is required to preserved any existing datafill in table LTCINV for tuples with the EXTDS512 option. There will be new fields which will be assigned a nil value, refer to GW 0006 Figure 5 on page 2762. It is expected that the user will correct this to more accurate data after the ONP is completed.

31.5.2.1.8 Translation verification other tools

Table LTCINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table LTCINV. The following Figure 4 on page 2584 shows the output from TABAUDIT when it is used to verify LTCINV.

Figure 4 Sample Tabaudit output for Verifying Table LTCINV Datafill

```
>tabaudit
TABAUDIT:
>include ltcinv

>execute
-------------------------------------------------------------------------------
|            TABAUDIT STATUS
-------------------------------------------------------------------------------

The following tables are included:
      table LTCINV (91)

The following tables are excluded:
  From table VERSIONS (0)              to table SERVRINV (90).
  From table MGCINV (92)               to table IPINV (299).
  From table X75INFO (301)             to table INWATNPA (1426).

Please confirm ("YES", "Y", "NO", or "N"):
>yes
Creating TABAUDIT summaryfile: SUMMARY$MAP on SFDEV.
Starting DMS data verification ...
Table LTCINV: New table control.
     Completed tuple checking.
     SUMMARY: Tbl LTCINV: tuples checked 2, passed 2, failed 0.
Data verification is completed.
```

31.5.3 Table GATWYINV Database Schema Information

31.5.3.1 Name: GATWYINV

Long Table Name: Gateway Inventory

31.5.3.1.1 Functional Description

Table GATWYINV is where gateway configuration information is provisioned. Provisioning gateways in this table does not allocate IOUI nodes of any kind. For this release, this table contains configuration information only (no nodes) involving gateways. The term “gateway” could either mean a physical gateway or logical gateway, it depends on the actual “gateway” in question.

31.5.3.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table SERVRINV - GWC datafill, no change
2. Table SERVSINV - AUD datafill, no change
3. Table GATWYINV - New table, Gateway datafill. Dependencies on both SERVRINV and SERVSINV.
4. Table LTCINV - Dependency on GATWYINV for ABI XPM tuples

31.5.3.1.3 Size

The maximum number of tuples is 32767 for this table GATWYINV. Currently limited to 1024 (0-1023) for only ABI gateways for SN07.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
GATWYINV	0	32767	Memory is automatically allocated in increments of 32 tuples at a time up to 32767. The multiple of 32 allows for an exact allocation of store to accommodate the maximum number of tuples.

31.5.3.1.4 Fields

Table 5 Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYPMNO	New	2 Subfields:		Two part Key:
		GWTYPE	GW_TYPE - only valid SN07 value is “ABI”.	GW_TYPE - This is the type of the gateway as defined on the Core.
		GWNO	GW_NO - {0 - 1023} - any valid number in this range.	GW_NO - This is the unique external number of the gateway.
GTWYPRFL	New	n/a	An enumerated list of gateway profiles consisting of Alpha-numeric Characters. Examples:MG9KITP, MG9KABI, PVG. only valid SN07 value is MG9KABI.	The name of the profile for the gateway. The profile provides a way to assign a finer level of grandularity (as opposed to GW_TYPE) to specify specific gateway behaviors.
GTWYNAME	New	n/a	32 Alphanumeric characters.	The name of the gateway, could be upper and lower characters with special characters.
GTWYADDR	New	n/a	IPADDR Table of 4 {0 TO 255}	The IP address of the gateway. For this release this could be either the Callp address or Mtce address.(aka CIPOA address)
GTWYCSPM	New	3 Subfields: SITE_ID	4 Alphanumerics	SITE_ID: The physical Site of the Hosting Gateway Controller. Site name must be defined in table SITE. The only valid value for SN07 is HOST.
		PMT	PM_TYPE - any valid PM type.	PM_TYPE - This is a valid PM type of the cside host XPM. This could be any valid PM type but generally will be a GWC.
		EXT_PMNO	{0 TO 255} - any valid number in this range.	PMNO - The unique external number of the cside host Gateway Controller.

Table 5 Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYOPTS	New	Refinement GTWYLOC with 8 fields.	GTWY_SITE (4 alpha numerics)	SITE_NAME: The physical site of the gateway. Valid values are verified against entries in table SITE. Example datafill 'CARY'.
			FRAME_TYPE	FRAME_NAME - existing data dictionary type. The unique frame type. Example datafill, MG9Ks have a frame type of 'MG9F'.
			FRAME_NUMBER {0 - 511}	FRAME - existing data dictionary type. The unique number given to a frame within an Office.
			FLOOR_POSITION {0 TO 99}	FLOOR_POS - existing data dictionary type. The unique floor with a unique Site (generally a building).
			ROW_POSITION {A,B,C...X,Y,Z,AA, BB,CC...XX,YY,ZZ}	ROW_POS - existing data dictionary type. The unique row within a floor.
			FRAME_POSITION {0 TO 99}	FRAME_POS - existing data dictionary type. The unique frame position within a row.
			SHELF_POSITION {0 TO 77}	SHELF_POS - existing data dictionary type. Traditionally, this is the bolt hole position as measured in inches from the floor up. For MG9K shelves, it should be equal to the Shelf Number as specified in the Lgrp Key. The unique shelf position within a specific frame.
			GW_CARD_SLOT_NB R {0-50}	SLOT_NO - existing data dictionary type. This is the slot number for a card. The SN07 use if for the ABI card slot.

Table 5 Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYOPTS (continued...)	New	ELMGR with 1 field.	GTWY_NE_NBR {0-999}	GW_NETWORK_ELEMENT_NUMBER_RANGE - existing data dictionary type. This is the network element number assigned when the gateway is added via the MG9K-EM. 0 is the NIL value.

31.5.3.1.5 Datafill Example

Figure 5 on page 2762 provides a view of a successfully added tuples with the location and element manager options. Note that other gateway types other than ABI are shown, this is just example data. Only ABI gateways are supported in SN07.

Figure 5 Sample GATWYINV Tuples with Options

```
>table gatwyinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: GATWYINV
GTWYPMNO   GTWYPRFL   GTWYNAME     GTWYADDR   GTWYCSPM          GTWYOPTS
-------------------------------------------------------------------------------------------------------------------
GW 0       MG9KITP    CARY-000-0-0   47 142 14 65    GWC 15  (GTWYLOC CARY MG9F 15  2  C  3  0
0)  (ELMGR 43)  $

GW 6       MG9KITP    AUTO_DISC     192 2 45 87     GWC 10  (GTWYLOC APEX MG9F  0  0  ZZ  99
77 8)  (ELMGR 32)  $

ABI 9      MG9KABI    EXPM10        192 1 23 184      GWC 15  (GTWYLOC APEX MG9F 12  3  C    2
0 18)  (ELMGR 61)  $

GW 15      PVGPRF     PVGGW-5       147 142 172 45    GWC 20  (GTWYLOC GRNS OTHR  5  1  E    4
0   0)  $

GW 4       CICMPRF    CICM-10       148 124 67 34     GWC 16   (GTWYLOC WKFT OTHR 4   1  B  7
0  6)   $
```

31.5.3.1.6 Table release history update

Release SN07, feature A00003486: Initial release of this new table GATWYINV.

31.5.3.1.7 Supplementary information

ONP Upgrade to SN07:

— During the upgrade to SN07, tuples will be auto populated in table GWCINV. This is required to preserved any existing datafill in table LTCINV for tuples with the EXTDS512 option. There will be new fields which will be assigned a nil value, refer to GW 0006 Figure 5 on page 2762. It is expected that the user will correct this to more accurate data after the ONP is completed.

31.5.3.1.8 Translation verification other tools

Table GATWYINV does not impact translations. TABAUDIT is the tool used to verify the contents of table GATWYINV. Examples will be provided once the new table is functioning.

31.6 Service Orders (SO) (CM & SESM)

Not Applicable.

31.7 Software optionality control (SOC)

Not Applicable.

31.8 Element Management

Not Applicable.

31.9 Command interface changes

31.9.1 Map Level: QUERYPM MAPCI command

The QUERYPM command is used to query miscellaneous information about the currently posted XPM at the PM level of the MAP. This feature modifies the legacy QUERYPM command by displaying an additional screen to the default QUERYPM command (without arguments) which reflects the following ABI MG9K:

- Site
- Floor
- Row Position
- Frame Position
- Frame Type
- Frame Number

- Shelf Number
- ABI Slots
- Network Element Number
- ABI card IP address

  Note: New output only occurs if the posted XPM is an ABI XPM.

31.9.1.1 Current QUERYPM for ABI XPM

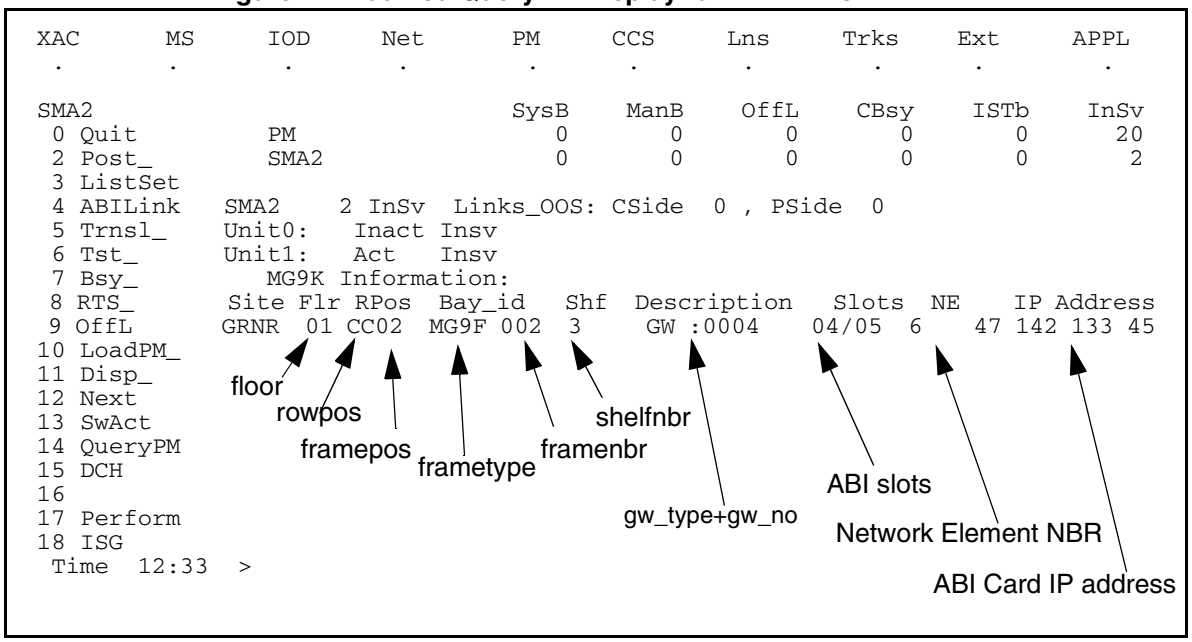
.

Figure 6 Current QueryPM Display for ABI XPMs

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
  .       .      .       .       .      .       .       .       .       .

LGC                                 SysB    ManB    OffL    CBsy    ISTb    InSv
 0 Quit          PM                    0       0       0       0       0      20
 2 Post_         LGC                   0       0       0       0       0       2
 3 ListSet
 4 ABILink   LGC     1 InSv  Links_OOS: CSide  0 , PSide  0
 5 Trnsl_    Unit0:  Inact  Insv
 6 Tst_      Unit1:  Act    Insv
 7 Bsy_       SITE  ABISlots   NE
 8 RTS_       GRNR   04/05      6
 9 OffL
10 LoadPM_
11 Disp_
12 Next
13 SwAct
14 QueryPM
15
16
17 Perform
18
  TEAM01
Time  03:47  >
```

31.9.1.2 Modified QUERYPM for ABI XPM

Figure 7 Modified QueryPM Display for ABI XPMs



31.9.1.3 Accessing directory: LGCDIR

31.9.1.3.1 Access to directory or MAP level and return to CI

To access the LGCDIR from the CI environment, enter:

>mapci;mtc;pm;post <<XPM #>>;querypm

To return to the CI environment, enter quit mapci.

31.9.2 Command: <command name>

Not Applicable.

31.9.2.1 Command type: <NON-MENU, Listed MENU, Unlisted MENU>

31.9.2.2 Command target: <NT40, SUPERNODE, BRISC, All, Other>

31.9.2.3 Command availability: <RES, NONRES or OTHER>

31.9.2.4 Command description

31.9.2.5 Command syntax

Table 6 <CommandName> command parameters and variables

Command	Parameters and variables
<command name> for example, CNTRS	<Plane Number> (0,1) <Display what> Card (0 to 10) All Proc
Parameters and variables	Description
Card	Displays ECC error counts for the specified card only
All	Displays ECC error counts for all the cards on the specified plane. This includes the processor ECC error counts.
Proc	Displays ECC error counts for only the processor memory

31.9.2.6 Qualifications and warnings

31.9.2.7 Responses

31.9.2.7.1 <response>

Table 7 MAP outputs with associated meanings and actions

Command
<RESPONSE>: <description> **Meaning:** **System or user actions:** Example: WARNING: The CPUs are out of sync due to a problem with mismatches. The mismatch logs and minfo should be analyzed before a manual resyncing is performed. Do you wish to continue? Please confirm (“Yes”, “Y”, “No”, “N”). **Meaning:** <description> for example “This response warns users that the CPUs are out of sync due to a mismatch and that the cause of the mismatch should be determined before resyncing.” **System or user actions:** <description> for example “You should analyze the mismatch logs and minfo to determine the type of faults in the system and deal with those problems before resyncing.”

Table 7 MAP outputs with associated meanings and actions

Command
<RESPONSE>: <description> **Meaning:** **System or user actions:**

31.9.2.8 Example

Table 8 Usage examples for <CommandName> command

Description of task:	
Description of task	Synchronize the two CPUs of the CM without matching memory after synchronization and without displaying any warnings regarding possible side effects beforehand.
Command: MAP response:	Example: SYNC Nomatch Noprompt Example: SYNCHRONIZATION SUCCESSFUL

31.10 Security

Not Applicable.

31.11 Configuration Walkthrough

32: Configuration (CN): A00003487

32.1 Hardware and Software Requirements

32.1.1 Hardware

No additional hardware is required in order to upgrade to a load capable of supporting multiple packet networks (support limited to IP interworking with AAL1 for SN07). All exisiting TDM/Packet configurations will continue to be supported, including:

- UA-AAL1
- PT-AAL1
- Ultralite AAL1
- UA-IP
- PT-IP
- PT-IP Compact (includes AAL2 via the PVG)
- AAL2 Wireless

In addition, the following new office configuration is supported:

- UA-AAL1/IP

New hardware will be required for the addition of the second packet network.

32.1.2 Software

The software reconfiguration to use the new networking tables (BEARNETS, NETBRDGE, NETPATH, NET2NET) will occur automatically to include default datafill dictated by the value of a new office parameter. This parameter, PRE_SN07_DUMPSIDE_PACKET_FABRIC, must be set by the engineering team and applied to the office prior to the table transfer.

SESM will align with the standard SESM requirements.

In order to provision a second packet network, the customer will have to provision the new network, any bridging resources for that network, and the connectivity supported between the networks via the bridging resource paths.

32.2 Initial Configuration.

32.2.1 Office parameters

32.2.1.1 NETWORK_ACTIVE

The network_active office parameter will be set to EXTENET when upgraded to the SN07 Succession load, even if it had been previously set to ENET.

If it had been set to JNET, the value will remain as JNET. In these offices, there will be no default network datafill in the new network tables.

> ***Note:*** If the value of the network_active office parameter is set to JNET, the packet connectivity function is not available.

32.2.1.2 PRE_SN07_DUMPSIDE_PACKET_FABRIC

Will be set to one of {UNDEF[1], NONE, AAL1, AAL2, IP}. Once the ONP is complete, there is no need to change this office parameter.

32.2.1.3 MULTINET_DISPLAY_ACTIVE = 'N'

The display control for the new OMs and Logs introduced by this activity is initially off.

32.2.2 New Network Tables - initial datafill

The examples that follow are the default tuples that will be in the new network tables after the ONP is complete. Note that the initial value of the NET 1 FABRIC field will be determined by the new office parameter PRE_SN07_DUMPSIDE_PACKET_FABRIC.

The following examples show the post TABXFER views of the new table data for the various "from" office network configurations.

[1]Should be set to something other than UNDEF by the engineering team prior to table transfer. UNDEF will be an error condition if the network_active = EXTENET.

Figure 1 JNET only on from side (JNET)

```
TABLE BEARNETS:
NETIDX  BNETNAME          DISPLAY          FABRIC           OPTIONS
-----------------------------------------------------------------

TABLE CLLI:
CLLI             ADNUM            TRKGRSIZ                  ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI         BRDGTYPE         DISPLAY                   ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                  NETPATH
-------------------------------------

TABLE NET2NET
BNETNAME                 CONNNETS
-------------------------------------

Note: If JNET, then the network_active = JNET, and packet networks are not supported
at all.
```

Figure 2 ENET only on from side (ENET)

```
TABLE BEARNETS:
NETIDX  BNETNAME          DISPLAY          FABRIC           OPTIONS
-----------------------------------------------------------------
NET 0   TDM_ENET         ENET             ENET         $

TABLE CLLI:
CLLI             ADNUM            TRKGRSIZ                  ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI         BRDGTYPE         DISPLAY                   ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                  NETPATH
-------------------------------------
0                        $

TABLE NET2NET
BNETNAME                 CONNNETS
-------------------------------------
TDM_ENET              $
```

Figure 3 ENET & AAL1 on from side (UA-AAL1 & PT-AAL1)

```
TABLE BEARNETS:
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET         $
NET 1   NET_AAL1        ATM             AAL1            (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    725             0                       ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    CORE_BRDG       E-A1                    (TDM_ENET NET_AAL1) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $
1                       (ENET_TO_AAL1) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_AAL1 1) $
NET_AAL1                (TDM_ENET 1) $
```

Figure 4 AAL1 on from side (Ultralite-AAL1)

```
TABLE BEARNETS:
NETIDX  BNETNAME       DISPLAY         FABRIC          OPTIONS
-----------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET         $
NET 1   NET_AAL1       ATM            AAL1          (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                $
NET_AAL1                $
```

Figure 5 ENET & IP on from side (UA-IP and PT-IP)

```
TABLE BEARNETS
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET       $
NET 1    NET_IP          IP              IP        (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_IP      725             0                       ENET_TO_IP_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_IP      CORE_BRDG       E-IP                    (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $
1                       (ENET_TO_IP) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_IP 1) $
NET_IP                  (TDM_ENET 1) $
```

Figure 6 IP on from side (PT-IP Compact)

```
TABLE BEARNETS
NETIDX  BNETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 1   NET_IP          IP              IP              (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
NET_IP                  $
```

32.2.3 New fields in existing tables

32.2.3.1 MNNODE

- IW SPM: will include new field BRDGCLLI set to key of only entry in table NETBRDGE.
- IW DPT: will include a new field BEARNETS set to (<name of NET 1> Y) $.
- MG4K: will include a new field BEARNETS set to (NET_AAL1 Y) $

  Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

32.2.3.2 TRKOPTS

- DPT tuples will be pulled out of the DYNAMIC option as an application type and moved into it's own option area.
- DPT tuples will contain a new BEARNETS field, that will contain (<name of NET 1> Y) $
- SIPT DPT tuples contain a new selector named NGSS. This selector indicates if the trunk group uses the new Next Generaion Session Server (NGSS) for SIP architecture implemented by activities A00003933. The values of this field is either 'Y' or 'N'.

Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

32.2.3.3 SERVRINV

- Will contain a new BEARNETS field, which will be set to:
  - (<name of NET 1> Y) $ if GWC is not a DPT GWC
  - $ if a DPT GWC

  Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

32.2.3.4 Routing tables: CND PKT selector

The existing CND PKT routing selector will be converted to CND FABRIC in all of the applicable routing tables.

32.2.4 SESM

Each non DPT GWC provisioned will have a network codec profile associated with it, using the existing network codec profile that is configured for the office.

DPT GWC's will not have a network codec profile associated with them.

32.3 Office/Subnet parameters (OP/SP) (CM & SESM)

32.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCOPT	network_active	Unchanged	CM
OFCVAR	multinet_display_active	New	CM
OFCSTD	pre_sn07_dumpside_packet_fabric	New	CM

32.3.2 Parameter information

32.3.2.1 OFCOPT::NETWORK_ACTIVE

- The parameter itself is not really changing in SN07. It will simply be used to aid in the detection of an upgrade to a Succession call server capable of supporting multiple packet networks.

- As of SN04, any ENET offices upgrading to a packet capable Succession load will have this office parameter converted to EXTENET automatically during the upgrade.
- The value EXTENET is now expanded to include the ability to support mutiple packet networks.
- The use of the network tables (BEARNETS, NETBRDGE, NETPATH, and NET2NET) is enforced in connectivity for interworking the various networks, even when only a single packet network exists.

32.3.2.1.1 Functional description
This parameter controls various aspects of call processing, most importantly the network connectivity capabilities that are supported by the system.

32.3.2.1.2 Provisioning rules
For JNET call processing, set the value of this parameter to JNET.

For Succession (single or multiple packet networks), the value should be set to EXTENET. “Succession” includes all cases where the load is packet capable, such that it includes the MSH DRU. This includes offices that currently only have an ENET provisioned.

32.3.2.1.3 Range information
Unchanged.

32.3.2.1.4 Activation
Unchanged.

32.3.2.1.5 Dependencies
No additional dependencies.

32.3.2.1.6 Consequences
Unchanged.

32.3.2.1.7 Verification
Not applicable.

32.3.2.1.8 Memory requirements
No memory impact.

32.3.2.1.9 Parameter release history update
Office parm value EXTENET now implies that the software can support multiple packet networks.

Note: The current SN06 NTP documentation does not reflect that this parameter will be changed on an ONP to EXTENET, if the from side is currently set at “ENET” and the to load contains the MSH DRU. The update that does this was submitted in TL16.

32.3.2.2 OFCVAR::MULTINET_DISPLAY_ACTIVE

Multiple Networks Display Active

32.3.2.2.1 Functional description

This is a new office parameter associated with Succession Call Server that activates the new and changed OMs and logs. This allows the customer the flexibility of enabling multiple packet networks (likely for testing purposes only) prior to having the back-office system (i.e., OSS systems) ready to support the new OMs and log fields. This is an Y/N type parameter. This parameter would be part of OFCVAR table. The default would be set to 'N'.

This parameter does not control the display of the IWBM per bridge pool OMs.

32.3.2.2.2 Provisioning rules

This office parameter cannot be turned on unless NETWORK_ACTIVE = EXTENET.

There are no restrictions for setting it to 'N'.

32.3.2.2.2.1 Behavior when the parameter is set to 'Y'

- Change from 'N' to 'Y' using table control.
  - — The tuples in the new OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are created/ (if non-existant) displayed.
  - — Pegging of the OM group registers in TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group is displayed. The bearer network is also displayed for DPTNODE OMs if the DPT node is SPM based. The bearer network will not be displayed for GWC hosted DPT.
  - — The display of the bridge pool in IWBM 800 series of LOGS is enabled.

32.3.2.2.2.2 Behavior when the parameter is set to 'N'

- Change from 'Y' to 'N' using table control
  - — A warning message would be displayed "All OM and LOGs data pertaining to multiple bearer networks on this call server will be lost.".
  - — The tuples in the new OM groups would not be displayed.
  - — The signaling type and bearer network for the DPT node tuple in the DPTNODE OM group would not be displayed.
  - — All the counters for the registers of the new OM groups would be set to zero.

— The counters of the registers of the new OM groups would not be pegged.

— The display of bridge pool in IWBM 800 series of LOGS would be disabled.

— The OMSHOW command would display the OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

32.3.2.2.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
Y/N	Y/N	N

32.3.2.2.4 Activation
Immediate

32.3.2.2.5 Dependencies

This parameter cannot be set to Y unless NETWORK_ACTIVE = EXTENET.

32.3.2.2.6 Consequences

Setting this parameter to Y will result in new OM tuples and log fields to be displayed. This could adversely affect downsteam OOS systems that have not yet been upgraded to handle this additional data.

32.3.2.2.7 Verification
To verify that the MULTINET Display is active and OM groups are created, use the CI command OMSHOW DPTOFCP. This command should display the OM group files and its tuples.

32.3.2.2.8 Memory requirements
Refer to the EI section for final details.

The new OM groups will be created at IPL time, but the tuples will not be created/displayed until the office parameter is set to Y.

- For the OM groups DPTOFCP, OFZ2NET1 and OFZ2NET2 the tuples would be created but not displayed.
- For the OM TRK2NET1 and TRK2NET2, the tuples would not be created and would be created when the office parameter “MULTINET_DISPLAY_ACTIVE” is set to Y for the first time.

32.3.2.2.9 Parameter release history update
New in SN07.

32.3.2.3 OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC
SN07 Dumpside Packet Fabric prior to Succession MULTINET upgrade.

32.3.2.3.1 Functional description

This office parameter is set by the Nortel engineering team in an office parm changes flat file prior to the night of ONP. It is to be applied after the transfer of the office parameters and prior to the TABXFER.

The purpose of the parameter is to identify the FABRIC type of the single packet fabric supported on the from side prior to the upgrade, in order for the proper network tuples to be created in tables BEARNETS, CLLI, NETBRDGE, NETPATH, and NET2NET, as well as allow the new network related fields in tables MNNODE, TRKOPTS, and SERVRINV to be assigned the proper default values.

It is very important that this parameter be set correctly.

32.3.2.3.2 Provisioning rules
This parameter has the following range: {UNDEF, NONE, AAL1, AAL2, IP}. It will be defaulted to UNDEF at IPL in a Succession load, and NONE if in a non-Succession load. It should be set to one of the other values (not UNDEF) on all upgrades to Succession loads. Although present in non Succession loads, it does not need to be set for these loads. Once an office is already on an SN07 or later load, it does not need to be set again.

A warning will be output on all changes except “UNDEF” to one of the other values that this parameter impacts the automatic creation of the network data on ONP, and should be changed with care.

Once a packet tuple is provisioned in table BEARNETS, changes will not be allowed.

In order to properly set the value, datafill will be required from the dump side from the following tables: MNNODE, MNCKTPAK, SERVRINV, TRKOPTS, LGRPINV.

Explanation of parameter values:

- UNDEF: Default value at IPL. Indicates that the engineering team has not looked at the data.
- NONE: The engineering team has analyzed the from side data and detected that no packet nodes are provisioned. Indications that a packet node existed would include:

— MNNODE: IW SPM, DPM SPM, or MG4K SPMs are provisioned.

— SERVRINV: any tuple provisioned.

— Although one could argue that datafill in tables SERVSINV or LGRPINV also indicates a packet node, it cannot be added without a GWC first.

- AAL1: The from side packet datafill contained one of the following:
  — MNNODE contained an SMG4 (MG4K).
  — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is ATM RM.
- AAL2:
  — Cannot be detected based on table datafill. Hopefully the engineering team knows if the PVG is using AAL2 or IP/AAL5.
- IP:
  — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is GEM RM.
  — Table LGRPINV contains tuples whose GRPTYPE field is ‘M’ or ‘C’. indicating IAD devices or CICM.
  — The parm should also be set to IP if dumpside was using IP/AAL5. This will not be distinguished as a seperate bearer network.

32.3.2.3.3 Range information

Table 3 Range Information

Minimum	Maximum	Default
{UNDEF, NONE, AAL1, AAL2, IP}	{UNDEF, NONE, AAL1, AAL2, IP}	ENET - if load does not contain the MSH DRU UNDEF - if load contains MSH DRU.

32.3.2.3.4 Activation

Not applicable. This office parameter is only used during the TABXFER of data to a new load. It should be set to the correct fabric PRIOR to the night of ONP, and not changed thereafter. It is not used by call processing.

32.3.2.3.5 Dependencies

The following tables rely on the proper provisioning of this parameter:

- BEARNETS
- NETBRDGE

- NETPATH
- NET2NET
- MNNODE
- TRKOPTS
- SERVRINV

32.3.2.3.6 Consequences

- There are no consequences of incorrect provisioning if there are no packet nodes currently supported at the site. If the parameter is set to a packet fabric in a site that does not have a packet network, then network tuples will automatically be created in tables BEARNETS, NETBRDGE, NETPATH, NET2NET.
- If a packet network was supported, and the parameter is provisioned incorrectly, tuple transfer errors could occur in the following tables:
  — TABXFER data errors in MNNODE, TRKOPTS, SERVRINV.
- For an SN07 to SN07 lab upgrade, where the new tables suddenly appear in the load:
  — The ONP will not detect this scenario as a multinet upgrade. Instead, the network tables will appear in the load first, and the lab primes will be notified of the change. They will be required to go to a website and download/apply a DMOPRO file for the type of lab they are working in that contains the default data. In a following load, the dependent fields will be added to the existing tables, and type reformats will pick up the default datafill.

32.3.2.3.7 Verification

Not applicable.

32.3.2.3.8 Memory requirements

Minimal. Just need to store the fabric type in a protected variable. Does not control the allocation of any additional memory.

32.3.2.3.9 Parameter release history update

New in SN07.

32.4 Upgrade Impact

32.4.1 Dump and Restore

Callp functionality should not be affected over an upgrade from pre-SN07 to post-SN07. In order to maintain this, the new/changed tables need to be datafilled over the ONP. It is required that this upgrade has minimum impact to the customer. Aside from the traditional issues with type specific reformats,

we have the additional issue of determining what the FABRIC type was on the from side, in order to properly create default tuples in the new network tables. Since call processing will start depending on this data to make inter-network connections, it is vital that this data is correct after the transfer is ONP.

Once the data transfer is complete, the goal is to have the correct network representation for the currently configured networks, such that only new network information is required for when the customer wishes to add additional networks.

The ONP strategy must handle the following information:

32.4.1.1 Office Parameters

- OFCOPT::NETWORK_ACTIVE - If ENET, convert to EXTENET, and ensure that appropriate datafill is created to handle the existing networks.
- OFCVAR::MULTINET_DISPLAY_ACTIVE - Ensure the new office parameter is defaulted to 'N'.
- OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC: the new office parameter *must be set by the upgrade engineering team* to indicate the default packet fabric on the from side network. This is set in a flat file that is applied after the office parameters have been transferred and before the tables are transferred. The engineering team is responsible for setting the correct values, and the application team is responsible for applying the changes at the proper point. Note that this is simply a new parameter included in the existing office parameter process. No changes are required to the process. This parameter applies only to alternative 1.

32.4.1.2 ONP Creation of Default Network Tuples

Tuples will be created automatically during the TABXFER via post data move procedures for the following tables. For more information see "New Network Tables - initial datafill" on page 2769.

- BEARNETS
  - — Create a NET 0 tuple representing the ENET if ENET is present.
  - — Create an appropriate NET 1 tuple representing the existing packet network. The FABRIC should be set to either AAL1, AAL2, or IP as appropriate.
- CLLI
  - — Create the appropriate CLLI used as the index to table NETBRDGE.
- NETBRDGE
  - — If there is both an ENET and a packet network defined, a bridge pool will be automatically created in table NETBRDGE for it.
- NETPATH

- Path 0 will be created as $. This is the nilpath, indicating that 2 networks can be interconnected without a bridge.
- If there are two networks defined, create a path using the bridge pool from NETBRDGE, assuming that bridges exist and that the bridgepool can connect them.

- NET2NET
  - For each network in table BEARNETS, create a tuple in NET2NET.
  - If there are multiple networks (both an ENET and a packet network), assume that both the ENET and the packet network can be connected to the other using the path index containing the bridge pool defined in table NETPATH.
  - Ensure that the NET 1 packet network detected is assigned the PACKET_NETWORK_DEFAULT option.

  Note: It is possible that an upgrade can occur in offices that have both an ENET and a packet network, but no interworking bridge nodes defined. In this case, the default datafill will still be created, but there will be no IW SPM nodes assigned to the bridge pool, so the interconnections defined in table NET2NET will not work. It is assumed that since this is an upgrade from a working office, that translations would prevent such attempts from occuring.

32.4.1.3 Initialization of new fields in existing tables

- MNNODE:
  - IW SPM: Initialize the new BRDGCLLI field to the single bridge group defined in table NETBRDGE.
  - DPT SPM: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
  - MG4K: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
- TRKOPTS:
  - Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the DPT trunk group.
  - Initialize the new NGSS field, on SIPT trunks, to ‘N’.
- SERVRINV:
  - If not a DPT GWC, initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the GWC.
  - If this is a DPT GWC, initialize the new BEARNETS field to $.

32.4.1.4 Type reformats on existing tables

- TRKOPTS: Remove DPT trunk groups as an application under the DYNAMIC trunk option, and create a DPT trunk option.
- OFRn, IBNRTn, HNPACONT::RTEREF, FNPACONT::RTEREF:
  - — Convert the CND PKT conditional selector to CND FABRIC in all of the applicable routing tables.

32.4.2 Element Management Upgrade

32.5 Data schema (DS) (CM, MIBS, RDB)

32.5.1 New/modified tables, MIBs, or Database Schema

Table 4 New or modified tables

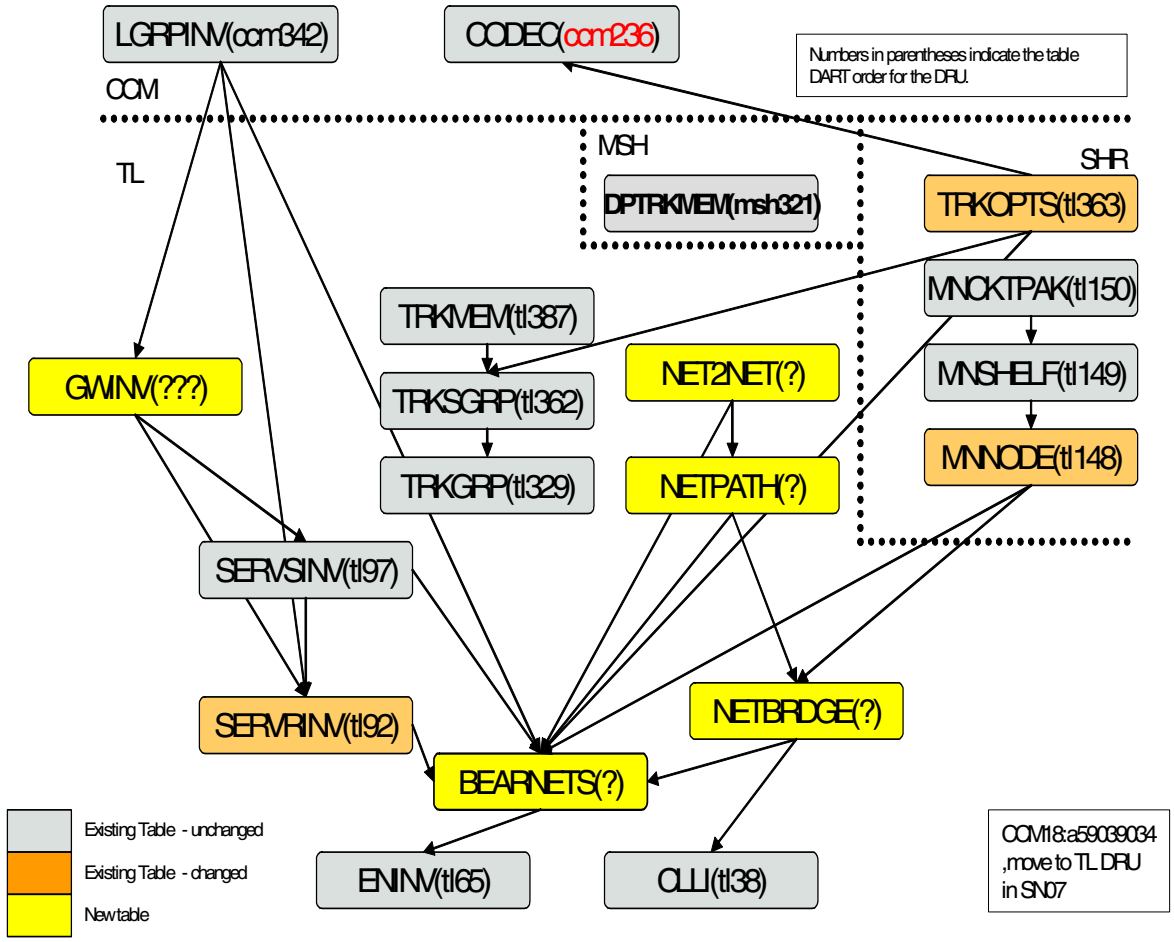
Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Core Tables:		
BEARNETS	NEW	NEW
NETBRDGE	NEW	NEW
NETPATH	NEW	NEW
NET2NET	NEW	NEW
MNNODE	Changed	Unchanged
SERVRINV	Changed	Unchanged
SERVSINV	Changed	Unchanged.
TRKOPTS	Changed	Unchanged
MNCKTPAK	n/a	Unchanged
OFRn	Changed	Unchanged
IBNRTn	Changed	Unchanged
HNPACONT:RTEREF	Changed	Unchanged
FNPACONT:RTEREF	Changed	Unchanged
SESM/GWCEM		
GWC_NETWORK_CODEC_PROFILE	New	New
GWC_NETWORK_RECOMMENDED_CODEC_SETTING	New	Old

Table 4 New or modified tables

Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GWCNode	Changed	New
GATEWAYPROFILE	Changed	Old

32.5.2 Table/MIB/Remote Database Schema information

32.5.2.1 Core Table Dependencies



32.5.2.2 Core Table BEARNETS

Bearer networks

32.5.2.2.1 Functional description

On a Succession Call Server, this table identifies the bearer networks supported by the server and the network options that apply to the packet networks.

The overall default packet network for the office is determined by the assignment of the packet_network_default option to a single tuple in the table. If no packet network is detected in the provisioning hierarchy for a packet agent, this default packet network will be used.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

32.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

ENINV

BEARNETS

NETBRDGE, NET2NET, MNNODE, SERVRINV, TRKOPTS

32.5.2.2.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
BEARNETS	0	8	Memory not allocated unless tuples are provisoned. (Required if NETWORK_ACTIVE = EXTENET).

32.5.2.2.4 Fields/OIDs

The following table lists fields for BEARNETS.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETIDX	New	No	0-7	Key to the table. Will be displayed as “NET 0” - “NET 7”.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	Vector of up to 32 characters.	Identifies the name of the bearer network.This will be used in other tables to reference the associated bearer network and its characteristics. Making the name a field of the tuple rather than the index allows the customer to make name changes to the networks defined. The 32 character name of the network must be unique across the table.
DISPLAY	New	No	Vector of up to 4 characters.	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control. Use of non-unique names will diminish the usefulness of MAPCI displays which use this field.
FABRIC	New	No	ENET, AAL1, AAL2, IP	Identifies the bearer network fabric type.
OPTIONS	New	Refinements	Vector of {pkt_network_default}	Vector of options against the bearer network.
pkt_network_default	New	OPTIONS refinement (not a field)	n/a	Indicates that this tuple is the packet bearer network default for the office. Primarily used in initializing dependant tables during an ONP. Restrictions: Only one tuple in the table can have this option.

32.5.2.2.5 Datafill example

The following example shows sample datafill for table BEARNETS.

```
TABLE: BEARNETS
NETIDX NETNAME      DISPLAY FABRIC OPTIONS
----------------------------------------
NET 0  TDM_ENET     ENET    ENET   $
NET 1  NET_AAL1     ATM     AAL1   (PKT_NETWORK_DEFAULT)$
NET 2  NET_IP       IP      IP     $
NET 3  NET_AAL2     AAL2    AAL2   $
```

32.5.2.2.6 Table release history update

New in SN07.

32.5.2.2.7 Supplementary information

Table BEARNETS, along with tables NETBRDGE, NETPATH, and NET2NET) is required to be provisioned in all Succession sites supporting bridged calls from a TDM network to a packet network.

When using the FINDREF tool on table BEARNETS, it is necessary to encapsulate the key field within single parentheses. For example:

FINDREF BEARNETS ‘NET 1’

On an ONP, this table will be automatically provisioned with both TDM and packet networks tuples where they exist.

— If the from side datafill contained an ENET, the NET 0 tuple from the datafill example will be automatically provisioned.

— If the from side supported packet nodes (as indicated by the setting of the PRE_SN07_DUMPSIDE_NETWORK_FABRIC), the NET 1 tuple will be provisioned and marked as the PKT_NETWORK_DEFAULT.

Table 7 BEARNETS Provisioning Restrctions

Field	Provisioning Restrictions
NETIDX	• Additions of packet networks to the table will not be allowed unless the NETWORK_ACTIVE = EXTENET. • Adding a tuple in table BEARNETS will automatically create a tuple in table NET2NET with $. • Cannot delete a BEARNETS tuple unless the NET2NET entry contains a $ and that tuple is the only reference. It is a counted tuple type.
BNETNAME	• Must be unique in table. • Changes to the BNETNAME will be reflected immediately in logs, OMs, etc. • Should only contain alphanumeric and underscore characters.

Table 7 BEARNETS Provisioning Restrctions

Field	Provisioning Restrictions
DISPLAY	• No restrictions, but recommend that this field be unique in the table. • Use of non-unique names will diminish the usefulness of MAPCI displays which use this field.
FABRIC	• Only 1 ENET tuple is allowed. • ENET tuple can only be added if ENET exists. • ENET tuple cannot be deleted if ENET exists. • Adds of UNDEF tuples are not allowed. • Changes are not allowed.
OPTION pkt_network_default	• The first packet network added must be the default. • Only one tuple may have this option assigned. If the option is added to another tuple, it will be removed from the first. • Cannot be added if FABRIC = ENET. • Cannot be deleted from a tuple, except by adding to another tuple. • Can only delete the network default tuple if it is the only remaining packet network tuple.

Refer to the supplementary information for table NET2NET for additional information.

32.5.2.2.8 Translation verification other tools

BEARNETS does not use translation verification tools. The Bearer Network (BNETNAME field) and Bearer Fabric (FABRIC field) are used to perform translation verification for Trunk Groups in the Trimodal configuration.

32.5.2.3 Core Table NETBRDGE

Network bridging resources.

32.5.2.3.1 Functional description

This table defines the network bridging resources for interconnecting networks. Bridges provide the ability to connect one network to another without regard to the call type. Bridges typically have two connectivity endpoints, one for each of the networks that it inter-connects.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

32.5.2.3.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

CLLI, BEARNETS

NETBRDGE

NETPATH, NET2NET, MNNODE

32.5.2.3.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	64	Refer to the EI section.

32.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BRDGCLLI	New	No	CLLI common_language_name	Identifies the name of the bridge resource group.
BRDGTYPE	New	No	CORE_BRDG	The type of the bridging resource. For SN07, this is limited to core bridges, but could be expanded in the future.
DISPLAY	New	No	Vector of up to 4 characters	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. It is recommended that this be a unique string across the bearer networks, but this will not be implemented in the table control. Use of non-unique names will diminish the usefulness of MAPCI displays which use this field.
BEARNETS	New	Structure	BNETNAME, BNETNAME	Identifies the two networks that can be bridged with this bridging resource group.

32.5.2.3.5 Datafill example

The following example shows sample datafill for table NETBRDGE.

```
TABLE: NETBRDGE
BRDGCLLI      TYPE        DISPLAY BEARNETS
-----------------------------------------
ENET_TO_AAL1  CORE_BRDG   E-A1    TDM_ENET NET_AAL1
ENET_TO_IP    CORE_BRDG   E-IP    TDM_ENET NET_IP
```

32.5.2.3.6 Table release history update

New in SN07.

32.5.2.3.7 Supplementary information

Table 10 NETBRDGE Provisioning Restrctions

Field	Provisioning Restrictions
BRDGCLLI	• Common_language_name provisioned in table CLLI. • Counted tuple type. Deletions are not allowed if referenced by another table.
BRDGTYPE	• Only allowable value in SN07 is {CORE_BRDG}. • Cannot change.
DISPLAY	• Recommended, but not enforced, to be unique. Use of non-unique names will diminish the usefulness of MAPCI displays which use this field. • No change restrictions.
BEARNETS	• The two network names provided must be provisioned in table BEARNETS. • The two network names must be different. • Changes to the BEARNETS field is allowed only if the tuple is not referenced by another table.

Since the BRDGCLLI is the key to this table, it cannot be changed through the table control interfaces. BRDGCLLI names can be changed for this table using the CI command RENAMECLLI. The name change will then be reflected in all tables, OM, and logs that reference the particular bridge CLLI.

32.5.2.3.8 Translation verification other tools

NETBRDGE does not use translation verification tools.

32.5.2.4 Core Table NETPATH

Interconnecting network path.

32.5.2.4.1 Functional description

Tuples in this table identify the list of bridging resource groups (the bridge path) that can be used to interconnect two networks. In SN07, two bridges are required to connect an AAL1 agent and an IP agent, so the path consists of a bridge resource from each of those NETBRDGE's.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

32.5.2.4.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

NETBRDGE

NETPATH

NET2NET

32.5.2.4.3 Size

Table 11 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETPATH	0	256	Refer to the EI section of this document.

32.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for NETPATH.

Table 12 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PATHIDX	New	New	0 to 255	The key to the table.
NETBRDGE	New	New	Vector of BRDGCLLI	A list of the bridge pools that are required to go from one network to another. Bridge CLLIs must be listed in the order of the traversal required, without regard to the direction of the traversal (forward or backward).

32.5.2.4.5 Datafill example

The following example shows sample datafill for table NETPATH

```
TABLE: NETPATH
PATHIDX       NETBRDGE
-----------------------------------------
0              $
1            (ENET_TO_AAL1)  $
2            (ENET_TO_IP)    $
3            (ENET_TO_AAL1) (ENET_TO_IP)$
```

32.5.2.4.6 Table release history update

New table in SN07.

32.5.2.4.7 Supplementary information

The following tuple will be created automatically for all Succession offices:

0 $

This will indicate the “nil path” that can be used in table NET2NET to indicate that two networks can be directed connected without the use of bridging resources.

Table 13 NETPATH Provisioning Restrctions

Field	Provisioning Restrictions
PATHIDX	• Counted tuple. Deletions not allowed if refenced by another table. • PATHIDX = 0 is reserved for connections between packet networks of the same fabric which do not require an IW bridge for connectivity.
NETBRDGE	• The same bridge pool should not be in the list more than once. • Limit of 2 bridge pools in SN07. • Order of the bridge pools should be maintained. • Changes are allowed, and take effect immediately for all NET2NET tuples provisioned with this path. • The bridge pools must be listed in the order they will be traversed to go from one network to the other. The pools can be listed in either the forward or reverse direction.

Note: Allowing the NETBRDGE field to be changed allows this user to deload a particular IW SPM by creating another PATH with another NETBRDGE pool of the same type and assigning the desired SPMs to it. The CI tool IWBMCI:DBL can be used to validate when the deloaded SPM is no longer in use.

32.5.2.4.8 Translation verification other tools

NETPATH does not use translation verification tools.

32.5.2.5 Core Table NET2NET

Network interconnection.

32.5.2.5.1 Functional description

Tuples in this table define the allowable interconnections between networks, and the network path used to interconnect them.

Call processing will assume that any agents on the same network can be connected with one another.

Once the normal translations have occurred, a request will be made to connectivity to connect the agents.

- If the agents are on the same network, the connection request will proceed.
- If the agents are provisioned on seperate networks, connectivity will check table NET2NET to see if the connection is allowed.
  - — If the two networks are provisioned as connecting in the table, the NETPATH and associated bridge resources will be retrieved and the connection request will continue. If there are no idle members in the bridge groups, the connection request will then fail.
  - — If the two networks are not provisioned as connecting in the table, the connection request will fail immediately.
- In SN07, no mechansim is provided for choosing an alternate bridging path if the bridging resources are unavailable in the provisioned path.

32.5.2.5.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS, NETPATH

NET2NET

32.5.2.5.3 Size

Table 14 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NET2NET	0	7	Allocated upon first tuple entry.

32.5.2.5.4 Fields/OIDs

The following table lists fields/OIDs for NET2NET.

Each CONNNETS vector entry consists of:

- NET2NET - the interconnecting network
- NETPATH - reference to tuple in table NETPATH definining the path by which the two networks interconnect.

Table 15 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	BNETNAME defined in table BEARNETS	Identifies the name of the bearer network. Must be datafilled in Table BEARNETS first.
CONNNETS	New	No	Vector of connecting_network	Identifies a list of other bearer networks that are allowed to interconnect to this bearer network.
NET2NET	New	Field of connecting_network	BNETNAME provisioned in table BEARNETS	The interworking bearer network. Must be provisioned in Table BEARNETS first.
NETPATH	New	Field of connecting_network	Key to table NETPATH 0 - 255	Index into Table NETPATH.

32.5.2.5.5 Datafill example

The following example shows sample datafill for table NET2NET.

Figure 7 ENET/AAL1/IP NET2NET Datafilll

```
TABLE BEARNETS
NETIDX  NETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $

TABLE CLLI
-----------------------------------------------
CLLI          ADNUM   TRKGRPSIZ    ADMININF
ENET_TO_IP    725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724      0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----------------------------------------------
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP           (TDM_ENET NET_IP) $

TABLE NETPATH
-----------------------------------------------
PATHIDX          NETPATH
0               $
1              (ENET_TO_AAL1) $
2              (ENET_TO_IP) $
3              (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----------------------------------------------
BNETNAME        CONNNETS
TDM_ENET        (NET_AAL1 1) (NET_IP 2) $
NET_AAL1        (TDM_ENET 1) (NET_IP 3) $
NET_IP          (NET_AAL1 3) (TDM_ENET 2) $
```

Figure 8 Enterprise/Carrier DatafilII

```
TABLE BEARNETS
NETIDX BNETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
CLLI         ADNUM   TRKGRPSIZ    ADMININF
-----------------------------------------------
ENET_TO_IP   725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724     0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
-----------------------------------------------
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX          NETPATH
-----------------------------------------------
0               $
1               (ENET_TO_AAL1) $
2               (ENET_TO_IP) $
3               (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
BNETNAME        CONNNETS
-----------------------------------------------
TDM_ENET        (NET_ATM 1) (NET_IP 2) $
NET_ATM         (TDM_ENET 1) (NET_IP 3) $
NET_IP          (TDM_ENET 2) (NET_ATM 3) $
NET_IPE         $
```

Note taht NET_IPE does not connect to NET_IP, even though they have the same FABRIC.

This is the SN07 configuration example to support Carrier Hosted Services (i.e. H.323 and Media Call Server 5200) via PVG looparounds.

Figure 9 Differet Networks, same Fabric

```
TABLE BEARNETS
NETIDX  BNETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
CLLI         ADNUM   TRKGRPSIZ    ADMININF
-----------------------------------------------
ENET_TO_IP   725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724     0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
-----------------------------------------------
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX          NETPATH
-----------------------------------------------
0               $
1               (ENET_TO_AAL1) $
2               (ENET_TO_IP) $
3               (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
BNETNAME        CONNNETS
-----------------------------------------------
TDM_ENET        (NET_ATM 1) (NET_IP 2) $
NET_ATM         (TDM_ENET 1) (NET_IP 3) $
NET_IP          (NET_AAL1 3) (TDM_ENET 2) (NET_IPE 0)$
NET_IPE         (NET_IP 0) $
```

To interconnect two different networks on the same fabric, define a NETPATH that requires no bridges, and put entries in NET2NET using that path.

32.5.2.5.6 Table release history update

New in SN07.

32.5.2.5.7 Supplementary information

- NET2NET tuples will automatically be created with CONNNETS = $ whenever new networks are added to table BEARNETS.
- On an ONP, the interconnecting networks should be provisioned with the appropriate bridges automatically.

Table 16 NET2NET Provisioning Restrctions

Field	Provisioning Restrictions
BNETNAME	• Deletions are not allowed from this table. • User may change the tuple to the point that CONNNETS = $. Tuple deletions will be handled via table BEARNETS, and allowed only if CONNNETS = $.
CONNNETS	• Networks that connect only with themselves will have CONNNETS = $. All provisioned networks in table BEARNETS will be represented in this table. • The order of the entries is used during trunk member selection as the network preference order for trunk members when a member that is on the originating agent's network is not avaiable. The most efficient path is recommended to be provisioned first. • Adding a connecting network to a tuple should also add the connection to the tuple for the other network. This addition will be added to the end of the CONNNETS list of that tuple. • Deleting a connecting network from a tuple will also delete the interconnection from the connecting network's tuple. • Changes to NET2NET tuples will take effect immediately upon the change for all new connection requests. Used should be warned when removing an existing interconnection ability.
CONNNETS: NET2NET	• Valid BNETNAME from table BEARNETS. • Should not be the same as the key for the tuple. It is understood that a network can connect to itself. • A given network should appear in the connecting network list only once. • Changing the order will change the order of trunk member selection based on the network of the originating agent.
CONNNETS: NETPATH	• A valid PATHIDX from table NETPATH. • Path changes take effect immediately for new connection requests. Existing connections will continue with the old path until the connection has been released. • If NETPATH = 0 is specified, verify that the network FABRIC for both the BNETNAME network and the NET2NET network are on the same fabric. • Verify that once the starting end of the path is chosen based on the BNETNAME network, the path can then be traced in the appropriate direction to reach the CONNNETS network.

32.5.2.5.8 Translation verification other tools

NET2NET does not use translation verification tools.

32.5.2.6 Core Table MNNODE

Maintenance node table used to provision Spectrum nodes.

32.5.2.6.1 Functional description

Unchanged.

32.5.2.6.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

All existing dependencies, plus BEARNETS, NETBRDGE

MNNODE

All existing dependant tables.

32.5.2.6.3 Size

Table 17 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNNODE	Unchanged	Unchanged	Refer to the EI section of this document .

32.5.2.6.4 Fields/OIDs

The following table lists fields/OIDs for MNNODE.

The following nodes provisioned in table MNNODE are impacted by these changes:

- Interworking bridges (NODEKEY=IW, DPT_INFO = BRDG_ONLY)
- DPT SPM (NODEKEY = IW, DPT_INFO = DPT_ONLY)
- MG4K (NODEKEY = SMG4)

Each of the applicable node type change is broken into it's own table below.

Table 18 Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged

Table 18 Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEINFO	Changed	IW refinement		Changes below impact the IW refinement of CLASS.
CLASS	Unchanged	IW refinement	Unchanged	The IW refinement is changed.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Changed	**BRDG_ONLY**	Refinements created based on this field.
BRDGCLLI	**New**	**New subfield when DPT_INFO = BRDG_ONLY**	**List of BRDGCLLI (common_language_identifier) provisioned in table NETBRDGE**	**List of the supported bridge groups the bridges belong to.**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 19 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	**IW**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged

Table 19 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	**DPT_ONLY**	Refinements created based on this field.
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEINFO	Changed	IW refinement		Changes below impact the IW refinement of CLASS.
CLASS	Unchanged	SMG4 refinement	Unchanged	The SMG4 refinement is changed.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
EXECTAB	Unchanged	Unchanged	Unchanged	Unchanged
DPT	Unchanged	Unchanged	Unchanged	Unchanged
DPT_NUM_REQ	Unchanged	Unchanged	Unchanged	Unchanged
SLINK_THRESHOLD_DATA	Unchanged	Unchanged	Unchanged	Unchanged
BOOTP_SUPPRESS	Unchanged	Unchanged	Unchanged	Unchanged
REMOTE	Unchanged	Unchanged	Unchanged	Unchanged
SGFABRIC	New	New subfield when CLASS = SMG4	{ATM, IP}	The type of fabric used to carry control signaling to/from the SPM. The values must be consistent with the fabric of the Bearer Network supported by the SPM.

Table 20 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARNETS	**New**	**New subfield when CLASS = SMG4**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**

32.5.2.6.5 Datafill example

The following examples show sample datafill for the affected nodetypes in table MNNODE.

Figure 10 Example Datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-----------------------------------------------
SPM  1 SPM_1  IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $(SYSB CR RPT)  (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT)(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

Figure 11 Example Datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM 1   SPM_1   IW  1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $ (SYSB CR RPT)  (MANB MJ RPT)  (ISTB MN RPT)
(SYSBNA CR RPT)(MANBNA MJ RPT)  (DTMFLOW MN RPT)  (ECANLOW MN RPT)
(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN CR RPT)(SMCHLD MF
RPT)  (SMCHLD24 CR RPT)  $DPT_ONLY  (NET_AAL1 Y) $
(SPMECIDX 0)$
```

Figure 12 Example Datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM  1              SPM_1          SMG4   0   SYNC   LINE   50
(COT 60)  (DTMF 60)  (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT)  (MANB MJ RPT)  (ISTB MN RPT)  (SYSBNA CR RPT)(MANBNA MJ
RPT)  (COTLOW MN RPT)  (DTMFLOW MN RPT)(ECANLOW MN RPT)  (MFLOW
MN RPT)  (CMRLOW MN RPT)(TONESLOW MN RPT)  (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT)(ATMBCN CR RPT)  (STE3HLD MJ RPT)  (STE3HLD24
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  (SPMSRMNTD MN RPT)
(LOCUR MJ RPT)  (TMCFAIL CR RPT)  $ $  N  0  $  N  N  (NET_AAL1 Y) $
```

32.5.2.6.6 Table release history update

In SN07, The following mandatory fields were added:

- BEARNETS field added to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node.
- BRDGCLLI field added to IW BRDG_ONLY nodes to indicate the list of bridge groups the particular SPM node contributes to.

32.5.2.6.7 Supplementary information

- As of SN07, in order for interworking bridges to be utilized, the BRDGCLLI for the IW must be included in a NETPATH used to interconnect two networks in table BEARNETS.
- Terminations to DPT will dynamically match the network of the DPT SPM to the network provsioned against the terminating trunk group in table TRKOPTS to properly select a DPT “terminal” on the correct network.

Table 21 MNNODE IW bridg_only Provisioning Restrctions

Field	Provisioning Restrictions
BRDGCLLI	• Must be provisioned as a single entry in SN07. Cannot have either a nil vector or more than one provisioned. • Ensure the CLLI entered is a bridge clli. • Do not allow BRDGCLLI's where the NETBRDGE packet network fabric is not IP or AAL1. AAL2 is currently not supported by SPM nodes. • Changes are allowed only if the IW is OOS (MANB or OFFL). • On changes, compare the packet fabrics for the networks bridged by the BRDGCLLI. If the fabrics are different, then this means the network cards must be changed as well. Network cards should be removed prior to changing the BRDGCLLI, so a check is made that no network cards are provisioned if the packet fabrics that are bridged are different.

Table 22 MNNODE IW dpt_only Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT}	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network with an IP or AAL1 fabric. • For changes, the SPM must be OFFL and all DPT carriers must be INB. (from DPTTRM, post spm <spm no>, bsy, bsy inb). • If the network fabric is changing, then the network cards must be removed before the change is allowed.

Table 23 MNNODE SMG4 Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network. • For changes, the SPM must be OFFL and all carriers must be INB. If DPT, then from DPTTRM, post <spm no>, bsy, bsy inb. If not DPT, then from TTP, post d spm <spm no>, bsy all, bsy inb all. • If the network fabric is changing, then the network cards must be removed before the change is allowed.

Generally, if the packet fabric for the IW is changing (whether a bridge or trunk members), then the following process must be followed to change the BEARNETS or BRDGCLLI provisioned:

- OFFL the SPM and bsy INB all carriers.
- Remove the network cards via table MNCKTPAK.
- Change the MNNODE BEARNETS or BRDGCLLI information.
- Add the correct circuit packs to MNCKTPAK (will be verified against the MNNODE datafill).
- RTS the SPM node.

32.5.2.6.8 Translation verification other tools

MNNODE does not use translation verification tools.

32.5.2.7 Core Table MNCKTPAK

Management Network Node Table

No sematice changes have been made to this table.

Additional validation checking has been added for when the GWM RM and ATM RM card provisioning, to ensure that the network implies by the card agrees with the bearer network provisioned against the node.

32.5.2.7.1 Supplementary information

Table 24 MNCKTPAK Provisioning Restrctions

Field	Provisioning Restrictions
CPKINFO - GEM card	• If SPM is IW brdg_only, ensure that at least one IP network is supported by the BRDGCLLI assigned. • If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is IP.
CPKINFO - ATM card	• If SPM is IW brdg_only, ensure that at least one AAL1 network is supported by the BRDGCLLI assigned. • If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is AAL1.

32.5.2.8 Core Table SERVRINV

Server Inventory

32.5.2.8.1 Functional description

A new field, BEARNETS is added to the SERVRINV table to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default.

In addition, DPT GWCs should not be provisioned with a bearer network, as it is a signalling only network element.

32.5.2.8.2 Usage sequence and implications (CM Only)

The following provisioning dependencies is added :

BEARNETS

SERVRINV

32.5.2.8.3 Size

Table 25 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	Unchanged	Unchanged	tbd

32.5.2.8.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 26 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SERVRNAME	Unchanged	Unchanged	Unchanged	Unchanged
SERVRADDR	Unchanged	Unchanged	Unchanged	Unchanged
SERVREXEC	Unchanged	Unchanged	Unchanged	Unchanged
SERVRTONE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	**New**	**New**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.** **DPT GWC's should not be provisioned with a bearer network. Enter $.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**
SERVROPTS	Unchanged	Unchanged	Unchanged	Unchanged

32.5.2.8.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Figure 13 Example Datafill

```
TABLE: SERVRINV
SERVRNAME SERVRADDR SERVREXEC SERVRTONE BEARNETS SERVROPTS
-----------------------------------------------------------
GWC 0     IP  47 192 48 24 (POTS POTSEX)  (KEYSET  KSETEX)  $
NORTHAA (NET_IP Y) $ $
```

32.5.2.8.6 Table release history update

Added BEARNETS field in SN07.

32.5.2.8.7 Supplementary information

- SERVRINV is the bearer network provisioning point for the following nodes, if the BEARNETS field contains a default network. If the GWC does not have a BEARNETS entry, the office default (the tuple in table BEARNETS with the default_packet_network option assigned) will be taken as the bearer network for the following agents.
  - — IP trunking gateways (PVG, Audiocodes)
  - — Logical groups
  - — ABI lines and trunks
  - — H.323 & Media Call Server 5200
  - — UAS (for CALEA)
- DPT GWCs do not have a bearer network provisioning against them, as the DPT TIDs against the GWC do not have associated hardware. If a network is provisioned against DPT GWC, it will have no effect on call processing. DPT trunk groups get their bearer network from table TRKOPTS.
- It is assumed that SERVRINV will be provisioned via SESM, which will ensure that a default bearer network is added for non-DPT GWCs, and that no bearer network will be added to DPT GWCs. A warning message is output to the user when provisioning changes are made to SERVRINV warning of potential data corruption. This warning message already exists.

Table 27 SERVRINV Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT{	• BEARNETS does not apply if the GWC is a DPT GWC. • If a nil entry is added for a non-DPT GWC, the bearere network will be taken from the office default provisoned in table BEARNETS as the pkt_default_network. • Entry must either be assigned a “$” or a single BNETNAME marked as the default. • Changes require that the GWC be OOS (MANB or OFFL). • Non-DPT trunks must be BSY INB prior to change. • Allow changes to a non-nil BEARNETS field only if not DPT in SERVSINV. Allow deletion of BEARNETS entry only if DPT.

32.5.2.8.8 Translation verification other tools

SERVRINV does not use translation verification tools.

32.5.2.9 Core Table SERVSINV

Server Subtending Inventory

Table unchanged by this activity. Only additional provsioning consistency checks are added for use during an ONP.

32.5.2.9.1 Supplementary information

DPT terminal groups are signalling only, and do not have any physical hardware associated. The DPT trunk group, via provisioning in table TRKOPTS, contains the bearer network information, and DPT “terminals” can be associated with any bearer network provisioned against the trunk group, as long as the signalling type matches.

When transferring table data during an ONP for table SERVRINV, it is not known if the GWC is a DPT GWC, so the BEARNETS will be automatically set to the bearer network default. Therefore, the write procedure for table SERVSINV will be hooked to check whether or not a multinet upgrade is in progress for DPT GWCs (SIPT or BICC) and if it is, it will delete the BEARNETS entry for it’s host GWC.

32.5.2.10 Core Table TRKOPTS

Trunk Options.

32.5.2.10.1 Functional description

Unchanged.

32.5.2.10.2 Usage sequence and implications (CM Only)

The following dependency is added to the existing provisioning order:

BEARNETS

TRKOPTS

32.5.2.10.3 Size

Table 28 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	Unchanged	Unchanged	Refer to EI section.

32.5.2.10.4 Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

```
>range
 1 OPTKEY            TRKOPTS_KEY
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
LOGICAL TUPLE TYPE: TRKOPTS_LOGICAL_TUPLE
>range 2
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
TYPE IS TRKOPTS_OPTINFO_VAR_AREA      MULTIPLE WITH
        OPTION                        TRKOPTS_OPTION REFINEMENTS:
{DYNAMIC}                             MULTIPLE WITH
      SIGNALING                       {ISUP,BICC,SIPT}
      SIGNALING_NETWORK               {IP,SS7,STRK}
      BEARER_NETWORK                  {IP,ATM,STRK}
      APPLICATION                     {OC,POS,DPT,RAS,SIPBCPT,STRK}
{DPT}                                 MULTIPLE WITH
      PROTOCOL                        {BICC,SIPT}
      BEARNETS                        {NETNAMES}
      PROTOCOL                        REFINEMENTS:
      {SIPT}                          MULTIPLE WITH
            NGSS                      MULTIPLE WITH
                NGSS_SELECTOR         {N,Y} REFINEMENTS:
                {Y}                   NGSS_YES_SELECTOR_AREA
                    INTER_DOMAIN      {N,Y}
                {N}                   MULTIPLE WITH
                    DEST_MGCNAME      MGCINV_KEY
                    TPROFILE          TPROFILE_KEY
                    ALT_HOST_MGCNAME  VECTOR OF UP TO 32 CHAR'S
                    INTER_DOMAIN      {N,Y}
      {BICC}                          MULTIPLE WITH
            CAPABILITY_SET            {1 TO 2}
```

Table 29 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Unchanged	No	Unchanged	Unchanged
OPTINFO	**Changed**	**No**	**Add DPT to list of valid OPTIONs**	**Add DPT to list of valid OPTIONs**
OPTION	**Changed**	**Selector subfield of OPTINFO**	**DYNAMIC**	**Added new DPT option and refinement.**
SIGNALING	**Changed**	**Subfiled of DYNAMIC option**	**Changed**	**ISUPPLUS renamed to BICC**
SIGNALING_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
BEARER_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
APPLICATION	**Changed**	**Subfiled of DYNAMIC option**	**{OC, POS, RAS, SPBCPT, STRK}**	**DPT Removed from valid entry range. Should now be provisioned as a DPT option.**
OPTION	**Changed**	**Selector subfield of OPTINFO**	**DPT**	**Remove DPT from list of valid APPLICATIONs**
PROTOCOL	**New**	**Subfiled of DPT option**	**{BICC, SIPT}**	**The DPT signalling protocol.**
BEARER_NETWORK	**New**	**Subfiled of DPT option**	**BNETNAME from table BEARNETS**	**The BNETNAME of a bearer network provisioned in table BEARNETS.**
PROTOCOL	**New**	**Subfiled of DPT option**	**SIPT**	**Subfields when protocol = SIPT.**
NGSS	**NEW**	**Subfield of SIPT protocol**	**{N,Y}**	**Identifies if the new NGSS SIP architecture is being used**

Table 29 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DEST_MGCNAME	New	Subfield of NGSS 'N' selector	MGCINV_ KEY	Enter the Media Gateway Controller (MGC) name from table MGCINV.
TPROFILE	New	Subfield of NGSS 'N' selector	TPROFILE _NAME	Enter the telephony profile name from table TELEPROF.
ALT_HOST_MGCNAME	New	Subfield of NGSS 'N' selector	Vector of up to 32 chars.	Enter an alternative Media Gateway Controller (MGC) name.
INTER_DOMAIN	New	Subfield of NGSS 'N' and NGSS 'Y' selector	N, Y	Refer to activity a89007980. Indicates if the SIP-T trunks are inter-domain or intra-domain (between Nortel Networks equipment in the same addressable range).
PROTOCOL	New	Subfiled of DPT option	BICC	Subfields when protocol = BICC (old ISUPPLUS)
CAPABILITY_SET	New	Subfield of BICC protocol	{1 to 2}	This represents the BICC capability set (CS). If the remote switch (other side of the DPT trunk) is unable to supoort CS2 then datafill the CAPABILITY_SET as 1. If the remote switch can support CS2 then datafill CAPABILITY_SET as 2.

32.5.2.10.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

Figure 14 Example Datafill

```
TABLE: TRKOPTS
OPTKEY          OPTINFO
----------------------------------------
DPTTRK DPT      DPT BICC NET_AAL1 1
SIPTRK DPT      DPT SIPT NET_IP N MGC2 PROF MGCTWO Y
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC $
```

32.5.2.10.6 Table release history update

- DPT is removed from APPLICATION field under the DYNAMIC option.
- DPT is added as a new OPTION.
- NGSS is added as a new selector field under the SIPT protocol

32.5.2.10.7 Supplementary information

The signaling network field is not required for DPT. The signaling protocol implies the signaling network: BICC implies SS7, and SIPT implies IP.

The bearer_fabric provisioned for DPT in table TRKOPTS indicates the bearer fabric for a specific DPT trunk group, and a given DPT trunk group can only have one bearer fabric.

GWC DPT trunk “agents” (provisioned in table SERVSINV) will be associated with the DPT trunk group during call processing based on the signaling protocol only. Bearer fabric is not provisioned against DPT GWCs in table SERVRINV.

SPM DPT trunk “agents” (provisioned in table MNNODE) will be associated with the DPT trunk group during call processing based on both the signaling protocol and the bearer network provisioned in table MNNODE.

The new NGSS (New Generation Session Server) selector identifies the SIP architecture used by the trunk group. When the new NGSS architecture is selected no additional data is necessary. However, when NGSS is not selected, the fields previously under the Dynamic tuple are required.

Table 30 TRKOPTS Provisioning Restrctions

Field	Provisioning Restrictions
BEARNETS	• BNETNAME must be provisioned in table BEARNETS. • Ensure compatibility of the signalling type with the fabric type of the bearer network. • Changes are allowed without restriction and will take effect immediately. Trunk members that are currently call processing will retain their existing network until the call is terminated.

Table 30 TRKOPTS Provisioning Restrctions

Field	Provisioning Restrictions
PROTOCOL	• Changes to the protocol field are not allowed for DPT.

32.5.2.10.8 Translation verification other tools
N/A

32.5.2.11 Core Tables OFRT, OFR2, OFR3, OFR4
Office Routing Tables

Same change applies to each

32.5.2.11.1 Functional description
Unchanged.

New CND/NOT selector condition of BEARNET, to allow conditional routing based on the originator's bearer network.

Changed the name of the PKT conditional selector to FABRIC, and increased the allowable FABRIC range from {ENET} to {ENET, AAL1, AAL2, IP}.

32.5.2.11.2 Usage sequence and implications (CM Only)
Tables must be datafilled in the following sequence:

BEARNETS

OFRT

32.5.2.11.3 Size
Not Changed

Table 31 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFRT	unchanged	unchanged	unchanged
OFR2	unchanged	unchanged	unchanged
OFR3	unchanged	unchanged	unchanged
OFR4	unchanged	unchanged	unchanged

32.5.2.11.4 Fields/OIDs
The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for FABSEL.

If CND/NOT condition is BEARNET, will be prompted for BEARNETSEL.

Table 32 OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~,** TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~**, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
FABSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
BEARNETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

32.5.2.11.5 Datafill example

The following examples shows sample datafill for table OFRT.

Figure 15 CND BEARNET

```
TABLE OFRT
POS 99
100 (CND BEARNET DFLTTDM ST 901)
(CND BEARNET DFLTIP ST 902)
(CND BEARNET DFLTATM ST 903) $ $
```

Figure 16 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901)
   (CND FABRIC IP ST 902)
   (CND FABRIC AAL1 ST 903)
   (CND FABRIC AAL2 ST 904) $ $
```

32.5.2.11.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

32.5.2.11.7 Supplementary information

The above mentioned changes are applicable to all the routing tables OFR2, OFR3, OFR4, IBNRTE, IBNRT2, IBNRT3, IBNRT4 and HNPACONT$RTEREF that have CND and NOT bound in as the route selector.
The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

32.5.2.11.8 Translation verification other tools

The following example shows the output from Traver when it is used to verify OFRT.

Figure 17 Traver example: with BEARNET Option

```
>traver tr S1S3ITISUP bearnet net_aal1 7905210227 b
TABLE TRKGRP
S1S3ITISUP IT 0 NPDGP NCRT 2W NIL MIDL 613 INC NSCR 613 613 000 N N $
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
TABLE STDPRTCT
INC ( 1) ( 0) 1
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 881 2 ( 75) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 790 790 FRTE 790
 . SUBTABLE RTEREF
 .  790 CND BEARNET TDM_ENET ST 814
 .  . SAME TABLE
 .  .  814 N D S3S1ITPTS 3 807 N
 .  . EXIT SAME TABLE
 .      CND BEARNET NET_AAL1 ST 807
 .  . SAME TABLE
 .  .  807 N D S1S3ITPTS 3 N N
 .  . EXIT SAME TABLE
 .      CND BEARNET NET_IP ST 804
 .  . SAME TABLE
 .  .  804 N D S1S3ITISUP 3 N N
 .  . EXIT SAME TABLE
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 S1S3ITPTS             5210227                       ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

32.5.2.12 Core Tables IBNRTn (IBNRTE, IBNRT2, IBNRT3, IBNRT4)

IBN Routing Table

32.5.2.12.1 Functional description

Unchanged

32.5.2.12.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

IBNRTE, IBNRT2, IBNRT3, IBNRT4

32.5.2.12.3 Size

Table 33 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNRTE	Unchanged	Unchanged	Unchanged
IBNRT2	Unchanged	Unchanged	Unchanged
IBNRT3	Unchanged	Unchanged	Unchanged
IBNRT4	Unchanged	Unchanged	Unchanged

32.5.2.12.4 Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for PKTSEL.

If CND/NOT condition is BEARNET, will be prompted for BEARNETSEL.

Table 34 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			

Table 34 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~,** TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,**~~PKT~~**, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
BEARNETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

32.5.2.12.5 Datafill example

Similar to the above examples.

32.5.2.12.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

32.5.2.12.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

32.5.2.12.8 Translation verification other tools

Refer to TRAVER information under table OFRT.

32.5.2.13 Core Tables HNPACONT::RTEREF and FNPACONT::RTEREF

Subtable Route Reference from the Home Numbering Plan Area

Subtable Route Reference from the Foreign Numbering Plan Area

Changes are the same as for OFRn and IBNRTn.

32.5.2.13.1 Functional description

Refer to OFRn.

32.5.2.13.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

HNPACONT::RTEREF & FNPACONT::RTEREF (order between these is unchanged)

32.5.2.13.3 Size

Table 35 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
HNPACONT::RTEREF	Unchanged	Unchanged	Unchanged
FNPACONT::RTEREF	Unchanged	Unchanged	Unchanged

32.5.2.13.4 Fields/OIDs

Same changes as table OFRn.

32.5.2.13.5 Datafill example

Refer to table OFRn.

32.5.2.13.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

32.5.2.13.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

32.5.2.13.8 Translation verification other tools

Refer to OFRn.

32.5.2.14 GWC_NETWORK_CODEC_PROFILE

32.5.2.14.1 Functional description

This new table is used to store network codec profiles that created by customer. The profiles will be used when customer add GWC node. Please refer to DID document for details.

32.5.2.14.2 Fields

The following table lists fields of this table.

Table 36 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
profilename	New	VARCHAR2 (32)	The name of the profile. It is not allow to be NULL. This field is the primary key of this table.
bearerpath	New	NUMBER	Indicates the bearer network fabric type. Refer to table “BEARERPATH_MAP“. The default value is “0”.
defaultcodec	New	NUMBER	Indicate the default codec. Refer to table “CODEC_MAP“. The default value is “0”.
preferredcodec	New	NUMBER	Indicate the preferred codec. Refer to table “CODEC_MAP“. The default value is “0”.
alternativecodec	New	NUMBER	Indicate the alternative codec. Refer to table “CODEC_MAP“. The default value is “0”.
packetizationinteger	New	NUMBER	Indicate the packetization rate. Refer to table “PACKETIZATION_MAP“. The default value is “0”.
t38	New	NUMBER(1)	Indicate whether the T38 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.

Field	New/ Changed	Entry	Explanation and action
rfc2833	New	NUMBER(1)	Indicate whether the RFC2833 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
comfortnoise	New	NUMBER(1)	Indicate whether the comfort noise setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
bearertypedefault	New	CHAR(1)	Indicate whether this profile is a default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is default profile for this bearer network type, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 default profile every bearer network fabric type.
networkdefault	New	CHAR(1)	Indicate whether this profile is network default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is the default profile in network, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 network default profile totally.

32.5.2.15 GWCPROFILE

32.5.2.15.1 Functional description

This table is used to store attributes of Gateway Controller profile. One new field will be added into this table, which is used to indicate whether network instance is needed to be associated to this GWC or not.

32.5.2.15.2 Fields

The following table lists the new field of this table.

Table 37 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_INSTANCE_REQUIRED	New	CHAR(1)	Indicate whether network instance is needed to be associated to this GWC or not. Available values are “Y” and “N”. Char “Y” indicates need, char “N” indicates not need. The default value is “Y”. This field can not be NULL.

32.5.2.16 GATEWAYPROFILE

32.5.2.16.1 Functional description

This table is used to store attributes of Gateway profile. One new field will be added into this table, which is used to enhance the fabric type check when customer associate gateway to GWC node. Please refer to DID document for details.

32.5.2.16.2 Fields

The following table lists fields of this table.

Table 38 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_FABRIC_RESTRICTION_LIST	New	Embedded table of "RestrictList_NT" type	The Name of this field is: Bearer fabric restriction list. This field can be NULL. This field would list the bearer fabrics to which the gateway is restricted. In most cases, this list will be empty and there will be no restriction. But for some special gateway (e.g. MG9000IP and ATM versions), the values would be provided.

32.6 Service Orders (SO) (CM & SESM)

Not applicable.

32.7 Software optionality control (SOC)

Not applicable.

32.8 Element Management

Prior to SN07, the SESM server could support only one bearer network fabric type (IP/AAL1/AAL2) at one time. As of SN07, each GWC will be associated with a beaer network instance, which defines the associated bearer network fabric type. This information will be provided by the customer as they add the GWC through the GWC-EM. In addition to the beaer fabric instance, GWC-EM will allow the cutomer to define multiple network codec "profiles" in the system and will allow the customer to select the desired profile as they add the GWC to the network.

32.8.1 New/modified GUIs

Table 39 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC-EM	Changed

32.8.2 GUI information

32.8.2.1 GWC-EM GUI

Gateway Controller Element Manager Graphical User Interface

32.8.2.1.1 Functional description

The GWC-EM database will be changed to include a new MIB table: GET_NETWORK_CODEC_PROFILE.

The following functionality is added to the GWC-EM:

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
   - — Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
   - — Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
   - — Change the associated network codec profile of one GWC node from GWC-EM GUI.

32.8.2.1.2 GUI usage and implications

GUIs must be used in the following sequence:

Current datafill order unchanged.

32.8.2.1.3 GUI size

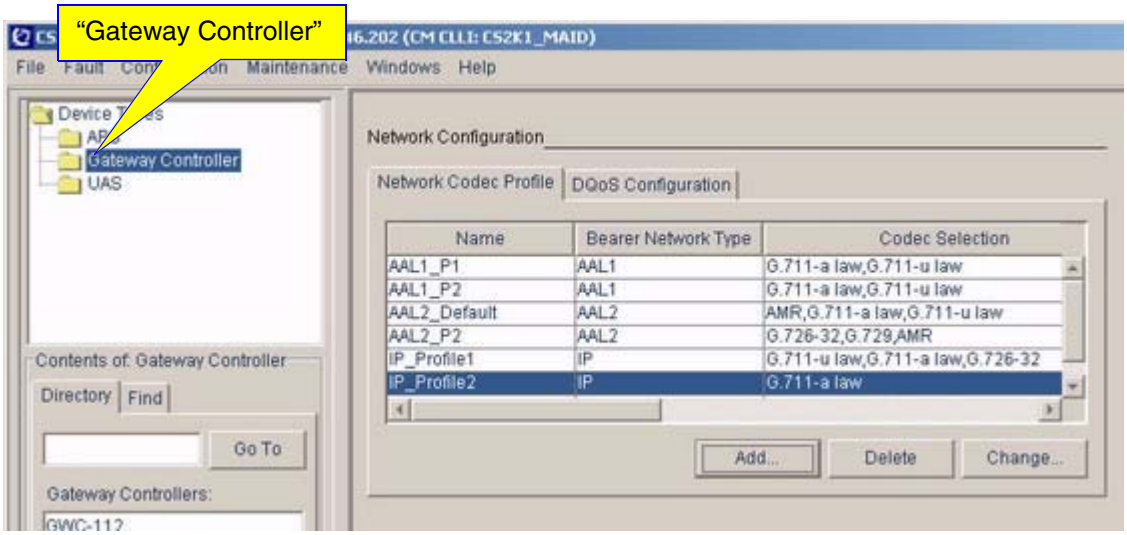
Table 40 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWC-EM	Unchanged	Unchanged	Unchanged

32.8.2.1.4 Usage Example: Display network codec profile

When customer click the “Gateway Controller” type from the device type tree at the left side, all network codec profiles will be displayed on the right side. (Please refer to “Figure 13 Network codec profile display panel”)

Figure 13 Network codec profile display panel



All existing codec profiles will be displayed in a table, each profile includes following parameters:

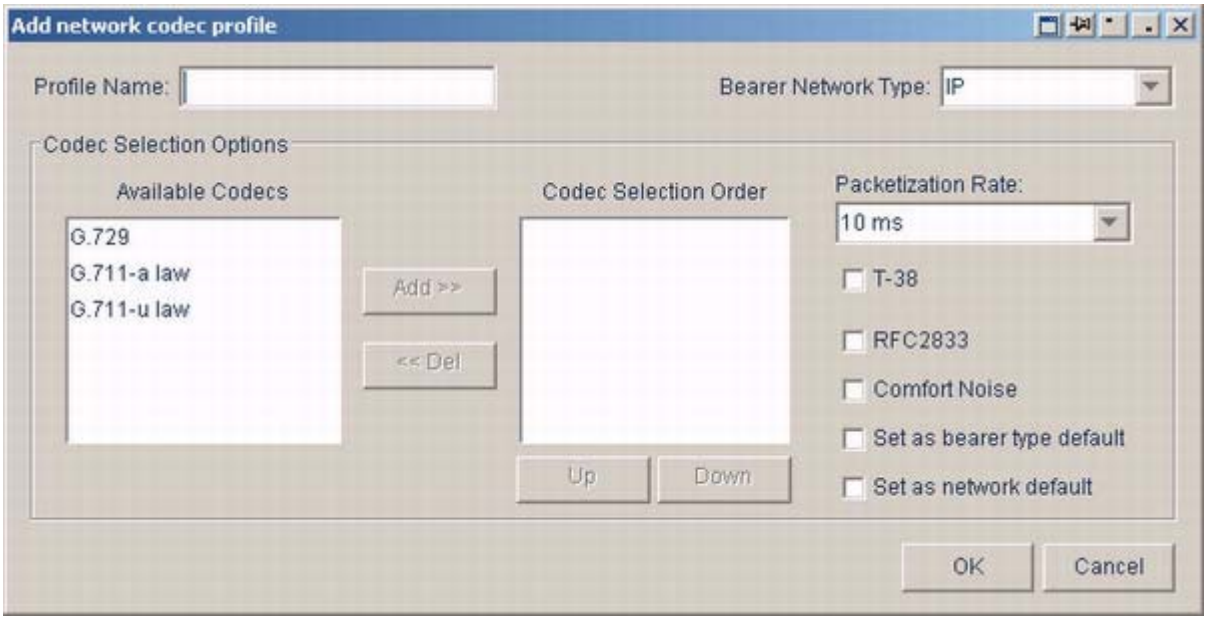
Table 2 Parameters of network codec profile

Parameter name	Description	Notes
Name	The name of the profile.	
Bearer Network Type	Indicates the bearer network fabric type.	
Codec Selection	Indicate the codecs used in this profile.	
Packetization rate	Indicate the packetization rate.	For IP bearer type only.
T-38	Indicate whether the T38 setting is enabled.	For IP bearer type only.
RFC2833	Indicate whether the RFC2833 setting is enabled.	For IP bearer type only.
Comfort noise	Indicate whether the comfort noise setting is enabled.	For IP bearer type only.
Default Profile	Indicate whether this profile is a default profile. Please note that there will be up to 1 default profile every bear network fabric type.	

32.8.2.1.5 Usage Example: Add network codec profile

Customer will be able to add one new network codec profile just by clicking the “Add” button, then a dialog “Add network codec profile” will be popped up. (Please refer to “Figure 14 Add network codec profile dialog”)

Figure 14 Add network codec profile dialog

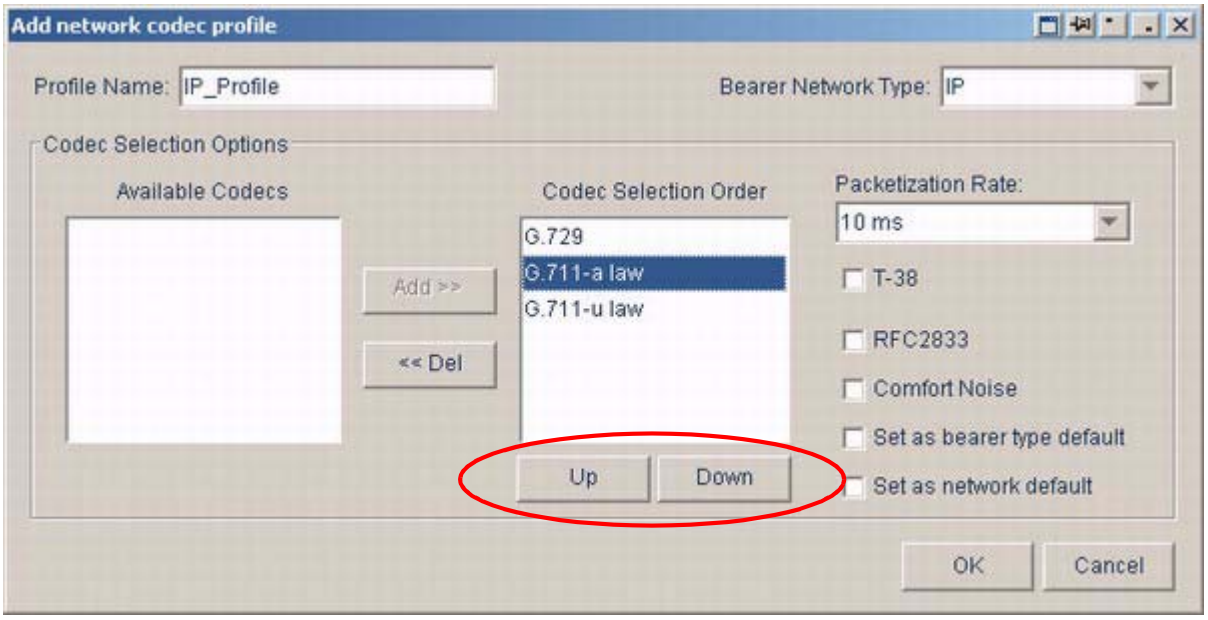


When customer select a bearer network type from the droplist box, the corresponding available codecs will be displayed below in the left list box. The available codec list may be different for different bearer network type.

Please note that the codec selecting is different from SN06 version. Customer won't select different codec for “Compression codec”, “Default codec” and “Alternative Codec” one by one. The available codecs will be listed at left side, customer should be able to select them just by highlighting codec item and clicking the “Add >>” button. Then the selected codec will be added into codec selection. Contrarily, customer could delete some codec from the selection by highlighting the codec item and clicking the button “<< Del”.

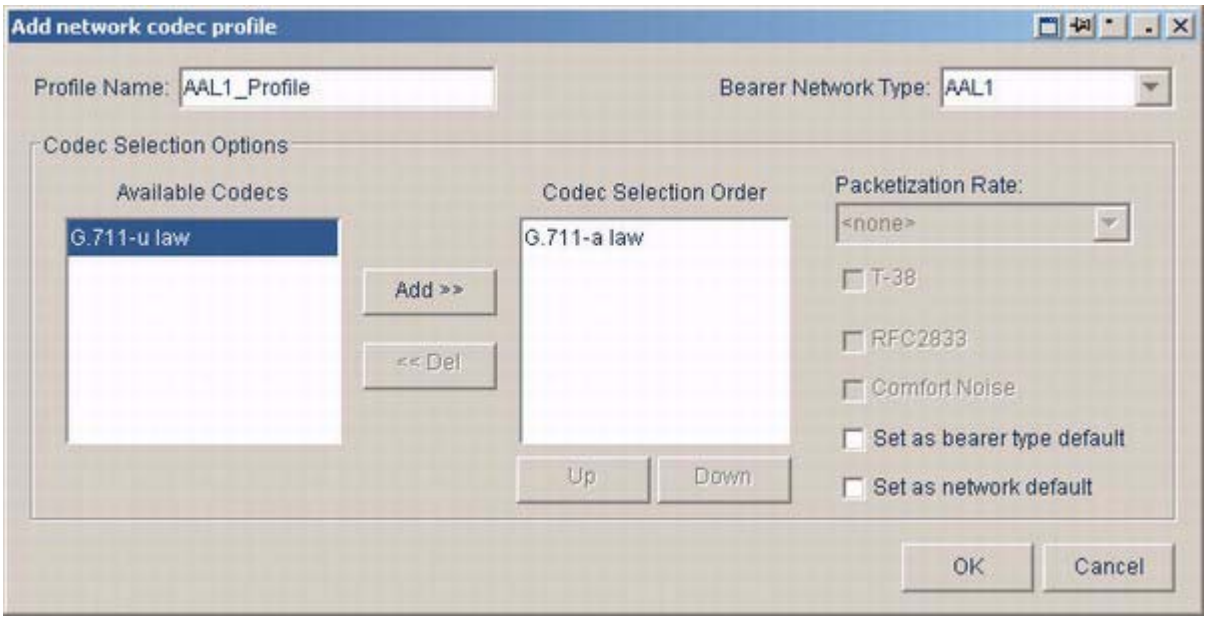
In the codec selection, the order of the codec determines how the device will treat them. For example, the first one will be mapped to “Compression codec”, the second one will be mapped to “Default Codec”, and the last one will be mapped to “Alternative Codec”. Additional, customer could change the order of codecs by highlighting the codec item and clicking the “Up” and “Down” buttons.

Figure 15 Change the order of codecs in the selection



Please note that parameters “Packetization Rate” and LCO options (T38, RFC2833, and Comfort Noise) are settings for IP bearer type only. If customer select “AAL1” or “AAL2” as the bearer network fabric type, these settings will be disabled.

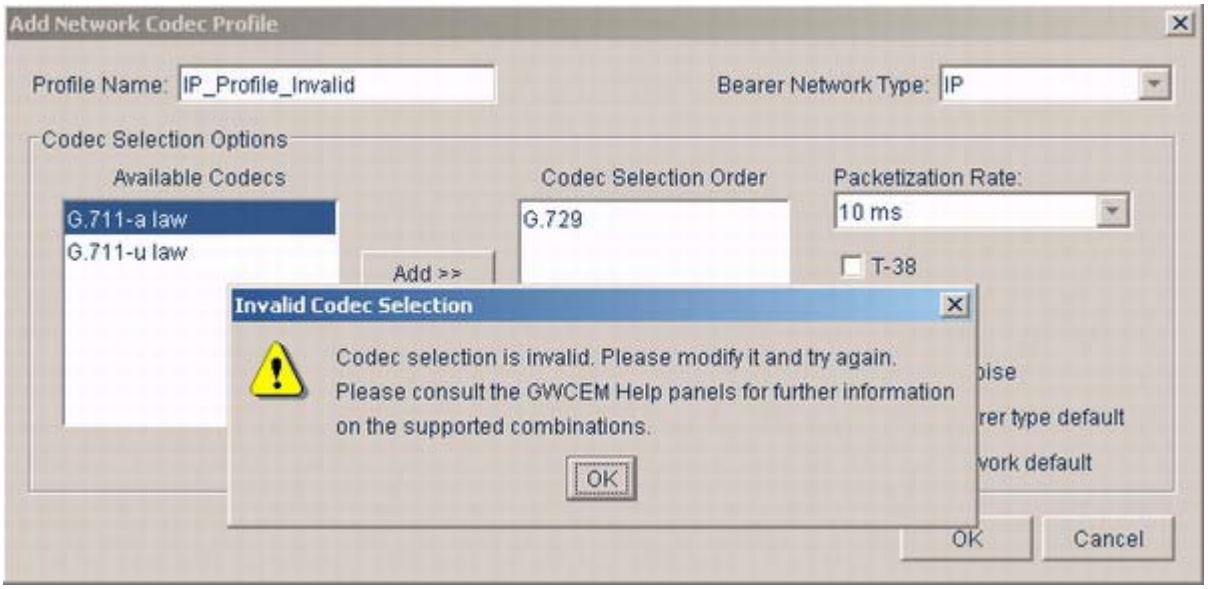
Figure 16 Select “AAL1” as the bearer network fabric type



Customer will be able to use the recommended codec setting by clicking the button “Recommended Codec Setting”, then the recommended setting will be restored into the dialog. Note that the recommended codec setting will be different for different bearer network type.

If customer select an invalid codec selection, alert dialog will be popped up. (Please refer to “Figure 17 Alert dialog for invalid codec selection”)

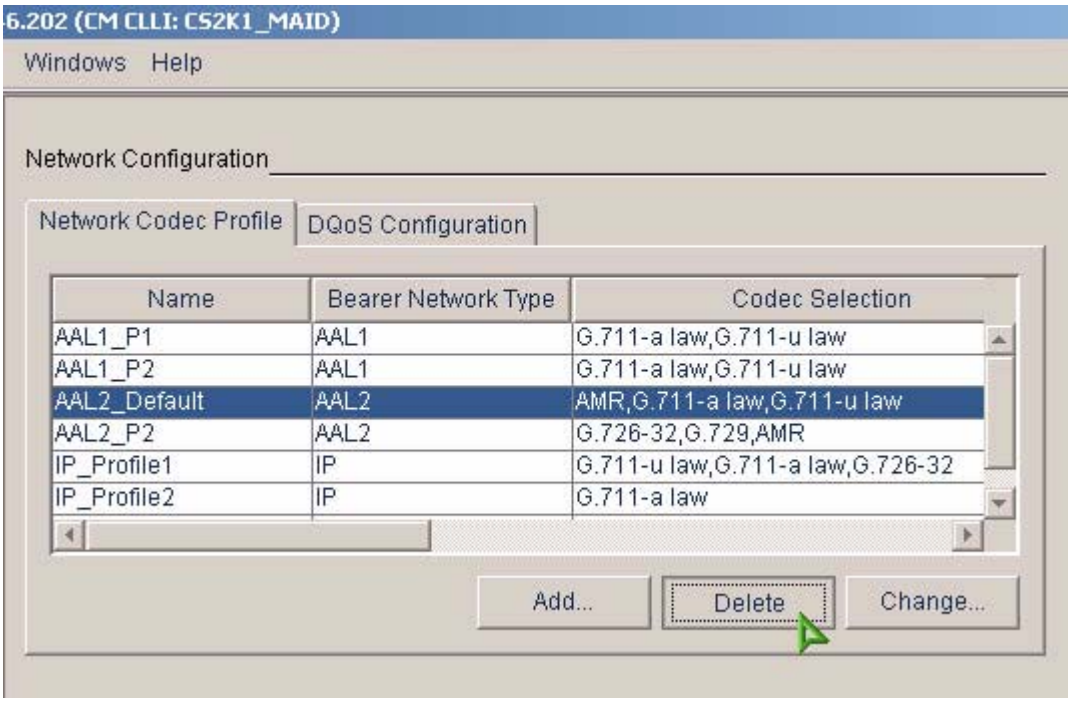
Figure 17 Alert dialog for invalid codec selection



32.8.2.1.6 Usage Example: Delete network codec profile

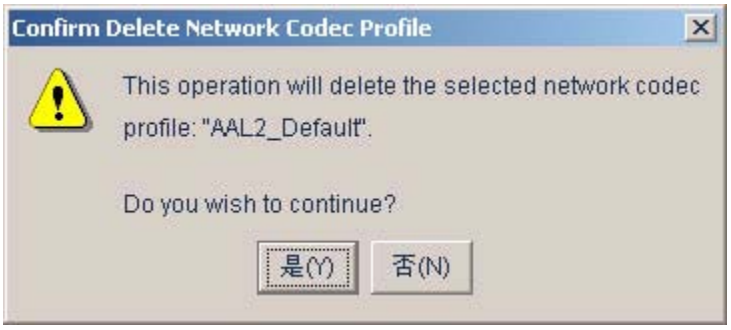
Customer will be able to delete one existing network codec profile just by highlighting the profile row from the table, and click the “Delete” button. (Please refer to “Figure 18 Delete existing network codec profile”)

Figure 18 Delete existing network codec profile



Once customer click the “Delete” button, one confirmation dialog will be popped up.

Figure 19 Delete network codec profile confirmation dialog

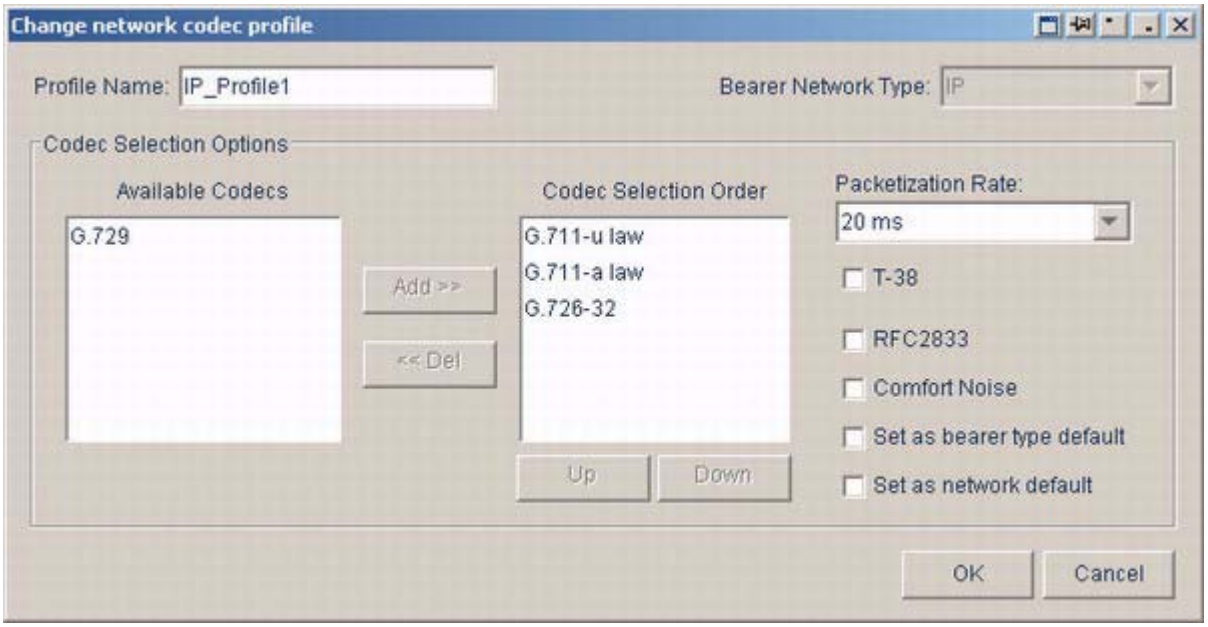


The operation result will be displayed in a pop-up dialog, and the codec profile table will be updated according to the result. Please note that if any GWC using this profile, the delete operation will be failed.

32.8.2.1.7 Usage Example: Change network codec profile

Customer will be able to change one existing network codec profile just by highlighting the profile row from the table, and click the “Change” button. Then the dialog “Change network codec profile” will be popped up. All parameters of the profile will be filled in the dialog. (Please refer to “Figure 20 Change existing network codec profile”)

Figure 20 Change existing network codec profile

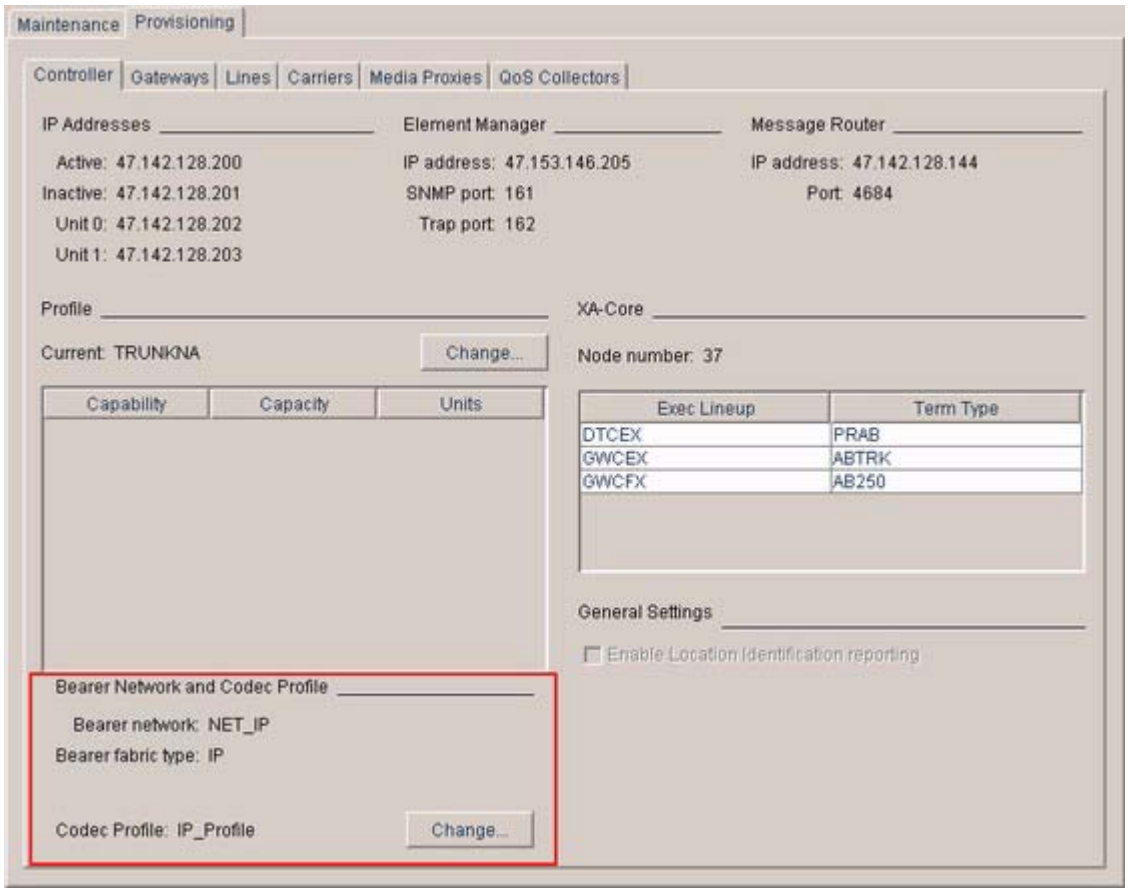


Note that the bearer network type of the profile is not allowed to be changed. Please refer to "32.8.2.1.5 Usage Example: Add network codec profile" section for how to change other parameters. Once the profile was updated successfully, these parameters will be updated into all GWCs using this profile.

32.8.2.1.8 Usage Example: Display GWC node

A new section will be added to the GWC provisioning panel to indicate the bearer network and codec profile configuration for the selected GWC.

Figure 21 Display GWC node



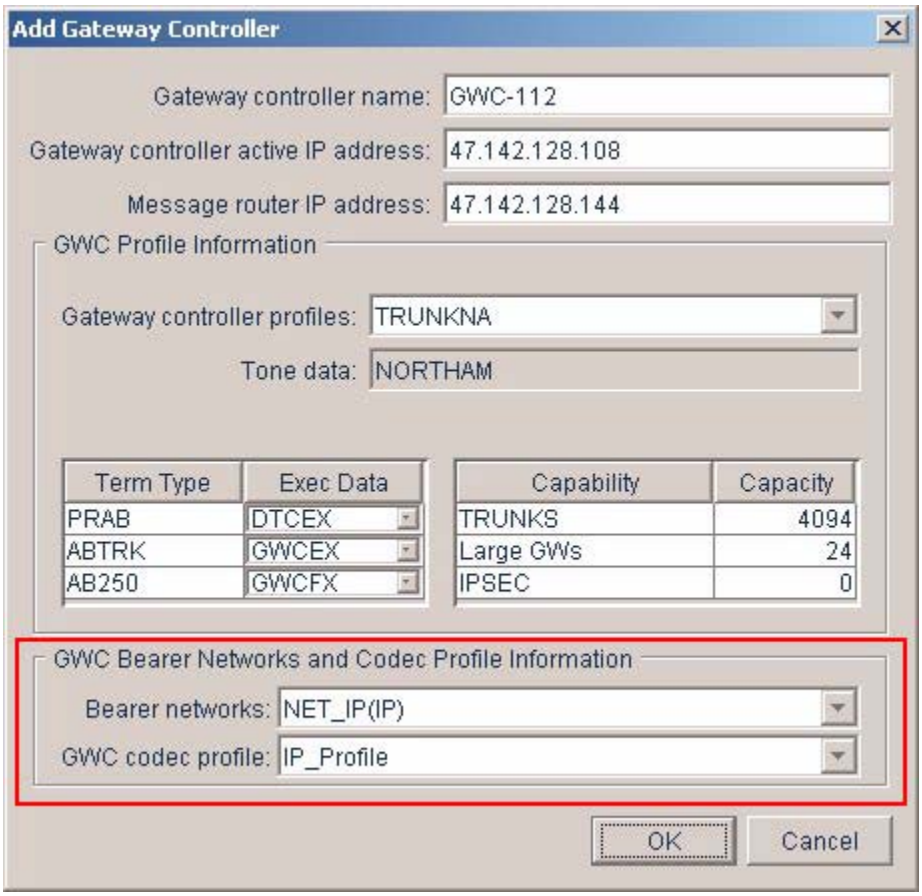
The new section includes two parts, one is bearer network area and another is codec profile area. A “Change...” button will be added to the right of the codec profile fields to allow customer to change the codec configuration for the GWC.

This information will be displayed on the GUI with other GWC’s informations together while customer select a GWC from the GWC device list tree.

32.8.2.1.9 Usage Example: Add GWC node

Two new list boxes will be added to the “Add GWC Node” dialog to allow customers to select a specific bearer network instance and codec profile while a GWC is adding to the system.

Figure 22 Add GWC node



One of these two new box contains the bearer network list, another contains the codec profile list. The codec profile list must match the bearer network, that means, if customers select a bearer network instance belonging to “IP” bearer type, then the codec profile box will only contain the names of “IP” codec profiles; if customer select a “AAL1” bearer network instance, the codec profile box will be changed to only contain the “AAL1” codec profile names.

And if customers leave the codec profile box not selected, a default codec profile based on the bearer network type will be selected automatically.

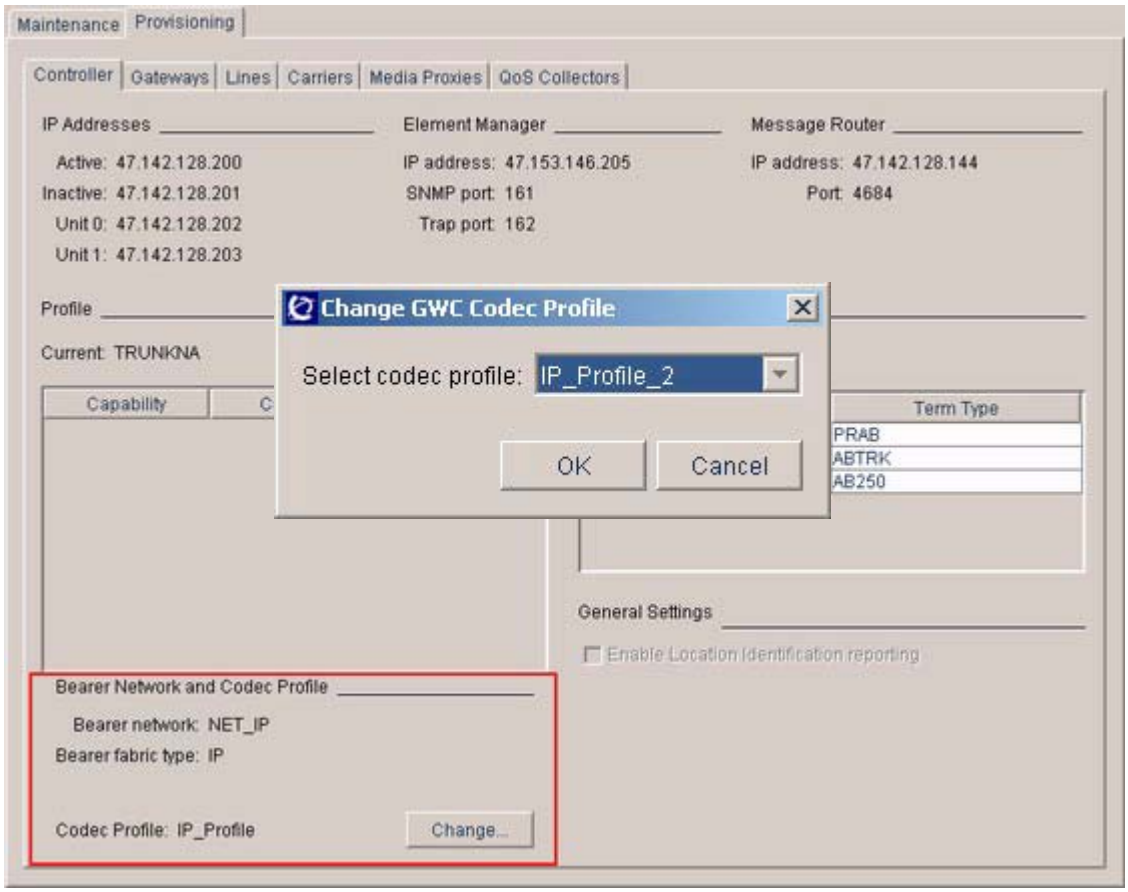
Once the addition operation has been performed successfully, a dialog like following will be pushed to the customer to indicate that the GWC was added to the system without errors.

Figure 23 Add GWC node result dialog

32.8.2.1.10 Usage Example: Change GWC network codec profile

When customers click the “Change...” button on the right of the codec profile fields on the GWC provisioning panel, a “Change Codec Configuration” dialog will be created like the following figure.

Figure 24 Change GWC's network codec profile



From this dialog, customers can select a different codec profile for the specific GWC even after the GWC has been provisioned already and a dialog with successful information will be displayed for customers if the operation has been performed without errors. Otherwise, a error message will be returned to the customers.

32.8.2.1.11 GUI release history update

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.

2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
   - — Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
   - — Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
   - — Change the associated network codec profile of one GWC node from GWC-EM GUI.

32.8.2.1.12 Supplementary information

32.9 Command interface changes

32.9.1 Directory: TRAVER

32.9.1.1 Directory description

TRAnslations VERification.

32.9.1.2 Accessing directory: TRAVER

32.9.1.2.1 Access to directory or MAP level and return to CI

CI> TRAVER <traver options>

Traver is a single command interface rather than an envirnment that is entered. You are automatically returned to the CI level after execution of the command.

32.9.2 Command: TRAVER TR

32.9.2.1 Command type: unchanged

32.9.2.2 Command target: unchanged

32.9.2.3 Command availability: unchanged

32.9.2.4 Command description

Traver an originating trunk based with the digits provided. The originating trunk (TRAVER TR) command is changed as follows:

When encountering a CND FABRIC or CND BEARNET selector in the translations route, three options are created for determining the originator's bearer fabric or network in order to determine how to interprete the CND route selection.

- TRKMEM option: The fabric or network of the member specified will be used.
- NEW BEARNET option: Allows the user to specify the bearer network (32 char vector identifying a BNETNAME provisioned in table BEARNETS) of the specifified trunk group.
- If none of the above options is specified, the TDM network will be assumed for the specified trunk group for non-DPT trunk groups.
- For DPT trunk groups, where none of the above options is specified, the bearer fabric or network will be obtained from table TRKOPTS.

32.9.2.5 Command syntax

Table 41 <CommandName> command parameters and variables

Command	Parameters and variables
TRAVER **TR**	Next par is: <CLLI> STRING Enter: <CLLI> [<CLLIOPT>] [<MBGOPTS>] [<TRIGOPT>] **[<TRKMEM>] [<BEARNET>]** <DIGITS OR N FOR NO DIGITS> [<CDNIE>] [<NSF>] [<TNSIE>] [<OSAIE>] [<BC>] [<SR>] [<PI>] [<TRI>] [<NETINFO>] [<FINFO>] [<RPOAP>] [<RPOAS>] [<NOA>] [<AIN_OPTIONS>] [<AIN_INFO>] [<SCAIIN>]
Parameters and variables	Description
[<TRKMEM>}	Existing option. Input is unchanged. Will now be used to obtain the bearer network and bearer fabric to be used when making conditional translations decisions CND FABRIC or CND BEARNET.
[<BEARNET>]	New option. Allows user to specify the bearer network (up to 32 character BNETNAME provisioned in table BEARNETS) to use as the originating bearer network. This will also imply the FABRIC, since the FABRIC is a field in table BEARNETS. Both of these will be used when making conditional routing decsions based on FABRIC or BEARNET (CND selectors). The network specified will be used, even if the trunk group does not have members on that network.

32.9.2.6 Qualifications and warnings

- Non-DPT trunk groups can have members that are spread across the varioius networks. During call processing, an effort will be made to match the originator's network to a trunk member of a like network. Traver will not be enhanced to show this selection process.

- Line group originations (eg: HUNT, MDN, ACD) will use the network fabric of the originating member of the group to determine the network fabric.
- If the FABRIC or BEARNET option is used to specify the bearer network information of a trunk group, this information will be used in TRAVER to determine the routing, even if the trunk group does not have members in that network. This allows users to test the translations before adding members, but also allows for verification to pass when during call processing it could actually fail.

32.9.2.7 Responses

32.9.2.7.1 Undefined BEARNET specified

Since the user will be prompted for a 32 character string rather than a list of tuples provisioned in table BEARNET, an invalid entry should be met with a response indicating where to look for the valid information.

Table 42 MAP outputs with associated meanings and actions

Command TRAVER TR <trunk group CLLI> <digits> BEARNET <BNETNAME>
<RESPONSE>: <description> **Meaning:** The BEARNET name entered does not exist in table BEARNETS. **System or user actions:** Choose a BNETNAME of out table BEARNETS.
<RESPONSE>: <description> **Meaning:** **System or user actions:**

32.9.2.8 Example of TRKMEM option

Table 43 Usage examples for TRAVER TR command with TRKMEM option

Description of task:	`traver tr S1S3ITISUP trkmem 1 7905210227 b`
Description of task	`Verify the translations for originating trunk group S1S3ITISUP dialing '7905210227' where the network and fabric used in the CND BEARNET conditional selectors will be obtained from the specified trunk member data.`

Table 43 Usage examples for TRAVER TR command with TRKMEM option

Command: MAP response:	NOTE: Trunk member specified is a TDM_ENET trunk >traver tr S1S3ITISUP trkmem 1 7905210227 b TABLE TRKGRP S1S3ITISUP IT 0 NPDGP NCRT 2W NIL MIDL 613 INC NSCR 613 613 000 N N $ TABLE OFCVAR AIN_OFFICE_TRIGGRP NIL TABLE STDPRTCT INC (1) (0) 1 . SUBTABLE STDPRT WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 881 2 (75) (1) (0) (0) 1 $. SUBTABLE HNPACODE . 790 790 FRTE 790 . SUBTABLE RTEREF . 790 CND BEARNET TDM_ENET ST 814 . . SAME TABLE . . 814 N D S3S1ITPTS 3 807 N . . EXIT SAME TABLE . CND BEARNET NET_AAL1 ST 807 . . SAME TABLE . . 807 N D S1S3ITPTS 3 N N . . EXIT SAME TABLE . CND BEARNET NET_IP ST 804 . . SAME TABLE . . 804 N D S1S3ITISUP 3 N N . . EXIT SAME TABLE . EXIT TABLE RTEREF EXIT TABLE HNPACONT LNP Info: Called DN is not resident. LNP Info: HNPA results are used. AIN Info Collected TDP: no subscribed trigger. AIN Info Analyzed TDP: no subscribed trigger. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 S3S1ITPTS 8075210227 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 ATB +++ TRAVER: SUCCESSFUL CALL TRACE +++

Table 44 Usage examples for TRAVER TR command with BEARNET option

Description of task:	traver tr S1S3ITISUP bearnet net_aal1 7905210227 b

Table 44 Usage examples for TRAVER TR command with BEARNET option

Description of task	Verify the translations for originating trunk group S1S3ITISUP dialing '7905210227' where the network and fabric used in the CND BEARNET conditional selectors will be obtained from the specified bearer network data.
Command: MAP response:	>traver tr S1S3ITISUP bearnet net_aal1 7905210227 b TABLE TRKGRP S1S3ITISUP IT 0 NPDGP NCRT 2W NIL MIDL 613 INC NSCR 613 613 000 N N $ TABLE OFCVAR AIN_OFFICE_TRIGGRP NIL TABLE STDPRTCT INC (1) (0) 1 . SUBTABLE STDPRT WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 881 2 (75) (1) (0) (0) 1 $. SUBTABLE HNPACODE . 790 790 FRTE 790 . SUBTABLE RTEREF . 790 CND BEARNET TDM_ENET ST 814 . . SAME TABLE . . 814 N D S3S1ITPTS 3 807 N . . EXIT SAME TABLE . CND BEARNET NET_AAL1 ST 807 . . SAME TABLE . . 807 N D S1S3ITPTS 3 N N . . EXIT SAME TABLE . CND BEARNET NET_IP ST 804 . . SAME TABLE . . 804 N D S1S3ITISUP 3 N N . . EXIT SAME TABLE . EXIT TABLE RTEREF EXIT TABLE HNPACONT LNP Info: Called DN is not resident. LNP Info: HNPA results are used. AIN Info Collected TDP: no subscribed trigger. AIN Info Analyzed TDP: no subscribed trigger. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 S1S3ITPTS 5210227 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 ATB +++ TRAVER: SUCCESSFUL CALL TRACE +++

32.10 Security

Not applicable.

32.11 Configuration Walkthrough

33: Configuration (CN): A00003489

This chapter documents the changes to the Data Schema introduced by activity A0003489. Specifically it documents the changes to the behavior of table LTCINV for the SMS Peripeheral Type.

33.1 Hardware and Software Requirements

Not required.

33.2 Initial Configuration

Not required.

33.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not required.

33.4 Upgrade Impact

Not required.

33.5 Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	Changed	Unchanged

33.5.1 Table/MIB/Remote Database Schema information

33.5.1.1 Name: LTCINV

Table LTCINV lists all the line and trunk controlling peripherals in the office. Historically they all were connected to the ENET and this table was used (among other things) to datafill the details of this connection. With the ABI program some XPM types were now allowed to subtend the packet network. To support this architectural change the EXTDS512 optional field was added to this table in SN06. Only those XPM types that were allowed to subtend the packet network were allowed to use this new optional field. This feature adds SMS to the list of XPM types that can be datafilled as subtending the packet network using this optional field.

There is no change in the format of the table or in the format of the optional field, all that has been changed is the types of peripherals that are allowed to have the field provisioned. All other types of peripherals that can be added in table LTCINV will continue to receive an error message if the EXTDS512 field is provisioned.

Note: Please refer to the documentation for SN05 activity A59038361 for more detailed information of the initial EXTDS512 design.

33.5.1.1.1 Usage sequence and implications (CM Only)

Current datafill order unchanged (SERVRINV must be datafilled prior to adding EXTDS512 peripherals in LTCINV).

33.5.1.1.2 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	Unchanged by this activity.	Unchanged by this activity.	All existing tuples, regardless of whether the EXTDS512 attribute is provisioned or not, have the physical space allocated for the information contained in this field; therefore, there is no memory impact from this activity as the memory is already allocated for all tuples in this table.

33.5.1.1.3 Fields/OIDs

The following table lists fields for LTCINV.

CSLNKTAB = “$”

OPT_ATTR = EXTDS512

When provisioning an external (non-ENET hosted) peripheral in LTCINV the EXTDS512 OPT_ATTR must be added. This optional attribute includes the IP Address of the DS512 (ABI) card in the MG9000 and Gateway Controller host name (as provisioned in table SERVRINV).

It should be noted that the CSLNKTAB portion of the tuple is not datafilled when adding external XPMs. The content of the CSLNKTAB field is automatically generated by the LTCINV code and no longer refers to real C-

side links to the ENET. A “$” should be entered when prompted for the CSLNKTAB entry (this is unchanged from SN05 behavior).

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSLNKTAB	Changed	Unchanged from SN05	None	For External XPMs this field no longer contains real C-side ENET links. Instead, “$” should be entered when prompted for this field. With this activity you should now enter “$” when provisioning External SMS tuples in LTCINV.
OPT_ATTR (EXTDS512)	Changed	Unchanged from SN05	Unchanged from SN05	When datafilling external SMS peripherals you should add this field and enter the IP address of the DS512 card in the MG9000 and the name of the host GWC (from table SERVRINV).

33.5.1.1.4 Datafill example

The following example shows sample datafill for table LTCINV. The changes from standard ENET-based peripheral datafill is highlighted with **bold** characters.

```
TABLE: LTCINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LTCNAME:
>sms 0
ADNUM:
>1007
FRTYPE:
>sme
FRNO:
```

```
>1
SHPOS:
>18
FLOOR:
>1
ROW:
>F
FRPOS:
>4
EQPEC:
>6X02AA
LOAD:
>ESS20BB
EXECTAB:
>POTS   POTSEX
EXECTAB:
>$
CSLNKTAB:
>$
OPTCARD:
>UTR17
OPTCARD:
>MSG6X69
OPTCARD:
>CMR16
CMRLOAD:
>CMR10A
OPTCARD:
>$
TONESET:
>northaa
PROCPEC:
>MX77AA MX77AA $
EXTLINKS:
>0
E2LOAD:
>UPFWNQ03
OPT_ATTR:
>EXTDS512
IPADDR:
>192   2   7 69
GWC_HOST:
>GWC 3
OPT_ATTR:
>$
PEC6X40:
>6X40FA
EXTSHELF: N
>
```

The following shows the range values for the OPTATTR field of table LTCINV. Note that this has not changed from the SN05 version.

```
TABLE: LTCINV
>ran
 1 LTCNAME           XPM_KEY
 2 ADNUM             ADMIN_NUMBER
 3 FRTYPE            FRAME_NAME
 4 FRNO              FRAME_NO
 5 SHPOS             SHELF_POS
 6 FLOOR             FLOOR_POS
```

```
 7 ROW                ROW_POS
 8 FRPOS              FRAME_POS
 9 EQPEC              PEC
10 LOAD               NPMLOAD_INFO
11 EXECTAB            TERM_EXEC_TC_TAB
12 CSLNKTAB           XPM_NET_CSLINK_TC_TAB
13 OPTCARD            EXT_OPT_CARD_TC_TAB
14 TONESET            TONE_SET_TYPE
15 PROCPEC            XPM_PEC_AREA_TAB
16 EXTLINKS           NUM_EXT_LNKS_RANGE
17 E2LOAD             NPMLOAD_INFO
18 OPTATTR            LTCINV_OPT_ATTR_VECTOR
19 PEC6X40            NT_6X40_PEC
20 EXTINFO            EXTENSION_INFO
LOGICAL TUPLE TYPE: LTC_LOGTUPLE
>ran 18
18 OPTATTR            LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
        OPT_ATTR               LTCINV_OPT_ATTR REFINEMENTS:
        {EXTDS512}             MULTIPLE WITH
             IPADDR            TABLE OF 4 {0 TO 255}'S
             GWC_HOST          MULTIPLE WITH
                  PMTYPE       PM_TYPE
                  PMNO         {0 TO 255}
        OTHERWISE              LTCINV_OPT_ATTR_NIL_DATA
>
```

33.5.1.1.5 Table release history update

following changes were made:

1. EXTDS512 OPT_ATTR is now allowed for the SMS peripheral type.
2. "$" should be entered in the CSLNKTAB field for external XPMs (the C-side link information will be generated automatically).

33.5.1.1.6 Supplementary information

- The CSLNKTAB and EXTDS512 optional attribute must align in each tuple in LTCINV. This means that if EXTDS512 exists then a "$" must have been entered in the CSLNKTAB field. A tuple must be either ENET based on External but not a combination of both.
- Multiple tuples of each type (ENET and External) can exist in the table at the same time.
- The EXTDS512 optional attribute can be provisioned only against LTC, LGC, LTCI, LGCI, SMA2, and SMS peripheral types. Attempting to add the optional attribute to other peripheral types will result in the tuple failing verification and an error will be displayed.
- The derived CSLNKTAB entries for External XPMs cannot be changed by the user.
- The ability to change the Host Gateway Controller for External XPMs is not allowed.

- The EXTDS512 optional attribute cannot be added to an existing tuple using the change command in table control, nor can it be removed using change.

33.5.1.1.7 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

33.5.1.1.8 Table Changes

As part of feature A00003486 ‘Gateway location information’ the format of the LTCINV tuple will be changing. This will impact how an External SMS will be datafilled in the CM. There will be no changes to this table unique to SMS. For details on the changes consult the documentation for that feature.

33.6 Service Orders (SO) (CM & SESM)

Not Required.

33.7 Software optionality control (SOC)

Not Required.

33.8 Element Management

Not Required.

33.9 Command interface changes

33.9.1 Directory: MAPCI;MTC;PM

33.9.1.1 Directory description

No new commands or parameters have been introduced, however due to the ABI supported host XPMs in this feature, certain maintenance functions and states will be supported for the ABI host XPMs. When an ABI peripheral (LTC, LTCI, LGC, LGCI, SMA2, or SMS) subtending a GWC is posted the display looks just like it did for the same peripheral posted as a direct HOST peripheral (legacy).

33.9.1.2 Accessing directory: PM

33.9.1.2.1 Access to directory or MAP level and return to CI

The updated displays are accessed through the PM (peripherals) level of the maintenance (MTC) level of the DMS core command interface (MAPCI).

33.9.1.3 SN07 Enhancements

Features A00003486 ‘Gateway location information’ and A00002137 ‘DS512 Link Mtc Robustness - CM’ will be adding additional information and commands to the PM level for External XPMs. This will provide more information on the nodes on the C-Side of the XPM. The SMS will get full advantage of those changes and there is no SMS specific information being added. See the documentation for those two features for more details.

33.9.2 Command: TRNSL C

33.9.2.1 Command type: Listed MENU

33.9.2.2 Command target: All

But will only appear for Succession ABI peripherals.

33.9.2.3 Command availability: RES

33.9.2.4 Command description

TRNSL C (translate c-side links) is not a new command, however when an LTC, LTCI, LGC, LGCI, SMA2, or SMS subtends a GWC (gateway controller), the TRNSL C will display the c-side links of the peripheral as connecting to a GWC.

Each c-side link will simply reflect the name of the gateway controller to which it subtends. Link 0, 1, 4 and 5 (the message links) reflect the actual status of the c-side links. Currently, the speech links have the following string hardcoded as their status “**;Cap S;Status:OK”.

It is important to note that TRNSL C indicates only which GWC supertends the ABI peripheral, it does not display the MG9K or ABI card that is in use for the messaging path.

33.9.2.5 Command syntax

Table 4 TRNSL C command parameters and variables

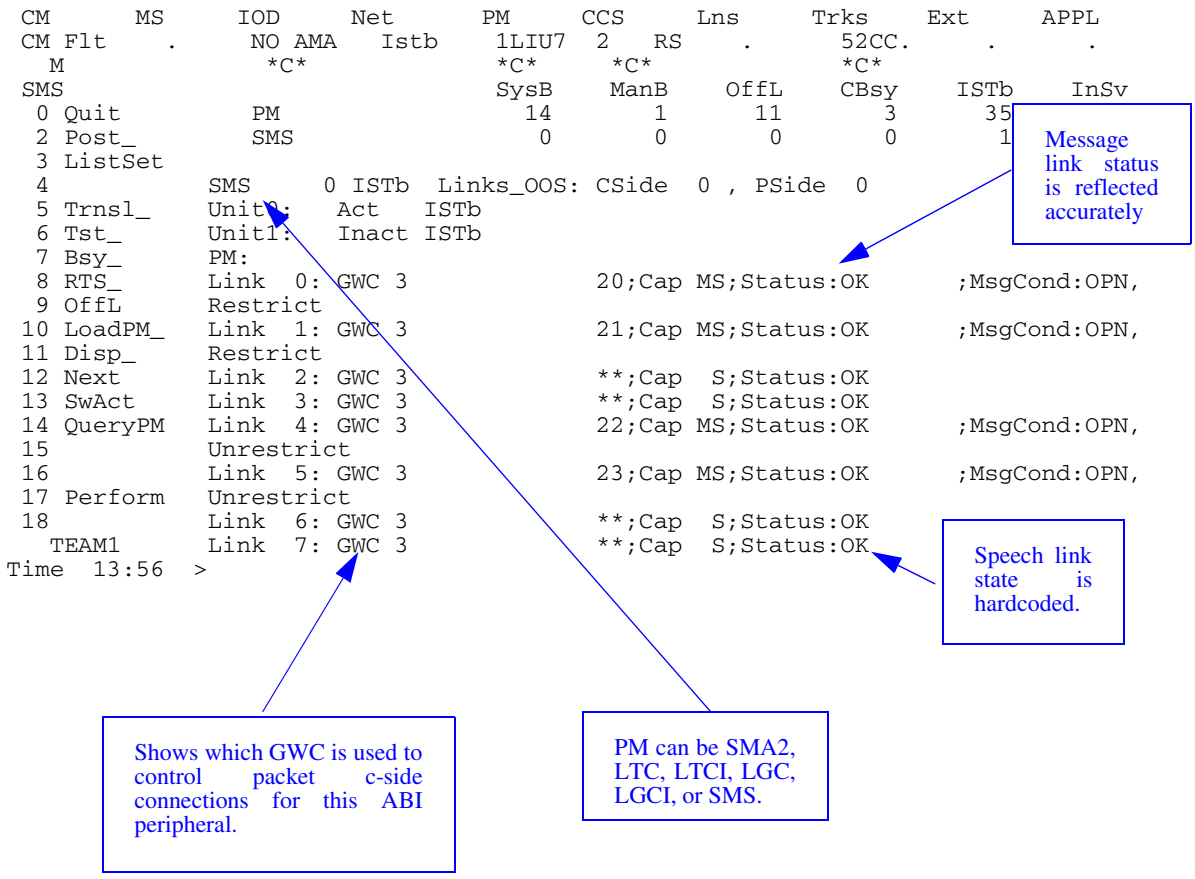
Command	Parameters and variables
TRNSL C	unchanged
Parameters and variables	unchanged

33.9.2.6 Qualifications and warnings

The TRNSL C command will provide the user with the following additional information when a GWC is involved:

“Please refer to the DS512 Interface EM for all link maintenance commands.”

It should be noted that maintenance actions on the c-side links (e.g. bsy link 0, rts link 1, etc.) can only be performed on the c-side message links for ABI peripherals.
Usage example for **“MAPCI;MTC;PM; POST <XPM>;TRNSL C “command**



33.10 Security

Not Required.

33.11 Configuration Walkthrough

Not Required.

34: Configuration (CN): A00003490

34.1 Hardware and Software Requirements

The purpose of this feature is to rehome existing ENET/JNET XPMs to the ABI DS-512 interface off MG 9000.

Therefore the following hardware is required:

- An available LGCI , SMA2, LGC, LTC, LTCI, SMS
- GWCs that will be hosting XPMs need to be configured and datafilled in table SERVRINV
- DS-512 Interface cards should be installed in the appropriate MG 9000 Gateways and their base IP address known.

Because this feature is a part of the larger installation method to rehome XPMs to the ABI configuration, please refer to the Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" for a complete list of required hardware to perform the rehome.

Software requirements:

- SN07 or later Succession Core load

34.2 Initial Configuration

This feature, when enabled, provides the ability to rehome an existing ENET/JNET XPM by changing its data in table LTCINV. The ability to rehome XPMs involves turning on the rehome capability via the ABIREHOME tool and splitting the Core. This is but one step of an overall process to rehome the ENET/JNET based XPMs. For the complete process, please refer to Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome."

34.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

34.4 Upgrade Impact

No Impact.

34.5 Data schema (DS) (CM, MIBS, RDB)

This feature does not introduce any new tables, fields, or field values in any table. It permits, when enabled, the ability to rehome an existing ENET/JNET XPM by *changing* its data in table LTCINV (rather than having to delete and re-add the tuple).

In order to provide this *change* capability, some limitations and restrictions have been modified. Please refer to"Limitations and Restrictions" in the Functional description (FN) section for a complete list of limitations and restrictions.

34.6 Service Orders (SO) (CM & SESM)

Not Applicable.

34.7 Software optionality control (SOC)

Not Applicable.

34.8 Element Management

Not Applicable.

34.9 Command interface changes

34.9.1 Directory: TASTOOLCI (changed)

Two commands removed:

- SET_ABI_REHOME_STATUS
- QUERY_ABI_REHOME_STATUS

34.9.1.1 Directory description

This CI command directory is password protected and exists for use by TAS (Technical Assistance) personnel in various upgrade scenarios which involve splitting the switch and using the SWACT functionality to enable behavior.

The above commands are reomved from TASTOOLCI, and are accessible only from the ABIREHOME tool, described below.

34.9.1.2 Accessing directory: TASTOOLCI

34.9.1.2.1 Access to directory or MAP level and return to CI

Not changed.

34.9.2 Directory: ABIREHOME (new)

Commands:

- QUERY_ABI_REHOME_STATUS / QRS
- QUERY_IMPACTED_NODES / QIN
- FIND_AFFECTED_NODES / FAN
- SHOW_NODE_STATUS / SHOWNS
- DISP_LINK_CHANNEL_MAP / DLC
- DISP_LINK_INFO / DLI
- DISP_IOUI_ROUTE_DATA / DRD
- SET_ABI_REHOME_STATUS
- ADJUST_FRAME_SYNC / AFS
- MARK_NODE_DS512_RESULT / VER512
- SEND_GWC_STATIC_DATA / GWCSD
- ABORT_GWC_STATIC_DATA / ABORT_GWCSD
- LINE_STATUS_CHG

Hidden Commands:

The following commands are HIDDEN and are used for debugging / correcting errors encountered as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

These HIDDEN commands should not be executed in the field, except by qualified Nortel person.

- SLC (set link channel map)
- SAN (set affected node)
- CAN (clear affected node)
- CLEAR_GWC_SD_TABLE
- SHOW_GWCSD

34.9.2.1 Directory description

This CI command directory is used for ABI rehome specific commands once the functionality has been enabled via TOOLSUP password control. Invasive commands within this directory require the execution of the

SET_ABI_REHOME_STATUS ON command before their functionality is enabled.

There are numerous commands which do not appear in the HELP documentation, and therefore are generally hidden from the average user. It is the intent that these commands are not to be executed except by TAS / GNPS in an error recovery and/or data collection mode.

34.9.2.2 Accessing directory: ABIREHOME

34.9.2.2.1 Access to directory or MAP level and return to CI

Prior to an attempt to access the ABIREHOME directory at the map, the tool must be enabled by executing the TOOLSUP command “access on abirehome,” and entering the proper daily password.

To access ABIREHOME from the CI environment, enter “abirehome” from the command interface.

To return to the CI environment, enter “quit”.

34.9.3 Command: ABIREHOME: QUERY_ABI_REHOME_STATUS / QRS

34.9.3.1 Command type: NON-MENU

34.9.3.2 Command target: All

34.9.3.3 Command availability: RES

34.9.3.4 Command description

This command is used to display the current state of the ABI Rehome.

34.9.3.5 Command syntax

Table 1 <CommandName> command parameters and variables

Command	Parameters and variables
QUERY_ABI_REHOME_STATUS or QRS	n/a
Parameters and variables	Description
n/a	

34.9.3.6 Qualifications and warnings

None.

34.9.3.7 Responses

34.9.3.7.1 QUERY_ABI_REHOME_STATUS responses

Table 2 MAP outputs with associated meanings and actions

QUERY_ABI_REHOME_STATUS
`Displays the status of the ABI Migration control structures.` **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
`Current ABI Rehome State is: {ON, OFF, SUSPENDED}` **Meaning:** Output regardless of status entered. If ON, the rehome process has been enabled. If OFF, the rehome process has been disabled, and all node rehome data is currently at default values. If SUSPENDED, a rehome was begun, and interrupted by the user. In this state, the control bool is FALSE, but there could be node rehome data that is not at default values. **System or user actions:** None. This is for informational purposes.
`ABI XPM Rehome Control Enabled: {Y, N}` **Meaning:** Displays the state of the control bool that enables the table control and ABIREHOME CI tool functionality. **System or user actions:** None. This is for informational purposes.

`There are nodes which have been marked as rehomed.`
`Please use QUERY_IMPACTED_NODES/QIN for more information.`
 	
Meaning: There are nodes which have been marked as impacted by Rehome. All node rehome data is cleared if SET_ABI_REHOME_STATE with ON or OFF is executed. Individual nodes can be cleared by utilizing the VER512 <node> FAIL command.
 	
System or user actions: None. This is for informational purposes.

`There are no nodes marked as impacted.` **Meaning:** There are no nodes which have rehome data associated with them. The rehome state can be turned ON or OFF without impacting any existing data. **System or user actions:** None. This is for informational purposes.

34.9.3.8 Example

Table 3 Usage examples for QUERY_ABI_REHOME_STATUS command

Description of task:	
QRS	Current ABI Rehome State is: ON ABI XPM Rehome Control Enabled: Y There are nodes which have been marked as rehomed. Please use QUERY_IMPACTED_NODES/QIN for more information.

34.9.4 Command: ABIREHOME: QUERY_IMPACTED_NODES / QIN

34.9.4.1 Command type: NON-MENU

34.9.4.2 Command target: All

34.9.4.3 Command availability: RES

34.9.4.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

Query impacted nodes will display all nodes that have been marked as impacted by the rehome.

34.9.4.5 Command syntax

Table 4 QUERY_IMPACTED_NODES command parameters and variables

Command	Parameters and variables
QUERY_IMPACTED_NODES or QIN	n/a
Parameters and variables	Description
n/a	

34.9.4.6 Qualifications and w arnings

None.

34.9.4.7 Responses

34.9.4.7.1 QUERY_IMPACTED_NODES responses

Table 5 MAP outputs with associated meanings and actions

QUERY_IMPACTED_NODES
`There are no nodes marked as impacted.` **Meaning:** No nodes have been marked as impacted. **System or user actions:** Informational purposes only.
`Displays all nodes currently marked as impacted in the rehome node data.` **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.

`Impacted Nodes`
`--------------`
`Node 68: LTC_NODE SMA2 1`
`Node 77: IDT_NODE IDT 99`
 	
Meaning: Node numbers 68 and 77 have been marked as impacted, and will be treated as rehomed during a NRS (norestartswact).
 	
System or user actions: Informational purposes.

34.9.4.8 Example

Table 6 Usage examples for command QUERY_IMPACTED_NODES

Description of task:	

QIN	`Impacted Nodes`
	`--------------`
	`Node 68: LTC_NODE SMA2 1`
	`Node 77: IDT_NODE IDT 99`

34.9.5 Command: FIND_AFFECTED_NODES / FAN

34.9.5.1 Command type: NON-MENU

34.9.5.2 Command target: All

34.9.5.3 Command availability: RES

34.9.5.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

Given a node number of an XPM, this command will show all nodes that would be impacted by a rehome of that XPM, by recursively searching its p-side links.

34.9.5.5 Command syntax

Table 7 command parameters and variables

Command	Parameters and variables
FIND_AFFECTED_NODES or FAN	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <NODE NUMBER> {0 to 4095}

34.9.5.6 Qualifications and warnings

None.

34.9.5.7 Responses

34.9.5.7.1 FIND_AFFECTED_NODES / FAN responses

Table 8 MAP outputs with associated meanings and actions

FIND_AFFECTED_NODES/FAN
FIND_AFFECTED_NODES: Displays the affected nodes for given XPM node --- Syntax: FIND_AFFECTED_NODES node or FAN node Parms: <NODE NUMBER> {0 TO 4095} **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
Node number is not a supported XPM. **Meaning:** The node number provided is not an XPM that can be supported from an ABI interface. The command will work whether the XPM is currently on an ENET/JNET interface or off of an ABI interface, but the XPM type must be able to be supported on either interface. **System or user actions:** Informational purposes.
Given node: --- Node 69: LTC_NODE SMA2 1 Subtending nodes: --- Node 77: IDT_NODE IDT 5 **Meaning:** For the given XPM number, display the node type and device information for each subtending nodes. Nodes which subtend a node are shown indented under that node. **System or user actions:** Informational purposes only.

34.9.5.8 Example

Table 9 Usage examples for command FIND_AFFECTED_NODES/FAN

Description of task:	
FIND_AFFECTED_NODES or FAN	Given node: --- Node 69: LTC_NODE SMA2 1 Subtending nodes: --- Node 77: IDT_NODE IDT 5

34.9.6 Command: ABIREHOME: SHOW_NODE_STATUS / SHOWNS

34.9.6.1 Command type: NON-MENU

34.9.6.2 Command target: All

34.9.6.3 Command availability: RES

34.9.6.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to Display the rehome status of a given node,or all Affected Nodes.

34.9.6.5 Command syntax

Table 10 <CommandName> command parameters and variables

Command	Parameters and variables
SHOW_NODE_STATUS or SHOWNS	<NODE NUMBER or ALL>
Parameters and variables	Description
NODE NUMBER	The Node number of the xpm.
ALL	Display the status of all the nodes.

34.9.6.6 Qualifications and warnings

None

34.9.6.7 Responses

34.9.6.7.1 SHOW_NODE_STATUS responses

Table 11 MAP outputs with associated meanings and actions

SHOW_NODE_STATUS

```
SHOW_NODE_STATUS:  Displays the status of XPM nodes which are marked as
'Impacted' by the rehome. It does not display the subtending nodes.
------------------------------------------------------------
Syntax: SHOW_NODE_STATUS node/ALL
        or
        SHOWNS node/ALL

Parms: <NODE NUMBER or ALL> {0 TO 4095,
                             ALL}
```

Meaning: Help associated with command.

System or user actions: Informational purposes only.

```
  DS512 link verification result is: UNEXECUTED
  Provisioning state is             : PASS
  NoRestartSwact state is           : UNEXECUTED
  GWC Static Data Download state is: UNEXECUTED
```

Meaning: Output of the SHOW_NODE_STATUS on a node.

System or user actions: None - informational only.

```
DS512 link Verification result is: {PASS, FAIL, UNEXECUTED}
```

Meaning: The SHOWNS command displays four key data points for a rehoming XPM. The DS512 link verification result is changed via the ABIREHOME VER512 command. The ABIREHOME VER512 command is executed as one of the steps in the Installation Method 72-1639 "XPM - ABI Link Verification." PASS indicates that the Installation Method has been executed successfully for the specified node. FAIL indicates that the Installation Method has been executed, but failed, for the specified node; the Installation Method should be referenced for appropriate action. UNEXECUTED indicates that the Installation Method has not been executed for the specified node.

System or user actions: If FAIL is encountered reference the Installation Method for appropriate action.

Table 11 MAP outputs with associated meanings and actions

SHOW_NODE_STATUS
`provisioning state is : {PASS, FAIL, UNEXECUTED}` **Meaning:** The SHOWNS command displays four key data points for a rehoming XPM. The Provisioning State indicates the status of the LTCINV and/or GATWYINV data manipulation while ABI Rehome is in progress on the Inactive XACore. This Provisioning State is only tracked for XPMs which are compatible with ABI C-side links. PASS indicates that the XPM's LTCINV and/or GATWYINV tuples have been successfully manipulated on the Inactive XACore while ABI Rehome is in progress. FAIL indicates that the XPM's LTCINV and/or GATWYINV tuples have failed manipulation on the Inactive XACore while ABI Rehome is in progress; the Installation Method should be referenced if this is unexpected. UNEXECUTED indicates that neither LTCINV nor GATWYINV tuple manipulation has been attempted for the XPM on the Inactive XACore while ABI Rehome is in progress. **System or user actions:** If FAIL is encountered reference the Installation Method for appropriate action.
`NoRestartSwact state is : {PASS, FAIL, UNEXECUTED}` **Meaning**: The SHOWNS command displays four key data points for a rehoming XPM. The NoRestartSwact state provides an indicator that the ABI Rehome functions associated with the NoRestartSwact have occurred. PASS indicates that the rehomed XPM has properly passed the NoRestartSwact step. FAIL indicates that the rehomed XPM has failed the NoRestartSwact step; the Installation Method should be referenced for appropriate action. UNEXECUTED indicates that the NoRestartSwact step has not yet been executed for the rehoming XPM. **System or user actions**: If FAIL is encountered reference the Installation Method for appropriate action.
`GWC Static Data Download state is : {PASS, FAIL, UNEXECUTED}` **Meaning:** The SHOWNS command displays four key data points for a rehoming XPM. The GWC Static Data Download state indicates the status of the static data download to the rehoming XPM's GWC. PASS indicates that the rehomed XPM's hosting GWC has received a static data update. FAIL indicates that the rehomed XPM's hosting GWC has not received a static data update, or the update was rejected. The GWC must properly receive a static data update following the ABI Rehome XACore SWACT. If the GWC does not properly receive the static data update, the rehomed XPM will not come in-service. If FAIL is encountered, reference the Installation Method for immediate corrective action. UNEXECUTED indicates that the GWC Static Data Download step has not yet been executed for the rehoming XPM. **System or user actions:** If FAIL is encountered reference the Installation Method for appropriate action.

Table 11 MAP outputs with associated meanings and actions

SHOW_NODE_STATUS
`Node number is not a supported ABI XPM` **Meaning:** The node number provided is not an XPM that can be supported from an ABI interface. The command will work whether the XPM is currently on an ENET/JNET interface or off of an ABI interface, but the XPM type must be able to be supported on either interface. **System or user actions:** None - informational only.

34.9.6.8 Example

Table 12 Usage examples for SHOW_NODE_STATUS command

Description of task:	

SHOW_NODE_STATUS 72	`Current ABI Rehome State is: ON`
	
	`Node 72: LTC_NODE LTC 1`
	`DS512 link verification result is: UNEXECUTED`
	`Provisioning state is : PASS`
	`NoRestartSwact state is : UNEXECUTED`
	`GWC Static Data Download state is: UNEXECUTED`

SHOW_NODE_STATUS ALL	`Current ABI Rehome State is: ON`
	
	`Node 18: LTC_NODE LGC 0`
	`DS512 link verification result is: UNEXECUTED`
	`Provisioning state is : PASS`
	`NoRestartSwact state is : UNEXECUTED`
	`GWC Static Data Download state is: UNEXECUTED`
	
	`Node 43: LTC_NODE LTC 4`
	`DS512 link verification result is: UNEXECUTED`
	`Provisioning state is : PASS`
	`NoRestartSwact state is : UNEXECUTED`
	`GWC Static Data Download state is: UNEXECUTED`
	
	`Node 72: LTC_NODE LTC 3`
	`DS512 link verification result is: UNEXECUTED`
	`Provisioning state is : PASS`
	`NoRestartSwact state is : UNEXECUTED`
	`GWC Static Data Download state is: UNEXECUTED`
	
	`Node 74: LTC_NODE LTC 5`
	`DS512 link verification result is: UNEXECUTED`
	`Provisioning state is : PASS`
	`NoRestartSwact state is : UNEXECUTED`
	`GWC Static Data Download state is: UNEXECUTED`

34.9.7 Command: ABIREHOME: DISP_LINK_CHANNEL_MAP / DLC

34.9.7.1 Command type: NON-MENU

34.9.7.2 Command target: All

34.9.7.3 Command availability: RES

34.9.7.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome"to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

This command is used to display the status of the node's links/channels.

34.9.7.5 Command syntax

Table 13 <CommandName> command parameters and variables

Command	Parameters and variables
DISP_LINK_CHANNEL_MAP or DLC	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <NODE NUMBER> {0 to 4095}

34.9.7.6 Qualifications and warnings

None.

34.9.7.7 Responses

34.9.7.7.1 DISP_LINK_CHANNEL_MAP responses

Table 14 MAP outputs with associated meanings and actions

DISP_LINK_CHANNEL_MAP

```
DISP_LINK_CHANNEL_MAP:  Displays the link/channel map for a node.
-----------------------------------------------------------------
Syntax: DISP_LINK_CHANNEL_MAP node
        or
        DLC node

Parms: <NODE NUMBER> {0 TO 4095}
```

Meaning: Help associated with command.

System or user actions: Informational purposes only.

```
ABIREHOME:
>dlc 68
Node Number:   68
Number of cside links:   16
     Link Information:
     LN: Link Number   LT: Link Type   FC: Free Channel
     LN    LT         FC       Link Channel Map (0 to 31)
                               0=busy, 1=idle
     ------------------------------------------------------
      0    Duplex      Y       01111111111111110111111111111111
      1    Duplex      Y       01111111111111110111111111111111
      2    Duplex      Y       01111111111111110111111111111111
      3    Duplex      Y       01111111111111110111111111111111
      4    Duplex      Y       01111111111111110111111111111111
      5    Duplex      Y       01111111111111110111111111111111
      6    Duplex      Y       01111111111111110111111111111111
      7    Duplex      Y       01111111111111110111111111111111
      8    Duplex      Y       01111111111111110111111111111111
      9    Duplex      Y       01111111111111110111111111111111
     10    Duplex      Y       01111111111111110111111111111111
     11    Duplex      Y       01111111111111110111111111111111
     12    Duplex      Y       01111111111111110111111111111111
     13    Duplex      Y       01111111111111110111111111111111
     14    Duplex      Y       01111111111111110111111111111111
     15    Duplex      Y       00000111111111110111111111111111
```

Meaning: Displays the link_chnl_map for the XPM. 0=busy, 1=idle. Messaging links show busy.

System or user actions: None. Information purposes only.

34.9.7.8 Example

Table 15 Usage examples for DISP_LINK_CHANNEL_MAP command

Description of task:	
dlc 68	Node Number: 68 Number of cside links: 16 Link Information: LN: Link Number LT: Link Type FC: Free Channel LN LT FC Link Channel Map (0 to 31) 0=busy, 1=idle --- 0 Duplex Y 01111111111111110111111111111111 1 Duplex Y 01111111111111110111111111111111 2 Duplex Y 01111111111111110111111111111111 3 Duplex Y 01111111111111110111111111111111 4 Duplex Y 01111111111111110111111111111111 5 Duplex Y 01111111111111110111111111111111 6 Duplex Y 01111111111111110111111111111111 7 Duplex Y 01111111111111110111111111111111 8 Duplex Y 01111111111111110111111111111111 9 Duplex Y 01111111111111110111111111111111 10 Duplex Y 01111111111111110111111111111111 11 Duplex Y 01111111111111110111111111111111 12 Duplex Y 01111111111111110111111111111111 13 Duplex Y 01111111111111110111111111111111 14 Duplex Y 01111111111111110111111111111111 15 Duplex Y 00000111111111110111111111111111

34.9.8 Command: ABIREHOME: DISP_LINK_INFO / DLI

34.9.8.1 Command type: NON-MENU

34.9.8.2 Command target: All

34.9.8.3 Command availability: RES

34.9.8.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

This command is used to display the status of the node and its links.

34.9.8.5 Command syntax

Table 16 DISP_LINK_INFO command parameters and variables

Command	Parameters and variables
DISP_LINK_INFO or DLI	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <NODE_NUMBER> {0 to 4095}

34.9.8.6 Qualifications and warnings

None.

34.9.8.7 Responses

34.9.8.7.1 DISP_LINK_INFO responses

Table 17 MAP outputs with associated meanings and actions

DISP_LINK_INFO

`DISP_LINK_INFO:  Displays the status of a node and its links.`
`----------`
`Syntax: DISP_LINK_INFO node`
`        or`
`        DLI node`
 	
`Parms: <NODE NUMBER> {0 TO 4095}`
 	
Meaning: Help associated with command.
 	
System or user actions: Informational purposes only.

`Node undefined.` **Meaning:** The given node is undefined. **System or user actions:** Try the command again with a valid node number.

Table 17 MAP outputs with associated meanings and actions

DISP_LINK_INFO

```
node 68:  LTC_NODE  SMA2 1,  node status:  status=sysb, cs=FALSE
cside links:
   0: node=  41, cap=MS-, port=   0; host=ok    port    0: ls=ok   cs=N ps=Y
   1: node=  41, cap=MS-, port=   1; host=ok    port    1: ls=ok   cs=N ps=Y
   2: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
   3: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
   4: node=  41, cap=MS-, port=   2; host=ok    port    2: ls=ok   cs=N ps=Y
   5: node=  41, cap=MS-, port=   3; host=ok    port    3: ls=ok   cs=N ps=Y
   6: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
   7: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
   8: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
   9: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  10: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  11: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  12: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  13: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  14: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  15: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  16: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  17: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  18: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  19: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  20: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  21: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  22: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  23: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  24: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  25: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  26: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  27: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  28: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  29: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  30: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
  31: node=  41, cap=-S-, port=4095; host=ok    port 4095: ls=ok   cs=N ps=N
pside links:
   0:   node=  77, cap=MS-, port=   0, ls=offl,clos cs=Y ps=Y;  psn: manb
   1:   node=  77, cap=MS-, port=   1, ls=offl,clos cs=Y ps=Y;  psn: manb
   2:   node=  77, cap=-S-, port=   2, ls=offl,clos cs=Y ps=Y;  psn: manb
   3:   node=  77, cap=-S-, port=   3, ls=offl,clos cs=Y ps=Y;  psn: manb
```

Meaning: Displays information about both the cside and pside links for an XPM.

System or user actions: None. Informational only.

34.9.8.8 Example

Table 18 Usage examples for DISP_LINK_INFO

Description of task:	
DISP_LINK_INFO 68	node 68: LTC_NODE SMA2 1, node status: status=sysb, cs=FALSE cside links: 0: node= 41, cap=MS-, port= 0; host=ok port 0: ls=ok cs=N ps=Y 1: node= 41, cap=MS-, port= 1; host=ok port 1: ls=ok cs=N ps=Y 2: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 3: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 4: node= 41, cap=MS-, port= 2; host=ok port 2: ls=ok cs=N ps=Y 5: node= 41, cap=MS-, port= 3; host=ok port 3: ls=ok cs=N ps=Y 6: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 7: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 8: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 9: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 10: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 11: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 12: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 13: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 14: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 15: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 16: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 17: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 18: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 19: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 20: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 21: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 22: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 23: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 24: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 25: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 26: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 27: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 28: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 29: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 30: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 31: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N pside links: 0: node= 77, cap=MS-, port= 0, ls=offl,clos cs=Y ps=Y; psn: manb 1: node= 77, cap=MS-, port= 1, ls=offl,clos cs=Y ps=Y; psn: manb 2: node= 77, cap=-S-, port= 2, ls=offl,clos cs=Y ps=Y; psn: manb 3: node= 77, cap=-S-, port= 3, ls=offl,clos cs=Y ps=Y; psn: manb

34.9.9 Command: ABIREHOME: DISP_IOUI_ROUTE_DATA / DRD

34.9.9.1 Command type: NON-MENU

34.9.9.2 Command target: All

34.9.9.3 Command availability: RES

34.9.9.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

Displays the current IOUI routing data associated with the given node.

34.9.9.5 Command syntax

Table 19 DISP_IOUI_ROUTE_DATA/DRD command parameters and variables

Command	Parameters and variables
DISP_IOUI_ROUTE_DATA or DRD	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <NODE NUMBER> {0 to 4095}

34.9.9.6 Qualifications and warnings

None.

34.9.9.7 Responses

34.9.9.7.1 DISP_IOUI_ROUTE_DATA / DRD responses

Table 20 MAP outputs with associated meanings and actions

DISP_IOUI_ROUTE_DATA/DRD

`DISP_IOUI_ROUTE_DATA:  Displays the IOUI Route Data for given node`
`----------`
`Syntax: DISP_IOUI_ROUTE_DATA node`
`or`
`DRD node`
 	
`Parms: <NODE NUMBER> {0 TO 4095}`
 	
Meaning: Help associated with command.
 	
System or user actions: Informational purposes only.

`Node undefined.` **Meaning:** The given node is undefined. **System or user actions:** Try the command again with a valid node number.

Table 20 MAP outputs with associated meanings and actions

DISP_IOUI_ROUTE_DATA/DRD
Node 69: LTC_NODE SMA2 1 node_data3 info: msg_format: jts mts network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 dms_msg_route: network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 **Meaning:** Shows the current values of the internal data structures relating to the IOUI routing data when the node provided is a packet node. This is the data that is impacted by the NRS procedures, and will be different on the active and inactive sides when a node has been rehomed. **System or user actions:** Informational and debug purposes only.
Node 47: LTC_NODE DTC 0 node_data3 info: msg_format: jts mts network: internal dms_msg_route: network: internal **Meaning:** Shows the current values of the internal data structures relating to the IOUI routing data when the node provided is a TDM node. This is the data that is impacted by the NRS procedures, and will be different on the active and inactive sides when a node has been rehomed. **System or user actions:** Informational and debug purposes only.

34.9.9.8 Example

Table 21 Usage examples for command

Description of task:	
drd 69	Node 69: LTC_NODE SMA2 1 node_data3 info: msg_format: jts mts network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 dms_msg_route: network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683

Table 21 Usage examples for command

drd 47	Node 47: LTC_NODE DTC 0 node_data3 info: msg_format: jts mts network: internal dms_msg_route: network: internal

34.9.10 Command: ABIREHOME: SET_ABI_REHOME_STATUS

34.9.10.1 Command type: NON-MENU

34.9.10.2 Command target: All

34.9.10.3 Command availability: RES

34.9.10.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

This command allows TAS personnel the ability to control the rehome status in an office. If affects both an overall control boolean and the initialization of per node rehome status data. In addition, this command enables the ability to position on the XPM's tuple in table LTCINV and execute a CHA, as opposed to deleting and re-adding the tuple.

34.9.10.5 Command syntax

Table 22 <CommandName> command parameters and variables

Command	**Parameters and variables**
SET_ABI_REHOME_STATUS	<STATUS> {ON, OFF, SUSPEND, RESUME}
Parameters and variables	Description
ON	Sets the control bool to TRUE and initializes all node rehome data to default values.
OFF	Sets the control bool to FALSE and initializes all node rehome data to default values.
SUSPEND	Sets the control bool to FALSE, leaving the per node rehome data as is.
RESUME	Sets the control bool to TRUE, leaving the per node rehome data as is.

34.9.10.6 Qualifications and warnings

In all cases, a warning message will be output to user that this command enables highly dangerous functionality and should be used by experienced personnel only, giving the user the option to quit.

In all cases, the current status of the rehome (ON, OFF, SUSPENDED) will be displayed prior to any parameter specific messages.

34.9.10.7 Responses

34.9.10.7.1 SET_ABI_REHOME_STATUS responses

Table 23 MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
SET_ABI_REHOME_STATUS: Turns on the main ABI Rehome status ---------- Syntax: SET_ABI_REHOME_STATUS Parms: <STATUS> Parms: <STATUS> {ON, OFF, SUSPEND, RESUME} **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command is intended for use during the rehoming of XPMs to an ABI interface on an MG9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with the IM. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): **Meaning:** Output regardless of status entered. This response warns the user that this command could result in an outage and that it should be executed by experienced personnel only. **System or user actions:** If the user is not qualified to proceed, he should enter NO and the command will exit at this point.

Table 23 MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
`Current ABI Rehome State is: {ON, OFF, SUSPENDED}` **Meaning:** Output regardless of status entered. If ON, the rehome process has been enabled. If OFF, the rehome process has been disabled, and all node rehome data is currently at default values. If SUSPENDED, a rehome was begun, and interrupted by the user. In this state, the control bool is FALSE, but there could be node rehome data that is not at default values. **System or user actions:** None. This is for informational purposes.
`ABI Rehome state is already ON. Rehome data not impacted..` **Meaning:** The user is attempting to turn ON the rehome status when it is already ON. **System or user actions:** None. This is for informational purposes.
`Continuing with this command will cause all existing node rehome data to be lost. Consider using RESUME instead. Do you wish to continue?` continue=no ‘SET_REHOME_STATUS command aborted by user.’ **Meaning:** The user is attempting to turn ON the rehome status when it is currently SUSPENDED. If there is an per node rehome data, it will be re initialized to default values. **System or user actions:** The user has an opportunity to abort the command, at which point they will receive the continue=no response.
`Command Successful. ABI Rehome has been turned ON.` **Meaning:** The ABI Rehome status has been turned ON and all per node rehome data has been initialized to default values. **System or user actions:** None.
`Failed to enable ABI Rehome. Please check for swerrs.` **Meaning:** The command to enable the ABI rehome has failed for some reason. **System or user actions:** Use the QUERY_ABI_REHOME_STATUS to determine current status and if any part is ON, use the SET_ABI_REHOME_STATUS to turn OFF.
`ABI Rehome state is already OFF. Rehome data not impacted.` **Meaning:** The user is attempting to turn OFF the ABI rehome status when it is already OFF. **System or user actions:** None.

Table 23 MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
`Continuing with this command will cause all existing node rehome data to be lost. Do you wish to continue?` continue=no ‘SET_REHOME_STATUS command aborted by user. **Meaning:** The user is attempting to turn OFF the ABI tool when it is currently ON or SUSPENDED. This could cause a loss of the per node rehome data. **System or user actions:** Opportunity to abort, in which case user gets the continue = no output.
`ABI Rehome has been turned OFF.` **Meaning:** The control bool has been turned OFF, and per node rehome data initialized to default values. **System or user actions:** None - informational only.
`Failed to disable the ABI Rehome. Please check for swerrs.` **Meaning:** The attempt to turn OFF the ABI rehome state has failed. **System or user actions:** Should not occur. Indicates a problem.
`Cannot SUSPEND - ABI Rehome is not ON.` **Meaning:** The user is attempting to SUSPEND the rehome status when it is not ON. **System or user actions:** None - informational only.
`ABI Rehome has been SUSPENDED.` **Meaning:** The control bool has been turned OFF, and per node rehome data was left intact. **System or user actions:** None - informational only.
`Failed to suspend ABI Rehome. Please check for swerrs.` **Meaning:** The attempt to suspend the ABI rehome state has failed. **System or user actions:** Should not occur. Indicates a problem.
`Cannot RESUME - ABI Rehome is not SUSPENDED.` **Meaning:** RESUME only makes sense when the rehome state was suspended. No data has been impacted. **System or user actions:** None - informational only.

Table 23 MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
`ABI Rehome has been RESUMED.` **Meaning:** The control bool has been turned ON, and per node rehome data was left intact. **System or user actions:** None - informational only.
`Failed to resume ABI Rehome. Please check for swerrs.` **Meaning:** The attempt to resume the ABI rehome state has failed. **System or user actions:** Should not occur. Indicates a problem.

34.9.10.8 Example

Table 24 Usage examples for SET_ABI_REHOME_STATUS command

Description of task:	
SET_ABI_REHOME_STATUS ON	`This command is intended for use during the rehoming of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed?` `Current ABI Rehome State is: SUSPENDED` `Continuing with this command will cause all existing node rehome data to be lost. Consider using RESUME instead. Do you wish to continue?` `>N` `SET_REHOME_STATUS command aborted by user.`
SET_ABI_REHOME_STATUS OFF	`This command is intended for use during the rehoming of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed?` `Current ABI Rehome State is: ON` `Continuing with this command will cause all existing node rehome data to be lost. Do you wish to continue?` `Y` `'ABI Rehome has been turned OFF.`
SET_ABI_REHOME_STATUS SUSPEND	`This command is intended for use during the rehoming of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed?` `Current ABI Rehome State is: ON` `ABI Rehome has been SUSPENDED.`

Table 24 Usage examples for SET_ABI_REHOME_STATUS command

SET_ABI_REHOME_STATUS RESUME	This command is intended for use during the rehoming of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Current ABI Rehome State is: SUSPENDED ABI migration has been RESUMED.

34.9.11 Command: ABIREHOME: ADJUST_FRAME_SYNC / AFS

34.9.11.1 Command type: NON-MENU

34.9.11.2 Command target: All

34.9.11.3 Command availability: RES

34.9.11.4 Command description

This command is used as a part of Installation Method 72-1639 “XPM - ABI Link Verification” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the XPM to be rehomed, this command will cause the ABI cards to adjust their frame sync to that of the inactive XPM unit. This is one step in the process of verifying the DS-512 fiber connection of the XPM before the actual rehome occurs.

34.9.11.5 Command syntax

Table 25 command parameters and variables

Command	**Parameters and variables**
ADJUST_FRAME_SYNC or AFS	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <XPM_NODE> {0 to 4095}

34.9.11.6 Qualifications and warnings

None.

34.9.11.7 Responses

34.9.11.7.1 ADJUST_FRAME_SYNC responses

Table 26 MAP outputs with associated meanings and actions

ADJUST_FRAME_SYNC
ADJUST_FRAME_SYNC: Adjust the frame sync on the ABI cards to sync to the inactive XPM unit. --- Syntax: ADJUST_FRAME_SYNC node or AFS node Parms: <NODE NUMBER> {0 TO 4095} **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command must be enabled via the SET_ABI_REHOME_STATUS command. Please refer to the installation method. **Meaning:** The ABI REHOME installation method has not been enabled. SET_ABI_REHOME_STATUS (ON or RESUME) commands must be enabled via ABIREHOME tool before proceeding. **System or user actions:** If user wishes to proceed with the command, ABIREHOME will have to enable the tool.
This command will RESET the frame sync on the ABI cards.Both ABI cards must be locked and unlocked to recover from this condition. Do you wish to continue? **Meaning:** Adjust the frame sync on the ABI cards to sync to the inactive XPM unit. **System or user actions:** Enter the correct response.
AFS command aborted by user. **Meaning:** Command was aborted by the user and no action has been taken. **System or user actions:** Informational purposes only.

Table 26 MAP outputs with associated meanings and actions

ADJUST_FRAME_SYNC
`No reply received from ABI. Adjust Frame Sync FAILED. Check for swerrs and traps.` **Meaning:**Indicates a problem with the software. Contact Nortel for support. **System or user actions:** Use the FAN command to see what nodes were likely impacted and compare to the QIN (impacted nodes) output. User should refer to the installation method to determine how to proceed.

34.9.11.8 Example

Table 27 Usage examples for command

Description of task:	

AFS 69	`>afs 103`
	`Node 103: LTC_NODE SMA2 7 ( SMA2 7 )`
	
	`This command will RESET the frame sync on the ABI cards.`
	`Both ABI cards must be locked and unlocked to recover from`
	`this condition.`
	`Do you wish to continue?`
	
	`Please confirm ("YES", "Y", "NO", or "N"):`
	`>y`

34.9.12 Command: ABIREHOME:MARK_NODE_DS512_RESULT /VER512

34.9.12.1 Command type: NON-MENU

34.9.12.2 Command target: All

34.9.12.3 Command availability: RES

34.9.12.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to set the DS512 verification result for a node.

34.9.12.5 Command syntax

Table 28 MARK_NODE_DS512_RESULT command parameters and variables

Command	Parameters and variables
MARK_NODE_DS512_RESULT or VER512	<NODE NUMBER> < FAIL or PASS>
Parameters and variables	Description
NODE NUMBER	The Node number of the xpm.
PASS	Sets the DS512 link verification result of the node to PASS.
FAIL	Sets the DS512 link verification result of the node to FAIL.

34.9.12.6 Qualifications and warnings

In all cases, a warning message will be output to user wether he wants to continue with the operation. It has options YES and NO.

In all cases, the current status of the DS512 is displayed(UNEXECUTED, PASS, FAIL).

34.9.12.7 Responses

34.9.12.7.1 MARK_NODE_DS512_RESULT responses

Table 29 MAP outputs with associated meanings and actions

MARK_NODE_DS512_RESULT

```
MARK_NODE_DS512_RESULT: Marks the PASS/FAIL result of the
                        specified node.
-------------------------------------------------------
Syntax: MARK_NODE_DS512_RESULT node PASS/FAIL
        or
        VER512 node PASS/FAIL

Parms: <NODE NUMBER> {0 TO 4095}
       <FAIL or PASS> {FAIL,
                       PASS}
```

Meaning: Help associated with command.

System or user actions: Informational purposes only.

Table 29 MAP outputs with associated meanings and actions

MARK_NODE_DS512_RESULT
Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): **Meaning:** This response warns the user wether he wants to continue with the setting of DS512 Result for the node. **System or user actions:** If the user is not qualified to proceed, he should enter NO and the command will exit at this point.
Current MARK_NODE_DS512_RESULT State is: {UNEXECUTED, PASS, FAIL} **Meaning:** Displays the current status of the DS512 Result of the node. **System or user actions:** None. This is for informational purposes.

34.9.12.8 Example

Table 30 Usage examples for MARK_NODE_DS512_RESULT command

Description of task:	
MARK_NODE_DS512_RESULT 72 PASS	Current DS512 result for this node is: UNEXECUTED Current ABI Rehome State is: SUSPENDED Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >N VER512 command aborted by user.
MARK_NODE_DS512_RESULT 72 PASS	Node 72: LTC_NODE LTC 3 Current DS512 result for this node is: UNEXECUTED Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y
MARK_NODE_DS512_RESULT 72 FAIL	Current DS512 result for this node is: UNEXECUTED Current ABI Rehome State is: SUSPENDED Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >N VER512 command aborted by user.
MARK_NODE_DS512_RESULT 72 FAIL	Node 72: LTC_NODE LTC 3 Current DS512 result for this node is: UNEXECUTED Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y

34.9.13 Command: ABIREHOME: SEND_GWC_STATIC_DATA / GWCSD

34.9.13.1 Command type: NON-MENU

34.9.13.2 Command target: All

34.9.13.3 Command availability: RES

34.9.13.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

This command will send limited static data updates to the GWCs affected by the XPM Rehomes.

34.9.13.5 Command syntax

Table 31 command parameters and variables

Command	Parameters and variables
GWCSD	n/a
Parameters and variables	Description
n/a	

34.9.13.6 Qualifications and warnings

None.

34.9.13.7 Responses

34.9.13.7.1 SEND_GWC_STATIC_DATA responses

Table 32 MAP outputs with associated meanings and actions

SEND_GWC_STATIC_DATA
GWCSD: Send ABI XPM static data to their GWCs. --- Syntax: GWCSD Parms: none **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command will send limited static data updates to the GWCs affected by the XPM Rehomes. Do you wish to continue? **Meaning:** Command to send the static data from the XACore to the GWC after a NoRestartSwact. **System or user actions:** Enter the correct response.
GWCSD command aborted by user. **Meaning:** Command was aborted by the user and no action has been taken. **System or user actions:** Informational purposes only.
Cannot execute GWCSD from the inactive core. **Meaning:** The GWCSD command needs to be executed from the Active core, and not from the inactive core. **System or user actions:** Execute this command in the Active core.

34.9.13.8 Example

Table 33 Usage examples for command

Description of task:	
GWCSD	>gwcsd This command will send limited static data updates to the GWCs affected by the XPM Rehomes. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y >

34.9.14 Command: ABIREHOME: ABORT_GWC_STATIC_DATA / ABORT_GWCSD

34.9.14.1 Command type: NON-MENU

34.9.14.2 Command target: All

34.9.14.3 Command availability: RES

34.9.14.4 Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/ JNET C-side links to an ABI DS-512 off of an MG 9000.

This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes.

34.9.14.5 Command syntax

Table 34 command parameters and variables

Command	Parameters and variables
ABORT_GWCSD	n/a
Parameters and variables	Description
n/a	

34.9.14.6 Qualifications and warnings

None.

34.9.14.7 Responses

34.9.14.7.1 ABORT_GWC_STATIC_DATA responses

Table 35 MAP outputs with associated meanings and actions

ABORT_GWC_STATIC_DATA
`ABORT_GWCSD command aborted by user.` **Meaning:** Command was aborted by the user and no action has been taken. **System or user actions:** Informational purposes only.

Table 35 MAP outputs with associated meanings and actions

ABORT_GWC_STATIC_DATA
ABORT_GWCSD: UNDO ABI XPM static data in the GWCs. --- Syntax: ABORT_GWCSD Parms: none **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. This command should only be used in conjunction with XACore AbortSwact. Do you wish to continue? **Meaning:** This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. **System or user actions:** Enter the correct response.
Cannot execute ABORT_GWC_STATIC_DATA from the inactive core. **Meaning:** The GWCSD command needs to be executed from the Active core, and not from the inactive core. **System or user actions:** Execute this command in the Active core.

34.9.14.8 Example

Table 36 Usage examples for command

Description of task:	
ABORT_GWCSD	This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. This command should only be used in conjunction with XACore AbortSwact. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y >

34.9.15 Command: ABIREHOME: LINE_STATUS_CHG

34.9.15.1 Command type: NON-MENU

34.9.15.2 Command target: All

34.9.15.3 Command availability: RES

34.9.15.4 Command description

This command is used as a part of Installation Method 72-0668 "XPM to MG 9000 DS-512 Rehome Office Collapse" to enable the ability to rehome an XPM with subdented LCMs from an ‘old’ end office to an ABI DS-512 interface in the CS 2000 end office.

This command will permit the user to change the status of a range of LENs from INstallation Busy, MANual Busy or Line Module Busy to INstallabion Busy, MANual Busy or Line Module Busy.

34.9.15.5 Command syntax

Table 37 command parameters and variables

Command	Parameters and variables
LINE_STATUS_CHG	<ACTION> {COUNT, CHANGE} FROM <STARTLEN> {SITE FRAME UNIT DRAWER CIRCUIT} TO <ENDLEN> {SITE FRAME UNIT DRAWER CIRCUIT} <From State> {INB, MAN, LMB} <To State> {INB, MAN, LMB}
Parameters and variables	Description
ACTION	This parameter specifies the task to be performed by the command. COUNT displays the current maintenance status for all LENs in the specified range. CHANGE alters the maintenance status for all LENs in the range, per user specified states. `<ACTION> {COUNT, CHANGE}`

STARTLEN	Keyword FROM followed by the first LEN in the desired range, including SITE FRAME UNIT DRAWER CIRCUIT information.
	
	`<STARTLEN> {FROM <Site:  > STRING`
	`<Frame:  > {0 TO 511}`
	`<Unit:  > {0 TO 9}`
	`<Drawer: > {0 TO 31}`
	`<Circuit:> {0 TO 99}}`

Table 37 command parameters and variables

Command	Parameters and variables

ENDLEN	Keyword TO followed by the last LEN in the desired range, including SITE FRAME UNIT DRAWER CIRCUIT information.
	
	`<ENDLEN> {TO <Site: > STRING`
	`<Frame: > {0 TO 511}`
	`<Unit: > {0 TO 9}`
	`<Drawer: > {0 TO 31}`
	`<Circuit:> {0 TO 99}}`

From State	This parameter is required if the ACTION is CHANGE. If the ACTION is COUNT, and the user includes a From State, this input is ignored. `<From State> {INB, MAN, LMB}`
To State	This parameter is required if the ACTION is CHANGE. If the ACTION is COUNT, and the user includes a From State, this input is ignored. `<To State> {INB, MAN, LMB}`

34.9.15.6 Qualifications and warnings

None.

34.9.15.7 Responses

34.9.15.7.1 LINE_STATUS_CHG responses

Table 38 MAP outputs with associated meanings and actions

LINE_STATUS_CHG
Command to count or change state of selected lines Parms: <ACTION> {COUNT, CHANGE} <STARTLEN> {FROM <Site: > STRING <Frame: > {0 TO 511} <Unit: > {0 TO 9} <Drawer: > {0 TO 31} <Circuit:> {0 TO 99}} <ENDLEN> {TO <Site: > STRING <Frame: > {0 TO 511} <Unit: > {0 TO 9} <Drawer: > {0 TO 31} <Circuit:> {0 TO 99}} [<From State> {INB, MAN, LMB}] [<To State> {INB, MAN, LMB}] **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command must be enabled via the SET_ABI_REHOME_STATUS command. Please refer to the installation method. **Meaning:** The current ABI Rehome state is not ON. LINE_STATUS_CHG is only available for use if the state is ON. **System or user actions:** Follow the instructions in the appropriate installation method, using SET_ABI_REHOME_STATUS command to enable the LINE_STATUS_CHG command.
CPB: 0 IDLE: 0 LMB: 0 MANB: 0 INB: 3 CUTOFF: 0 UNEQUIPPED: 5 OTHER: 0 ---------- TOTAL:8 LINESTAT: Number of lines scanned :8 LINESTAT: Number of lines changed :0 **Meaning:** The user entered a COUNT action for a range of 8 LENs. The states are displayed. **System or user actions:** Informational purposes only.

Table 38 MAP outputs with associated meanings and actions

LINE_STATUS_CHG

`You are about to CHANGE the maintenance state of these LENs.`
 	
`Do you wish to continue?`
 	
`Please confirm ("YES", "Y", "NO", or "N"):`
 	
Meaning: If the user executes the CHANGE action in LINE_STATUS_CHG, this prompt will provide an opportunity to confirm the action.
 	
System or user actions: The user must answer the YES / NO prompt.

`LINE_STATUS_CHG command aborted by user.` **Meaning:** Command was aborted by the user and no action has been taken. **System or user actions:** Informational purposes only.

`LINESTAT: Changing...`
`LINESTAT: Number of lines scanned :3`
`LINESTAT: Number of lines changed :2`
 	
Meaning: The user entered a CHANGE action for a range of 3 LENs, and 2 of those LENs in that range had their maintenance state changed. The other LEN did not match the original state, and therefore was not changed.
 	
System or user actions: Informational purposes only.

`EITHER incorrect optional parameter(s) OR too many parameters.` **Meaning:** User input invalid parameter information, and the request is rejected.. **System or user actions:** Informational purposes only.
`STARTLEN is invalid` **Meaning:** User input invalid STARTLEN information, and the request is rejected.. **System or user actions:** Informational purposes only.
`ENDLEN is invalid` **Meaning:** User input invalid ENDLEN information, and the request is rejected.. **System or user actions:** Informational purposes only.

34.9.15.8 Example

Table 39 Usage examples for command

Description of task:	
line_status_chg count from host 0 0 0 13 to host 0 0 0 20	CPB: 0 IDLE: 0 LMB: 0 MANB: 0 INB: 3 CUTOFF: 0 UNEQUIPPED: 5 OTHER: 0 ---------- TOTAL:8 LINESTAT: Number of lines scanned :8 LINESTAT: Number of lines changed :0
line_status_chg change from host 0 0 0 13 to host 0 0 0 20 inb lmb	You are about to CHANGE the maintenance state of these LENs. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y LINESTAT: Changing... LINESTAT: Number of lines scanned :8 LINESTAT: Number of lines changed :3

34.9.16 Hidden Commands: ABIREHOME:SLC (set link channel map)

34.9.16.1 Command type: NON-MENU

34.9.16.2 Command target: All

34.9.16.3 Command availability: RES

34.9.16.4 Command description

This HIDDEN command is used for debugging / correcting errors encounteed as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

This command allows the user to reset the link_chnl_map for an XPM. This command is invasive and dangerous, and should be used by qualified Nortel personnel.

34.9.16.5 Command syntax

Table 40 SET_LINK_CHANNEL_MAP command parameters and variables

Command	Parameters and variables
SLC	node
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <NODE NUMBER> {0 to 4095}

34.9.16.5.1 Qualifications and warnings

None.

34.9.16.6 Responses

34.9.16.6.1 SET_LINK_CHANNEL_MAP responses

Table 41 MAP outputs with associated meanings and actions

SET_LINK_CHANNEL_MAP

`SET_LINK_CHANNELS_IDLE:  Sets the link/channel map for a node to idle.`
`----------`
`Syntax:  SLC node`
 	
`Parms: <NODE NUMBER> {0 TO 4095}`
 	
Meaning: Help associated with command.
 	
System or user actions: Informational purposes only.

`This command must be enabled by TAS. Please refer to IM 72-1682.` **Meaning:** The control bool to enable the command has not been turned on. **System or user actions:** Go into ABIREHOME tool and use command SET_REHOME_STATUS ON to turn on the tool. Password required.

Table 41 MAP outputs with associated meanings and actions

SET_LINK_CHANNEL_MAP
`Node number is not a supported XPM.` **Meaning:** The command is ended because the node number entered is not a node number of a valid XPM that can exist off of an ABI interface. The node number can be either ABI connected or ENET/ JNET connected, but must be ABLE to be ABI connected. **System or user actions:** Get the right node number and reenter the command. The PMIST NODENO command can be used to get the correct node number.
`Current IO format is: External` **Meaning:** The node is currently provisioned as a packet node off of an ABI interface. **System or user actions:** None. Informational purposes.
`Current IO format is: Internal` **Meaning:** The node is currently provisioned as a tdm node off of an ENET/JNET. **System or user actions:** None. Informational purposes.

`This command can be service impacting. Do you wish to continue?`
`If continue=no: SLC command aborted by user.`
 	
Meaning: Resetting the link channel map is dangerous if used improperly. This is the last chance to change your mind.
 	
System or user actions: Enter desire to continue.

`Links/Channels have been reset for node <node number>.` **Meaning:** The command was successful. **System or user actions:** None, but user can choose to use DLC to verify results.
`Trouble resetting links/channels on node <node number>.` **Meaning:** Something was wrong and the link channel map could not be reset. **System or user actions:** Look for swerrs and report problem. Use DLC to display current values.

34.9.16.7 Example

Table 42 Usage examples for SET_LINK_CHANNEL_MAP command

Description of task:	

SLC 68	`Current IO format is: External`
	`This command can be service impacting. Do you wish to continue?`
	`Yes`
	`Links/Channels have been reset for node 68.`

34.9.17 Hidden Command: ABIREHOME: SAN (SET AFFECTED NODES)

34.9.17.1 Command type: NON-MENU

34.9.17.2 Command target: All

34.9.17.3 Command availability: RES

34.9.17.4 Command description

This HIDDEN command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, sets the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

This command should not be executed manually during the rehome process. All nodes being rehomed will be properly marked as 'affected' by table control operations or by NDS personnel. This command is available only for trouble recovery by qualified personnel.

34.9.17.5 Command syntax

Table 43 command parameters and variables

Command	Parameters and variables
SAN	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <XPM_NODE> {0 to 4095}

34.9.17.6 Qualifications and warnings

None.

34.9.17.7 Responses

34.9.17.7.1 responses

Table 44 MAP outputs with associated meanings and actions

SET_AFFECTED_NODES/SAN
SAN (SET_AFFECTED_NODES) Protected command for ABI Rehomes. Sets the rehome node bits for all nodes that are impacted by rehoming the given XPM, including its subtending nodes. Nodes must be marked as impacted on the INACTIVE processor. ---------- Syntax: SAN node Parms: <NODE NUMBER> {0 TO 4095} **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
Node number is not a supported XPM. **Meaning:** The node number entered cannot be homed off of an ABI interface, and is therefore not a valid XPM for this command. **System or user actions:** Enter the correct node number of the rehomed XPM.
This command will SET the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? **Meaning:** Warning that using this command will set triggers that will impact the behavior of a NRS. **System or user actions:** Enter the correct response.
SAN command aborted by user. **Meaning:** Response indicating the command was aborted by the user and no action was taken. **System or user actions:** Informational purposes only.
Node 69: LTC_NODE SMA2 1 Set affected nodes PASSED. Use FIND_AFFECTED_NODES/FAN to see the nodes impacted. **Meaning:** Displays the XPM node provided, shows that the command passed, and suggests using the FAN command to see what nodes were impacted. **System or user actions:**

34.9.17.8 Example

Table 45 Usage examples for command SET_AFFECTED_NODES

Description of task:	

Table 45 Usage examples for command SET_AFFECTED_NODES

SAN 69	This command will SET the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y Node 69: LTC_NODE SMA2 1 Set affected nodes PASSED. Use FIND_AFFECTED_NODES/FAN to see the nodes impacted.

34.9.18 Hidden Command: ABIREHOME: CAN (CLEAR AFFECTED NODE)

34.9.18.1 Command type: NON-MENU

34.9.18.2 Command target: All

34.9.18.3 Command availability: RES

34.9.18.4 Command description

This HIDDEN command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, clears the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

This command should not be executed manually during the rehome process. Nodes which have been marked as 'affected' during table control operations, or by NDS personnel, should not be cleared by this command. This command is available only for trouble recovery by qualified personnel.

34.9.18.5 Command syntax

Table 46 command parameters and variables

Command	Parameters and variables
CAN	<NODE NUMBER> {0 to 4095}
Parameters and variables	Description

Table 46 command parameters and variables

Command	Parameters and variables
node	Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map. <XPM_NODE> {0 to 4095}

34.9.18.6 Qualifications and warnings

None.

34.9.18.7 Responses

34.9.18.7.1 CLEAR_AFFECTED_NODES responses

Table 47 MAP outputs with associated meanings and actions

CLEAR_AFFECTED_NODES

`CAN (CLEAR_AFFECTED_NODES) Protected command for ABI Rehomes.`
`Clear the rehome node bits for all nodes that are impacted by`
`rehoming the given XPM, including its subtending nodes.`
`----------`
`Syntax: CAN node`
 	
`Parms: <NODE NUMBER> {0 TO 4095}`
 	
Meaning: Help associated with command.
 	
System or user actions: Informational purposes only.

`This command will CLEAR the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue?` **Meaning:** Warning that using this command will set triggers that will impact the behavior of a NRS. **System or user actions:** Enter the correct response.
`CAN command aborted by user.` **Meaning:** Command was aborted by the user and no action has been taken. **System or user actions:** Informational purposes only.

Table 47 MAP outputs with associated meanings and actions

CLEAR_AFFECTED_NODES

`Node 69: LTC_NODE SMA2 1`
`Clear affected nodes PASSED.`
`Use FIND_AFFECTED_NODES to see the nodes impacted.`
 	
Meaning: The impacted node bools have been cleared for this XPM and all of its subtending nodes. To see the nodes affected, use the FAN command. To see the current list of impacted nodes, use the QIN command. This command can be used to clear the impacted node table if it was inadventantly set via the SAN command.
 	
System or user actions: Informational purposes.

`Clear affected nodes FAILED. Check for swerrs and traps.` **Meaning:**Indicates a problem with the software. Contact Nortel for support. **System or user actions:** Use the FAN command to see what nodes were likely impacted and compare to the QIN (impacted nodes) output. User should refer to the installation method to determine how to proceed.

34.9.18.8 Example

Table 48 Usage examples for command

Description of task:	

CAN 69	`>can 69`
	
	`This command will CLEAR the impacted node table bools for this XPM and all of its subtending nodes.`
	`Do you wish to continue?`
	
	`Please confirm ("YES", "Y", "NO", or "N"):`
	`>y`
	`Node 69: LTC_NODE SMA2 1`
	
	`Clear affected nodes PASSED.`
	`Use FIND_AFFECTED_NODES to see the nodes impacted.`

34.9.19 Hidden Command: ABIREHOME: CLEAR_GWC_SD_TABLE

34.9.19.1 Command type: NON-MENU

34.9.19.2 Command target: All

34.9.19.3 Command availability: RES

34.9.19.4 Command description

This HIDDEN command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

When this command is executed, it will clear the Rehome static data updates that have been stored through the Rehome procedure.

34.9.19.5 Command syntax

Table 49 command parameters and variables

Command	Parameters and variables
CLEAR_GWC_SD_TABLE	n/a
Parameters and variables	Description
n/a	n/a

34.9.19.6 Qualifications and warnings

In all cases, a warning message will be output to user wether he wants to continue with the operation. It has options YES and NO.

34.9.19.7 Responses

34.9.19.7.1 CLEAR_GWC_SD_TABLE responses

Table 50 MAP outputs with associated meanings and actions

CLEAR_GWC_SD_TABLE
CLEAR_GWC_SD_TABLE: Clear all GWC static data transactions. NOT for use in the field! --- Syntax: CLEAR_GWC_SD_TABLE Parms: none **Meaning:** Help associated with command. **System or user actions:** Informational purposes only.
This command will clear the Rehome static data updates that have been stored through the Rehome procedure. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): **Meaning:** Clears the static data updates that have been stored through the Rehome process. **System or user actions:** Enter the correct response.
CLEAR_GWC_SD_TABLE command aborted by user. **Meaning:** The Rehome static data updares will not be cleared. The command has been aborted. **System or user actions:** Informational purposes only. If user wishes to proceed with the command, TAS will have to enable the tool.

34.9.19.8 Example

Table 51 Usage examples for command

Description of task:	
CLEAR_GWC_SD_TABLE	This command will clear the Rehome static data updates that have been stored through the Rehome procedure. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y
CLEAR_GWC_SD_TABLE	This command will clear the Rehome static data updates that have been stored through the Rehome procedure. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >n CLEAR_GWC_SD_TABLE command aborted by user.

34.9.20 Hidden Command: ABIREHOME: SHOW_GWCSD

34.9.20.1 Command type: NON-MENU

34.9.20.2 Command target: All

34.9.20.3 Command availability: RES

34.9.20.4 Command description

This HIDDEN command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

When this command is executed, it will show the Rehome static data updates that have been stored through the Rehome procedure.

34.9.20.5 Command syntax

Table 52 command parameters and variables

Command	Parameters and variables
SHOW_GWCSD	none
Parameters and variables	Description
n/a	n/a

34.9.20.6 Qualifications and warnings

none.

34.9.20.7 Responses

none.

34.9.20.8 Example

Table 53 Usage examples for command

Description of task:	

Table 53 Usage examples for command

SHOW_GWCSD	curr: 0 config_upd_data: 0 changed: 0 added : N deleted: N cslinks: N csnodes: node: 0 node: 0 node: 0 node: 0

34.10 Security

Not Applicable.

34.11 Configuration Walkthrough

34.11.1 Walkthrough XPM Rehome to ABI Networks

This feature is a step in the overall Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome." This feature provides the functionality to change an XPM from ENET C-side links to DS-512 ABI links. The use of this feature is restricted and must be activated by appropriate Nortel personnel. A general sequence of events follow however, for full details please refer to the Installation method mentioned above.

1. Enter the ABIREHOME tool and use command ‘set_abi_rehome_status on’ to enable the table control functionality.
2. Add a ABI tuple in the Table GATWYINV which will be used in while adding a tuple in the table LTCINV for the option EXTDS512

Figure 1 View of ABI tuple in Table GATWYINV

```
GTWYPMNO GTWYPRFL GTWYNAME GTWYADDR GTWYCSPM GTWYOPTS
-----------------------------------------------------
ABI 0 MG9KABI TEST (1 2 3 4) $ HOST GWC 3
(GTWYLOC HOST MG9F 2 3 D 4 4 4) (ELMGR 44) $
```

3. Split the Core
4. On Inactive Core, Busy and Offline the XPM to be rehomed
5. On Inactive Core, position on the XPM to be rehomed via Table LTCINV

6. Change the tuple by removing the C-side links ($) and adding the optional parameter EXTDS512. Please refer to "Figure 2 Before and After rehome view of the XPM in table LTCINV" on page 2905
7. Repeat steps 4 and 5 for each XPM to be rehomed
8. Provision/create the VMG on the ABI board via the MG9K-EM
9. Enable the VMG via the MG9K-EM
10. On Active Core, Busy and Offline the rehomed XPM

    Note: Call-P Outage Starts
11. Move fibers and following the steps in the installation method, perform the NoRestartSwact to activate the table control changes.
12. On newly Active Core, Busy and RTS the XPM(s)

Figure 2 Before and After rehome view of the XPM in table LTCINV

Before view of the LGC tuple with ENET links and no EXTDS512 option.

```
TABLE: LTCINV
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
----------------------------------------------------------------------------------------------------------------------------
LGC 1 1001 LTEI 2 18 1 CC 2 6X02NA QLI19AZ (POTS POTSEX) (KEYSET KSETEX) $ (0 12 1 0)
(0 12 1 1) (0 12 1 2) (0 12 1 3) (0 12 1 4)(0 12 1 5) (0 12 1 6) (0 12 1 7) (0 12 1 8) (0 12 1 9) (0 12 1 10)
(0 12 1 11) (0 12 1 12) (0 12 1 13) (0 12 1 14) (0 12 1 15) $ (UTR15 ) (MSG6X69 ) (CMR13 CMR10A)
(ISP 16) $ NORTHAM SX05AA $ SX05AA $ 0 SXFWAE08 $ 6X40FB N
```

After view of the LGC tuple after the change operation has rehomed the XPM to the ABI DS-512 interface. The XPM now has ABI links (derived by the system, user entered a "$") and the EXTDS512 options.

```
TABLE: LTCINV
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
----------------------------------------------------------------------------------------------------------------------------
LGC 20 1021 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) $ (4 0) (4 1) (4 2) (4 3) $
(MSG6X69 ) $ NORTHAM SX05AA $ SX05AA $ 0 SXFWAE08 (EXTDS512 host abi 0) $ 6X40FA N
```

35: Configuration (CN): A00003506

35.1 Hardware and Software Requirements

It is assumed the hardware and software installation of the CS2K is complete. Additionally, the SESM GWC EM is initialized and available for provisioning data related to this activity.

This activity has the following software dependencies:

- CS2K North American load - SNNCSH07
- GWC load - GC070
- SN07.1 PVG load - availability TBD
- SN07 CS2M load - CSM0007

In summary, the SN07 release load lineup is required.

35.2 Initial Configuration

Refer to section “35.11 Configuration Walkthrough” on page 2930

35.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. Please refer to Section “35.12 PVG Profiles” on page 2931. The chart below shows which key PTS office parameters are and are not applicable to GWC PTS trunks.

Office Parameter	Still applicable to GWC PTS trunks?	Notes

PRE_SND_WK_DD_TIME (OFCSTD)	Yes	On originating wink start or delay dial trunks, this is the amount of time that the switch waits (minimum) before sending the leading edge of the start signal (either wink or DD) after origination has been detected. This parameter is in 10 millisecond granularity. This timing is not started until after the origination has been filtered (see ORIGFLTR in TRKGRP datafill).
REC_MAX_DD_TIME (OFCSTD)	No	Maximum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of greater than this value will be considered glare. This is in 160 millisecond granularity.
REC_MAX_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_MIN_DD_TIME (OFCSTD)	No	Minimum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of less than this value will be ignored (probably resulting in a 'no start dial' condition with a route advance). This parameter is in 10 millisecond granularity.
REC_MIN_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_PRE_DD_TIME (OFCSTD)	No	Timeout for receiving Delay Dial signal leading edge. On terminating DD trunks, the leading edge of the start signal must be received within this time or a "no start dial" condition will be experienced. This parameter is in 150 millisecond granularity. A value of 10 is recommended for legacy and GWC based trunks inter-connection.
REC_PRE_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.

SND_DD_TIME (OFCSTD)	No	For DP trunks, this is the start signal duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_MF_WK_TIME (OFCSTD)	No	For non-DP trunks (MF trunks), this is the start signal wink duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_DP_WK_TIME (OFCSTD)	No	Same as above except for DP originators.
WK_DD_PRE_DIAL_ DELAY (OFCSTD)	Yes	On terminating wink and delay dial trunks, this is the time delay after the trailing edge of the start signal before outpulsing begins.
EA_REC_MAX_WK_ TIME (OFCSTD)	Yes	Equal Access Receive Maximum Wink Time - This parameter specifies the maximum time for recognition of wink for ATC type trunk groups, in 10-ms intervals.
EA_REC_SUB_PRE_ WK_TIME (OFCSTD)	Yes	Equal Access Receive Subsequent Pre-wink - This parameter specifies the timeout for receiving the leading edge of next wink signals for ATC type trunk groups, in 160ms intervals.
EA_REC_1ST_PRE_ WK_TIME (OFCSTD)	Yes	Equal Access Receive First Pre-wink Time - This parameter specifies the timeout for receiving the leading edge of the first wink signal for ATC type trunk groups, in 160-ms intervals.
EAEO_REC_1ST_PRE _WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive First Pre-wink Time - This parameter specifies the time of the first pre-wink delay associated with outpulsing from an equal access end office (EAEO), in 160 ms intervals.
EAEO_REC_2ND_PR E_WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive Second Pre-wink Time - This parameter specifies the time of the second pre-wink delay associated with outpulsing from an Equal Access End Office (EAEO), in 160-ms intervals.

IMMED_PRE_DIAL_DELAY (OFCSTD)	No, GWC PTS trunks will use a value of 1 second.	Two-way Immediate Start Trunks Pre-dial Delay - This parameter only applies to two-way immediate start and outgoing trunks. This parameter specifies the delay between seizure and outpulsing of digits, in 10-ms intervals.
MIN_REC_DP_PULSE_WD (OFCSTD)	No	Minimum Received Dial Pulse Width - This parameter allows variable settings for the minimum received dial pulse (DP) width.
PRE_ANI_SPILL_DELAY (OFCSTD)	Yes	Pre-automatic Number Identification Spill Delay - Switching units with outgoing trunks that perform wink and reversal signal calling number outpulsing require this parameter. This parameter specifies the delay between receiving the calling number request signal (wink), and outpulsing the calling number.
DPREC_INTER_DGT_TIMING (OFCSTD)	No	Interdigit timing in DP reception. This parameter specifies the end of digit timing value between two consecutive digits.
SHORT_TIMED_RELEASE_DISC_TIME (OFCSTD)	Yes	Disconnect timing performed on terminator disconnect. The Short TRD is typically used for unbilled calls.
LONG_TIMED_RELEASE_DISC_TIME (OFCENG)	Yes	Disconnect timing performed on terminator disconnect. The Long TRD is typically used for billed calls.
MF_LAST_DIGIT_DELAY (OFCENG)	No	This is a special interdigit delay between the second-to-last and last digit of an MF outpulsing stream. A value of 0 means the delay is no different than between other digits. This parameter is in 10 millisecond granularity.
ACK_WINK_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the delay between the end of the address stream and the leading edge of the acknowledgment wink. This parameter is in 10 millisecond granularity.

ANS_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the minimum delay between the trailing edge of the acknowl-edgment wink and offhook indicating answer. This parameter is in 10 millisecond granularity. 500 milliseconds seems large; however, in many cases the in-switch delay to route the call may be greater than 1/2 second.

35.4 Upgrade Impact

35.4.1 Dump and Restore

None

35.4.2 Element Management Upgrade

None

35.5 Data schema (DS) (CM, MIBS, RDB)

35.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVRINV	changed	unchanged
TRKGRP	changed	unchanged
TRKSGRP	changed	unchanged
TRKOPTS	changed	unchanged
TRKMEM	changed	unchanged

35.5.2 Table/MIB/Remote Database Schema information

35.5.2.1 Name: SERVRINV

Server Inventory Table

35.5.2.1.1 Functional description

This activity adds three new exec line-up, GWCEX , GWCFX, and GWC250 for GWC node types. The new exec line-ups are specific to Per Trunk Signaling (PTS) trunk types that are configured on a GWC node type.

The following table provides a mapping of which exec line-up and termtype combinations can be used to support the various PTS trunk group types since not all supported PTS trunks can be supported by one GWC at the same time..

Table 2 Supported PTS Exec Lineup/Term Type Combinations

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWC250	All GWC PTS trunk groups except for PX trunk groups using FXS signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FXS signalling except for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FXS signalling and EANT, ONAT, and DAL trunk groups.

35.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged by this activity.

35.5.2.1.3 Size

The size of this table is unchanged.

35.5.2.1.4 Fields/OIDs

The following table lists fields for SERVRINV that are changed by this activity. The configuration information for all other fields in table SERVRINV are unchanged.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	changed	TRMTYPE	ABTRK unchanged	The TRMTYPE subfield is unchanged. This activity adds 1 new EXEC entry for TRMTYPE ABTRK and 2 new EXEC entries for TRMTYPE AB250
		EXEC	GWCEX	ABTRK / GWCEX supports GWC PTS trunks OP, ES, PX, IBN, ATC, IT, SC & CELL, but does not support PX trunks using FXS signalling.
		TRMTYPE	AB250	
		EXEC	GWCFX	ABTRK / GWCFX supports PX trunks using FXS signalling only.
		EXEC	GWC250	AB250 / GWCAB250 supports DMS250 GWC PTS trunks EANT, DAL, and ONAT. Also supports DAL with FXS signalling.

35.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV.

```
SRVRNAME        SRVRADDR
                SRVREXEC                SRVRTONE    SRVROPTS
-------------------------------------------------------------------------------
GWC  0      IP  47  174  66  4
            (ABTRK   GWCEX) (AB250   GWC250)$  NORTHAM  $
GWC  1      IP  47  174  66  8
            (ABTRK   GWCEX) (AB250   GWCFX)$  NORTHAM  $
GWC  2      IP  47  174  66  12
            (ABTRK   GWCEX) $                 NORTHAM  $
```

35.5.2.1.6 Table release history update

The following information was added to table SERVRINV:

exec line-up GWCEX is added to field SRVREXEC

exec line-up GWCFX is added to field SRVREXEC

exec line-up GWC250 is added to field SRVREXEC

35.5.2.1.7 Supplementary information

Tuples in table SERVRINV should not be added or changed via manual table control commands. Provisioning of this table should be performed using SESM node provisioning.

35.5.2.1.8 Translation verification other tools

Not Applicable

35.5.2.2 Name: TRKGRP

Trunk Group Table Table

35.5.2.2.1 Functional description

This activity introduces new provisioning restrictions in table TRKGRP for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when a PTS group tuple is changed in table TRKGRP.

Table 4 Supported GWC PTS Trunk Group Types

Trunk Group Type
OP
ES
PX
IBNTO
IBNTI
IBNT2
ATC

Table 4 Supported GWC PTS Trunk Group Types

Trunk Group Type
IT
SC
CELL
DAL
EANT
ONAT

35.5.2.2.2 Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

35.5.2.2.3 Size

The size of this table is unchanged by this activity.

35.5.2.2.4 Fields/OIDs

Not Applicable

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

35.5.2.2.5 Datafill example

Not Applicable

35.5.2.2.6 Table release history update

The following information was added to table TRKGRP:

Restrictions are added for GWC PTS trunk groups

35.5.2.2.7 Supplementary information

When PTS trunk group data is changed in table TRKGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKGRP data is provisioned correctly. Table 6, "TRKGRP Restrictions," on page 2916 lists the new error messages that may be generated by table control.

Table 6 TRKGRP Restrictions

Trunk Type	Error Messages
ALL support GWC PTS groups	Trunk Members exist in table TRKMEM
	Non-GWC trunk members are disallowed
	CCONT in table TRKSGRP must be set to NO
	ESUPR in table TRKSGRP must be set to N
	Table Control Operation not allowed
	PRELOADANI must be set to N for this trunk type
	CCONT in table TRKSGRP must be set to NO or MW for this trunk type
Non-Supported trunk groups	It is not supported with this trunk group type
OP	ANITYPE in table TRKGRP must be set to WK or REV
	EAOSS in table TRKGRP must be set to N when EA is Y
	OPULSTYP in TRKSGRP must be set to MF for this trunk type
	OSTARTSG in TRKSGRP must be set to WK for this trunk type
	IPULSTYP in TRKSGRP must be set to MF for this trunk type
	ISTARTSG in TRKSGRP must be set to WK for this trunk type
	ANITYPE in table TRKGRP must be set to REV for this trunk type
	ANITYPE in table TRKGRP must be set to NO for this trunk type
ES	Only OG direction is supported with this trunk type
	FDISCTIM in table TRKGRP must be set to 0
	SWST in table TRKGRP must be set to DC
	ANI in table TRKGRP must be set to ANISPILL
	OPULSTYP in TRKSGRP must be set to MF for this trunk type
	OSTARTSG in TRKSGRP must be set to WK for this trunk type
PX	PRELOADANI must be set to N for this trunk group type

Table 6 TRKGRP Restrictions

Trunk Type	Error Messages
IBNTO	PRELOADANI must be set to N for this trunk group type
	ANITYPE in table TRKGRP must be set to WK or REV
	FLASH in table TRKGRP must be set to N for this trunk type.
	DNIS option disallowed for this trunk type.
	CLID option disallowed for this trunk type.
	OUTSCHM option disallowed for this trunk type.
	PROPANS option disallowed for this trunk type.
	ANISEND option disallowed for this trunk type.
IBNTI	PRELOADANI must be set to N for this trunk group type
	DTI in table TRKGRP must be set to N for this trunk type.
	TRKDSR in table TRKGRP must be set to N for this trunk type.
	REORIG in table TRKGRP must be set to N for this trunk type.
IBNT2	PRELOADANI must be set to N for this trunk group type
	ANITYPE in table TRKGRP must be set to WK or REV
	DTI in table TRKGRP must be set to N for this trunk type.
	TRKDSR in table TRKGRP must be set to N for this trunk type.
	REORIG in table TRKGRP must be set to N for this trunk type.
	FLASH in table TRKGRP must be set to N for this trunk type.
	DNIS option disallowed for this trunk type.
	CLID option disallowed for this trunk type.
	OUTSCHM option disallowed for this trunk type.
	PROPANS option disallowed for this trunk type.
	ANISEND option disallowed for this trunk type.
ATC	PRELOADANI must be set to N for this trunk group type
IT	PRELOADANI must be set to N for this trunk group type
SC	PRELOADANI must be set to N for this trunk group type.
	ANITYPE in table TRKGRP must be set to WK or REV
	NOUTR option is disallowed.
CELL	PRELOADANI must be set to N for this trunk group type
DAL	PRELOADANI must be set to N for this trunk group type
	DETDIAL option is disallowed.
	ATDANS option is disallowed.

Table 6 TRKGRP Restrictions

Trunk Type	Error Messages
EANT	PRELOADANI must be set to N for this trunk group type
ONAT	PRELOADANI must be set to N for this trunk group type

35.5.2.2.8 Translation verification other tools
Not Applicable

35.5.2.3 Name: TRKSGRP
Trunk Subgroup Table

35.5.2.3.1 Functional description
This activity introduces new provisioning restrictions in table TRKSGRP for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when adding or changing the GWC PTS trunk subgroup tuples in table TRKSGRP.

35.5.2.3.2 Usage sequence and implications (CM Only)
When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required.(NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

35.5.2.3.3 Size
The size of this table is unchanged by this activity.

35.5.2.3.4 Fields/OIDs
Not Applicable

35.5.2.3.5 Datafill example
Not Applicable

35.5.2.3.6 Table release history update
The following information was added to table TRKSGRP:

Restrictions are added for GWC PTS trunk groups

35.5.2.3.7 Supplementary information

When PTS trunk groups are provisioned or tuples are changed in table TRKSGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKSGRP data is provisioned correctly. Please refer to "Table 7 TRKSGRP Restrictions" on page 2919..

Table 7 TRKSGRP Restrictions

TRKSGRP Field	Error Messages
SGRP	Only trunk subgroup 0 is allowed.
CARDCODE	CARDCODE is not supported with this trunk type
Signaling Data Selector	SGRPVAR in table TRKSGRP must be set to STD
DIR	n/a
IPULSTYP	Disallowed IPULSTYP in TRKSGRP. IPULSTYP in TRKSGRP must be set to MF for this trunk type
ISTARTSG	ISTARTSG in TRKSGRP must be set to WK for this trunk type Disallowed ISTARTSG in TRKSGRP.
OVLP	OVLP in table TRKSGRP must be set to N.
PSPDSEIZ	n/a
PARTDIAL	n/a
OPULSTYP	OPULSTYP in TRKSGRP must be set to MF for this trunk type Disallowed OPULSTYPE in TRKSGRP.
OSTARTSG	OSTARTSG in TRKSGRP must be set to WK for this trunk type Disallowed OSTARTSG in TRKSGRP.
IDGTIME	n/a
NUMSTOPS	NUMSTOPS in table TRKSGRP must be set to 0.
GLAREYD	n/a
CCONT	CCONT in table TRKSGRP must be set to NO CCONT in table TRKSGRP must be set to NO or MW for this trunk type.
RNGBCK	RNGBCK in table TRKSGRP must be set to NO or MW for this trunk type.

TRKSGRP Field	Error Messages
ESUPR	ESUPR in table TRKSGRP must be set to N
SAT	n/a
REMBSY	n/a
DIALMODE	n/a
TRKGRDTM	n/a
ECSTAT	ECSTAT in table TRKSGRP must be set to INTERNAL or EXTERNAL
SPMECIDX	SPMECIDX option is disallowed.

35.5.2.3.8 Translation verification other tools
Not Applicable

35.5.2.4 Name: TRKOPTS
Trunk Options Table

35.5.2.4.1 Functional description
This activity adds the new trunk group option, GWCPTSTK, to table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). In the SN07 release, GWCPTSTK is supported with all GWC PTS supported trunk group types that are configured on a GWC. Please refer to "Table 4 Supported GWC PTS Trunk Group Types" on page 2914. This option must be provisioned prior to configuring trunk members in table TRKMEM.

35.5.2.4.2 Usage sequence and implications (CM Only)
When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required. (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Table TRKOPTS may be provisioned following table TRKSGRP. Table control restrictions will enforce table TRKOPTS be provisioned after table TRKGRP and before table TRKMEM.

35.5.2.4.3 Size

The size of this table is unchanged by this activity.

35.5.2.4.4 Fields/OIDs

The following table lists fields for TRKOPTS that are changed by this activity.

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	changed	CLLI	unchanged	The CLLI subfield is unchanged.
		OPTION	GWCPTSTK	The option GWCPTSTK enables a PTS trunk group to be configured on a GWC..
OPTION	changed	OPTION	GWCPTSTK	The option GWCPTSTK enables a PTS trunk group to be configured on a GWC.
		PRELOAD ANI	Y or N	The sub-option PRELOADANI is for GWC PTS trunks which support a call model that allows the ANI digits to be sent from the Core prior to receiving an ANI request. To enable this capability, set the field to “Y”.

35.5.2.4.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

```
                OPTKEY                  OPTINFO

-------------------------------------------------------------------------
```

PTSCLLI GWCPTSTK GWCPTSTK N

35.5.2.4.6 Table release history update

The following information was added to table TRKOPTS:

Option GWCPTSTK is added for GWC PTS trunk groups

35.5.2.4.7 Supplementary information

Option GWCPTSTK is used to identify PTS trunk groups to be configured on a GWC that can provide connectivity between the CS2K's packet network and the PSTN. This option applies only to all GWC PTS supported trunk group types in the SN07 release. Table control in table TRKOPTS will block the addition of this option to a non-supported trunk type. Please refer to "Table 4 Supported GWC PTS Trunk Group Types" on page 2914.. The following error message will result:

"GWCPTSTK cannot be assigned for the following reasons:"
"It is not supported with this trunk type."

This option can not be added if existing datafill in either table TRKGRP or table TRKSGRP that is incompatible with GWC PTS trunks. If an error message occurs when provisioning GWCPTSTK in table TRKOPTS, the tuple entry in table TRKGRP and/or table TRKSGRP must be changed. Please refer to "Table 6 TRKGRP Restrictions" on page 2916. and Table 7, "TRKSGRP Restrictions," on page 2919.

This option can not be added if the PTS trunk group already has members provisioned in table TRKMEM. This can occur if the members were provisioned on a peripheral type other than a GWC. Note that trunks members can not be assigned to a GWC in table TRKMEM if the GWCPTSTK option is not present in table TRKOPTS. Hybrid PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are ***not*** supported. If trunk members exist while provisioning the GWCPTSTK option, the following error will result:

"GWCPTSTK cannot be assigned for the following reasons:"
"Trunk Members exist in table TRKMEM"

This option can not be deleted from table TRKOPTS until all members on the trunk group have been deleted from table TRKMEM. The following error will result:
"GWCPTSTK cannot be deleted for the following reasons:"
"Trunk Members exist in table TRKMEM"

35.5.2.4.8 Translation verification other tools

Not Applicable

35.5.2.5 Name: TRKMEM

Trunk Member Table

35.5.2.5.1 Functional description

This activity introduces new provisioning restrictions in table TRKMEM for PTS trunks groups configured on a GWC.

35.5.2.5.2 Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required. (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

35.5.2.5.3 Size

The size of this table is unchanged by this activity.

35.5.2.5.4 Fields/OIDs

Not Applicable

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

35.5.2.5.5 Datafill example

Not Applicable

35.5.2.5.6 Table release history update

The following information was added to table TRKMEM:

Restrictions are added for GWC PTS trunk groups

35.5.2.5.7 Supplementary information

Table control for table TRKMEM determines if the option GWCPTSTK is provisioned in table TRKOPTS. If option GWCPTSTK is provisioned, table

control performs error checking to ensure the TRKMEM data is provisioned correctly. Please refer to “Table 10 TRKMEM Restrictions” on page 2924.

Table 10 TRKMEM Restrictions

TRKMEM Action	Error Messages
Attempt to ADD member with GWC PMTYPE to PTS group without GWCPTSTK option.	To assign a trunk member with SGRPVAR = STD to a GWC, option GWCPTSTK must be present in table TRKOPTS
Attempt to ADD member with non-GWC PMTYPE to PTS group with GWCPTSTK option	With the GWCPTSTK option assigned for this trunk group: Non-GWC trunk members are disallowed TRKMEM data conflicts with data in table TRKOPTS
Attempt to Change PMTYPE from GWC to non-GWC.	With the GWCPTSTK option assigned for this trunk group: Non-GWC trunk members are disallowed TRKMEM data conflicts with data in table TRKOPTS
Attempt to CHANGE PMTYPE from Non-GWC to GWC	To assign a trunk member with SGRPVAR = STD to a GWC, option GWCPTSTK must be present in table TRKOPTS

35.5.2.5.8 Translation verification other tools

Not Applicable

35.6 Service Orders (SO) (CM & SESM)

Not Applicable

35.7 Software optionality control (SOC)

Not Applicable

35.8 Element Management

35.8.1 New/modified GUIs

The following levels of the MAP are changed by this activity.

Table 11 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
TTP	changed
MANUAL	changed

Table 11 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
MONITOR	changed
DATATTP	changed

35.8.2 GUI information

35.8.2.1 GUI name: TTP

Trunk Test Position

35.8.2.1.1 Functional description

New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

35.8.2.1.2 GUI usage and implications

Not Applicable

35.8.2.1.3 GUI size

Unchanged

35.8.2.1.4 GUI fields

Not applicable

35.8.2.1.5 Usage example

Not applicable

35.8.2.1.6 GUI release history update

The following information was added:
TTP restrictions are added for GWC PTS trunks.

35.8.2.1.7 Supplementary information

New restrictions are added to the TTP level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- BSY SB
- Cktloc
- TrnslVf
- Pads

The following error message is displayed if an attempt is made to execute any of these commands:

"Action not supported on GWC trunks."

35.8.2.1.8 CLUI Interface
Not applicable

35.8.2.2 GUI name: MANUAL
Manual Trunk Test Position

35.8.2.2.1 Functional description
New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

35.8.2.2.2 GUI usage and implications
Not Applicable

35.8.2.2.3 GUI size
Unchanged

35.8.2.2.4 GUI fields
Not applicable

35.8.2.2.5 Usage example
Not applicable

35.8.2.2.6 GUI release history update
The following information was added:
MANUAL restrictions are added for GWC PTS trunks.

35.8.2.2.7 Supplementary information
New restrictions are added to the MANUAL level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- Jack
- Calltrf

The following error message is displayed if an attempt is made to execute any of above commands:

"Action not supported on GWC trunks."

The following commands are not supported for PTS trunks because a hybrid office configuration is not supported by this feature. An error message is generated indicating no test equipment is available.

- LOSS
- TGEN
- NOISE
- TDET
- Hset

The following error message is displayed if an attempt is made to execute any of above commands in a non-hybrid office:

'No IW SPM IP Bridges Available To Perform Action.'

35.8.2.2.8 CLUI Interface
Not applicable

35.8.2.3 GUI name: MONITOR
MONITOR Trunk Test Position

35.8.2.3.1 Functional description
New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

35.8.2.3.2 GUI usage and implications
Not Applicable

35.8.2.3.3 GUI size
Unchanged

35.8.2.3.4 GUI fields
Not applicable

35.8.2.3.5 Usage example
Not applicable

35.8.2.3.6 GUI release history update
The following information was added:
MONITOR restrictions are added for GWC PTS trunks.

35.8.2.3.7 Supplementary information
New restrictions are added to the MONITOR level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- MONPOST
- MONLINK
- MonTalk
- CktMOn
- CPOS

The following error message is displayed if an attempt is made to execute any of these commands:

"Action not supported on GWC trunks."

35.8.2.3.8 CLUI Interface
Not applicable

35.8.2.4 GUI name: DATATTP
Trunk Test Position

35.8.2.4.1 Functional description
New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

35.8.2.4.2 GUI usage and implications
Not Applicable

35.8.2.4.3 GUI size
Unchanged

35.8.2.4.4 GUI fields
Not applicable

35.8.2.4.5 Usage example
Not applicable

35.8.2.4.6 GUI release history update
The following information was added:
DATATTP restrictions are added for GWC PTS trunks.

35.8.2.4.7 Supplementary information
New restrictions are added to the DATATTP level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- BTerm

The following error message is displayed if an attempt is made to execute any of these commands:

“Action not supported on GWC trunks.”

35.8.2.4.8 CLUI Interface
Not applicable

35.8.2.5 GUI name: CS2M - ADD GWC NODE
Call Server 2000 Management Tools Configuration- Add GWC Node

35.8.2.5.1 Functional description
The Add GWC Node command provides functionality to select a GWC profile that corresponds to the required termtype and exec_lineups that support the specific type GWC PTS trunk group types that will be provisioned on the GWC node being added.

35.8.2.5.2 GUI usage and implications
Not Applicable

35.8.2.5.3 GUI size
Unchanged

35.8.2.5.4 GUI fields
Not applicable

35.8.2.5.5 Usage example
Not applicable

35.8.2.5.6 GUI release history update
The following information was added:
Add GWC node command enhanced to select TERMTYPE and EXEC_LINEUP required for to support specific PTS group types on the GWC being added.

35.8.2.5.7 Supplementary information
N/A

35.8.2.5.8 CLUI Interface
Not applicable

35.9 Command interface changes
Not Applicable - No new or changed CIs.

35.10 Security

Not Applicable

35.11 Configuration Walkthrough

Following is a high-level walkthrough of the steps required to provision supported PTS trunk groups on a GWC.

- Provision the GWC node using the CS2M. The CS2M will provision table SERVRINV on the CS2K core. A new Gateway Controller Profile must be selected when provisioning the GWC node. Select "TRUNKNA" and choose exec lineups as specified in the following table:

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWC250	All GWC PTS trunk groups except for PX trunk groups using FXS signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FXS signalling except for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FXS signalling and EANT, ONAT, and DAL trunk groups.

- Provision the PTS MG(s) using the CS2M. Use the PVG gateway profile which corresponds to gateway profile number 58. Additionally, Megaco protocol must be specified.
- When provisioning the PTS MGs, the GWC name must be entered. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.
- Provision the PTS MG endpoints on the GWC using the CS2M. The endpoint names and terminal numbers returned by the CS2M should be noted. The terminal numbers are required when provisioning table TRKMEM on the CS2K core.
- Provision table CLLI with the PTS group clli.
- Provision table TRKGRP with the PTS trunk group data. Please refer to “Table 6 TRKGRP Restrictions” on page 2916..
- Provision the GWCPTSTK option for the PTS trunk group CLLI in table TRKOPTS.

- Provision table TRKSGRP with the PTS trunk subgroup data. Please refer to “Table 7 TRKSGRP Restrictions” on page 2919..
- Provision table TRKMEM with the PTS trunk group members. The terminal number information provided by the CS2M is required when entering tuples in table TRKMEM.

35.12 PVG Profiles

For the PVG, a profile is provisioned on a DS1 carrier basis during installation of the PVG by Nortel Networks. Currently there are four profiles which support PTS trunks and are dependent on the supported cardcode and pulse types provisioned in table TRKSGRP. A PVG profile table mapping is shown below in Table 12, “PVG DS1 Profile Mapping,” on page 2931.

Table 12 PVG DS1 Profile Mapping

PVG Profile Name	TRKSGRP Cardcode	TRKSGRP InComing Pulsetype	TRKSGRP OutGoing Pulsetype	Trunk Group Restrictions
ds1sig_mfr1.prof	DS1SIG	MF,DT, DP	MF,DP	None
ds1SigMwMfr1.prof *	DS1SIG	MF,DT,DP	MF,DP	None *.
ds1sig_dtmf.prof	DS1SIG	DT,DP	DT,DP	Not Supported for OP, SC, ES, ATC, IT, ONAT, and EANT.
fxsls.prof	FXSLS	DT,DP	DT,DP	Supported for DAL and PX groups only
fxsgs.prof	FXSGS	DT,DP	DT,DP	Supported for DAL and PX groups only

36: Configuration (CN): A00003531

36.1 Hardware and Software Requirements

NA

36.2 Initial Configuration

NA

36.3 Office / Subnet parameters (OP/SP) (CM & SESM)

NA

36.4 Upgrade Impact

36.4.1 Element Management Upgrade

While upgrading MG9K Manager software from SN06.2 to SN07, follow the steps given below.

1. Start SN07 MG9KEM
2. Start SN07 OM Collector
3. NE is deleted from SN06.2 MG9KEM manually
4. NE is deleted from SN06.2 OMC (should happen during the MG upgrade window)
5. NE is upgraded to SN07 software
6. NE is added (manually or automatically) to SN07 MG9KEM. If device was previously being polled for OMs, operator will check 'yes' in the checkbox "NE OMCollection" in MG9KEM either while adding the NE or after adding the NE.
7. NE is deleted from SN06.2 MG9KEM manually (This does not happen until NE is successfully upgraded to SN07 EM).

36.5 Data schema (DS) (CM, MIBS, RDB)

A new column OMCSTATUS is introduced in the database table NODE_ATTRIBUTES. No existing external interfaces are changed.

36.6 Service Orders (SO) (CM & SESM)

None

36.7 Software optionality control (SOC)

NA

36.8 Element Management

36.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI Name	NEW, CHANGED or DELETED
MG9K-EM Frame-view	Changed
MG9K-EM “Provision a Virtual Media Gateway” GUI	Changed
MG9K-EM Alarm browser GUI	Changed
MG9000 Provisioning GUI	Changed
MG9K-EM NE Properties GUI	Changed
MG9K-EM NE Discovery GUI	Changed

36.8.2 GUI information

36.8.2.1 GUI name: MG9K-EM Frame-view

36.8.2.1.1 Functional description

Following changes will be done in this GUI;

1. In MG9K-EM Frameview, frames are displayed without gap. However, any gap present between shelves will continue to be displayed.

   With this change, MG9K-EM Frame view is displayed in a cleaner way. Some of the examples for this cleaner display are;

   - MG9K-EM Craft-person can see Master frame as and when he/she opens the Frame view, even when Master frame has two or more empty frames to its left side.
   - MG9K-EM Craft-person can see adjacent frames, without scrolling to right in Frameview, even when there is gap between the frames.

2. In MG9K-EM Frameview, Master frame is shown far left and all subtending frames are shown to the right of Master frame going by following logic.

- Show Master frame far left.
- Show other frames, whose frame number is higher than that of Master frame on right of Master frame, in increasing order of their Internal frame number (IFN).
-And then, show other frames, whose IFN is lower than that of Master frame, in increasing order of their IFNs.

As a result of these changes, Frameview may not be a mirror reflection of actual line-up of frames in MG9K.

Note that, as in SN6.2, in MG9K-EM Frame view, Internal frame number is shown at the bottom of each frame and Office frame number is shown at the top of each frame. With this, Craft-person can map the MG9K-EM Frame view to actual line-up of frames in MG9K.

36.8.2.1.2 GUI Usage and implications

NA

36.8.2.1.3 GUI size

No changes in SN07.

36.8.2.1.4 GUI fields

No changes in SN07.

36.8.2.1.5 Usage example

Let us consider two scenarios.

Scenario 1:

Let us consider a scenario wherein frames are lined-up from left to right as follows;

- First frame is numbered as 1 and is Master frame
- Second frame is numbered as 3 and is subtending frame

For this scenario, in SN06.2, craft-person need to use horizontal scroll bar to see the non-empty frames (frame #1 and frame #3) and MG9K-EM Frame view would looks like figure #1 and figure #2.

For this scenario, in SN07, craft-person see the non-empty frames as and when he/she opens the Frameview and MG9K-EM Frame view would looks like figure #3.

Even when frames are lined-up from right to left, in both SN06.2 and SN07, Frame view will look the same way as in left to right lineup.

Scenario 2:

Let us consider a scenario wherein frames are numbered as follows;

- First frame is numbered as 5 and is Master frame
- Subsequent three subtending frames are numbered as 7, 0 and 2 .

For this scenario, in SN06.2, frames would be shown in increasing order of their Internal frame numbers. i.e, as [frame #0][frame #2][frame #5][frame #7]).

For this scenario, in SN07, frames would be shown as [frame #5][frame #7][frame #0][frame #2]); refer to the logic given in section 12.8.2.1.1 point #2.

Figure 1 MG9K-EM Frame view in SN06.2 and prior when Frame view comes up

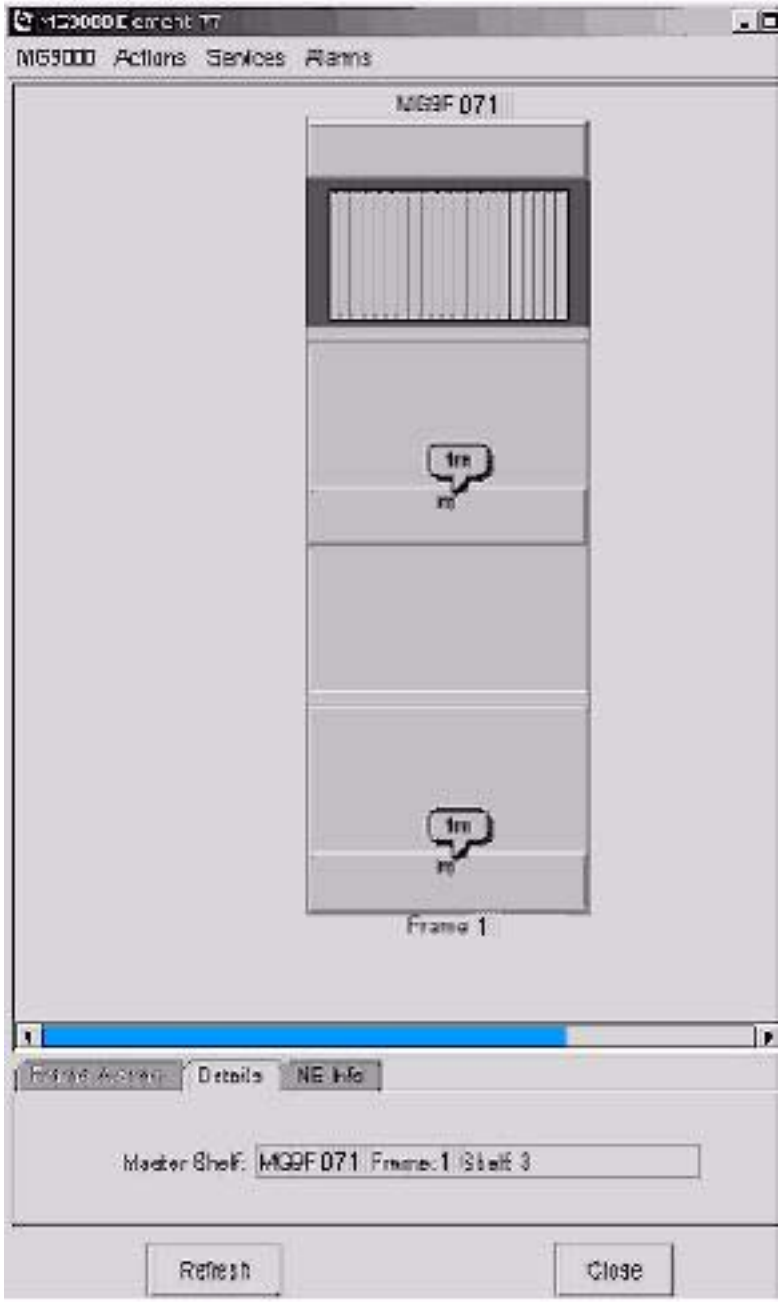


Figure 2 MG9K-EM Frame view in SN06.2 and prior when horizontally scrolled far right

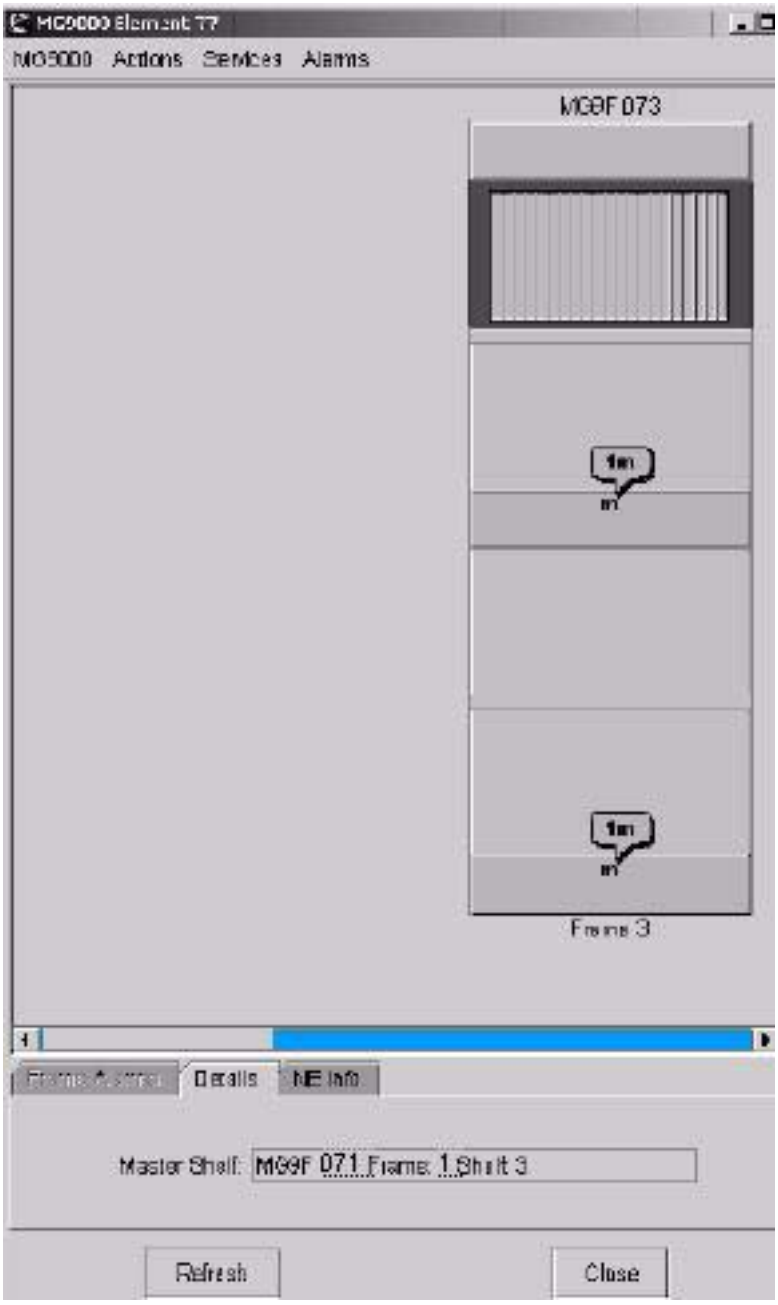
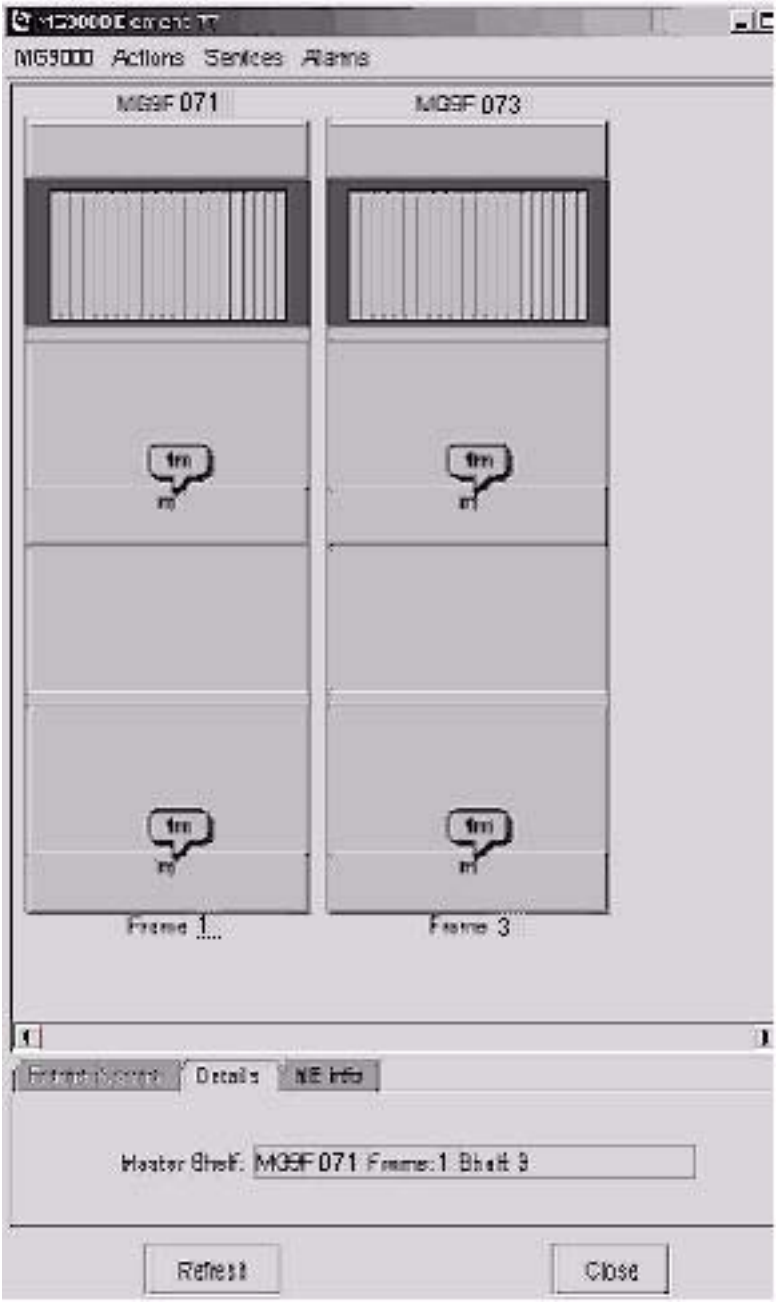

MO3000 Actions Services Alarms
MG9F 073
Frame 3
Details
NE Info
Master Shelf: MG9F 071 Frame: 1 Shelf: 3
Refresh
Close

Figure 3 MG9K-EM Frame view in SN07



36.8.2.1.6 GUI release history update

SN07, following changes will be done to MG9K-EM Frameview GUI;

a. frames are displayed without gap.

c. In MG9K-EM Frameview, Master frame is shown far left and all sub-

tending frames are shown to the right of Master frame going by following logic.

- Show Master frame far left.
- Show other frames, whose frame number is higher than that of Master frame on right of Master frame, in increasing order of their Internal frame number (IFN).
- And then, show other frames, whose IFN is lower than that of Master frame, in increasing order of their IFNs.

36.8.2.1.7 Supplementary information

None

36.8.2.1.8 CLUI Interface

NA

36.8.2.2 GUI name: MG9K-EM "Provision a Virtual Media Gateway" GUI

36.8.2.2.1 Functional description

Following changes will be done in this GUI;

Internal frame number is hard-coded to zero in VMG name, while provisioning VMG. So, VMG name of a VMG which is provisioned in SN07, will be as follows;

<SITE_name><Office frame number><Internal frame number = 0><Shelf number>

An example VMG name is 'SLOA007-0-1'.

36.8.2.2.2 GUI Usage and implications

No changes in SN07.

36.8.2.2.3 GUI size

No changes in SN07.

36.8.2.2.4 GUI fields

Following table describes fields of this GUI.

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Virtual Media Gateway Name	Changed	NA	No change in SN07	Internal frame number is hard-coded to zero in VMG name, while provisioning VMG.	No change in SN07

There is no change in SN07 for other GUI fields.

36.8.2.2.5 Usage example

The field “Virtual Media Gateway” is not configurable by MG9K-EM Craft-person. This field is populated based on value of the fields “Virtual Media Gateway type” and “Virtual Media Gateway physical location”. Note that, in figure-4, Internal frame number of 1 is used to construct VMG name and in figure-5, Internal frame number is hardcoded to zero while constructing VMG name.

Figure 4 MG9K-EM “Provision a Virtual Media Gateway” GUI in SN06.2 and prior

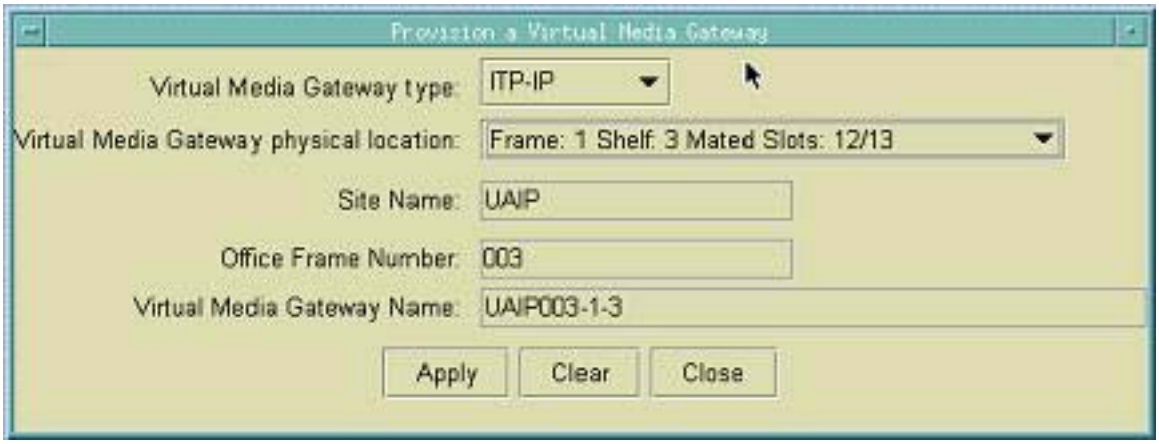


Figure 5 MG9K-EM "Provision a Virtual Media Gateway" GUI in SN07

36.8.2.2.6 GUI release history update

SN07, following changes will be done to MG9K-EM GUI;

- Internal frame number is hard-coded to zero in VMG name

36.8.2.2.7 Supplementary information

VMGs which are provisioned in SN05/SN06+ with non-zero Internal frame number, continue to exist as they are. i.e., they continue to exist with non-zero Internal frame number.

36.8.2.2.8 CLUI Interface

NA

36.8.2.3 GUI name: MG9K-EM Alarm browser GUI

36.8.2.3.1 Functional description

In SN07, following changes will be done in "Description" field of this GUI;

- Until Frame location information is not provisioned, default filler F's are appended in following format to the data which is shown in this field in SN06.2.

  ```
  Site Flr RPos Bay_id
  FFFF   FF FFFF  MG9F FFF
  i.e., <Site=FFFF><3 blank space><Flr=FF><2 blank space><RPos=FFFF><3 blank space><Bay-id>
  <Bay-id> = MG9F<One blank space><FFF>
  ```

- When Frame location information is (re)provisioned for a Master frame, all alarms (both Gateway alarms and EM alarms) reported on components in the frame are updated with latest frame location information.
- When Frame location information is (re)provisioned for a subtending frame, only Gateway alarms reported on components in the frame are updated with latest frame location information.

36.8.2.3.2 GUI Usage and implications

As explained in 12.8.2.3.1, data shown in "Description" field of this GUI depends on whether Frame location information is provisioned or not.

36.8.2.3.3 GUI size

No changes in SN07.

36.8.2.3.4 GUI fields

Following table describes the fields of this GUI.

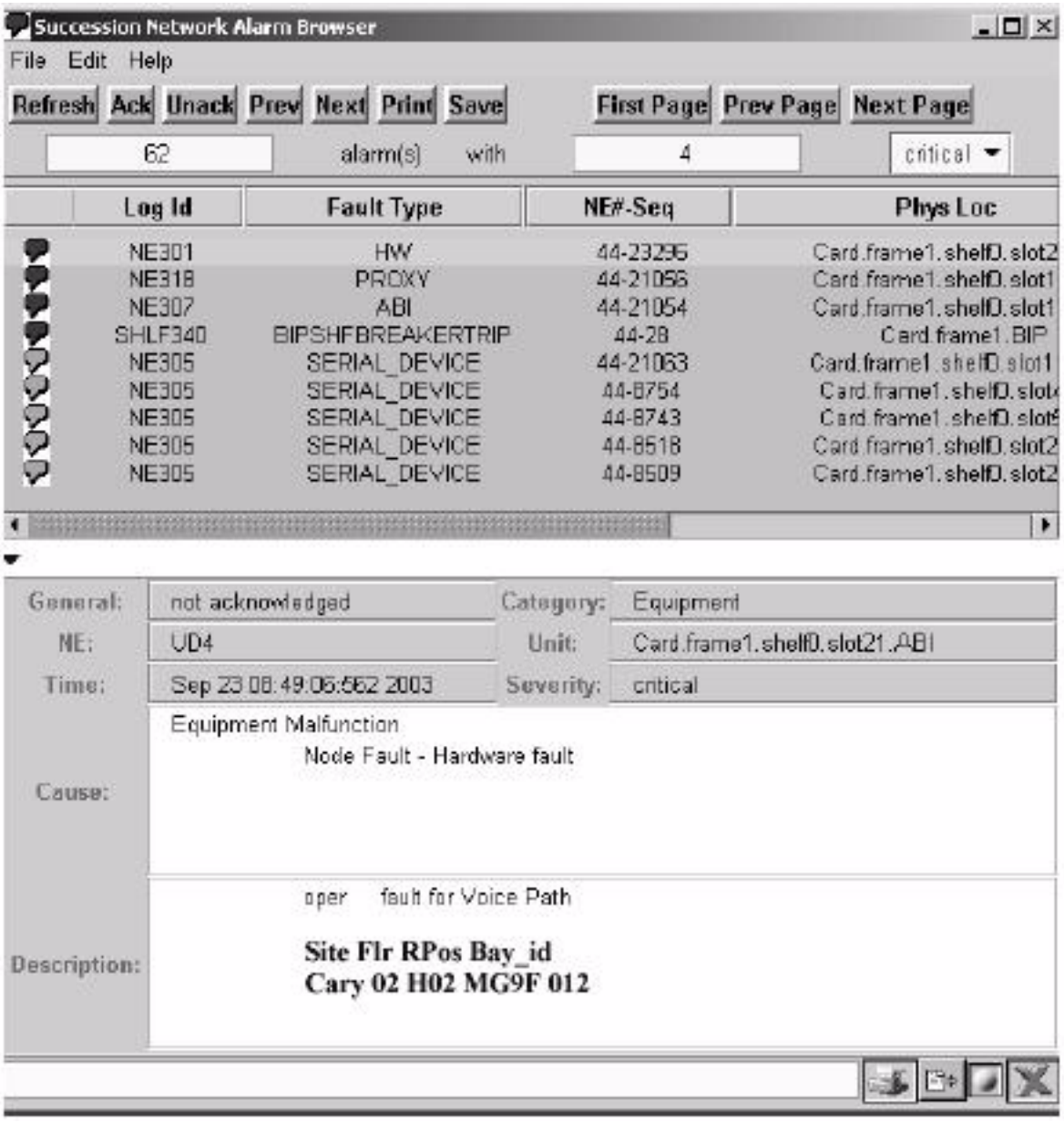
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Description	Changed	NA	No change in SN07	Refer to 12.8.2.3.1	No change in SN07

There is no change in SN07 for other GUI fields.

36.8.2.3.5 Usage example

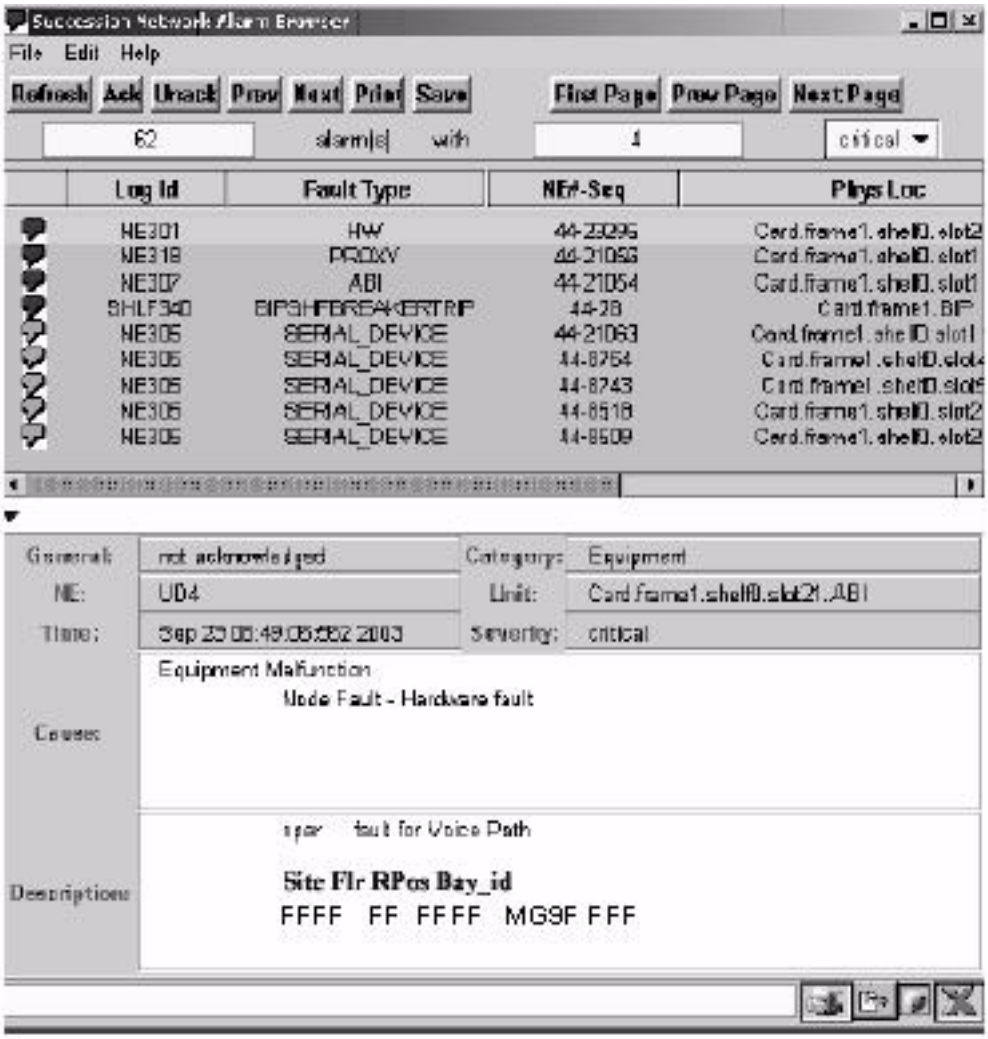
After Frame location information is provisioned for frame 1, if an alarm is raised on an entity say card, which is present in frame 1, then in SN07, it will look as in figure-6.

Figure 6 MG9K-EM Alarm browser GUI in SN07 when Frame location information is provisioned for frame 1



If an alarm is raised on an entity say card, which is present in frame 1, for which Frame location information is not provisioned, then in SN07, it will look as in figure-7.

Figure 7 MG9K-EM Alarm browser GUI in SN07 when Frame location information is not provisioned for frame



36.8.2.3.6 GUI release history update

SN07, following changes will be done in Description field of this GUI;

- Until Frame location information is not provisioned, default filler F's are shown
- When Frame location information is (re)provisioned for a Master frame, all alarms (both Gateway alarms and EM alarms) reported on components in the frame are updated with latest frame location information.
- When Frame location information is (re)provisioned for a subtending frame, only Gateway alarms reported on components in the frame are updated with latest frame location information.

36.8.2.3.7 Supplementary information

If Frame location is (re)provisioned when Alarm audit is underway, Frame location information for Gateway alarm may not be updated immediately on Alarm browser.

36.8.2.3.8 CLUI Interface

NA

36.8.2.4 GUI name: MG9K-EM MG9000 Provisioning GUI

36.8.2.4.1 Functional description

In SN07, a new checkbox “NE OMCollection” is introduced in MG000 Provisioning GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

36.8.2.4.2 GUI Usage and implications

NA

36.8.2.4.3 GUI size

No changes in SN07.

36.8.2.4.4 GUI fields

Following table describes the fields of this GUI.

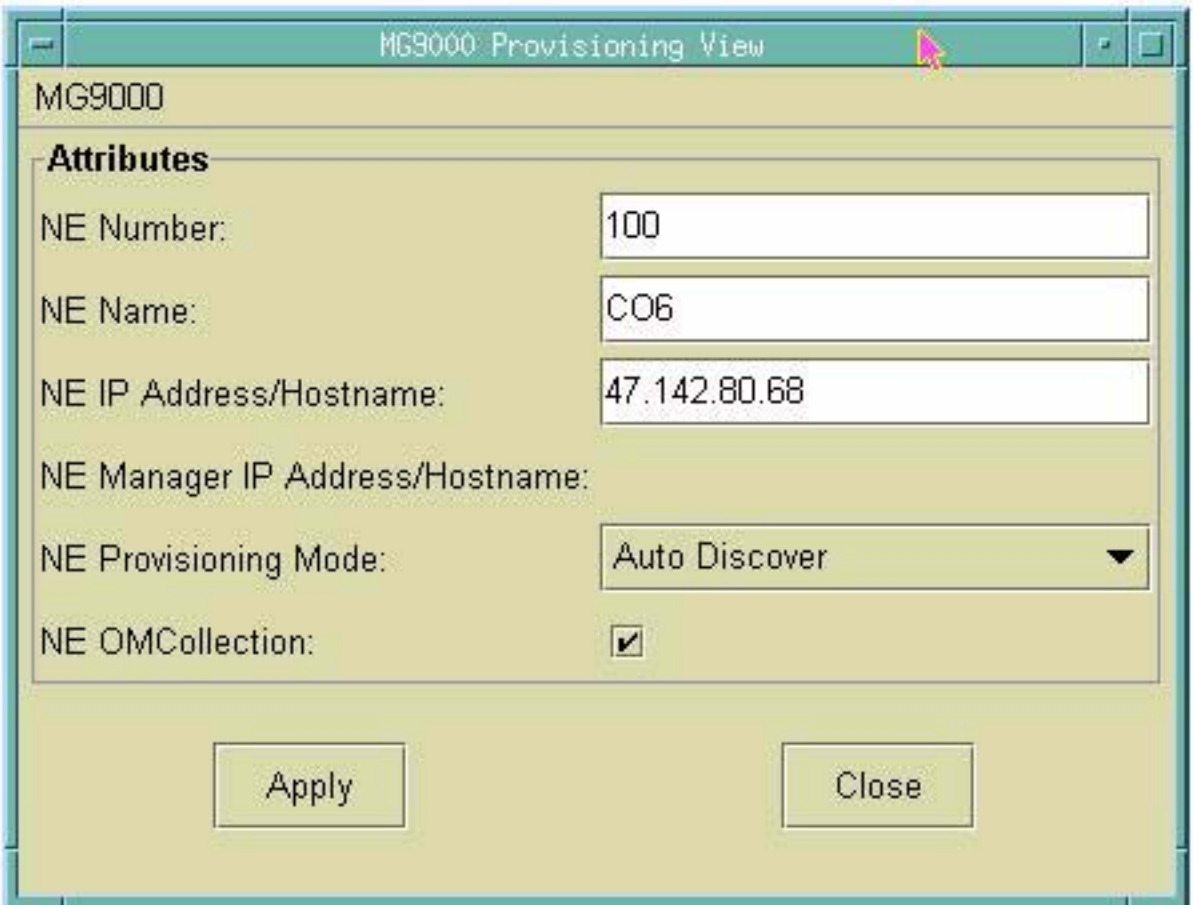
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
NE OMCollection	New	NA	checked/ unchecked	Refer to 12.8.2.4.1	None

There is no change in SN07 for other GUI fields.

36.8.2.4.5 Usage example

Operator can either check or uncheck the “NE OMCollection” checkbox.

Figure 8 MG9K-EM “MG9000 Provisioning” GUI when “NE OMCollection“is checked



36.8.2.4.6 GUI release history update

In SN07, a new checkbox “NE OMCollection” is introduced in “MG9000 Provisioning” GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

36.8.2.4.7 Supplementary information

None

36.8.2.4.8 CLUI Interface

NA

36.8.2.5 GUI name: MG9K-EM NE Properties GUI

36.8.2.5.1 Functional description

In SN07, a new checkbox “NE OMCollection” is introduced in NE Properties GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

36.8.2.5.2 GUI Usage and implications

NA

36.8.2.5.3 GUI size

No changes in SN07.

36.8.2.5.4 GUI fields

Following table describes the fields of this GUI.

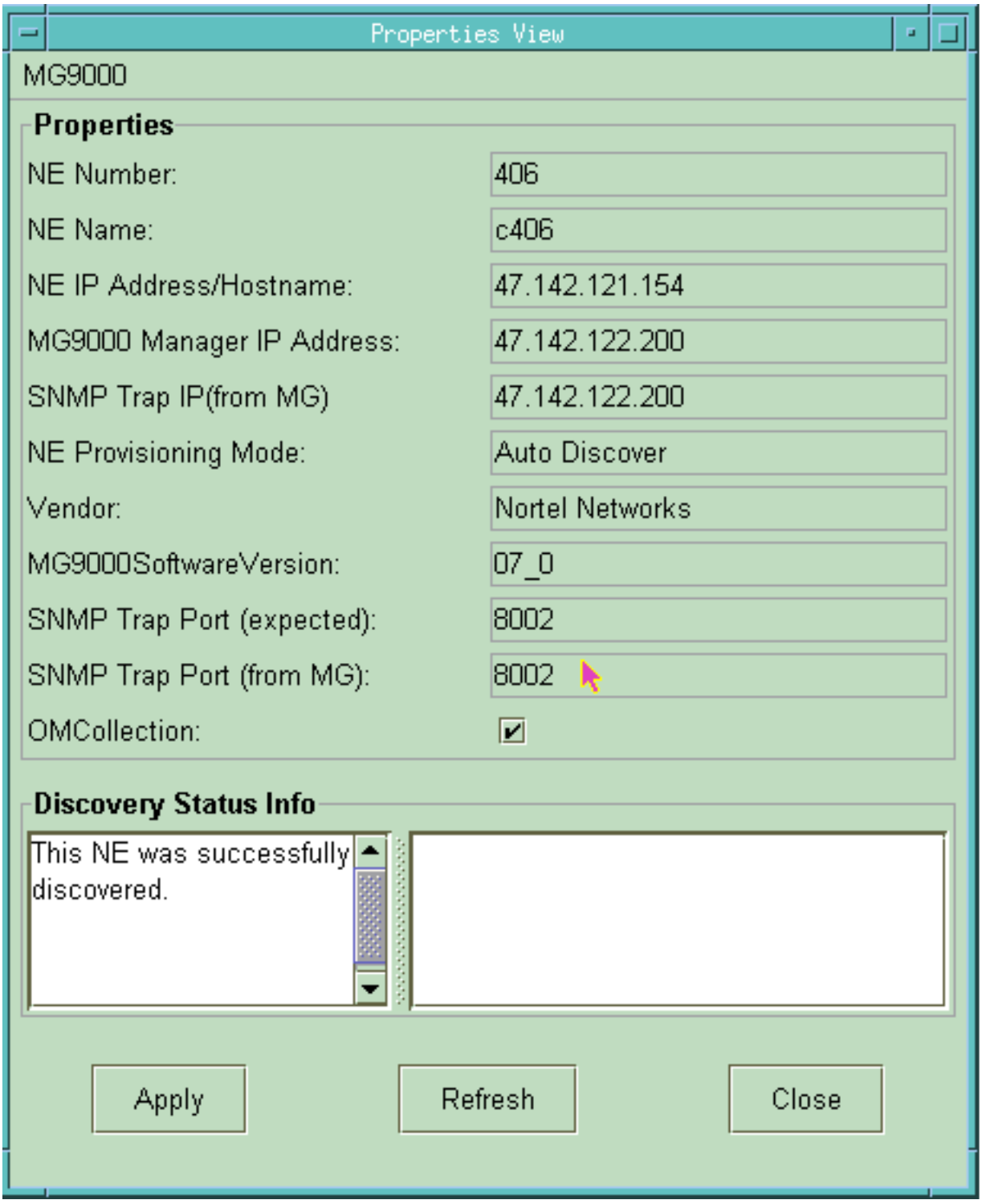
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
NE OMCollection	New	NA	checked/ unchecked	Refer to 12.8.2.3.1	None

There is no change in SN07 for other GUI fields.

36.8.2.5.5 Usage example

Operator can either check or uncheck the “NE OMCollection” checkbox.

Figure 9 MG9K-EM “NE properties” GUI when “NE OMCollection” is checked


Properties View
MG9000
Properties
NE Number:
406
NE Name:
c406
NE IP Address/Hostname:
47.142.121.154
MG9000 Manager IP Address:
47.142.122.200
SNMP Trap IP(from MG)
47.142.122.200
NE Provisioning Mode:
Auto Discover
Vendor:
Nortel Networks
MG9000SoftwareVersion:
07_0
SNMP Trap Port (expected):
8002
SNMP Trap Port (from MG):
8002
OMCollection:
Discovery Status Info
This NE was successfully discovered.
Apply
Refresh
Close

36.8.2.5.6 GUI release history update

In SN07, a new checkbox “NE OMCollection” is introduced in NE Properties GUI. Operator can check or uncheck this checkbox. If it is checked, OM Collector will collect OM data starting from its next collection cycle. If it is unchecked, OM Collector will stop collecting OM data starting from its next collection cycle.

36.8.2.5.7 Supplementary information

None

36.8.2.5.8 CLUI Interface

NA

36.8.2.6 GUI name: MG9K-EM NE Discovery GUI

36.8.2.6.1 Functional description

In SN07, a new checkbox “NE OMCollection” is introduced in NE Discovery GUI. This is a read-only field. It indicates whether OM data collection is enabled or disabled.

36.8.2.6.2 GUI Usage and implications

NA

36.8.2.6.3 GUI size

No changes in SN07.

36.8.2.6.4 GUI fields

Following table describes the fields of this GUI.

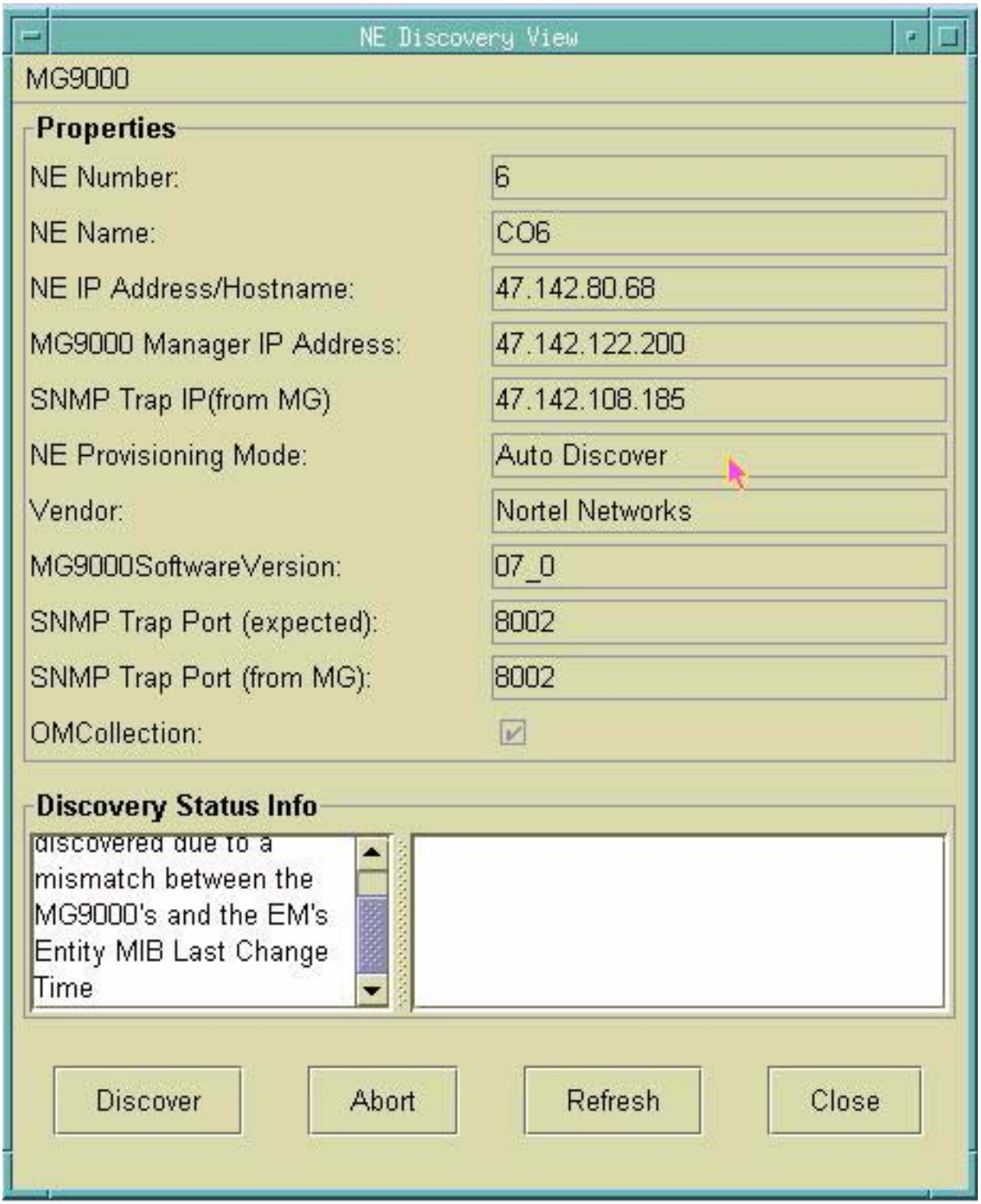
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
NE OMCollection	New	NA	checked/ unchecked	Refer to 12.8.2.6.1	None

There is no change in SN07 for other GUI fields.

36.8.2.6.5 Usage example

Operator can not change the “NE OMCollection” checkbox. He//she can come to know whether OM data collection is enable or disabled for a specific NE.

Figure 10 MG9K-EM “NE Discovery” GUI when “NE OM Collection” is checked



36.8.2.6.6 GUI release history update

In SN07, a new checkbox “NE OMCollection” is introduced in NE Discovery GUI. This is a read-only field. It indicates whether OM data collection is enabled or disabled.

36.8.2.6.7 Supplementary information

None

36.8.2.6.8 CLUI Interface

NA

36.9 Command interface changes

None

36.10 Security

36.10.1 Authentication.

- MG9K OM Collector access MG9K EM Oracle database tables, namely NODE_ATTRIBUTES, DEM_APPS and FRAME_LOC. It gets database password from the SSFPS password file “/opt/nortel/sspfs/db/pfsora.pwd”
- MG9K OM Collector open FTP/SFTP session with MG9K periodically. It get password for this FTP/SFTP session by querying a database table, maintained by MG9K EM.

36.11 Configuration Walkthrough

36.12 Glossary

Term	Description
EM alarm	Alarm generated internally by MG9K EM. Ex; When communication from MG9K EM to MG9K goes down, MG9K-EM generates an alarm with specific problem “Comm Channel Down - Communication Lost to the NE”.
Frame location information	It consists of frame type, floor position, row position, frame position, shelf position
Internal (logical) frame number	Frame number, which is unique within a MG9K
Gateway alarm	Alarm reported from gateway.
MG9K frame line-up	MG9K frames are lined-up either left to right or right to left. When frames are lined-up left to right, new frames are positioned/added to right of existing frames, as MG9K grows and frames are numbered from left to right. That means, Master frame will be the left-most frame in the NE. When frames are lined-up right to left, new frames are positioned/added to left of existing frames, as MG9K grows and frames are numbered from right to left. That means, Master frame will be the right-most frame in the NE.
NE	Network Element. Each NE has a Master shelf and zero or more subtending shelves/s, whose ITP cards are connected to the ITX card present in Master shelf.
Office (External) frame number	Frame number, which is unique within an office
Subtending frame	It has the subtending shelves of a MG9K

36.13 References

[1] A00003531_MG9000_Frame_Location_DID.pdf V1.3

[2] A00003531_MG9000_Frame_Location_FN_V2.pdf

[3] A00003486 Gateway location information FN

37: Configuration (CN): A00003567

37.1 Hardware and Software Requirements

This functionality is for MG9000 EM that has SN07 or higher software version.

37.2 Initial Configuration

No changes to the initial configuration.

37.3 Upgrade Impact

37.3.1 Dump and Restore

N/A

37.3.2 Element Management Upgrade

ABI ESA functionality is only applicable if the MG9000 is at a software release of SN07 or higher.

37.4 Element Management

37.4.1 GUI information

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Configuration View	Changed
Subnet View	Changed

37.4.1.1 ESA Configuration View

37.4.1.1.1 Functional description

In release SN07, this view will be enabled for ABI as well as ITP VMGs.For the ABI VMGs only enhanced ESA capability will be supported.

37.4.1.1.2 GUI usage and implications

From MG9kEMS software UE9000 MG Element Manager View, when you click Services submenu ‘Switched Line Services Manager’, this action invokes

Switched Line Services for MG9000 Element View. The ESA Config Panel View which is displayed when the “ESA Config” tab is selected.

37.4.1.1.3 GUI size

Not Applicable

37.4.1.1.4 GUI fields

The following table lists the new fields in the ESA Config View:

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Mode	Changed	N/A	“Enhanced (North American)” or “Basic”	The “Enhanced” will use the ESA data provided by the Core. This will be used by both ABI and ITP VMGs The “Basic” will work in the same manner that ESA is configured in SN06 using the MG9000 EM for ITP VMGs but will not be supported for ABI VMGs.	None
ESA Capability	Not Changed	N/A	“Yes” or “No”	“Yes” means that the selected VMG is capable of going into ESA. “No” means that the VMG is not capable of going into ESA.	nnEsaConfigAdminStatus
ESA Dialing Plan	Not Changed	N/A	add “7 and 10 Digit Dialing”	7 and 10 digit dialing is supported in SN06.2. It is supported only for “Enhanced” ESA mode. It will be disabled.	nnEsaConfigDialingPlan

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Notify Tone	Not Changed	N/A	“Yes” or “No”	“Yes” means that a notify tone is given to alert user that in ESA mode. “No” means that there is no indication to the user that in ESA mode. It will be disabled if “Enhanced” is selected.	nnEsaConfigNotifyTone
Default Pretranslator Name	Not Changed	N/A	Default Pretranslator name which is from Core	This field is the Default Pretranslator name that is associated with the selected VMG.It will be disabled if “Enhanced” is selected.	nnEsaConfigDefPretranslationId
ESA Operational Status	Not Changed	N/A	“Not in ESA” or “In ESA”	“Not in ESA” means that the VMG is not in ESA mode. “In ESA” means that the VMG is in ESA mode.	nnEsaConfigOperStatus
Download	Not Changed	N/A	N/A	When user clicks on this button, it will perform a manual downloading the EM ESA data to Gateway in order to resync the MG9000 with EM latest Core data for selected VMG.The button will be disabled if “Basic” is selected.	None
Customer Group	Not Changed	N/A	N/A	Click on this button, “ESA Customer Group List” View will be displayed. It will be disabled if “Basic” is selected.	None

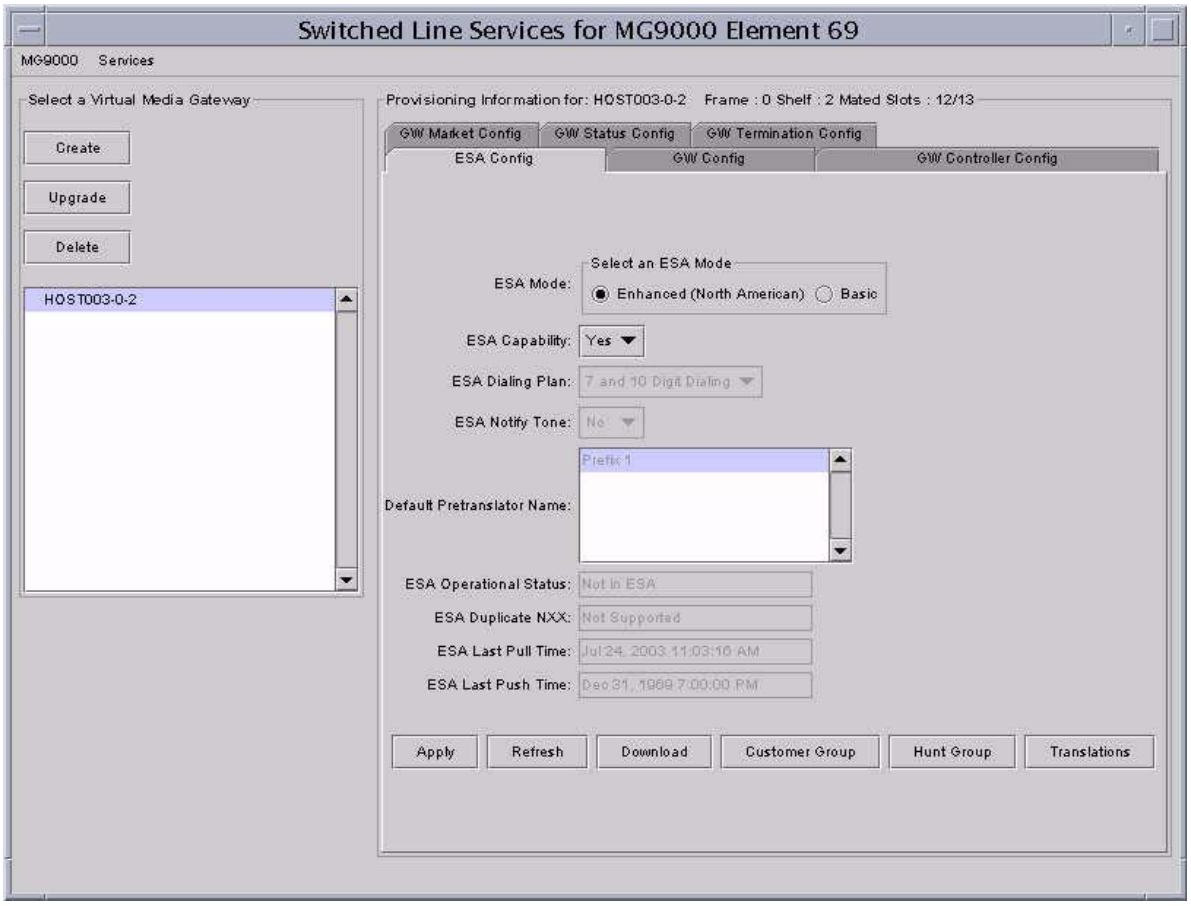
Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Hunt Group	Not Changed	N/A	N/A	Click on this button, “ESA Hunt Group List” View will be displayed. It will be disabled if “Basic” is selected.	None
Translations	Not changeds	N/A	N/A	Click on this button, “ESA Translation List” View will be displayed. It will be disabled if “Basic” is selected.	None

37.4.1.1.5 Usage example

The following example shows sample datafill in ESA Config View:

Figure 1 ESA Config View (Enhanced (North American) ESA)



37.4.1.2 Subnet View

37.4.1.2.1 Functional description

37.4.1.2.2 GUI usage and implications

37.4.1.2.3 GUI size

Not Applicable

37.4.1.2.4 Usage example

The following screenshot shows the additions to the subnet view.

Figure 2 Subnet View

37.4.1.2.5 Usage example

The following figure shows the sample datafill in GW Termination Config View:

37.4.1.2.6 GUI release history update

MG9000 EM Update: The ESA config GUI is modified to support ABI ESA, for enhanced ESA only. Subnet view changed to show DMS icon and subtending nodes.

37.4.1.2.7 Supplementary information

None.

37.4.1.2.8 CLUI Interface

N/A

37.4.1.2.9 Supplementary information

None.

37.4.1.2.10 CLUI Interface

N/A

37.5 Security

N/A

37.6 Configuration Walkthrough

37.6.1 SDM Configuration:

Please ensure that the SDM has the latest available fileset as part of the CS2E06 SDM load, for the package SDM_BASE.fts for the application ‘File Transfer Service”.

37.6.2 MG9K EM Configuration:

37.6.2.1 Set up the SSH authentication

This feature requires a key exchange between the MG9K EM server and the SDM for downloading the ESA data.

37.6.2.1.1 Procedure

1. Configure the SDM IP and SDM USER for this system. Log in to the MG9K EM server as ‘root’ and run the command:

   $ *cli*

   Select "Configuration", then select "OAMP Application Configuration", then select "Configure SDM IP and User" and set the SDM IP to the correct IP address of the SDM.

   Set the SDM user name to be “*esauser*”

2. For the user, ‘mgems’ on the MG9K EM server, generate the ssh key pair needed for data transmission between the MG9K EM and the SDM. As the ‘root’ user, execute the following commands:

   # *su - mgems*

   $ *ssh-keygen -t rsa*

   Accept the default location and enter an empty passphrase. This will create the following key file:

   /export/home/mgems/.ssh/id_rsa.pub

3. The key information contained in the file /export/home/mgems/.ssh/id_rsa.pub must be placed in the following file on the SDM:

   /home/esauser/.ssh/authorized_keys2

   — Secure copy the id_rsa.pub file to the SDM, using the command

$ *scp /export/home/mgems/.ssh/id_rsa.pub root@$SDM_IP:/home/esauser/tempkey*

Answer "yes" to the prompt "Are you sure you want to continue connecting (yes/no)?", then enter the password of the ‘root’ SDM user.

— Secure append the public key to the authorized keys list on the SDM, using the command

$ *ssh root@$SDM_IP ’cat /home/esauser/tempkey >> /home/esauser/.ssh/authorized_keys2’*

Enter the password of the ‘root’ SDM user when prompted for it.

Once completed, the MG9K EM will have the required access to the SDM for downloading the ESA data.

37.6.2.2 Set up ESA data download properties

ESA properties must be set up appropriately to download the right ESA data file from the Core at the right time. The Core will have an office parm configured to a specific time to start the collection of ESA data on the Core daily. The download of the ESA data is a nightly process and the corresponding time on the EM must be configured such that there is atleast half an hour delay between this time and the Core configured time.

There are 3 ESA data download properties that need to be properly configured. These include the time that will be used for nightly downloads, the name of the device on the Core where the ESA data file will be stored and the name of the ESA data file itself. These properties have the following default values:

ESA.DataDownloadTime=1:30 AM

ESA.DataDeviceName=/SFDEV

ESA.DataFileName=ESA_SYSTEM_SD$XML

ESA.DataFileNameUnix=ESA_SYSTEM_SD.XML

Notes:

- The ESA.DataFileNameUnix property is not editable. This is dynamically derived from the ESA.DataFileName property by the MG9K EM software.
- The ESA.DataFileName on the core should adhere to the following naming conventions:
  a. There can only be one ‘$’ sign in the name separating the ‘name’ part from the ‘extension’ part. (Please see the default value for an example).
  b. No spaces are allowed in the file name.

Use the following procedure only if you need to change the default values of the ESA properties.

37.6.2.2.1 Procedure

Telnet into the MG9K EM server and launch the ‘mg9kserver’ script, located under the “bin” directory under the server where it is installed. The menu walk through is described as follows only to be used as an example:

./mg9kserver config

Main Configuration Menu

1) Change Distribution Policy

2) Change SESM IP Address

3) Change Oracle IP Address

4) Change Debug Level for logs

5) Change Persistence settings

6) Change ESA data download settings

7) Display current settings

8) Exit from Main Menu

Please make a selection => 6

ESA Configuration Menu

1) Change ESA data download time

2) Change ESA data device name

3) Change ESA data file name

4) Exit to Main Menu

Please make a selection => 1

Please enter the new ESA data nightly download time ?

Default: [1:30 AM] => 5:30 PM

ESA Configuration Menu

1) Change ESA data download time

2) Change ESA data device name

3) Change ESA data file name

4) Exit to Main Menu

Please make a selection => 2

Please enter the new ESA data device name on the core ?

Default: [/SFDEV] => /ESADEV

ESA Configuration Menu

1) Change ESA data download time

2) Change ESA data device name

3) Change ESA data file name

4) Exit to Main Menu

Please make a selection => 3

Please enter the new ESA data file name on the core ?

Default: [ESA_SYSTEM_SD$XML] => ESADATA$XML

Name of the ESA data file on the EM: ESADATA.XML

ESA Configuration Menu

1) Change ESA data download time

2) Change ESA data device name

3) Change ESA data file name

4) Exit to Main Menu

Please make a selection => 4

Once completed, the new ESA data download properties will become effective on the future downloading of the ESA data.

37.6.3 Core Configuration:

37.6.3.1 Overview

ESA data file will be downloaded from the core using FTP. Hence, it is important to ensure that enough TCP connections are configured on the core for the FTP Server sessions.

The maximum number of FTP sessions is controlled by the “CM” tuple in TABLE IPHOST in the “CM”. The “CM” tuple is usually the first tuple in the table. This tuple contains the following fields:

NODENAME: Node name = CM.

CMINDEX: Index = 0.

TCPCONN: The total number of TCP connections allowed. This number must be greater than or equal to (*FTPCLCON* + *FTPSVCON*) * 2.

FTPCLCON:The maximum number of FTP client sessions allowed. SFT is not impacted by this value.

FTPSVCON:The maximum number of FTP server sessions allowed. SFT shares this resource with other CM FTP users.

Care must be taken when determining the value of *FTPSVCON*. Other telnet applications may have been configured and the value of *FTPSVCON* should be incremented taking this into account.

If *FTPSVCON* is incremented, ensure that *TCPCONN* is large enough to support the total of *FTPCLCON* and *FTPSVCON*. Each FTP session will consume 2 TCP connections. This will be enforced by the *IPHOST* table control.

38: Configuration (CN): A00003571

38.1 Hardware and Software Requirements

The Software requirement is MG9KEM SN07 release and MG9K sn07 release.

This feature supports the following new card release:

- Internet Telephony Processor (ITP): NTNY30CA (IP & AAL1 modes)
- Access Bridging Interface (ABI): NTNY43BA (IP & AAL1 modes)

38.2 Initial Configuration

The ITP and/or ABI must be discovered.

38.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

38.4 Upgrade Impact

38.4.1 Dump and Restore

N/A

38.4.2 Element Management Upgrade

These new releases of ITP and ABI are supported only in SN07 and higher.

The MG9kEM must upgrade first to SN07 and then New ITP and ABI cards can be upgraded.

The Downgrade process MUST:

FIRST downgrade the hardware (ITP and/or ABI) before downgrade the MG9KEM software.

38.5 Data schema (DS) (CM, MIBS, RDB)

N/A

38.6 Service Orders (SO) (CM & SESM)

Not Applicable.

38.7 Software optionality control (SOC)

Not Applicable.

38.8 Element Management

38.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Siwtched Line Services manager - GW config Tab	Changed
Provision a Virtual Media Gateway	Changed

38.8.2 GUI information

38.8.2.1 GUI name: Switched Line Services manager

<Switched Line Services for MG9000 Element #>

38.8.2.1.1 Functional description

This GUI provisions the Configuration for VMGs.

38.8.2.1.2 GUI usage and implications

Current datafill order unchanged.

38.8.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Switched Line Services for MG9000 Element ##	1	60	extra memory required by JAVA swing library to display one text field and its label

38.8.2.1.4 GUI fields

Table 3 GUI field descriptions

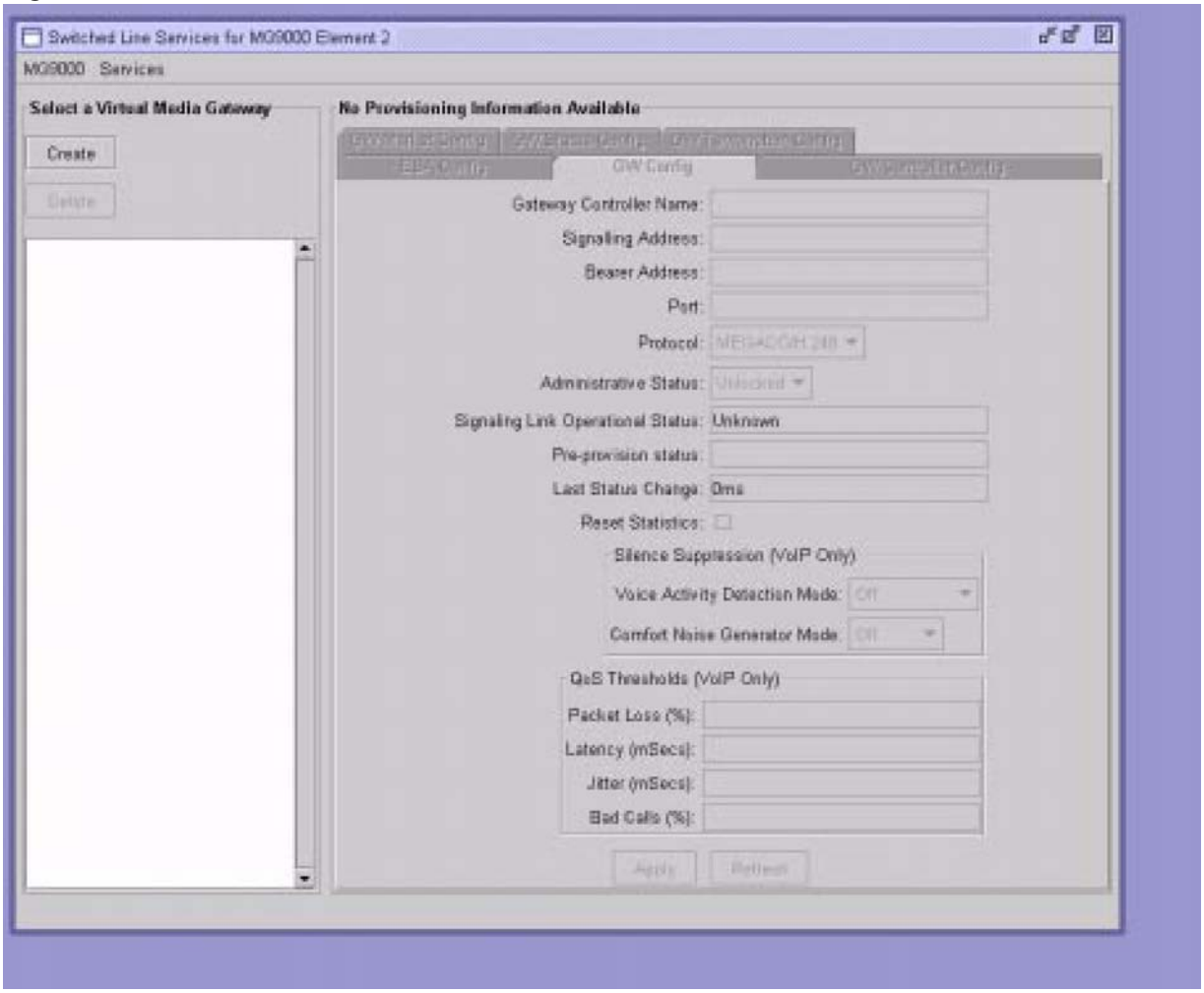
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Bearer Address	new	NA	IP Address	Provides the Address of the bearer Path	NORTEL-UEMGMEGACO-MIB, NnMegacoBearerTable, nnMegacoBearerIpAddress

38.8.2.1.5 Usage example

The following Image shows the existing GUI with the new field ëBearer Addressí in the GW config Tab.

The value to be entered must be an IP address format: 1.2.3.4

Figure 1 Switched Line Services with Bearer Address field



38.8.2.1.6 GUI release history update

38.8.2.1.7 Supplementary information

38.8.2.1.8 CLUI interface

38.8.2.2 GUI name: Provision a Virtual Media Gateway

<Provision a Virtual Media Gateway>

38.8.2.2.1 Functional description

This GUI provisions the Configuration for VMGs.

38.8.2.2.2 GUI usage and implications

Current datafill order unchanged.

38.8.2.2.3 GUI size

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Provision a Virtual Media Gateway	1	60	Extra memory required by JAVA swing library to display one field in a pull-down menu.

38.8.2.2.4 GUI fields

The following table lists fields for GUI or pull down menu Provision a Virtual Media Gateway.

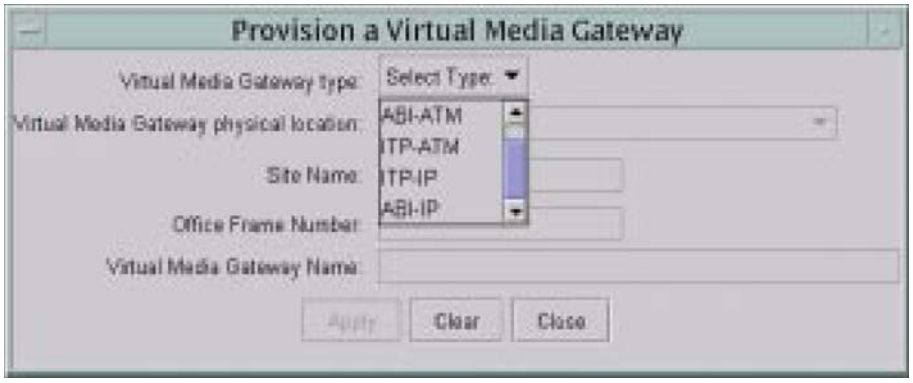
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
VMG type	change	NA	Pull down	identify tyhe VMG type to provision	NORTEL-UEMGMEGACO-MIB, NnMegacoBearerTable, nnMegacoBearerType

38.8.2.2.5 Usage example

The following Image shows the GUI with the new field in the GW config Tab.

The value to be selected can be: ABI_ATM, ABI_IP, ITP_ATM, ITP_IP.

VMG type ABI_IP is only supported in the new release of ABI card.



38.8.2.2.6 GUI release history update

38.8.2.2.7 Supplementary information

38.8.2.2.8 CLUI interface

38.9 Command interface changes

N/A

38.10 Security

Not Applicable.

38.11 Configuration Walkthrough

Not Applicable.

39: Configuration (CN): A00003591

39.1 Hardware and Software Requirements

NA

39.2 Initial Configuration

NA

39.3 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

39.4 Upgrade Impact

NA

39.5 Data schema (DS) (CM, MIBS, RDB)

39.5.1 New/modified tables, MIBs, or Database Schema

This feature uses new MIBs - channelized carrier configuraton details introduced by a Gateway feature A00003604

39.6 Service Orders (SO) (CM & SESM)

NA

39.7 Software optionality control (SOC)

NA

39.8 Element Management

The Element manager will display channelization carrier configuration details from SN07 release.

39.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
OC3STS1PortView	New
Performance browser	changed

39.8.2 GUI information

39.8.2.1 GUI name: Carrier configuration display

OC3STS1PortView

39.8.2.1.1 Functional description

If the carrier is channelized, the port view will display OC3 Section/Line and three STS1 path information. When the user clicks on the OC3 port on the OC3CardView, if the carrier is channelized, three ilog graphics will be displayed on the graphical panel in the portview for STS1 path information. The OC3Section/Line information is displayed by default in a tab. Double clicking on the ilogs will display STS1 path information in a separate tab.

The OC3 Section/Line details is unchanged for channelized carrier details. The STS1 path information displayed will be Circuit identifier, Description, speed, NETWORK field and status of the STS1 path. The status includes administrative, operational and configuration status. The user can lock/unlock or online/offline the OC3 Section/Line and three STS1 path separately. To lock OC3 Section/Line, all the three STS1 paths should be locked first. . To unlock nertwork carrier the OC3 Section/Line should be unlocked. . In the release SN07 traffic will be sent on only one STS1 path and that path is the network carrier. The STS1 path description will mention DS3 payload if the DS3 is opted on the STS1. For the network carrier, the destination will be NETWORK. For other STS1 paths the destination will be NONE. The STS1 path label will mention if DS3(plcp or clearchannel) payload is supported on STS1.

The carrier can be changed from OC3c to OC3 and viceversa dynamically from LCI. But a coldstart has to be sent to EM from Gateway after changing the carrier to EM know that the carrier has been modified

39.8.2.2 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
channelized OC3 carrier	3	3 per MG9000	NA

39.8.2.2.1 GUI fields

39.8.2.2.2 GUI release history update

None

39.8.2.2.3 Supplementary information

The carrier can be provisioned (concatenated/channelized) from LCI.The EM will display the carrier details. The EM user will be able to change only the administrative(lock/unlock) and configuration state. The user will not be able to provision the carrier from EM.

39.8.2.2.4 CLUI Interface

NA

39.8.2.3 Performance parameters for channelized carrier

39.8.2.3.1 GUI name: channelized carrier performance parameter

Performance browser

39.8.2.3.2 Functional Description

If the carrier is in channelized mode, the performance browser will display the OC3 Section/Line, STS1 path performance parameters and DS3 path information(if DS3 payload is selected) The information remains unchanged for OC3c.

In the performance browser, if the carrier is channelized, clicking on OC3 port will just display OC3 Section/Line performance parameters. Three nodes will be displayed under OC3 port for 3 STS1 paths information.Clicking on each of STS1 path will display STS1 path and DS3 performance parameters statistics. If DS3 payload is selected on the STS1 paths, the DS3 performance parameters will be displayed.

39.8.3 New Alarms

The STS1 and DS3 alarms will be handled at EM. The new alarms will be

LOP, UNEQ, PLM, AIS and RDI for STS1 and LOF, RAI and AIS for DS3.

39.8.4 Upgrade and Downgrade

To support channelization in SN07, the DCC card uses new hardware. So, SN06.2 and below , GW load should not be loaded on this card.A SN06.2 MG9K should have new hardware to has to be loaded with SN07 load.

39.9 Command interface changes

NA

39.10 Security

NA

39.11 Configuration Walkthrough

NA

40: Configuration (CN): A00003615

40.1 Hardware and Software Requirements

For the reduction of upgrade downtime, the user must have fieldgrade Netra t1400s or N240s.

40.2 Initial Configuration

The only initial configuration required would be the registration of SSPFS into PSE/NPM. This will be automatically handled via the SSPFS installation/ upgrade scripts.

40.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

40.4 Upgrade Considerations

The only impact to upgrade will be the required new step in the process which will re-attach the mirrors. This new step will replace the “boot -s” step in the current documentation. The new step will ask the user to run the command link_mirrors as root to get the mirrors reattached. Please refer to the DSUM for A00003615 for details on the internals of this script.

40.5 Data schema (DS) (CM, MIBS, RDB)

N/A

40.6 Service Orders (SO) (CM & SESM)

N/A

40.7 Software optionality control (SOC)

N/A

40.8 Element Management

New interface additions into cli will be described in the User Interface section of this document.

40.9 User interface changes

40.9.1 Directory: View

40.9.1.1 Directory Description

This existing menu level contains commands to view various informational items on the SSPFS unit.

40.9.1.2 Accessing directory: View

40.9.1.2.1 Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the user enters “x” or “X” to exit to the higher level menu

40.9.2 Command: sspfs_patch

40.9.2.1 Command type: MENU

40.9.2.2 Command target: Other, SSPFS System

40.9.2.3 Command availability: RES

40.9.2.4 Command description

The command will allow the user to view the status of the patches for SSPFS.

40.9.2.5 Command syntax

The command take no options or user input.

40.9.2.6 Qualifications and warnings

N/A

40.9.2.7 Responses

40.9.2.7.1 Example

The option will provide a table listing of the patch information in a fashion such as:

SSPFS Patch	Installed	Active
SSPFS07MA	Yes	Yes
SSPFS07MB	Yes	

40.9.3 Directory: Other

40.9.3.1 Directory Description

This existing menu level contains miscellaneous commands to manage items on the SSPFS unit.

40.9.3.2 Accessing directory: Other

40.9.3.2.1 Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the user enters “x” or “X” to exit to the higher level menu

40.9.4 Command: sun_explorer

40.9.4.1 Command type: MENU

40.9.4.2 Command target: Other, SSPFS System

40.9.4.3 Command availability: RES

40.9.4.4 Command description

The command will allow the user to execute the Sun Explorer software.

40.9.4.5 Command syntax

The command take no options or user input.

40.9.4.6 Qualifications and warnings

N/A

40.9.4.7 Responses

40.9.4.7.1 Example

=== Executing “sun_explorer” ===
=== “sun_explorer” completed successfully.

When this command is finished, the sun “dump” will reside in the directory /tmp.

40.9.5 Command: mount_image

40.9.5.1 Command type: MENU

40.9.5.2 Command target: Other, SSPFS System

40.9.5.3 Command availability: RES

40.9.5.4 Command description

The command will allow the user to mount a generic iso image to the SSPFS unit

40.9.5.5 Command syntax

This command only takes one parameter which must be a full path string to the iso image.

40.9.5.6 Qualifications and warnings

The user must be the root user to run this command

40.9.5.7 Responses

40.9.5.7.1 Example

=== Executing “mount_image” ===

Enter the full path to the iso image: /tmp/junk.iso
Mounting /tmp/junk.iso to /mnt
=== “mount_image” completed successfully.

40.10 Security

N/A

40.11 Configuration Walkthrough

All “cli” additions are purely optional, however, their use should be encouraged. This is especially true in the event of a field issue where the debugging options would be helpful.

41: Configuration (CN): A00003630

41.1 Hardware and Software Requirements

It is assumed the hardware and software installation of the CS2K is complete with the SN07 load lineup for the CS2K core, GWC, and CS2M. The MG is provided by a third party gateway vendor supporting TGCP as described in the PKT-SP-TGCP-I05-030728 TGCP Specification. Additionally, CS2M and OSSGate is initialized and available for provisioning data related to this activity.

41.2 Initial Configuration

Refer to section “41.11 Configuration Walkthrough” on page 2999.

41.3 Office/Subnet parameters (OP/SP) (CM & SESM)

No new office parameter or subnet parameter is introduced by this activity.

41.4 Upgrade Impact

41.4.1 Dump and Restore

None

41.4.2 Element Management Upgrade

Since TGCP profile is a new gateway profile introduced in SN07, there is no upgrade work required to upgrade existing TGCP gateways to the ones with the new profile.

However, through this feature, all the 5 existing PVG profiles are collapsed into one profile -- PVG.

PVG15K
PVG15K_1000
PVG15K_PARTIAL
PVG7K
PVG_VSP3

All existing PVG gateway profiles share the same information other than the maximum reserved endpoints. The new PVG profile is defined to have the maximum reserved endpoints to be the maximum of all the ones defined in the existing PVG profiles..

Similarly, all the following “Motorola” profiles are collapsed into one profile -- “MOTOROLA.

MOTOROLAMTA_1

MOTOROLAMTA_2
MOTOROLAMTA_4

All the following four “TouchTone” profiles are collapsed into one profile -- “TOUCHTONE”.

TOUCHTONE_NN01_1
TOUCHTONE_NN01_2
TOUCHTONE_NN01_3
TOUCHTONE_NN01_4

All the following “MediaTrix” profiles are collapsed into one profile -- “MEDIATRIX”.

MEDIATRIX_LINE_GW_24
MEDIATRIX_LINE_GW_4

All the following “ASKEY” profiles are collapsed into one profile -- ”ASKEY”.

ASKEY_LINE_GW_12
ASKEY_LINE_GW_30
ASKEY_LINE_GW_4

All the following “CVX” profiles are collapsed into one profile -- “CVX”.

CVX1800_2688
CVX600_612

All the following “ARRIS” profiles are collapsed into one profile -- “ARRIS”.

ARRIS_TOUCHTONE_NN01_4
ARRIS_TOUCHTONE_NN02_4

All the following “PVG” profiles are collapsed into one profile -- “PVG_APG”.

PVG_APG
PVG_APG_VSP3

Because of the collapse activity, upgrade plug-ins are written to upgrade all the existing gateways to reference their new respective gateway profile.

41.5 Data schema (DS) (CM, MIBS, RDB)

41.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NORTEL-GWC-COMMON-TC	changed	unchanged
SERVRINV	changed	unchanged
TRKGRP	changed	unchanged
TRKSGRP	changed	unchanged
TRKOPTS	changed	unchanged
TRKMEM	changed	unchanged

41.5.2 Table/MIB/Remote Database Schema information

41.5.2.1 Name: NORTEL-GWC-COMMON-TC

Nortel GWC Common attributes MIB

41.5.2.1.1 Functional description

This MIB is used for defining all the supported gateway protocols.

In this MIB, a new protocol “TGCPPROTOCOL” is added in the supported protocol list for the field “GWCDeviceProtocol” as shown below. The rest of the MIB stays the same.

```
GWCDeviceProtocol ::= TEXTUAL-CONVENTION
   STATUS       current
   DESCRIPTION
         "Represents device protocol type defined in gwcdtype.h and
          callpdefs.h on the Gateway Controller. The module gwcdtype.h,
        enum gw_protocols { NIL_PROTOCOL, NCS_PROTOCOL, ASPEN,
DSMCC, MEGACO, MGCP, TGCPPROTOCOL,
FILLER3_PROTOCOL,GWCRESERVED, DQOSPROTOCOL,
MGCP_PLUS, H323}."
   SYNTAX       INTEGER { nilprotocol     (0),
                          ncsprotocol      (1),
                          aspen            (2),
                          dsmcc            (3),
                          megaco           (4),
```

```
mgcp                (5),
tgcpprotocol        (6),
filler3protocol     (7),
gwcreserved         (8),  -- GWC internal use only
dqosprotocol        (9),
mgcpplus            (10),
h323                (11)}
```

41.5.2.1.2 Usage sequence and implications (CM Only)

Not Applicable

41.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NORTEL-GWC-COMMON-TC	0	115000	

41.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for **NORTEL-GWC-COMMON-TC**.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GWCDevice Protocol	Changed	N/A	TGCPPROTOCOL	When provisioning a TGCP gateway, TGCP protocol information needs to be sent down to the GWC device from SESM.

41.5.2.1.5 Datafill example

When sending SNMP set to the GWC device, GWCDeviceProtocol should be set to 12 for provisioning TGCP gateways.

GWCDeviceProtocol = 6;

41.5.2.1.6 Table release history update

41.5.2.1.7 Supplementary information

41.5.2.1.8 Translation verification other tools
Not Applicable

41.5.2.2 Name: SERVRINV
Server Inventory table

41.5.2.2.1 Functional description
This activity adds a new exec line-up, GWCABEX, for GWC node types. The new exec line-up is specific to Succession End Office and Tandem Per Trunk Signaling (PTS) trunk types configured on a GWC node type. For GWCs configured with MF OP and/or ES trunk group members, GWCABEX must be provisioned with the **ABTRK** TERMTYPE in table SERVRINV.

41.5.2.2.2 Usage sequence and implications (CM Only)
Current datafill order unchanged by this activity.

41.5.2.2.3 Size
The size of this table is unchanged by this activity.

41.5.2.2.4 Fields/OIDs
The following table lists fields for table SERVRINV changed by this activity. The configuration information for all other fields in table SERVRINV are unchanged.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	changed	TRMTYPE	unchanged	The TRMTYPE subfield is unchanged. This activity adds a new EXEC entry for the existing TRMTYPE of **ABTRK**.
		EXEC	GWCABEX	The new exec line-up, GWCABEX, is added. For GWCs configured with either OP or ES trunk group members, GWCABEX must be provisioned with a TRMTYPE **ABTRK.**

41.5.2.2.5 Datafill example

The following example shows sample datafill for table SERVRINV.

```
SRVRNAME        SRVRADDR
                                                    SRVREXEC
SRVRTONE    SRVROPTS
-------------------------------------------------------------------------
            GWC         0       IP  47  174  66  4
            (                   ABTRK   GWCABEX)
NORTHAM             $
```

41.5.2.2.6 Table release history update

The following information is added to table SERVRINV:

exec line-up GWCABEX added to field SRVREXEC

41.5.2.2.7 Supplementary information

Tuples in table SERVRINV should not be added or changed via manual table control commands. Provisioning of this table should be performed using CS2M GWC node provisioning.

The modifications to table SERVRINV is a shared requirement with activity A00003506. See activity A00003506 for further details.

41.5.2.2.8 Translation verification other tools

Not applicable.

41.5.2.3 Name: TRKGRP

Trunk Group Table Table

41.5.2.3.1 Functional description

This activity introduces new provisioning restrictions in table TRKGRP for MF OP and ES trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and the trunk group tuple is changed in table TRKGRP.

Table 5 Supported GWC MF Trunk Group Types for TGCP MG

Trunk Group Type	Supported Services
OP	Operator Services
ES	Emergency Services

41.5.2.3.2 Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

41.5.2.3.3 Size

The size of this table is unchanged by this activity.

41.5.2.3.4 Fields/OIDs

Not Applicable

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

41.5.2.3.5 Datafill example

Not Applicable

41.5.2.3.6 Table release history update

The following information is added to table TRKGRP:

restrictions added for GWC MF OP and ES trunk groups

41.5.2.3.7 Supplementary information

When MF OP or ES trunk group data is changed in table TRKGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKGRP data is provisioned correctly. Table 6, "TRKGRP Restrictions," on page 2916 lists the new error messages that may be generated by table control.

Table 7 TRKGRP Restrictions

Trunk Type	Error Messages
OP	"GWCPTSTK option exists in table TRKOPTS. DIR must be IC or OG." "GWCPTSTK option exists in table TRKOPTS. ANITYPE must be REV." "GWCPTSTK option exists in table TRKOPTS. EAOSS must be N."
ES	"GWCPTSTK option exists in table TRKOPTS. DIR must be OG." "GWCPTSTK option exists in table TRKOPTS. ANI must be ANISPILL." "GWCPTSTK option exists in table TRKOPTS. SWST must be DC." "GWCPTSTK option exists in table TRKOPTS. FDISCTIM must be 0."

The modifications to table TRKGRP is a shared requirement with activity A00003506. See activity A00003506 for further details.

41.5.2.3.8 Translation verification other tools

Not Applicable

41.5.2.4 Name: TRKSGRP

Trunk Subgroup Table

41.5.2.4.1 Functional description

This activity introduces new provisioning restrictions in table TRKSGRP for MF OP and ES trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and adding or changing the trunk subgroup tuples in table TRKSGRP.

41.5.2.4.2 Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP

5. table TRKMEM

41.5.2.4.3 Size
The size of this table is unchanged by this activity.

41.5.2.4.4 Fields/OIDs
Not Applicable

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

41.5.2.4.5 Datafill example
Not Applicable

41.5.2.4.6 Table release history update
The following information is added to table TRKSGRP:

restrictions added for GWC MF OP and ES trunk groups

41.5.2.4.7 Supplementary information
When MF OP or ES trunk groups are provisioned or tuples are changed in table TRKSGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKSGRP data is provisioned correctly. Table 7, "TRKSGRP Restrictions," on page 2919 lists the new error messages that may be generated by table control.

Table 9 TRKSGRP Restrictions

TRKSGRP Field	Error Messages
OP, ES	"GWCPTSTK option exists in table TRKOPTS. CCONT must be NO." "GWCPTSTK option exists in table TRKOPTS. OPULSTYPin table TRKSGRP must be MF for this trunk type." "GWCPTSTK option exists in table TRKOPTS.OSTARTSG in table TRKSGRP must be WK for this trunk type.." "GWCPTSTK option exists in table TRKOPTS. SGRPVAR must be STD." "GWCPTSTK option exists in table TRKOPTS. RNGBCK must be MW." "GWCPTSTK option exists in table TRKOPTS. ESUPR must be N." "GWCPTSTK option exists in table TRKOPTS. ECSTAT must be INTERNAL or EXTERNAL."

Provisioning of this table may also be performed using OSSGate. The error checking described above is performed on TRKSGRP data enter through OSSGate.

The modifications to table TRKSGRP is a shared requirement with activity A00003506. See activity A00003506 for further details.

41.5.2.4.8 Translation verification other tools
Not Applicable

41.5.2.5 Name: TRKOPTS
Trunk Options Table

41.5.2.5.1 Functional description
A new trunk group option, GWCPTSTK, is added to table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. In the SN07 release, GWCPTSTK is supported with all GWC PTS supported trunk group types configured on a GWC. This option must be provisioned prior to configuring MF OP and/or ES trunk group members in table TRKMEM.

Additionally, this activity adds a sub-option , PRELOADANI, to the GWCPTSTK trunk group option. PRELOADANI sub-option identifies PTS packet trunks which support a call model that allows the ANI digits to be sent from the Core to the GWC prior to receiving any ANI request from the far-end.

41.5.2.5.2 Usage sequence and implications (CM Only)
When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI

2. table TRKGRP

3. table TRKOPTS, option GWCPTSTK

4. table TRKSGRP

5. table TRKMEM

Table TRKOPTS may be provisioned following table TRKSGRP. Table control restrictions enforce table TRKOPTS be provisioned after table TRKGRP and before table TRKMEM.

41.5.2.5.3 Size
The size of this table is unchanged by this activity.

41.5.2.5.4 Fields/OIDs

The following table lists fields for TRKOPTS that are changed by this activity.

Table 10 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	changed	CLLI	unchanged	The CLLI subfield is unchanged. Provision the OP or ES trunk group CLLI.
		OPTION	GWCPTSTK	The new option GWCPTSTK is added. For MF OP and ES trunks configured on a GWC, this option must be provisioned.
OPTION	changed	OPTION	GWCPTSTK	The new option GWCPTSTK is added. For PTS trunks configured on a GWC, this option must be provisioned.
		PRELOADANI	Y/N	The new sub-option PRELOADANI is added. For GWC PTS trunks which support a call model that allows the ANI digits to be sent from the Core prior to receiving an ANI request, the field must be to Y.

41.5.2.5.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

```
                OPTKEY                  OPTINFO

-------------------------------------------------------------------------

     PTSCLLI    GWCPTSTK            GWCPTSTK N
```

41.5.2.5.6 Table release history update

The following information is added to table TRKOPTS:

option GWCPTSTK added for GWC PTS trunk groups

41.5.2.5.7 Supplementary information

Option GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. This option applies to all GWC PTS trunk group types supported in the SN07 release. Table control in table TRKOPTS blocks the addition of this option to a non-supported trunk type (see Table 4, "Supported GWC PTS Trunk Group Types," on page 2914 and activity A00003506 for the list of supported PTS trunk types on a GWC). The following error message will result:

"GWCPTSTK cannot be assigned for the following reasons:"
"It is not supported with this trunk type."

This option cannot be added for PTS trunk groups if there is existing datafill in either table TRKGRP or table TRKSGRP not supported on the GWC. If this error occurs when provisioning GWCPTSTK in table TRKOPTS, the tuple entry in table TRKGRP and/or table TRKSGRP must be changed. See Table 6, "TRKGRP Restrictions," on page 2916 and Table 7, "TRKSGRP Restrictions," on page 2919 for the list of restrictions.

This option cannot be added to a supported PTS trunk group that contains members on a peripheral type other than a GWC. PTS trunk groups on a GWC can not consist of members on different peripheral types, such as a GWC and DTC (hybrid PTS trunk groups are not supported). A check is made of other trunk members already present in table TRKMEM prior to assigning the GWCPTSTK option. If members are present it is assumed they do not have a PMTYPE of GWC, since the option isn't assigned yet. The following error will result:

"GWCPTSTK cannot be assigned for the following reasons:"
"Trunk Members exist in table TRKMEM"

This option cannot be deleted from table TRKOPTS until all members on the trunk group have been deleted from table TRKMEM. The following error will result:

"GWCPTSTK cannot be deleted for the following reasons:"
"Trunk Members exist in table TRKMEM"

The PRELOADANI sub-option applies only to GWC PTS trunk group types of OP and ES. The PRELOADANI sub-option cannot be set to "Y" for other GWC PTS trunk group types (see activity A00003506 for the list of supported PTS trunk types on a GWC).

41.5.2.5.8 Translation verification other tools
Not Applicable

41.5.2.6 Name: TRKMEM
Trunk Member Table

41.5.2.6.1 Functional description
This activity introduces new provisioning restrictions in table TRKMEM for MF OP and ES trunks groups configured on a GWC.

41.5.2.6.2 Usage sequence and implications (CM Only)
When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

41.5.2.6.3 Size
The size of this table is unchanged by this activity.

41.5.2.6.4 Fields/OIDs
Not Applicable

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

41.5.2.6.5 Datafill example
Not Applicable

41.5.2.6.6 Table release history update
The following information is added to table TRKMEM:

restrictions added for GWC MF OP and ES trunk groups

41.5.2.6.7 Supplementary information
Table control for table TRKMEM determines if the option GWCPTSTK is provisioned in table TRKOPTS. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKMEM data is provisioned correctly (see Table 10, “TRKMEM Restrictions,” on page 2924).

Table 12 TRKMEM Restrictions

TRKMEM Action	Error Messages
Attempt to ADD member with GWC PMTYPE to PTS group without GWCPTSTK option.	TBD
Attempt to ADD member with non-GWC PMTYPE to PTS group with GWCPTSTK option	TBD
Attempt to Change PMTYPE from GWC to non-GWC.	TBD
Attempt to CHANGE PMTYPE from Non-GWC to GWC	TBD

Provisioning of this table may also be performed using OSSGate. The error checking described above is performed on TRKMEM data enter through OSSGate.

The modifications to table TRKMEM is a shared requirement with activity A00003506. See activity A00003506 for further details.

41.5.2.6.8 Translation verification other tools

Not Applicable

41.6 Service Orders (SO) (CM & SESM)

Service Order unchanged by this activity.

41.7 Software optionality control (SOC)

Not Applicable. There is no SOC control for this activity

41.8 Element Management

41.8.1 New/modified GUIs

Table 13 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Associate Gateway	Changed
Add GWC	Changed

41.8.2 GUI information

41.8.2.1 GUI name: Add GW

Associate Gateway Dialog

41.8.2.1.1 Functional description

Associate Gateway Dialog is a graphic tool that provides the crafts person with the ability to associate a gateway. For this activity, a TGCP gateway can be associated via the Associated Gateway Dialog from CS2M GUI.

41.8.2.1.2 GUI usage and implications

There is no requirement to datafill the Associate Gateway Dialog in a specific order.

41.8.2.1.3 GUI size

Table 14 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add GW	0	10	64k

41.8.2.1.4 GUI fields

The following table lists fields for the Associate Gateway Dialog.

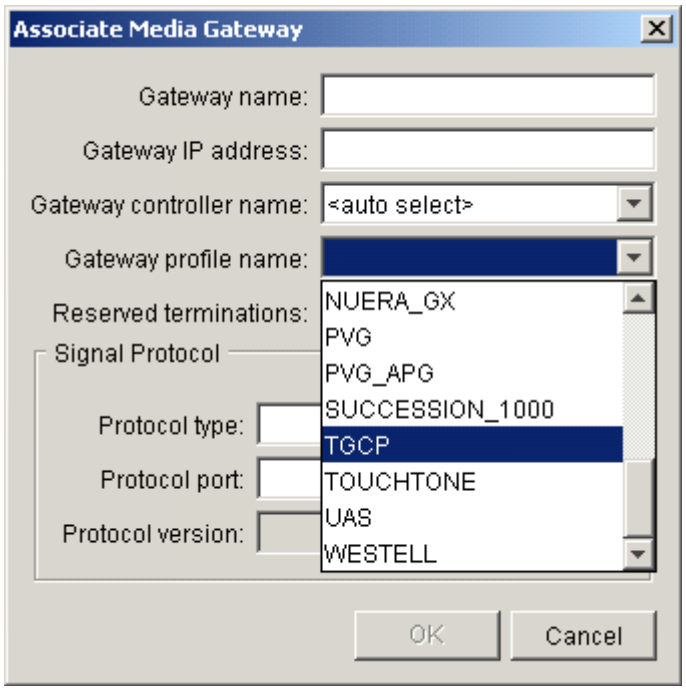
- Gateway Name
- Gateway IP Address
- Gateway Controller Name
- Gateway Profile Name
- Reserved Terminations
- Protocol Type
- Protocol Port
- Protocol Version

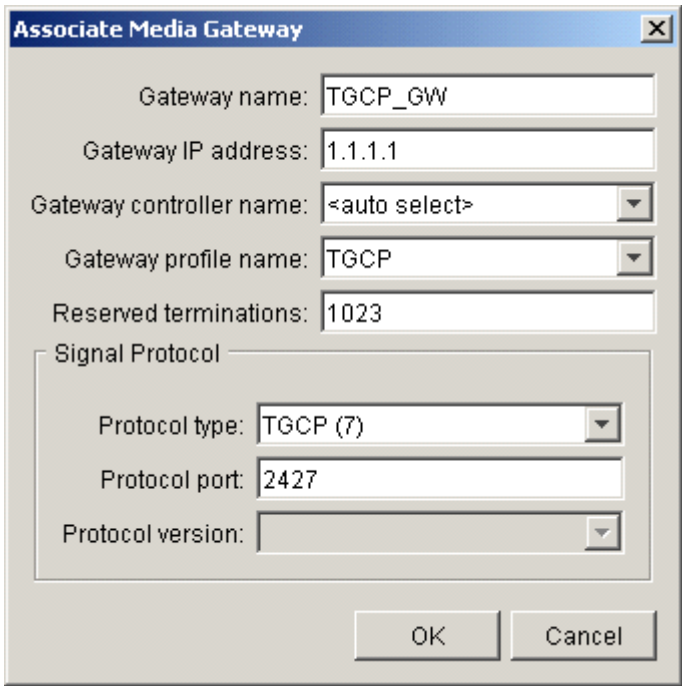
Table 15 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Gateway Profile Name	Changed	N/A	TGCP	When adding a TGCP gateway, the TGCP gateway profile should be selected from the provided profile list.	GWC-GW-MIB

41.8.2.1.5 Usage example

The following example shows sample datafill or menu selection for GUI Associate Gateway Dialog:





41.8.2.1.6 GUI release history update

41.8.2.1.7 Supplementary information

41.8.2.1.8 CLUI Interface

41.8.2.1.9 OSSGate Interface

The following is an example of an XML input file when using OSSGate interface to datafill a TGCP gateway.

```
<?xml version="1.0" encoding="UTF-8"  ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
    <assocMG usn="1" version="1.0">
     <Parameters>
       <mgUIName>mg1.nortel.net</mgUIName>
       <mgProfileName>TGCP_GW</mgProfileName>
       <mgIpAddr>47.49.23.43</mgIpAddr>
       <mgProtocolType>12</mgProtocolType>
       <mgProtocolVersion>1.0</mgProtocolVersion>
       <mgProtocolPort>2427</mgProtocolPort>
       <gwcUIName>GWC-0</gwcUIName>
     </Parameters>
    </assocMG>
  </Methods>
 </Command>
</CommandList>
```

41.8.2.2 GUI name: Add GWC

Add Gateway Controller Dialog

41.8.2.2.1 Functional description

Add Gateway Controller Dialog is a graphic tool that provides the crafts person with the ability to add a gateway controller.

When PTS functionality is provided, a different TRUNK profile needs to be selected to provision different EXEC types in the XACore.

41.8.2.2.2 GUI usage and implications

There is no requirement to datafill the Add Gateway Controller Dialog in a specific order.

41.8.2.2.3 GUI size

Table 16 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add GWC	0	10	64k

41.8.2.2.4 GUI fields

The following table lists fields for the Add Gateway Controller Dialog.

- Gateway Controller Name
- Gateway Controller Active IP Address
- Message Router IP Address
- Gateway Controller Profiles

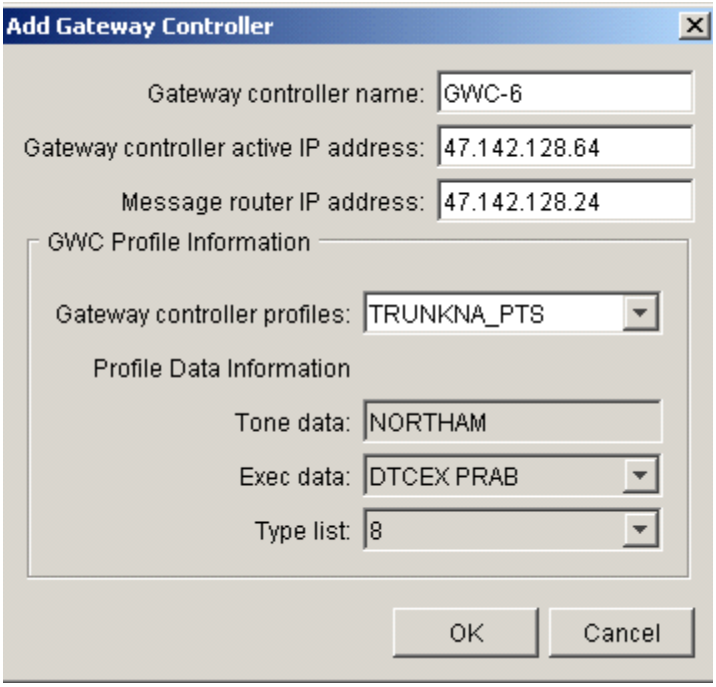
- Tone Data
- Exec Data
- Type List

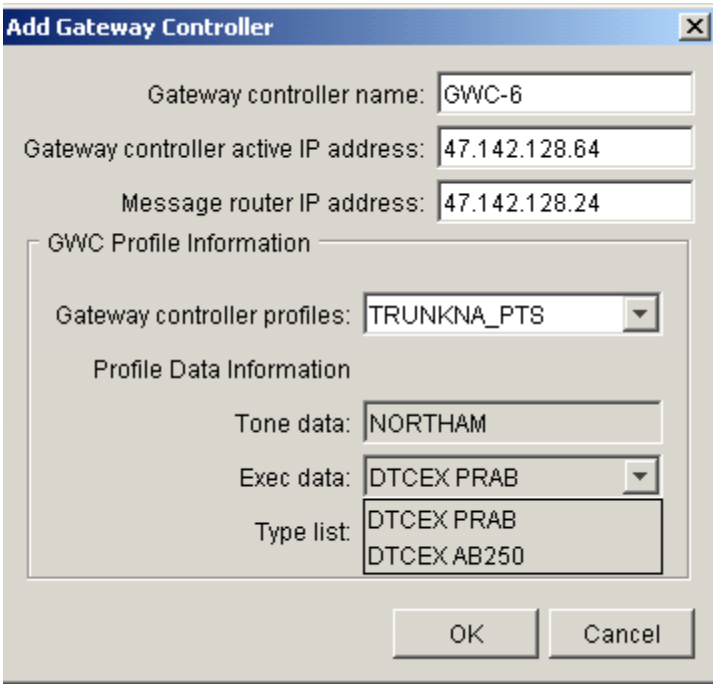
Table 17 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Gateway Controller Profile Name	Changed	N/A	TRUNKNA	When PTS functionality is provided, TRUNKNA needs to be selected when adding a GWC	GWC-GWC-MIB
EXEC Type	Changed	N/A	(DTCEX, PRAB) (GWCABEX, ABTRK)	When PTS functionality is provided, EXEC type needs to include ABTRK	

41.8.2.2.5 Usage example

The following example shows sample datafill or menu selection for GUI Add Gateway Controller Dialog:





41.8.2.2.6 GUI release history update

41.8.2.2.7 Supplementary information

41.8.2.2.8 CLUI Interface

41.8.2.2.9 OSSGate Interface

The only method of adding a gateway controller is through GUI. There is no XML interface for it.

41.9 Command interface changes

41.9.1 Directory: TTP

41.9.1.1 Directory description

Trunk Test Position (TTP) is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

41.9.1.2 Accessing directory: TRKS

41.9.1.2.1 Access to directory or MAP level and return to CI

To access TTP for the CI environment enter “mapci;mtc;trks;ttp”

To return to the CI environment enter “quit all”.

41.9.1.3 Supplementary information

New restrictions are added to the TTP level of the MAP for MF OP and ES trunks configured on a GWC.

The "Seize" and "Cktinfo" commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

"Action not supported on GWC trunks."

The "TST" and "Ckt" commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

"Action not supported on GWC trunks." or
"No IW SPM IP Bridges Available to Perform Action."

41.9.2 Directory: MONITOR

41.9.2.1 Directory description

MONITOR is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

41.9.2.2 Accessing directory: TTP

41.9.2.2.1 Access to directory or MAP level and return to CI

To access MONITOR for the CI environment enter "mapci;mtc;trks;ttp;level monitor"

To return to the CI environment enter "quit all".

41.9.2.3 Supplementary information

New restrictions are added to the MONITOR level of the MAP for MF OP and ES trunks configured on a GWC.

The "CktMon", "CPos_", and "RLS" commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

"Action not supported on GWC trunks."

The "TST" and "MonTalk" commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

"Action not supported on GWC trunks." or
"No IW SPM IP Bridges Available to Perform Action."

MONITOR level is not accessible for posted MF OP and ES trunks configured on a GWC if Succession IW bridges are not available. The following error message is displayed if an attempt is made to enter the MONITOR map level without the available components:

"No IW SPM IP Bridges Available to Perform Action."

41.9.3 Directory: MANUAL

41.9.3.1 Directory description

MANUAL is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

41.9.3.2 Accessing directory: TTP

41.9.3.2.1 Access to directory or MAP level and return to CI

To access MANUAL for the CI environment enter "mapci;mtc;trks;ttp;level manual"

To return to the CI environment enter "quit all".

41.9.3.3 Supplementary information

New restrictions are added to the MANUAL level of the MAP for MF OP and ES trunks configured on a GWC.

The "OP_", "SGNL", and "RLS" commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

"Action not supported on GWC trunks."

The "Loss", "TGEN", "TST", "Noise", "TDET", and "HSET" commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

"Action not supported on GWC trunks." or
"No IW SPM IP Bridges Available to Perform Action."

41.9.4 Directory: DATA

41.9.4.1 Directory description

DATA is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

41.9.4.2 Accessing directory: TTP

41.9.4.2.1 Access to directory or MAP level and return to CI

To access DATA for the CI environment enter “mapci;mtc;trks;ttp;level datattp”

To return to the CI environment enter “quit all”.

41.9.4.3 Supplementary information

New restrictions are added to the DATA level of the MAP for MF OP and ES trunks configured on a GWC.

The “Seize”, “BTerm_”, and “RLS” commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

“Action not supported on GWC trunks.”

The “BERT_” command require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute this command without the available components:

“Action not supported on GWC trunks.” or
“No IW SPM IP Bridges Available to Perform Action.”

41.10 Security

Not covered by this activity. See activity A00003576.

41.11 Configuration Walkthrough

Following is a high-level walkthrough of the steps required to provision MF OP and ES trunk groups on a GWC.

1. Add the GWC node using the CS2M GWC EM. The CS2M GWC EM will provision table SERVRINV on the CS2K core. The new exec line-up, **GWCABEX**, must be selected when provisioning the GWC node.
2. Provision the TGCP MG(s) using the CS2M GWC EM. The gateway profile name that should be provisioned for a TGCP MG is “**tbd**[1]”. Additionally, TGCP protocol must be specified.

   When provisioning the TGCP MGs, the GWC name must be entered. In the SN07 release, MF OP and ES trunks must be configured on a GWC reserved for PTS trunks only. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.

[1]The profile name can not be confirmed at this time, but will be updated when the activity is completed.

3. Provision the TGCP MG endpoints on the GWC using the CS2M GWC EM. The endpoint names and terminal numbers returned by the GWC EM should be noted. The terminal numbers are required for provisioning table TRKMEM on the CS2K core.
4. Provision table CLLI with the OP and/or ES trunk group clli.
5. Provision table TRKGRP with the OP and/or ES trunk group data. Note the table control restrictions described in Table 6, "TRKGRP Restrictions," on page 2916.
6. Provision the GWCPTSTK option for MF OP and/or ES trunk group clli in table TRKOPTS.
7. Provision table TRKSGRP with the OP and/or ES trunk subgroup data. Note the table control restrictions described in Table 7, "TRKSGRP Restrictions," on page 2919.
8. Provision table TRKMEM with the OP and/or ES trunk group members. The terminal number information provided by the CS2M GWC EM is required when entering tuples in table TRKMEM. Note the table control restrictions described in section "41.5.2.6 Name: TRKMEM" on page 2989.

Following is a high-level walkthrough of the steps required to provision TGCP ISUP IT and/or ATC trunk groups on a GWC.

1. Add the GWC node using the CS2M GWC EM. The CS2M GWC EM will provision table SERVRINV on the CS2K core.
2. Provision the TGCP MG(s) using the CS2M GWC EM. The gateway profile name that should be provisioned for a TGCP MG is "**tbd**[1]". Additionally, TGCP protocol must be specified.

   When provisioning the TGCP MGs, the GWC name must be entered. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.
3. Provision the TGCP MG endpoints on the GWC using the CS2M GWC EM. The endpoint names and terminal numbers returned by the GWC EM should be noted. The terminal numbers are required for provisioning table TRKMEM on the CS2K core.
4. Provision table CLLI with the ISUP IT and/or ATC trunk group clli.
5. Provision table TRKGRP with the ISUP IT and/or ATC trunk group data.
6. Provision table TRKSGRP with the ISUP IT and/or ATC trunk subgroup data.
7. Provision table TRKMEM with the ISUP IT and/or ATC trunk group members. The terminal number information provided by the CS2M GWC EM is required when entering tuples in table TRKMEM.

[1]The profile name can not be confirmed at this time, but will be updated when the activity is completed.

8. Provision table ISUPDEST with the C7 routeset for the ISUP IT and/or ATC trunk subgroups.
9. Provision table C7TRKMEM with the C7 circuit ID code (CIC) for the ISUP IT and/or ATC trunk group members.

42: Configuration (CN): A00003667

42.1 Hardware and Software Requirements

No change due to this feature.

42.2 Initial Configuration

No change due to this feature.

42.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

42.4 Upgrade Impact

42.4.1 Dump and Restore

N/A

42.4.2 Element Management Upgrade

This feature introduces a new mechanism for sending SESM alarm logs northbound. Previously this was handled via syslog to the SDM. In this release, it can be handled by CORBA notifications to the IEMS.

For customers that use IEMS in SN07, the syslog generation should be turned off to avoid duplication of the alarm logs. This cannot be turned off over the upgrade because some customers will not have IEMS in SN07. So this should be a manual step post-insallation.

To turn the SESM syslog generation off:

1) As root on the SESM server: > cd /opt/nortel/NTsesm/admin/bin/

2) Run: ./configure

3) Select option 5: SESM logging configuration (syslog, sesm debug log)

4) Select option 3: SESM Alarm Logging configuration

5) Enter n

6) Exit the configuration tool

7) Restart the SESM application: ./ptmctl restart

In the case of new installations, this northbound syslog generation will still be turned on by default. To turn this off for customers with IEMS, the same commands listed above should be run post installation.

42.5 Data schema (DS) (CM, MIBS, RDB)

N/A

42.6 Service Orders (SO) (CM & SESM)

N/A

42.7 Software optionality control (SOC)

N/A

42.8 Element Management

42.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
SESM Alarm Manager	Changed
SESM Alarm History	Changed

42.8.2 GUI information

42.8.2.1 GUI name: SESM Alarm Manager and Alarm History

42.8.2.1.1 Functional description

The Alarm Manager is the SESM GUI used to monitor active alarms in on devices it manages. It receives CORBA notifications when new alarms occur or when existing alarms are cleared. Because of the addition of IEMS and its alarm manager, the alarm acknowledgment feature is no longer required at this level. Alarms should be acknowledged at the network management level.

Alarm History is the SESM GUI used to view all alarms received by the system (to save disk space, old alarms are cleared after some preconfigured time period, usually 1 week). This GUI shows both active and cleared alarms.

42.8.2.1.2 GUI usage and implications

Because of the addition of IEMS and its alarm manager, the alarm acknowledgment feature is no longer required at this level. Alarms should be acknowledged at the network management level.

In the Alarm Manager, the ability to acknowledge and de-acknowledge the alarms will be removed. In the Alarm History, the check box to filter on acknowledged alarms will be removed so as to not be confusing.

42.8.2.1.3 GUI size
N/A

42.8.2.1.4 GUI fields

N/A

42.8.2.1.5 Usage example
N/A

42.8.2.1.6 GUI release history update
N/A

42.8.2.1.7 Supplementary information
N/A

42.8.2.1.8 CLUI Interface
N/A

42.9 Command interface changes
N/A

42.10 Security
N/A

42.11 Configuration Walkthrough
N/A

43: Configuration (CN): A00003669

43.1 Hardware and Software Requirements

Standard MG4K SPM node with all the datafills and RMs.

43.2 Initial Configuration

Not Applicable.

43.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

43.4 Upgrade Impact

Not Applicable.

43.5 Data schema (DS) (CM, MIBS, RDB)

43.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	changed-New field SGFABRIC is added for SMG4 (MG4K) class SPM.	new
MNMGPIP	changed- New fields GEMSIGIP, SIGSUBMASK, BEARERVLAN, SIGVLAN, SIGIPENABLED are added	new
MNIPPARM	changed - new fields DIFFSERV and MEDIA_INTEG are added	new

43.5.2 Table/MIB/Remote Database Schema information

43.5.2.1 Name: MNNODE

Management Network Node Table

43.5.2.1.1 Functional description

This feature adds a new ***SGFABRIC*** field to the MG4K class of SPM in table MNNODE. T. For ATM MG4K nodes, this new field, ***SGFABRIC*** , is set to 'ATM' and for IP MG4K nodes, it is set to 'IP'.

43.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

43.5.2.1.3 Size

It does not change.

43.5.2.1.4 Fields/OIDs

Table 3, gives the information about the new fields introduced in table MNNODE.

Table 2 MNNODE Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SGFABRIC	New		ATM or IP	If the value is set to 'ATM', it indicates that the particular MG4K is of ATM framework. The value of 'IP' indicates that the MG4K node is of IP framework. The default value is set to 'ATM' after TABXFR from previous releases to release having this change.

43.5.2.1.5 Datafill example

Figure 1 MAP display for table MNNODE

```
NODEKEY ALIAS NODEINFO
----------------------
SPM 4 SPM_4 SMG4 0 SYNC LINE 50 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $(SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (SMG4CN MN RPT)
(PATCHFAIL MJ RPT) (ATMBCN CR RPT) (ST3EHLD MJ RPT) (ST3EHLD24 CR RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMSRMNTD MN RPT) (LOCUR MJ RPT)
(TSRCFAIL CR RPT) $ $ N 0 $ N N ATM
```

43.5.2.1.6 Table release history update

SN07:

New field ***SGFABRIC*** is added to the table for SMG4 variant of SPM. This field is defined as a signalling FABRIC type. If this field is set to 'ATM', then only ATM RMs can be datafilled in MNCKTPAK.If the field is set to IP then only GEM RMs can be datafilled in MNCKTPAK.

43.5.2.1.7 Supplementary information

The field ***SGFABRIC*** can be changed for a datafilled MG4K node.Node must be in OFFL state for SGFABRIC field change operation. Steps to be followed during MG4K-ATM to MG4K-IP are listed below.

- BSY/OFFL the RM and CEM on the MG4K-ATM
- Delete all the tuple entries in table ATMCONN for the desired node.
- Delete All entries for MG4K-ATM from table MNATMIF.
- BSY/OFFL all ATM carriers.
- Delete ATM Carriers from table MNHSCARR
- Delete ATM RM datafill from the table MNCKTPAK.
- Delete ATM_GRP from table MNPRTGRP
- Add GEM_GRP in table MNPRTGRP
- Add load info in table PMLOADS.
- Change SGFABRIC field value from ATM to IP in table MNNODE
- Datafill GEM RM in the table MNCKTPAK for the desired node.
- Datafill table MNMGPIP, with entries for newly added GEM RMs.
- Change entries in table MNIPPARM for fine tuning of IP parameters.
- BSY/RTS MG4K-IP CEM and RMs.

For MG4K-IP to MG4K-ATM similar steps are followed with little changes.

43.5.2.1.8 Error messages for MNNODE :

- Trying a SGFABRIC change when the node is MANB/INSV/ISTb state.

```
For ATM to IP change:
Error: Failed to change SGFABRIC from ATM to IP.
       Please OFFL the node before attempting SGFABRIC change.

For IP to ATM change:
Error: Failed to change SGFABRIC from IP to ATM.
       Please OFFL the node before attempting SGFABRIC change.
```

- SGFABRIC change fails to verify node update tuple due to internal error.

```
Error: Failed to change SGFABRIC due to internal error.
```

- SGFABRIC change from ATM to IP fails because table ATMCONN datafill related to node undergoing change is not deleted.

```
Error: Failed to change SGFABRIC from ATM to IP.
       Delete all the tuples corresponding to
       SPM 10 from table ATMCONN
```

- SGFABRIC change from IP to ATM fails because table MNMGPIP datafill related to node undergoing change is not deleted.

```
Error: Failed to change SGFABRIC from IP to ATM.
       Delete all the tuples corresponding to
       SPM 10 from table MNMGPIP
```

- SGFABRIC change verification passes for ATM to IP operation.

```
Warning: Verification passed for SGFABRIC change from ATM to IP.
         Please ensure that MNMGPIP is datafilled.
```

- SGFABRIC change verification passes for IP to ATM operation.

```
Warning: Verification passed for SGFABRIC change from IP to ATM.
         Please ensure that ATMCONN is datafilled.
```

43.5.2.2 Name: MNCKTPAK

Management Network Circuit Pack

43.5.2.2.1 Functional description

This feature adds datafill restrictions for slot 1, 2, 9 & 10 of shelf 1 for RMs.

43.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

43.5.2.2.3 Size

It does not change.

43.5.2.2.4 Fields/OIDs

No Change.

43.5.2.2.5 Datafill example

No Change.

43.5.2.2.6 Table release history update

SN07:

New datafill restrictions are applicable only if the GEM RM is provisioned in the SPM.

43.5.2.2.7 Supplementary information

None.

43.5.2.2.8 Error messages in MNCKTPAK

- Block ATM RM addition in table MNCKTPAK if the sgfabric of the node is IP.

```
Error: ATM RM cannot be datafilled because the SGFABRIC field in
       table MNNODE is set to IP. Only GEM RM can be datafilled.
```

- Block GEM RM addition in table MNCKTPAK if the fabric of the node is ATM.

```
Error: GEM RM cannot be datafilled because the SGFABRIC field in
       table MNNODE is set to ATM. Only ATM RM can be datafilled.
```

- No CPKs are allowed to be datafilled in slots 1, 2, 9 & 10 of shelf 1 if GEM RM is datafilled in any of these slots of shelf 0 because of thermal dissipation.

```
Error: No CPKs are allowed to be datafilled in slots 1/2/9/10
       of shelf 1 while GEM RM is already datafilled in the
       same slot on shelf 0 since thermal restrictions dictate
       that we leave the slot empty over a GEM RM.
```

- GEM RM is not allowed to be datafilled in slot 1, 2, 9 & 10 of shelf 0 if any other RM is already datafilled in any of these slots of shelf 1.

```
Error: GEM RM is not allowed to be datafilled in slots 1/2/9/10
       of shelf 0 while any other RM is already datafilled in the
       same slot on shelf 1 since thermal restrictions dictate
       that we leave the slot empty over a GEM RM.
```

43.5.2.3 Name: MNMGPIP

Management Network Media Gateway Processor Internet Protocol

43.5.2.3.1 Functional description

This feature adds 5 fields to the MNMGPIP table: the signalling IP address, the signalling mask, the signalling enabled status, the VLAN TCI for the signalling interface, and VLAN TCI for the bearer interface.

43.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

Restrictions on VLAN TCI values:

- Upon ONP to SN07, the default value showing a 0 N 0 will be used
- For the Bearer VLAN TCI, changes to this field will not be allowed without BSYing or OFFLing the GEM RMs. For signalling VLAN TCI, the change can be made on the fly for the FIRST CHANGE ONLY - once the TCI has been set, then the GEMs will have to be BSY in order to change the value. This is because the IP interface is active when the GEM is INSV - changing these values requires re-provisioning the far-end switch for VLAN as well and this would cause an INSV GEM to go SYSB.
- If the default value of'0 N 0' is present for a VlanTCI in the table, that GEM interface will not perform VLAN tagging of outgoing packets but will instead fill that word with the NULL VLAN tag.

Restrictions on Signalling address:

- GEMSIGIP and SIGSUBMASK default to 0.0.0.0 for an IW-SPM during an ONP to SN07; this ensures the signalling interface starts out disabled on the new load.
- SIGIPENABLED field defaults to N during an ONP to SN07. It can be changed to Y only after a valid address has been entered in SIGIPADDR and SIGSUBMASK. It can be changed back to N at any time to disable IP signalling on the GEM.
- On an IW-SPM, GEMSIGIP and SIGSUBMASK are allowed to change from 0.0.0.0 to any valid value and back to 0.0.0.0 while the GEM is INSV and the SIGIPENABLED boolean is FALSE. All other changes are blocked.
- In the future, an MG4K-IP SPM will be provisioned; for these nodes, the SIGIP fields must all contain valid values and are not allowed to change while the GEM is INSV.

43.5.2.3.3 Size

Table tuple limits unchanged.

43.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for MNMGPIP.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GEMSIGIP	new	none	0 0 0 0 to 255 255 255 255	The usual DMS-format IP Address range (no “dots” in the field) used as the address for signalling interface
SIGSUBMASK	new	none	0 0 0 0 to 255 255 255 255	The usual DMS-format IP Address range (no “dots” in the field) used as the mask for signalling interface
SIGIPENABLED	new	none	Y or N	Is
BEARVLAN	new	PRIORITY	0-7	User Priority
BEARVLAN	new	CFI	Y or N	Canonical Format Indicator - only N is supported
BEARVLAN	new	VID	0-4095 (*255 for Calisto-based GEM RMs)	VLAN ID - a unique number to identify the VLAN (* NTLZ20AA, BA, and CA boards are restricted to 255 due to Broadcom Calisto DSP implementation), and 1& 4095 are reserved by spec and are not allowed to be entered.
SIGVLAN	new	PRIORITY	0-7	User Priority
SIGVLAN	new	CFI	Y or N	Canonical Format Indicator - only N is supported
SIGVLAN	new	VID	0-4095	VLAN ID - a unique number to identify the VLAN - 1and 4095 are reserved by the spec and are not allowed to be entered.

43.5.2.3.5 Datafill example

The following example shows sample datafill for table MNMGPIP.

Figure 2 MAP display for table MNMGPIP

```
>table mnmgpip
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MNMGPIP
>list
            MGPKEY         GEMMGMIP         SUBNMASK          BCASTIP
           GWIP        GEMBARIP AUTONEG         GEMSIGIP       SIGSUBMASK
SIGIPENABLED BEARERVLAN  SIGVLAN
-------------------------------------------------------------------------
       SPM  2 0  9 172  16 121   8 255 255 255   0 172  16 121 255
172  16 121   1 172  16 121  10       Y 172  16 121  11 255 255 255   0
           Y    253 N 6 2032 N 5
```

43.5.2.3.6 Table release history update

SN07:

New fields are present and datafilled “benignly” so that their features are not enabled over an ONP. They must be manually enabled at the customers need.

43.5.2.3.7 Supplementary information

The “range” command from the switch, just in case anyone is interested:

```
11 BEARERVLAN         T_VLAN_TCI
12 SIGVLAN            T_VLAN_TCI
LOGICAL TUPLE TYPE: T_SMGPCT_LT
Mate>range 11
11 BEARERVLAN         T_VLAN_TCI
TYPE IS T_VLAN_TCI MULTIPLE WITH
        VID         {0 TO 4095}
        CFI         {N,Y}
        PRIORITY    {0 TO 7}
Mate>range 12
12 SIGVLAN            T_VLAN_TCI
TYPE IS T_VLAN_TCI MULTIPLE WITH
        VID         {0 TO 4095}
        CFI         {N,Y}
        PRIORITY    {0 TO 7}
```

43.5.2.3.8 Translation verification other tools

None

43.5.2.4 Name: MNIPPARM

Management Network Internet Protocol PARaMeters

43.5.2.4.1 Functional description

This feature adds 2 fields to the MNIPPARM table: the DIFFSERV codepoints and the Media Integrity Indicator.

43.5.2.4.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

43.5.2.4.3 Size

Table tuple limits unchanged.

43.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for MNIPPARM.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIFFSERV	new	EF_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint, ie: CP101110	The codepoint for voice band defaults to CP101110
DIFFSERV	new	EF_PRIORITY	0-7	The priority for voice defaults to 6
DIFFSERV	new	CS5_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint,, ie: CP101000	The codepoint for signalling data defaults to CP101000
DIFFSERV	new	CS5_PRIORITY	0-7	The priority for signalling defaults to 6
MEDIA_INTEG	new	MI_STATUS	ENABLE or DISABLE	Indicates the state of Media Integrity on this GEM card, defaults to DISABLE

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MEDIA_INTEG	new	MI_ACTION	NONE, LOGONLY, TEARDOWN	Indicates the action to be taken when MI fails.
MEDIA_INTEG	new	MI_INTEGER	0 to 32767	Today, this is unused but will be required when MI functionality is fully defined.

43.5.2.4.5 Datafill example

The following example shows sample datafill for table MNIPPARM.

Figure 3 MAP display for table MNIPPARM

```
>table mnipparm
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MNIPPARM
Mate>list all
TOP
MNKEY  DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG
         ECAN   VOICE CMFNOISE     T38 RFC2833 RTCP      TONESET LOGINT
CRCERROR USIZEPKT OSIZEPKT FRAGMENT  JABBER DROPEVNT BRDCAST  JITTER LATENCY
VPKTLOST  MINLOG         OMPARMS              DIFFSERV
          MEDIA_INTEG
-------------------------------------------------------------------------------
-
IWSPM G711ULAW     NONE      10       0      0      0    100       0
     DISABLE      OFF  DISABLE DISABLE DISABLE   N  NORTHAMERICA      5
  20  10   20  10   20  10   20  10  20  10   20  10  20  10  20  10  20  10
  20  10    1000  50  1000  1000 CP101110 6 CP101000 6
              DISABLE

 MG4K G711ULAW     NONE      10       0      0      0    100       0
     DISABLE      OFF  DISABLE DISABLE DISABLE   N  NORTHAMERICA      5
  20  10   20  10   20  10   20  10  20  10   20  10  20  10  20  10  20  10
  20  10    1000  50  1000  1000 CP101110 6 CP101000 6
              DISABLE

BOTTOM
```

43.5.2.4.6 Table release history update

SN07:

New fields are present and datafilled with their default values so that their features are not enabled over an ONP. They must be manually enabled at the customers need.

43.5.2.4.7 Supplementary information

Media Integrity requires that RTCP field be set to “Y” before it can be enabled.

Once MI is enabled, RTCP can no longer be set to “N” until MI is disabled once again.

The range commands from the switch, just in case anyone wants to see them:

```
30 DIFFSERV          DIFFSERV_TYPE
31 MEDIA_INTEG       MEDIA_INTEGRITY_STATUS_TYPE
LOGICAL TUPLE TYPE: T_MNPARM_LT
Mate>range 30
30 DIFFSERV          DIFFSERV_TYPE
TYPE IS DIFFSERV_TYPE MULTIPLE WITH
        EF_CODEPOINT  DIFFSERV_CODEPOINT
        EF_PRIORITY   {0 TO 7}
        CS5_CODEPOINT DIFFSERV_CODEPOINT
        CS5_PRIORITY  {0 TO 7}
Mate>range 31
31 MEDIA_INTEG       MEDIA_INTEGRITY_STATUS_TYPE
TYPE IS MEDIA_INTEGRITY_STATUS_TYPE MULTIPLE WITH
        MI_STATUS                   {ENABLE,DISABLE} REFINEMENTS:
        {DISABLE}                   MI_DISABLE_ACTION_FIELD
        {ENABLE}                    MULTIPLE WITH
             MI_ACTION              {NONE,LOGONLY,TEARDOWN}
             MI_INTEGER             {0 TO 32767}
```

None

43.5.2.4.8 Translation verification other tools

None

43.6 Service Orders (SO) (CM & SESM)

Not Applicable

43.7 Software optionality control (SOC).

Not Applicable.

43.8 Element Management

Not Applicable.

43.9 Command interface changes

Not Applicable

43.10 Security

Not Applicable

43.11 Configuration Walkthrough

44: Configuration (CN): A00003672

Note: All unnecessary sections have been deleted from this document section. If it has been deleted then the reader can assume it is not applicable.

44.1 Hardware and Software Requirements

none.

44.2 Upgrade Impact

None.

44.3 Data schema (DS) (CM, MIBS, RDB)

44.3.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNCKTPAK	CHANGED	UNCHANGED

44.3.2 Table/MIB/Remote Database Schema information

44.3.2.1 Name: MNCKTPAK

MN (SPM) RM Circuit Pack Table

44.3.2.1.1 Functional description

This is an addition of a new value to an existing field:

Existing Field: PEC

New Value: NTLZ20CA

Existing Format:

```
TABLE: MNCKTPAK
>ran
 1 CPKKEY            T_SPMCKT_KEY
 2 CPKINFO           T_SPMCKT_CKTPAK
 3 PEC               T_SPMCKT_CPK_PEC
 4 RELEASE           T_CPK_RELEASE
 5 LOAD              EIGHT_CHAR_VECTOR
LOGICAL TUPLE TYPE: T_SPMCKT_LT
>ran 3
 3 PEC               T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
         NORTEL Product Engineering Code:
         {NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
```

```
          NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
          NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
          NTLX82AB,NTLX82BA,NTLX89DA,NTLX67AA,
          NTLX99BA,NTLX73BB,NTLX72BA,NTLX89AA,
          NTLX83AA,NTLX92AA,NTLX74AA,NTLX76AA,
          NTLX44AA,NTLX82EA,NTLZ20BA}

          Non-NORTEL Product Identification Code:
           TABLE OF 8 CHARs
```

New Format:

```
TABLE: MNCKTPAK
>ran
 1 CPKKEY              T_SPMCKT_KEY
 2 CPKINFO             T_SPMCKT_CKTPAK
 3 PEC                 T_SPMCKT_CPK_PEC
 4 RELEASE             T_CPK_RELEASE
 5 LOAD                EIGHT_CHAR_VECTOR
LOGICAL TUPLE TYPE: T_SPMCKT_LT
>ran 3
 3 PEC                 T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
          NORTEL Product Engineering Code:
          {NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
          NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
          NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
          NTLX82AB,NTLX82BA,NTLX89DA,NTLX67AA,
          NTLX99BA,NTLX73BB,NTLX72BA,NTLX89AA,
          NTLX83AA,NTLX92AA,NTLX74AA,NTLX76AA,
          NTLX44AA,NTLX82EA,NTLZ20BA,NTLZ20CA}

          Non-NORTEL Product Identification Code:
           TABLE OF 8 CHARs
```

44.3.2.1.2 Usage sequence and implications (CM Only)

Not within scope of this document.

44.3.2.1.3 Size

Size of tuples or number of allowed tuples are not changed by this design.

44.3.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	CHANGED	None	new value to be added: NTLZ20CA	New circuit pack for the GEM MG4K RM.

44.3.2.1.5 Datafill example

The following example shows sample datafill for table MNCKTPAK for the GEM RM.

```
CPKKEY CPKINFO PEC RELEASE LOAD
-------------------------------
SPM 0 0 1 GEM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
(PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $ NTLZ20CA 03 GEM20BO
```

Note: The above example may not have the correct slots or load file name. This example is solely meant to show the new value for the peccode field.

44.3.2.1.6 Table release history update

NA

44.3.2.1.7 Supplementary information

NA

44.3.2.1.8 Translation verification other tools

The following example shows the output from DDEDIT when it is used to verify the addition of the new field in table MNCKTPAK field PEC:

```
>ddedit
DDE:
>printtype T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
         NORTEL Product Engineering Code:
         {NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
         NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
         NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
         NTLX82AB,NTLX82BA,NTLX89DA,NTLX67AA,
         NTLX99BA,NTLX73BB,NTLX72BA,NTLX89AA,
         NTLX83AA,NTLX92AA,NTLX74AA,NTLX76AA,
         NTLX44AA,NTLX82EA,NTLZ20BA,NTLZ20CA}

         Non-NORTEL Product Identification Code:
          TABLE OF 8 CHARs
```

44.4 Configuration Walkthrough

NA

45: Configuration (CN): A00003687

45.1 Hardware and Software Requirements

The Mobile Switching Centers (MSCs) and the TOPS switches must have SS7 connectivity. ISUP voice trunk connectivity is necessary for Wireless ADACC with Release.

The customer's SS7 network must have global title translations set up such that short messages from the TOPS node can route to the correct message centers.

The MSCs must have MSC and network translations set up such that the TOPS TLDN routes the call to the TOPS node for service processing.

45.2 Initial Configuration

Not applicable.

45.3 Office parameters (OP)

Existing Table OFCENG parameter `NUM_OF_IS41TOPS_EXT_BLKS` is replaced with new Table OFCAUT parameter `NUM_OF_WIN_TOPS_EXT_BLKS`. This parameter provisions the WIN TOPS extension block (formerly `IS41TOPS_EXT_BLK`; now `WIN_TOPS_EXT_BLK`). The extension block serves both IS-41 and GSM TOPS calls, so it has been renamed to be more general. Since it has been moved to Table OFCAUT, it is now allocated automatically.

45.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCAUT	NUM_OF_WIN_TOPS_EXT_BLKS	New	CM
OFCENG	NUM_OF_IS41TOPS_EXT_BLKS	Deleted	CM

45.3.2 Parameter information

45.3.2.1 NUM_OF_WIN_TOPS_EXT_BLKS

Number of Wireless Intelligent Network TOPS Extension Blocks

45.3.2.1.1 Functional description

This parameter controls how many extension blocks are allocated for use by Wireless Intelligent Network (WIN) TOPS calls.

WIN TOPS extension blocks are used for TOPS calls originating from IS-41 wireless networks as well as calls originating from GSM wireless networks. Each extension block stores data about a wireless call while TOPS is waiting for the MSC to outpulse to TOPS on a voice trunk.

45.3.2.1.2 Provisioning rules

This parameter is located in Table OFCAUT, so additional EXT blocks are allocated automatically when needed. Attributes of the parameter can be modified in Table OFCAUT.

By default, WIN TOPS extension blocks are allocated in groups of 100 using the capabilities of Table OFCAUT.

45.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	32767	By default, 10 WIN TOPS extension blocks are allocated, at 128 words per block. Whenever the number available drops to 9, a new block of 100 is allocated.

45.3.2.1.4 Activation

The parameter is allocated automatically. No restarts are necessary.

45.3.2.1.5 Dependencies

None.

45.3.2.1.6 Consequences

Since the parameter is under the control of Table OFCAUT, it should not be underprovisioned. If there are not enough extension blocks, TOPS131 logs will appear, and wireless calls will be routed to treatment in the MSCs.

By default, WIN TOPS extension blocks are allocated in blocks of 100, so the extension blocks should normally be overprovisioned, using slightly more memory than is required during peak periods.

45.3.2.1.7 Verification

To verify that the WIN TOPS extension blocks are allocated, use the CI command OMSHOW EXT ACTIVE WIN_TOPS_EXT_BLK.

45.3.2.1.8 Memory requirements

Each WIN TOPS extension block requires 128 words. So the total memory used by the EXT blocks is (NUM_OF_WIN_TOPS_EXT_BLKS * 128 words).

45.3.2.1.9 Parameter release history update

SN06: Parameter NUM_OF_IS41TOPS_EXT_BLKS created.

SN07: Parameter NUM_OF_IS41TOPS_EXT_BLKS removed and parameter NUM_OF_WIN_TOPS_EXT_BLKS added to accommodate IS-41 and GSM.

45.4 Upgrade Impact

45.4.1 Dump and Restore

Not applicable. NUM_OF_WIN_TOPS_EXT_BLKS starts with a default value of10 and is increased automatically as needed.

45.4.2 Element Management Upgrade

Not applicable.

45.5 Data schema (DS)

45.5.1 New/modified tables

Table 3 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISUPTRK	Changed	Unchanged
MSCIDMAP	New	New
TOPSFTR	Changed	Unchanged
TOPSMCDB	New	New
TOPSPARM	Changed	Unchanged
TOPSTLDN	Changed	Unchanged
TOPSTOPT	Changed	Unchanged

45.5.2 Table information

45.5.2.1 Name: ISUPTRK

ISUP Trunk

45.5.2.1.1 Functional description

Table ISUPTRK is a TOPS table which associates TOPS options and features with ISUP trunk groups. TOPS ISUP calls use standard ISUP trunk group datafill in Table TRKGRP, and Table ISUPTRK was created to allow datafill of TOPS options and features without affecting standard ISUP trunk group datafill.

45.5.2.1.2 Usage sequence and implications (CM Only)

A trunk group must be datafilled in Table TRKGRP and Table TRKSGRP before it can be datafilled in Table ISUPTRK. This sequence is unchanged.

45.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISUPTRK	Unchanged	Unchanged	Unchanged

45.5.2.1.4 Fields

The following table lists changed fields for Table ISUPTRK.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RLT	Changed	Unchanged	NONE, RLT_REL, RLT_FAR, RLT_IS41, RLT_GSM	Release link trunking: Value RLT_GSM is added by this feature. When the user selects RLT_GSM, they are presented with the existing subfields added in SN06 for value RLT_IS41: RLT_VERSION, RESETTIMER, and TIMERVAL

45.5.2.1.5 Datafill example

The following example shows sample datafill for Table ISUPTRK. The RLT type is set to GSM, the RLT version is set to 1, and the reset timer is enabled and set to 20 seconds.

RLT_GSM is for future use and cannot be datafilled at this time.

```
TABLE: ISUPTRK
          GRPKEY              CONNTYPE  LCANAME          BILLCD CALLSRC
ANI2CLI             RLT SNTPDRST DNLKUP DISPLAY ININTWRK BRANDCHC
-------------------------------------------------------------------------
       MSC_DACC1     CELL_MOBILE  IEC     NLCA      TOPSBC   0    ORIG
      Y RLT_GSM  1 Y 20        N      N       0     NONE        N
```

45.5.2.1.6 Table release history update

SN06: Value RLT_IS41 plus subfields RLT_VERSION, RESETTIMER, and TIMERVAL added to RLT field to accommodate WIN TOPS calls using IS-41.

SN07: Value RLT_GSM added to RLT field to accommodate WIN TOPS calls using GSM. The same subfields are used.

45.5.2.1.7 Supplementary information

No dump and restore necessary, since value RLT_GSM did not exist in SN06.

45.5.2.1.8 Translation verification other tools

Not applicable.

45.5.3 Table information

45.5.3.1 Name: MSCIDMAP

Mobile Switching Center Identifier Mapping

45.5.3.1.1 Functional description

This table maps Mobile Switching Center Identifiers (MSCIDs) to TLDN pool identifiers from Table TOPSTLDN. This allows the customer to control TLDN allocation on a per-MSC basis.

An MSCID consists of a Market ID (16 bit value) and a Switch ID (8 bit value). Less than 1,000 market IDs are in use today in the United States, so the datafill of Table MSCIDMAP is held to a maximum of 4,096 different market IDs to limit data store usage.

MSCIDs are IS-41-specific, so **this table is used on TOPS IS-41 calls only**. New table MSCINMAP (section 45.5.4) is used on GSM calls.

The switch ID can be any number from 0 to 255. The total number of tuples which can be datafilled is 32,767 (the DMS maximum for any table).

Wildcarding can be used to limit datafill in this table. The market ID and switch ID can be wildcarded as follows:

Market ID	Switch number	Meaning
$	$	Match all MSCIDs not otherwise found in table. This combination, when datafilled, serves as the default.
<0 to 65535>	$	Match exact market ID and any switch number, providing exact MSCID and exact switch number is not datafilled.
<0 to 65535>	<0 to 255>	Match exact market ID and switch number
$	<0 to 255>	Not allowed. A wildcard market ID cannot be datafilled with a specific switch number.

45.5.3.1.2 TLDN selection

The list of pools for a given MSCID indicates the order in which the pools are searched for an idle TLDN. If no idle TLDNs are found in the first pool, the DMS examines the next pool in the list.

This allows the customer to set aside groups of TLDNs for certain groups of MSCs. Such datafill reduces shared store contention (that is, XA-Core blocking) during periods of heavy traffic.

The holding time for a TLDN is very short (under once second), so if a pool of 100 or 200 TLDNs is datafilled first in the pool list, it is possible that TLDNs in later pools in the list will only be used in periods of extremely heavy traffic.

45.5.3.1.3 Usage sequence and implications (CM Only)

Table TOPSTLDN must be datafilled before Table MSCIDMAP.

45.5.3.1.4 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MSCIDMAP	0	32767	The store is allocated and deallocated dynamically. When the first tuple is entered, 20K words are allocated. Subsequent tuples cause store allocation as follows: -150 words when a **new** market ID is added with a specific switch number - 32 words when a **new** market ID is added with a wildcard switch number. These estimates include an allocation of one word for each pool ID in each tuple. An addition of an **existing** market ID with a specific switch number results in allocation of one word per pool ID in the tuple. Store is deallocated when tuples are deleted. All store is deallocated when the last remaining tuple is deleted.

45.5.3.1.5 Fields

The following table lists fields for Table MSCIDMAP.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MSCIDKEY	New	MARKETID	{0 to 65535}, or '$'	Market Identifier (vector). First part of two-part key MSCIDKEY.
		SWITCHNO	{0 to 255}, or '$'	Switch Number (vector). Second part of two-part key MSCIDKEY.
POOLLIST	New	None	Vector of up to 255 TLDN pool identifiers from Table TOPSTLDN	Temporary local directory number pool list. Pointer to TLDN pool IDs in Table TOPSTLDN. The order of the pool list in this field indicates the order in which TLDN pools are searched for an idle TLDN. If the first pool in the list contains 100-200 TLDNs, it is likely that the remaining pools in the tuple will never be needed by the MSCs associated with the tuple. This is because the holding time of a TLDN is very short (normally under one second).

45.5.3.1.6 Datafill example

The following example shows sample datafill for Table MSCIDMAP.

```
TABLE: MSCIDMAP
MSCIDKEY        POOLLIST
------------------------
$ $    (0) (1) (2) (3) $
64 $           (0) (2) $
64 5           (0) (1) $
312 444    (0) (1) (2) $
312 445    (0) (1) (2) $
```

45.5.3.1.7 Table release history update

Created in SN07

45.5.3.1.8 Supplementary information

During dump and restore from SN06 to a later load, Table TOPSTLDN is checked. If it has any entries, they are restored using sequential pool IDs beginning with pool ID 0. Then a single tuple with the key {$, $} is added to Table MSCIDMAP. This is a wildcard tuple which matches all MSCIDs and which contains all pool IDs from restored Table TOPSTLDN.

45.5.3.1.9 Translation verification other tools

Not applicable.

45.5.4 Table information

45.5.4.1 Name: MSCINMAP

Mobile Switching Center Identifier Number Mapping

45.5.4.1.1 Functional description

This table maps Mobile Switching Center Identification Numbers (MSCINs) to TLDN pool identifiers from Table TOPSTLDN. This allows the customer to control TLDN allocation on a per-MSC basis.

An MSC Identification Number is a directory number of up to 18 digits. It is also called an MSC Address. MSCINs are GSM-specific, so **this table is used on TOPS GSM calls only**. New table MSCIDMAP is used on IS-41 calls.

This table is a digilator table, meaning the first few digits of an MSCIN can be datafilled, and the tuple will match all MSCINs beginning with those digits. So a single tuple can provide a TLDN pool ID list for hundreds or thousands of MSCs.

This table allows the datafill of up to 4,096 unique TLDN pool ID lists. Note that two lists containing the same pool IDs but in a different order are considered different lists.

The following table shows how digilator matching works.

MSCINMAP key	MSCIN matches
6	Matches all MSCINs (up to 18 digits) beginning with the digit 6.
919	Matches all MSCINs (up to 18 digits) beginning with the digits 919.
704991	Matches all MSCINs (up to 18 digits) beginning with the digits 704991.
2022201111	Matches all MSCINs (up to 18 digits) beginning with the digits 2022201111.

45.5.4.1.2 TLDN selection

The list of pools for a given MSCIN indicates the order in which the pools are searched for an idle TLDN. If no idle TLDNs are found in the first pool, the DMS examines the next pool in the list.

This allows the customer to set aside groups of TLDNs for certain groups of MSCs. Such datafill reduces shared store contention (that is, XA-Core blocking) during periods of heavy traffic.

The holding time for a TLDN is very short (under once second), so if a pool of 100 or 200 TLDNs is datafilled first in the pool list, it is possible that TLDNs in later pools in the list will only be used in periods of extremely heavy traffic.

45.5.4.1.3 Usage sequence and implications (CM Only)

Table TOPSTLDN must be datafilled before Table MSCINMAP.

45.5.4.1.4 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MSCINMAP	0	32767	The store is allocated and deallocated dynamically. When the first tuple is entered, 16K words are allocated. Subsequent tuples cause store allocation as follows: - One word per pool ID when a new TLDN pool ID list is added or a tuple change results in a new list - No store increase when a tuple is added with a TLDN pool ID list identical to one already in the table. To be identical, two lists must contain the same pool IDs in the same order. Store is deallocated when tuples are deleted. All store is deallocated when the last remaining tuple is deleted.

45.5.4.1.5 Fields

The following table lists fields for Table MSCINMAP.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MSCINKEY	New	None	Digilator table key	A digilator key is a vector of up to 18 digits.
POOLLIST	New	None	Vector of up to 255 TLDN pool identifiers from Table TOPSTLDN	Temporary local directory number pool list. Pointer to TLDN pool IDs in Table TOPSTLDN. The order of the pool list in this field indicates the order in which TLDN pools are searched for an idle TLDN. If the first pool in the list contains 100-200 TLDNs, it is likely that the remaining pools in the tuple will never be needed by the MSCs associated with the tuple. This is because the holding time of a TLDN is very short (normally under one second).

45.5.4.1.6 Datafill example

The following example shows sample datafill for Table MSCINMAP.

```
TABLE: MSCINMAP
MSCINKEY             POOLLIST
----------------------------
619         (0)(1)(1000)(10)$
919320            (1)(1000)$
2022201111              (0)$
2032201111        (10)(1)(0)$
2042201111              (0)$
```

45.5.4.1.7 Table release history update
Created in SN07

45.5.4.1.8 Supplementary information
None.

45.5.4.1.9 Translation verification other tools
Not applicable.

45.5.5 Table information

45.5.5.1 Name: TOPSFTR
TOPS Feature

45.5.5.1.1 Functional description
Table TOPSFTR is a TOPS table which allows optional TOPS functions to be activated and deactivated easily. Once the SOC option has been turned on for a TOPS feature, the customer can use Table TOPSFTR to turn the function on and off.

This feature adds tuple `RLT_FOR_GSM`, which controls GSM ADACC with Release.

45.5.5.1.2 Usage sequence and implications (CM Only)
Tuple `RLT_FOR_GSM` must be set to `Y` in order for TOPS to process wireless calls using GSM CAMEL.

45.5.5.1.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSFTR	Unchanged	Increased by 1	Unchanged

45.5.5.1.4 Fields
The following table lists fields for Table TOPSFTR.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FTRNAME	Changed	None	RLT_FOR_GSM	Feature name: This tuple allows the customer to enable GSM TOPS ADACC with release. In order to activate the feature, the SOC option OSEA0104 must be on, and this tuple must be set to Y.
FTRENABL	Unchanged	None	Y/N	Feature enable: Activates or deactivates an optional TOPS feature. The tuple's default value is N.

45.5.5.1.5 Datafill example

The following example shows sample datafill for Table TOPSFTR. The TOPS WIN and TOPS SMS features have been activated.

```
TABLE: TOPSFTR
               FTRNAME FTRENABL
------------------------------
          RLT_FOR_GSM         Y
```

45.5.5.1.6 Table release history update

Table initially added in TOPS15.

45.5.5.1.7 Supplementary information

None.

45.5.5.1.8 Translation verification other tools

Not applicable.

45.5.6 Table information

45.5.6.1 Name: TOPSMCDB

TOPS Message Center Database

45.5.6.1.1 Functional description

This table provides datafill for a TOPS SMS SS7-based message center simulator. An operator position or automated node can send SMS messages using either IS-41 TCAP or GSM TCAP. When the simulator receives the SMS, it looks up the data stored against the SMS destination number to determine the disposition of the SMS. The simulator can successfully acknowledge the SMS, send back a failure message, or ignore the SMS so the TOPS SMS time-out code executes.

45.5.6.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

45.5.6.1.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSMCDB	0	64	2 words per tuple

45.5.6.1.4 Fields

The following table lists fields for TOPSMCDB.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DESTDIGS	New	None	1-18 digits	Digilator field containing the destination number
RESPAREA	New	RESULT	SUCCESS, REJECT, or ERROR	Tells disposition of SMS to this destination number. Different refinements appear depending on the value of RESULT.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESPAREA (continued)	New	PROBTYPE (Subfield of RESPAREA when RESULT set to REJECT)	GENPROB, INVPROB, RESPROB, ERRPROB, TRANSPROB	Defines problem type. This field currently provides IS-41 values. The field can be used for GSM testing by picking IS-41 problem types and code whose integer values are the same as the desired GSM problem types and codes.
		PROBCODE (Subfield of RESPAREA when RESULT set to REJECT)	UNRECCOMP INCORRCOMPPOR BADCOMPSTRUCT INCORRCOMPCOD	Defines problem code. These entries are possible when PROBTYPE is set to GENPROB.
			DUPINVOKEID UNRECOPERATION INCORRPARM UNRECCORRID RESLIMIT INITRELEASE LINKEDRESPUN UNEXPCORRID	Defines problem code. These entries are possible when PROBTYPE is set to INVPROB.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESPAREA (continued)	New	PROBCODE (continued)	UNRECCORRID UNEXPRESULT INCORRPARM	Defines problem code. These entries are possible when PROBTYPE is set to RESPROB.
			UNRECCORRID UNEXPRETURN UNRECERROR UNEXPERROR INCORRPARM	Defines problem code. These entries are possible when PROBTYPE is set to ERRPROB.
			UNRECPACKAGE INCORRTRANS BADTRANS UNRECTRANS PERMRELEASE RESUNAVAIL	Defines problem code. These entries are possible when PROBTYPE is set to TRANSPROB.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESPAREA (continued)	NEW	IS41CODE (Subfield of RESPAREA when RESULT set to ERROR)	ADDRVACANT ADDRXLAFL NETRESSHORT NETFAILURE INVTELSVID OTHERNETPROB NOPAGERESP DESTBUSY NOACK DESTRESSHORT DELPOSTPONED DESTOUTSERV DESTNOLONGAT OTHERTERMPROB RADIORESSHORT RADIOINCOMPAT	Contains cause code to send for IS-41 message center negative acknowledgment. Several dozen cause codes are defined in IS-41.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESPAREA (continued)	NEW	IS41CODE (continued)	OTHERRADIOPROB ENCODINGPROB SMSORIGDENIED SMSTERMDENIED SUPPSVCNOTSUP SMSNOTSUPPORT MISSEXPPARM MISSMANDPARM UNRECPARMVAL UNEXPPARMVAL USERDATASIZE OTHERGENPROB	Contains cause code to send for IS-41 message center negative acknowledgment. Several dozen cause codes are defined in IS-41.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESPAREA (continued)	New	GSMCODE (Subfield of RESPARE A when RESULT set to ERROR)	0 to 255	Contains error code to send for GSM message center negative acknowledgment. Many error codes are defined in GSM 29.002. The byte value datafilled in this field is returned as the error code in the GSM ERROR message.
DELAYSEC	New	None	0 to 255	Delay in seconds before sending response. Helps simulate real-world response time.

45.5.6.1.5 Datafill example

The following example shows sample datafill for Table TOPSMCDB.

```
TABLE: TOPSMCDB
DESTDIGS RESPAREA DELAYSEC
-------------------------------------------------
6199421465 ERROR SMSNOTSUPPORT FACILITYNOTSUPPORT 2
9194321234 REJECT GENPROB BADCOMPSTRUCT 2
9199910000 SUCCESS 2
```

45.5.6.1.6 Table release history update

Created in SN07

45.5.6.1.7 Supplementary information

None.

45.5.6.1.8 Translation verification other tools

Not applicable.

45.5.7 Table information

45.5.7.1 Name: TOPSPARM

TOPS Parameter

45.5.7.1.1 Functional description

Table TOPSPARM is a TOPS-specific version of the office parameter tables. This feature adds two new parameters, SMS_MC_LOG_FAILURE and SMS_TIMEOUT. These parameters apply to SS7-based TOPS Short Message Service (SMS). They do not apply to position-based Internet Protocol (IP) SMS.

SMS_MC_LOG_FAILURE

The telco can use the first parameter, SMS_LOG_MC_FAILURE, to limit the number of TOPS131 logs generated in SMS failure situations. There are many normal situations in which the message center (MC) will return an error code. These might include wireless phone powered off, or destination number not subscribed to SMS. The telco might not wish to have TOPS131 logs generated for these situations. Note that OMs in group SMSTOPS are pegged for these situations.

SMS_LOG_MC_FAILURE is a set field consisting of the following values. These values are related to the cause code returned by the MC when an SMS fails. This parameter only controls the TOPS131 log upon receipt of a negative acknowledgment from the MC. The TOPS131 is always generated as a result of global title translation failure or SS7 routing failure.

- NONE: Do not generate the TOPS131 for any of the following reasons.
- NETWK: Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a network problem value.
- TERM: Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a terminal problem value.
- RADIO: Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a radio interface problem value.
- MISC: Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a general problem value.
- TIMEOUT: Generate the TOPS131 when no response is received from the MC.
- ALL: Generate the TOPS131 for all of the above reasons.

SMS_LOG_MC_FAILURE can be set to NONE, ALL, or any combination of NETWK, TERM, RADIO, and MISC.

The default value of SMS_LOG_MC_FAILURE is ALL.

SMS_TIMEOUT

The second parameter, SMS_TIMEOUT, controls how long TOPS waits before marking an SMS attempt as timed out. The time-out period is datafilled in seconds. The default value of SMS_TIMEOUT is 10 seconds, since operators and automated nodes do not wait while the SMS attempt is in progress, and the SMS acknowledgment can be received after the call is ended.

The time-out value is required since the position or service node cannot send a second SMS while the first SMS transaction is in progress. Also, the time-out ensures DMS resources are cleaned up if the SMS is lost in the network.

45.5.7.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

45.5.7.1.3 Size

Table 14 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSPARM	Increased by 2	Increased by 2	Unchanged

45.5.7.1.4 Fields

The following table lists fields for Table TOPSPARM.

Table 15 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PARMNAME	Changed	None	SMS_LOG_MC_FAILURE is added to the range of TOPS parameters.	This parameter controls when the TOPS131 log is generated in certain SMS failure situations.

Table 15 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PARMVAL	Unchanged	None	Set of {NONE, NETWK, TERM, RADIO, MISC, TIMEOUT ALL}	This parameter can be set to NONE, ALL, or any combination of the four remaining values. Its default value is ALL, meaning generated the TOPS131 in all failure situations.
PARMNAME	Changed	None	SMS_TIMEOUT is added to the range of TOPS parameters.	This parameter controls the amount of time in seconds before TOPS marks an SMS attempt as timed out.
PARMVAL	Unchanged	None	0 to 255	Parameter SMS_TIMEOUT can be set to values 0 to 255. Its default value is 10.

45.5.7.1.5 Datafill example

The following example shows sample datafill for Table TOPSPARM.

```
TABLE: TOPSPARM
PARMNAME PARMVAL
-------------------------
SMS_LOG_MC_FAILURE   ALL $
SMS_TIMEOUT             30
```

45.5.7.1.6 Table release history update

Table initially added in BCS31.

45.5.7.1.7 Supplementary information

When performing a dump and restore from an SN06 load to an SN07 or later load, SMS_LOG_MC_FAILURE will be restored with a value of ALL, and SMS_TIMEOUT will be restored with a value of 10.

45.5.7.1.8 Translation verification other tools

Not applicable.

45.5.8 Table information

45.5.8.1 Name: TOPSTLDN

TOPS Temporary Local Directory Numbers

45.5.8.1.1 Functional description

Table TOPSTLDN provides all TLDNs which can be used by TOPS when providing a Wireless Intelligent Network (WIN) service such as ADACC with release. When a cell phone caller initiates a wireless directory assistance (DA) call and TOPS receives an IS-41 AnalyzedInformation or a GSM InitialDP, TOPS selects an idle TLDN from Table TOPSTLDN and sends it back to the originating mobile switching center (MSC).

Tuples in Table TOPSTLDN define pools of TLDNs from a low TLDN to a high TLDN. Each pool has a numerical index, the pool ID. Two new tables, MSCIDMAP and MSCINMAP, map MSC identifiers to one or more pool IDs. When an MSC sends an AnalyzedInformation or InitialDP, the MSC identifier in the message is used to index Table MSCIDMAP (IS-41) or Table MSCINMAP (GSM) to determine a pool ID. Then an idle TLDN is selected from the pool in Table TOPSTLDN and sent back to the MSC.

A maximum of 2,000 TOPS TLDNs can be defined. The holding time of a TOPS TLDN is very short (around one second), so this number of TLDNs should be able to accommodate heavy TOPS WIN traffic.

45.5.8.1.2 Usage sequence and implications (CM Only)

Table TOPSTLDN must be datafilled before Table MSCIDMAP and Table MSCINMAP.

45.5.8.1.3 Size

Table 16 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSTLDN	0	2000	Memory for all 2000 tuples (10 words each) is allocated when the first tuple is added. Memory is deallocated when the last tuple is deleted.

45.5.8.1.4 Fields

The following table lists fields for Table TOPSTLDN.

Table 17 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POOLID	New	None	0-1999	Pool Identifier: an integer field identifying the pool of TLDNs.
FROMDIGS	Changed	None	Up to 18 digits	From Digits: the start of the TLDN range for this tuple.
TODIGS	Changed	None	Up to 18 digits	To Digits: the end of the TLDN digit range for this tuple.

45.5.8.1.5 Datafill example

The following example shows sample datafill for Table TOPSTLDN.

```
TABLE: TOPSTLDN
POOLID   FROMDIGS     TODIGS
----------------------------
0      2012201234 2012201234
1      2013364400 2013364899
2      2018591400 2018591489
```

45.5.8.1.6 Table release history update

SN06: Added by Feature A00000816

SN07: Modified to use a pool ID as the key field.

45.5.8.1.7 Supplementary information

During dump and restore from SN06 to a later release, if Table TOPSTLDN contains datafill on the SN06 side, it is restored into Table TOPSTLDN on the restore side with sequential pool IDs beginning with 0.

See the Functional Description chapter for illustrations of Table TOPSTLDN before and after a dump and restore.

45.5.8.1.8 Translation verification other tools

Not applicable.

45.5.9 Table information

45.5.9.1 Name: TOPSTOPT

TOPS Trunk Options

45.5.9.1.1 Functional description

This table contains various options datafilled against trunk groups used by TOPS.

45.5.9.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

45.5.9.1.3 Size

Table 18 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSTOPT	Unchanged	Unchanged	Negligible (additional 4 bits per tuple)

45.5.9.1.4 Fields

The following table lists fields for Table TOPSTOPT.

Table 19 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
WIRELESS	New	None	NIL, IS41, or GSM	Wireless: Indicates if the trunk group carries wireless (cellular) traffic. This field controls whether TOPS can use wireless functions on a non-WIN (non-CAMEL) call. If the field is set to IS41 or GSM, all traffic is assumed to be from a wireless phone. A trunk group can only support one network type, so all traffic is assumed to be either IS-41 or GSM.

45.5.9.1.5 Datafill example

The following example shows sample datafill for Table TOPSTOPT.

```
TABLE: TOPSTOPT
GRPKEY ORGAREA DISPCLG ADASERV ADASANS ANITOCLI OLNSQRY DCIBIDX LNPCLGAM
XLASCHEM SPIDPRC TRKSPID BILLSCRN ANIFSPL MAXCONNS DISPSPID WIRELESS
-------------------------------------------------------------------------
TEAOSSIC N Y NONE NA Y N NONE 0 N N N N N N 0 N N
TOSSIC N Y NONE NA Y N NONE 0 N N N N N N 0 N Y IS41
TBELLBIC N Y NONE NA N NONE 0 N N N N N N 0 N Y GSM
```

45.5.9.1.6 Table release history update

SN07 - Added field WIRELESS.

45.5.9.1.7 Supplementary information

The default value of WIRELESS on a dump and restore is NIL. Currently this field is only used when sending a TOPS SMS on a non-WIN (non-CAMEL) call. On an IS-41 WIN or GSM CAMEL call, the originating wireless network type is already known through signaling.

45.5.9.1.8 Translation verification other tools

Not applicable.

45.6 Service Orders (SO)

Not applicable.

45.7 Software optionality control (SOC)

No new SOCs are added by this feature. Regarding the two main components of this feature:

- GSM ADACC with Release is under the control of an existing SOC (OSEA0104, which also controls IS-41 ADACC with Release).
- TOPS SMS is not under the control of SOC.

45.8 Element Management

Not applicable.

45.9 Command interface changes

Not applicable.

45.10 Security

Not applicable.

45.11 Configuration Walkthrough

Tables C7GTTYPE and C7GTT must be datafilled before TOPS can send short messages into the SS7 network. These must use a global title translation number for MDN to Message Center (MDNMCGT) routing such that when the TOPS-sent SMS arrives at the STPs, it is routed to the calling party's message center.

Since SMS has been supported over SS7 for some time, much of the necessary SMS global title translation datafill is probably already present. TOPS might require large amounts of MDNMCGT datafill, but a more likely scenario is that large blocks of MDNMCGT global title translations can be off-loaded to existing STPs using a small number of MDNMCGT tuples in the TOPS switch.

46: Configuration (CN): A00003767

46.1 Hardware and Software Requirements

46.2 Initial Configuration

46.3 Office/Subnet parameters (OP/SP) (CM & SESM)

46.4 Upgrade Impact

46.5 Data schema (DS) (CM, MIBS, RDB)

46.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NORTEL-UEMG-RELMSGING-MIB	NEW	

46.5.2 Table/MIB/Remote Database Schema information

46.5.2.1 Name: NORTEL-UEMG-RELMSGING-MIB

Nortel-UEMG-Reliable Messaging- MIB

46.5.2.1.1 Functional description

The MIB has four sections

- Association general info - This contains basic information for an association, most of it will only ever be read, but it contains some thresholds for the alarms which in the future functionality could be added to change these values.
- Current OMs - Counts for the sample of OM data which is currently being collected. These OMs will give information to current health of the association and can be used to diagnose problems as they occur.
- Interval OMs - Historical samples of the OMs that have been collected. Each sample is for a 15 minute period and will retain the last 96 of these

samples. These OMs can be used to help diagnose problems that occurred in the past.

- Alarms - If a threshold is crossed or the association fails/recovers an alarm will be raised or cleared. The MIB contains the data which will be contained in the alarm.

46.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

<abbreviated names of tables before the current table if applicable>

<abbreviated name of the current table>

<abbreviated names of tables after the current table if applicable>

OR

There is no requirement to datafill tables in a specific order.

OR

Current datafill order unchanged.

46.5.2.1.3 Size

One instance of the MIB will exist for each SCTP association on an ABI card.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DDPACDEV	0	8 000 000	Memory is automatically allocated for 16 DPC devices.

46.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

<conditional information>

Table 3 MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctpAssocTable The association information table which contains an entry for each association	NnRelMsgSctpAssocEntry An individual entry into the nnRelMsgSctpAssocTable	nnRelMsgSctpAssocId	Unsigned 32 bit	A numerical representation of an association
		nnRelMsgSctpAssocRemHostName	Octet String	The IP address of the farend of the SCTP association.
		nnRelMsgSctpAssocRemHostPort	Unsigned 32 bit	The IP port number of the farend for which the association was setup to.
		nnRelMsgSctpAssocLocalPort	Unsigned 32 bit	The IP port number on the ABI for the association
		nnRelMsgSctpAssocEntPhysIndex	Unsigned 32 bit	The numerical representation for the frame, shelf, and slot of the ABI which the association exists on
		nnRelMsgSctpAssocState	Integer closed (1), cookieWait (2), cookieEchoed (3), established (4), shutdownPending (5), shutdownSent (6), shutdownReceived(7), shutdownAckSent (8), deleteTCB (9)	The state of the association
		nnRelMsgSctpAssocMsgLoss	Unsigned32 (1..1000000000)	Error rate...expressed as an integer, with 10 digits, the decimal point is in the 1st place. A value of 10**-5, 0.00001 is expressed 0000100000 or 100,000. A value of 0.05 is 0500000000 or 500,000,000 and so forth.
		nnRelMsgSctpAssocRetrans	Unsigned32 (1..1000000000)	Error rate...expressed as an integer, with 10 digits, the decimal point is in the 1st place. A value of 10**-5, 0.00001 is expressed 0000100000 or 100,000. A value of 0.05 is 0500000000 or 500,000,000 and so forth.

Table 3 MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctpAssocOmCurr Table The table which contains an entry for the OMs currently being collected for each association	NnRelMsgSctpAssocEntry An individual entry into the nnRelMsgSctpAssocOmCurr Table.	nnRelMsgSctpAscCurrClosed	Unsigned 32 bit	Number of times an association has been closed
		nnRelMsgSctpAscCurrAbort	Unsigned 32 bit	Number of times an association has been aborted
		nnRelMsgSctpAscCurrOutPacks	Unsigned 32 bit	Number of packets which have been sent using the association
		nnRelMsgSctpAscCurrInPacks	Unsigned 32 bit	Number of packets which have been received from the association
		nnRelMsgSctpAscCurrDiscPacks	Unsigned 32 bit	Number of packets which have been discarded
		nnRelMsgSctpAscCurrRetranPacks	Unsigned 32 bit	The number of packets which have been retransmitted
		nnRelMsgSctpAscCurrT1expires	Unsigned32	Number of times the T1 timer has expired.
		nnRelMsgSctpAscCurrT2expires	Unsigned 32 bit	Number of times the T2 timer has expired.
		nnRelMsgSctpAscCurrT3expires	Unsigned 32 bit	Number of times the T3 timer has expired.
		nnRelMsgSctpAscCurrCongCount	Unsigned32	The number of times the association has become congested
		nnRelMsgSctpAscCurrCongCleared	Unsigned32	The number of times the association has cleared up from being congested

Table 3 MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctpAssocOmIntervTable The table which contains an entry for the historical OMs that have been collected for each association	NnRelMsgSctpAssocOmIntervEntry An individual entry into the nnRelMsgSctpAssocOmIntervTable.	nnRelMsgSctpAsclnterval	Integer (1-96)	Number of times an association has been closed
		nnRelMsgSctpAsclntervClosed	Unsigned 32 bit	Number of times an association has been closed
		nnRelMsgSctpAsclntervAbort	Unsigned 32 bit	Number of times an association has been aborted
		nnRelMsgSctpAsclntervOutPacks	Unsigned 32 bit	Number of packets which have been sent using the association
		nnRelMsgSctpAsclntervInPacks	Unsigned 32 bit	Number of packets which have been received from the association
		nnRelMsgSctpAsclntervDiscPacks	Unsigned 32 bit	Number of packets which have been discarded
		nnRelMsgSctpAsclntervRetranPacks	Unsigned 32 bit	The number of packets which have been retransmitted
		nnRelMsgSctpAsclntervT1expires	Unsigned32	Number of times the T1 timer has expired.
		nnRelMsgSctpAsclntervT2expires	Unsigned 32 bit	Number of times the T2 timer has expired.
		nnRelMsgSctpAsclntervT3expires	Unsigned 32 bit	Number of times the T3 timer has expired.
		nnRelMsgSctpAsclntervCongCount	Unsigned32	The number of times the association has become congested
		nnRelMsgSctpAsclntervCongCleared	Unsigned32	The number of times the association has cleared up from being congested

Table 3 MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgNotifications Contains the data collected for each alarm as it is raised or cleared	nnRelMsgFault	nnRelMsgFaultType	INTEGER relMsgLinkFail (1), relMsgLinkSevDegraded (2), -- msgLoss Thresh exceeded relMsgLinkDegraded (3)	Gives the type of the fault being raised or cleared.
		nnUemgAlarmSeverity	INTEGER indeterminate (1), warning (2), minor (3), major (4), critical (5)	Tells how much the system will be affected when the alarm is raised.
		nnUemgAlarmDescrip	String	Brief description of the alarm being raised or cleared
		nnRelMsgSctpAssocState	Integer closed (1), cookieWait (2), cookieEchoed (3), established (4), shutdownPending (5), shutdownSent (6), shutdownReceived(7), shutdownAckSent (8), deleteTCB (9)	The state of the association when the alarm is raised
		nnUemgAlarmDefinition	INTEGER set (1), -- Alarm is Set clear (2), -- Alarm is Cleared notAlarmed(3) -- Fault is NOT Alarmed (event only)	If the alarm is raised or cleared
		nnUemgAlarmEventTime	DateAndTime,	The time when the alarm is raised or cleared.

46.5.2.1.5 Datafill example

This MIB currently can not be set or changed.

46.5.2.1.6 Table release history update

46.5.2.1.7 Supplementary information

46.5.2.1.8 Translation verification other tools

Does not use translation verification tools.

46.6 Service Orders (SO) (CM & SESM)

46.7 Software optionality control (SOC)

46.8 Element Management

46.9 Command interface changes

46.9.1 Directory: mapci;mtc;pm;<pm name & number>;querypm flts

Three new messaging faults may appear for HOST ABI XPMs. The following new text strings are added to QUERYPM FLTS:

- External Pkt Ntwk Msg Link(s) Problems - CRITICAL links down
- External Pkt Ntwk Msg Link(s) Problems - Major severe message loss
- External Pkt Ntwk Msg Link(s) Problems - Minor degraded

46.9.1.1 Directory description

46.10 Dshell command changes

46.10.1 Directory: SctpAppIf

46.10.1.1 Directory description

This Dshell directory on the ABI contains commands to obtain information about any SCTP associations that exist on that ABI card. The information that can be obtained will be OM data and basic data on the health of the association.

46.10.1.2 Accessing directory: SctpAppI

46.10.1.2.1 Access to directory or MAP level and return to CI

To access the /SctpAppl command, first telnet to the desired ABI. This will take the user to the root directory of the Dshell which will look like: ABI[0 1 15] dSH>

Now type the following command to enter the SctpAppI directory: cd / SctpAppI

To return to the root directory the user can enter either of the following commands: cd.. or cd

46.10.2 Command: ListAssociations

46.10.2.1 Command type: ABI Dshell Command

46.10.2.2 Command target: MG9K ABI card

46.10.2.3 Command availability: Other

In house tool

46.10.2.4 Command description

The listAssociations command will list the SCTP associations on the ABI card and provide a status of each association. The command will provide the SCTP association number which will be used to view the OM data in the other commands in the SctpAppIf directory.

46.10.2.5 Command syntax

Table 4 listAssociations command parameters and variables

Command	Parameters and variables
ListAssociations	[-h]
Parameters and variables	Description

Table 4 listAssociations command parameters and variables

Command	Parameters and variables
-h	Prints a basic help statement for the command

46.10.2.6 Qualifications and warnings

None

46.10.2.7 Responses

None

46.10.2.8 Example

Table 5 Usage examples for listAssociations command

Description of task	Prints out an Association number, a text description of the association and the state of the association.
Command: Dshell response:	ABI[0 1 15] dSH>listAssociations Number: Association : State 01 : ABI CARD 1 Assoc : Connected

46.10.3 Command: activeOMs

46.10.3.1 Command type: ABI Dshell Command

46.10.3.2 Command target: MG9K ABI card

46.10.3.3 Command availability: Other

In house tool

46.10.3.4 Command description

The activeOMs command will print out the set of OMs that are currently being collect of the requested association number.

46.10.3.5 Command syntax

Table 6 activeOMs command parameters and variables

Command	Parameters and variables
activeOMs	[-h] <association #>
Parameters and variables	Description

Table 6 activeOMs command parameters and variables

Command	Parameters and variables
-h	Prints a basic help statement for the command
association #	The number of the SCTP association that the OM data is being requested for. This can be obtained from the listAssociations command.

46.10.3.6 Qualifications and warnings

None

46.10.3.7 Responses

46.10.3.7.1 Bad parameter entered for the command

Table 7 Outputs with associated meanings and actions

Command
Association not defined or Usage: activeOMs [association#]) Will print the OM data that is currently being collected Will print the OM data for the specific association that corresponds to the number supplied. The association numbers can be obtained using the listAssociation command **Meaning:** Either a valid association number was entered but that association was not created or a invalid number was entered for the association number. **System or user actions:** Use the command listAssociations to determine a valid association number to use as the parameter for this command

46.10.3.8 Example

Table 8 Usage examples for activeOMs command

Description of task:	Prints out a table of the currently collected OM values for the specified association number

Table 8 Usage examples for activeOMs command

Command: MAP response:	activeOMs 0 Active SCTP OMs ABI CARD 1 Assoc Closd Abort OutPack InPack Discrd Retrns T1exp T2exp T3exp Cong CngCl 0001 0003 0123543 0323453 00094 00163 00021 00034 00054 00011 00011 The above table the fields have the following meanings Closd - The number of times the association was closed Abort - The number of times the association was aborted OutPack - Number of packets sent out the association InPack - Number of packets received by the association Discrd - Number of packets discarded by the association Retrns - Number of packets retransmitted by the association T1exp - Number of T1 timer expiries on the association T2exp - Number of T2 timer expiries on the association T3exp - Number of T3 timer expiries on the association Cong - Number of times the association entered congestion CngCl - Number of times the congestion was cleared

46.10.4 Command: HistoryOMs

46.10.4.1 Command type: ABI Dshell Command

46.10.4.2 Command target: MG9K ABI card

46.10.4.3 Command availability: Other

In house tool

46.10.4.4 Command description

The historyOMs command will print one or more sets of OMs that had been previously collected. The users will be able to specify which set 1-96 with 1 being the latest set collected and 96 being the oldest set collected. If a range is specified it will print out the sets in the range from latest to oldest.

46.10.4.5 Command syntax

Table 9 historyOMs command parameters and variables

Command	Parameters and variables
historyOMs	[-h] <Association#> [lower bound (1-96)] [upper bound (1-96)]
Parameters and variables	Description
-h	Prints a basic help statement for the command
Association #	The number of the SCTP association that the OM data is being requested for. This can be obtained from the listAssociations command.
lower bound	This parameter has a range from 1 to 96, with 1 being the latest and 96 being the oldest set of OMs collected. If this is not supplied it will default to 1, which will cause the latest set of OMs to be printed out.
upper bound	This parameter has a range of 1 to 96, with one being the newest and 96 being the oldest set of OMs being collected. If the parameter is supplied it has to be equal or greater than the lower bound parameter. This parameter will cause multiple sets of OMs to be printed out between the range of the lower and upper bound. If this parameter is not supplied it will be defaulted to the lower bound parameter and cause only one set of OMs to be printed.

46.10.4.6 Qualifications and warnings

None

46.10.4.7 Responses

46.10.4.7.1 Bad parameter entered for the command

Table 10 Outputs with associated meanings and actions

Command	
	Association not defined or Usage: historyOMs <Association#> [lower bound (1-96)] [upper bound (1-96)] Will print the OM history for the specific association requested. The association numbers can be obtained using the listAssociation command If no lower bound is entered it will print out the last saved interval of OMs for the specified one association number. If one bound parameter is supplied it will print that OM set. If both bound parameters are supplied it will print the sets between the two numbers. The upper bound has to be larger or equal to the lower bound.
Meaning: Either a valid association number was entered but that association was not create or a bad association number was entered, or the upper or lower bounds were out of range [1 - 96] or the upper bound was smaller than the lower bound	
System or user actions: Use the command listAssociations to determine a valid association number to use as the parameter for this command. Also check to make sure the upper bound (if one was entered) is not smaller than the lower bound and that both lower and upper bounds (if supplied) are in the range of 1 through 96.	

46.10.4.8 Example

Table 11 Usage examples for historyOMs command

Description of task:	Prints out a table of the currently collected OM values for the specified association number

Table 11 Usage examples for historyOMs command

Command:	historyOMs 0 5 7
MAP response:	History SCTP OMs ABI CARD 1 Assoc # Closd Abort OutPack InPack Discrd Retrns T1exp T2exp T3exp Cong CngCl 05 0001 0003 0123543 0323453 00094 00163 00021 00034 00054 00011 00011 06 0000 0001 0223345 0245672 00067 0099 00012 00015 00023 00007 00007 07 0001 0002 0321456 0212345 00153 00173 00041 00014 00034 00004 00004 The above table the fields have the following meanings # - number of the set of OMs being displayed closd - The number of times the association was closed Abort - The number of times the association was aborted OutPack - Number of packets sent out the association InPack - Number of packets received by the association Discrd - Number of packets discarded by the association Retrns - Number of packets retransmitted by the association T1exp - Number of T1 timer expiries on the association T2exp - Number of T2 timer expiries on the association T3exp - Number of T3 timer expiries on the association Cong - Number of times the association entered congestion CngCl - Number of times the congestion was cleared

46.11 Security

46.12 Configuration Walkthrough

47: Configuration (CN): A00003773

47.1 Hardware and Software Requirements

This functionality requires SN07 load in the Call Server, and SN07.1 or higher load in the MG4K-IP CEM and GEM RM.

47.2 Initial Configuration

Not Applicable

47.3 Office/Subnet parameters (OP/SP) (CM & SESM)

47.3.1 New/modified office/subnet parameters

Table 1 Office parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	PACKET_QOS_OM_THRESHOLDS	UNCHANGED	CM

This office parameter is introduced by feature A89007725 in SN06. This is being reused by this activity and explained for better understanding.

47.3.2 Parameter information

47.3.2.1 PACKET_QOS_OM_THRESHOLDS

Packet Quality of Service Operational Measurement Thresholds

47.3.2.1.1 Functional description

In SN06 the activity A89007725 - '*Trunk Group based QoS OM'* introduced a new office parameter PACKET_QOS_OM_THRESHOLDS to define QOS OM threshold values for GWC.

This parameter defines the QOS thresholds values used for pegging QOS issues on GWC based trunk groups. In addition, it allows the QOS reporting threshold feature to be enabled or disabled.

The same QOS OM threshold values (PACKET_QOS_OM_THRESHOLDS) defined in table OFCVAR will be applied to all MG4K-IP nodes datafilled on the Call Server. These QOS thresholds values will be used for pegging QOS issues on MG4K-IP based TDM trunk groups.

The values may be changed at any time without the need for Call Server/ MG4K-IP/GWC restart.

47.3.2.1.2 Provisioning rules

To activate the QOS OM pegging feature for GWC and MG4K-IP based TDM trunk groups, set the enabled value to Y and specify the desired thresholds for jitter, packet loss, and delay.

47.3.2.1.3 Range information

Table 2 Range information

Parameter	Field		Range	Units
PACKET_QOS_OM_THRESHOLDS	Enabled		Y/N	
	Jitter		0 TO 100	Milliseconds (ms)
	Delay		0 TO 500	Milliseconds (ms)
	Loss	Whole	0 TO 9	% packet loss range from 0 TO 9.999999%
		Fraction	0 TO 999999	

47.3.2.1.4 Activation

Changes take effect immediately.

47.3.2.1.5 Dependencies

A new log - *MG4K-IP OM Failure log,* shall be introduced by feature *A00003650 - 'MG4K-IP ECAN, SCTP and OM Failure logs'*. The QOS measurements shall be pegged on the GEM card per CLLI basis. The pegs are stored in 16 bit integers. If these overflow, then the MG4K-IP OM Failure log shall be generated with a reason. The reason code description for the log are Jitter peg overflow, Delay Peg Overflow, Packet Loss Peg Overflow. The pegs in the GEM shall be reset to 0 when this log is generated.

47.3.2.1.6 Consequences

None.

47.3.2.1.7 Verification

None.

47.3.2.1.8 Parameter release history update

In SN06, this parameter is created and used by GWC to peg the trunk group based QoS OMs. From SN07.1 the MG4K-IP nodes also uses these threshold to peg trunk group based QoS OMs.

47.4 Upgrade Impact

47.4.1 Dump and Restore

No Impact.

47.4.2 Element Management Upgrade

No Impact.

48: Configuration (CN): A00003789

48.1 Hardware and Software Requirements

N/A

48.2 Initial Configuration

N/A

48.3 Office/Subnet parameters (OP/SP) (CM & SESM)

48.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	RTE_ADVANCE_FOR_INTRA_IMT_NCRT	New	CM

48.3.2 Parameter information

48.3.2.1 RTE_ADVANCE_FOR_INTRA_IMT_NCRT

Route Advance For IntraLata IMT Release Cause (34) “No Circuit Available”

48.3.2.1.1 Functional description

This parm enables the optionality to route advance for release cause “No Circuit Available”. The SOC NSER0005 must be set to ON and the INTRACSE option in table TRKOPTS must be datafilled in order for the functionality of this parm to be enabled. The following table shows the behavior of Release Cause “No Circuit Available” when the office parm is enabled.

Table 2

Option INTRACSE.RTEADV_CHOICE	RTE_ADVANCE_FOR_INTRA_IMT_NCRT	Action
Yes	Yes	Route Advance from option INTRACSE
Yes	No	Do not route advance from option INTRACSE however table CSEMAP may override and route advance
No	Yes	Do not route advance from option INTRACSE however table CSEMAP may override and route advance
No	No	Do not route advance from option INTRACSE however table CSEMAP may override and route advance

48.3.2.1.2 Provisioning rules

The values for this parm are boolean {N,Y}.

48.3.2.1.3 Range information

Table 3 Range Information

Minimum	Maximum	Default
{N,Y}	{N,Y}	N

48.3.2.1.4 Activation

Immediate.

48.3.2.1.5 Dependencies

SOC NSER0005 must be set to ON and the INTRACSE option in table TRKOPTS must be present in order to enable the functionality of this parameter.

48.3.2.1.6 Consequences

None

48.3.2.1.7 Verification
None

48.3.2.1.8 Memory requirements
No memory impact.

48.3.2.1.9 Parameter release history update
Office parm RTE_ADVANCE_FOR_INTRA_IMT_NCRT is a new parm added in table OFCVAR.

48.4 Upgrade Impact

48.4.1 Dump and Restore
No customer interaction is required.

- Patch SBB41 status is checked during ONP and if patch is active the SOC status for NSER0005 is set to ON.
- Patch SBB59 status is checked during ONP and if the patch is active the office parm RTE_ADVANCE_FOR_INTRA_IMT_NCRT is set to “Y”. Otherwise the parm is set to “N”.

48.4.2 Element Management Upgrade
N/A

48.5 Data schema (DS) (CM, MIBS, RDB)

48.5.1 New/modified tables, MIBs, or Database Schema
New option is added to existing table TRKOPTS

Table 4 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	Changed	Unchanged

48.5.2 Table/MIB/Remote Database Schema information

48.5.2.1 Name: TRKOPTS
TRunK OPTionS

48.5.2.1.1 Functional description
A new Trunk option, INTRACSE is introduced to Table TRKOPTS. The INTRACSE option contains a subfield called RTE_ADV_CHOICE that must be datafilled to Y or N to determine route advance behavior for specific CAUSE values. The CAUSE Enhancement capability is dependant on the the originating trunk and therefore The INTRACSE option can only be assigned to IC or 2W INTRA IMT trunks. The option can be assigned to both SS7 and

PTS INTRA IMT signaling trunks. The option allows the customer to activate the CAUSE enhancements capability on a per trunk group basis. INTRA IMT originators with this option assigned must terminate to an SS7 terminating trunk to enable the CAUSE Enhancement capability.

Only CAUSE values 34 (NOCIRCAV), 42 (SWEQCONG), 47 (RESUNAV) and 51 (CSE_51) are impacted by this option. CAUSE values 42, 47 and 51 will always route advance if the RTE_ADV_CHOICE field is set to Y.

If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT is set to Y, CAUSE value 34 will route advance according to the RTE_ADV_CHOICE and table CSEMAP. If the office paramter is set to N, CAUSE value 34 will NOT route advancing regardless of the Y/N value of the RTE_ADV_CHOICE field.

48.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

48.5.2.1.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	0	131072	Dynamically Allocated

48.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	refinement	Option: INTRACSE subfield: RTE_ADV_CHOICE - Y/N	INTRA IMT CAUSE Enhancements Enables route advance capabilities for CAUSE values 34, 42, 47 and 51. Subfield RTE_ADV_CHOICE is a Y/N prompt. When datafilled to Y CAUSE 34, 42, 47 and 51 will route advance. When datafilled to N CAUSE values 34, 42, 47 and 51 will go to thier respective default treatments.

48.5.2.1.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

```
TABLE: TRKOPTS
 -------------------------
TRKCLLI   INTRACSE   INTRACSE  RTE_ADV_CHOICE  Y
```

INTRACSE data fill incompatibilties result in the following Error Messages

Attempts to datafill the INTRACSE option on a trunk type other than IMT results in the following error message:

'INTRACSE option is supported only for IMT trunk types'

Attempts to datafill the INTRACSE option on an IMT trunk with a NETWKSPC value other than INTRA, results in following error message

'INTRACSE option requires NETWKSPC to be INTRA'

Attempts to datafill the INTRACSE option on an outgoing (OG) trunk result in the following error message:

'INTRACSE option supports IC and 2W direction only.'

48.5.2.1.6 Table release history update

INTRACSE with subfield RTE_ADV_CHOICE is added as an additional OPTION in table TRKOPTS.

48.5.2.1.7 Supplementary information

N/A

48.5.2.1.8 Translation verification other tools

N/A - Table TRKPOTS references are not displayed in TRAVER

48.6 Service Orders (SO) (CM & SESM)

N/A

48.7 Software optionality control (SOC)

Table 7 SOC

SOC option name:	Intra IMT Cause Enhacenements
SOC option title:	Yes
SOC option control type:	Usage
New SOC option?	Yes

Table 7 SOC

SOC option order code	NSER0005
Option defined in DRU:	UCS
Affected products:	SN07

48.8 Element Management

N/A

48.9 Command interface changes

N/A

48.10 Security

N/A

48.11 Configuration Walkthrough

N/A

49: Configuration (CN): A00003905

49.1 Hardware and Software Requirements

Feature A00003905 allows 72 disk volumes to be provisioned per DIRP pool in table DIRPPOOL. Previously, only 24 volumes could be allocated per pool.

Feature A00002186 expands DDU capacity from 1G to 4G. IOM load XXXYYYZZZ is required by feature A00002186.

In order for full 4G DDU capacity to be available for DIRP, feature A00002186 must be at SOC state ON. IOM load XXXYYYZZZ must be used. Feature A00003905 must also be at SOC state ON.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

49.2 Initial Configuration

Feature A00003905 SOC state defaults to IDLE.

72 possible volumes are displayed in table DIRPPOOL. Access to provisioning more than 24 volumes is SOC controlled.

49.3 Upgrade Impact

49.3.1 Dump and Restore

Feature A00003905 sources the functionalities provided by software bridge SBB28. SBB28 created a new table DIRPOOL2 which linked together three 24 volume pools in table DIRPPOOL in order to achieve 72 volumes of storage per DIRP subsystem.

Over an ONP when bridge SBB28 is active and table DIRPOOL2 contains linked pools, feature A00003905 will consolidate all of the pools' volumes under the main pool that is provisioned against the subsystem in table DIRPSSYS. The emptied unused pools will be deleted from table DIRPPOOL.

Any files present in table DIRPHOLD from the volumes being consolidated will be deleted as part of the consolidation process. Files in table DIRPHOLD should be processed prior to an ONP. The following warning is displayed during POSTSWACT:

```
WARNING - ALL DIRPHOLD FILES FOR VOLUME <volume name> DELETED
FROM TABLE DIRPHOLD, AND ARE THE USERS' RESPONSIBILITY
```

Table DIRPOOL2 is present active on the new load only during the ONP and is only used for consolidation. The table is rendered inert in the system at the end of the ONP.

SOC state is not considered during an ONP. Feature A00003905 will always transfer and consolidate if needed. SOC state IDLE will prevent any future provisioning of volumes in a pool that has more than 24 volumes.

49.4 Data schema (DS) (CM, MIBS, RDB)

49.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
DIRPPOOL	CHANGED	UNCHANGED
DIRPOOL2	NEW	NEW

49.4.2 Table/MIB/Remote Database Schema information

49.4.2.1 Name: DIRPPOOL

49.4.2.1.1 Functional description

Table DIRPPOOL contains information regarding the pool of available devices to be used by a DIRP subsystem for recording.

49.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

49.4.2.1.3 Size

Increasing the number of volumes per pool to 72 from 24 increases the memory requirements of table DIRPPOOL. Essentially, volume related store now requires 3x as much memory (72/24=3). Modules DIRPGI and DIRPDSON carry the bulk of the increase in storage. The following information shows the increase:

```
BEFORE:
>store ds scan module dirpgi
Storetype    Ttl      Ttl        Min        Max
             Blks     Size       Blk        Blk
             Owned    Owned      Owned      Owned
DSTEMP_B           1 #00000A00 #00000A00 #00000A00
DSPROT_W          10 #0000C200 #000000C0 #00006300
DSPERM_B          28 #00047F40 #00006000 #00006000
DSSOS_B            1 #00000A00 #00000A00 #00000A00
```

```
DSSOS_W            1 #00000A00 #00000A00 #00000A00
Totals:           41 #00055F40
>store ds scan module dirpdson
Storetype    Ttl     Ttl       Min       Max
             Blks    Size      Blk       Blk
             Owned   Owned     Owned     Owned
DSPROT_W           1 #00001D00 #00001D00 #00001D00
DSPERM_B           1 #00001440 #00001440 #00001440
Totals:            2 #00003140
AFTER:
>store ds scan module dirpgi

Storetype    Ttl     Ttl       Min       Max
             Blks    Size      Blk       Blk
             Owned   Owned     Owned     Owned
DSTEMP_B           1 #00000A00 #00000A00 #00000A00
DSPROT_W          67 #00018540 #000004A0 #00005900
DSPERM_B          67 #00015880 #00001420 #00001420
DSSOS_B            1 #00000A00 #00000A00 #00000A00
DSSOS_W            1 #00000A00 #00000A00 #00000A00

Totals:          137 #0002FBC0
>store ds scan module dirpdson

Storetype    Ttl     Ttl       Min       Max
             Blks    Size      Blk       Blk
             Owned   Owned     Owned     Owned
DSPROT_W           1 #00002300 #00002300 #00002300
DSPERM_B           1 #00001740 #00001740 #00001740

Totals:            2 #00003A40
```

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DIRPPOOL	SAME	SAME	Volume memory requirements increase by 3x. See above.

49.4.2.1.4 Fields

The following table lists changed fields for DIRPPOOL.

Every individual volume field, i.e. VOLUME12, is changed to a TABLE of three volume names.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME0	Changed	None	eight_char_vector	New Field Name: VOL00X02 The field will be provisioned with 3 volume names for volumes 00 to 02. Default: $ $ $
VOLUME1	Changed	None	eight_char_vector	New Field Name: VOL03X05 The field will be provisioned with 3 eight_char_vector for volumes 03 to 05. Default: $ $ $
VOLUME2	Changed	None	eight_char_vector	New Field Name: VOL06X08 The field will be provisioned with 3 eight_char_vector for volumes 06 to 08. Default: $ $ $
VOLUME3	Changed	None	eight_char_vector	New Field Name: VOL09X11 The field will be provisioned with 3 eight_char_vector for volumes 09 to 11. Default: $ $ $

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME4	Changed	None	eight_char _vector	New Field Name: VOL12X14 The field will be provisioned with 3 eight_char_vector for volumes 12 to 14. Default: $ $ $
VOLUME5	Changed	None	eight_char _vector	New Field Name: VOL15X17 The field will be provisioned with 3 eight_char_vector for volumes 15 to 17. Default: $ $ $
VOLUME6	Changed	None	eight_char _vector	New Field Name: VOL18X20 The field will be provisioned with 3 eight_char_vector for volumes 18 to 20. Default: $ $ $
VOLUME7	Changed	None	eight_char _vector	New Field Name: VOL21X23 The field will be provisioned with 3 eight_char_vector for volumes 21 to 23. Default: $ $ $
VOLUME8	Changed	None	eight_char _vector	New Field Name: VOL24X26 The field will be provisioned with 3 eight_char_vector for volumes 24 to 26. Default: $ $ $

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME9	Changed	None	eight_char _vector	New Field Name: VOL27X29 The field will be provisioned with 3 eight_char_vector for volumes 27 to 29. Default: $ $ $
VOLUME10	Changed	None	eight_char _vector	New Field Name: VOL30X32 The field will be provisioned with 3 eight_char_vector for volumes 30 to 32. Default: $ $ $
VOLUME11	Changed	None	eight_char _vector	New Field Name: VOL33X35 The field will be provisioned with 3 eight_char_vector for volumes 33 to 35. Default: $ $ $
VOLUME12	Changed	None	eight_char _vector	New Field Name: VOL36X38 The field will be provisioned with 3 eight_char_vector for volumes 36 to 38. Default: $ $ $
VOLUME13	Changed	None	eight_char _vector	New Field Name: VOL39X41 The field will be provisioned with 3 eight_char_vector for volumes 39 to 41. Default: $ $ $

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME14	Changed	None	eight_char _vector	New Field Name: VOL42X44 The field will be provisioned with 3 eight_char_vector for volumes 42 to 44. Default: $ $ $
VOLUME15	Changed	None	eight_char _vector	New Field Name: VOL45X47 The field will be provisioned with 3 eight_char_vector for volumes 45 to 47. Default: $ $ $
VOLUME16	Changed	None	eight_char _vector	New Field Name: VOL48X50 The field will be provisioned with 3 eight_char_vector for volumes 48 to 50. Default: $ $ $
VOLUME17	Changed	None	eight_char _vector	New Field Name: VOL51X53 The field will be provisioned with 3 eight_char_vector for volumes 51 to 53. Default: $ $ $
VOLUME18	Changed	None	eight_char _vector	New Field Name: VOL54X56 The field will be provisioned with 3 eight_char_vector for volumes 54 to 56. Default: $ $ $

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME19	Changed	None	eight_char _vector	New Field Name: VOL57X59 The field will be provisioned with 3 eight_char_vector for volumes 57 to 59. Default: $ $ $
VOLUME20	Changed	None	eight_char _vector	New Field Name: VOL60X62 The field will be provisioned with 3 eight_char_vector for volumes 60 to 62. Default: $ $ $
VOLUME21	Changed	None	eight_char _vector	New Field Name: VOL63X65 The field will be provisioned with 3 eight_char_vector for volumes 63 to 65. Default: $ $ $
VOLUME22	Changed	None	eight_char _vector	New Field Name: VOL66X68 The field will be provisioned with 3 eight_char_vector for volumes 66 to 68. Default: $ $ $
VOLUME23	Changed	None	eight_char _vector	New Field Name: VOL69X71 The field will be provisioned with 3 eight_char_vector for volumes 69 to 71. Default: $ $ $

49.4.2.1.5 Datafill example

The following example shows sample datafill and how volumes would now be added and deleted for table DIRPPOOL.

Changing the volumes with a one line command is not recommended. Table control does not recognize NIL volume names, and unexpected provisioning may result. Always verify table changes before confirming. Changing individual volumes is possible, but the approach taken in the example below and in the sample datafill is recommended. An example of a one line volume name change is below.

> CHA VOL00X02 $ $ D000VOL2

Preferred method:

> CHA VOL00X02

> VOL00X02: $ $ $

> $ $ D000VOL2

```
>table dirppool;pos 14
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DIRPPOOL
    14 MEGAPOOL  REGULAR    DISK  D000CDR D000CDR1  D000AMA
D000OCC1         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $  F17LAMA  F02LAMA         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $         $         $         $
       $         $         $
>format pack;lis
<line length>:   76 columns can be output per line.
<pack mode>:     Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>:  The first column of output is column 1.
POOLNO POOLNAME POOLTYPE DEVTYPE VOL00X02 VOL03X05 VOL06X08 VOL09X11
VOL12X14 VOL15X17 VOL18X20 VOL21X23 VOL24X26 VOL27X29 VOL30X32 VOL33X35
VOL36X38 VOL39X41 VOL42X44 VOL45X47 VOL48X50 VOL51X53 VOL54X56 VOL57X59
VOL60X62 VOL63X65 VOL66X68 VOL69X71
------------------------------------------------------------------------
14 MEGAPOOL REGULAR DISK D000CDR D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
>ran
 1 POOLNO            DIRPPOOL_KEY
 2 POOLNAME          EIGHT_CHAR_VECTOR
 3 POOLTYPE          DIRPFILEUSE
```

```
 4 DEVTYPE           DEVICETYPESR
 5 VOL00X02          THREE_VOLUME_TABLE
 6 VOL03X05          THREE_VOLUME_TABLE
 7 VOL06X08          THREE_VOLUME_TABLE
 8 VOL09X11          THREE_VOLUME_TABLE
 9 VOL12X14          THREE_VOLUME_TABLE
10 VOL15X17          THREE_VOLUME_TABLE
11 VOL18X20          THREE_VOLUME_TABLE
12 VOL21X23          THREE_VOLUME_TABLE
13 VOL24X26          THREE_VOLUME_TABLE
14 VOL27X29          THREE_VOLUME_TABLE
15 VOL30X32          THREE_VOLUME_TABLE
16 VOL33X35          THREE_VOLUME_TABLE
17 VOL36X38          THREE_VOLUME_TABLE
18 VOL39X41          THREE_VOLUME_TABLE
19 VOL42X44          THREE_VOLUME_TABLE
20 VOL45X47          THREE_VOLUME_TABLE
21 VOL48X50          THREE_VOLUME_TABLE
22 VOL51X53          THREE_VOLUME_TABLE
23 VOL54X56          THREE_VOLUME_TABLE
24 VOL57X59          THREE_VOLUME_TABLE
25 VOL60X62          THREE_VOLUME_TABLE
26 VOL63X65          THREE_VOLUME_TABLE
27 VOL66X68          THREE_VOLUME_TABLE
28 VOL69X71          THREE_VOLUME_TABLE
LOGICAL TUPLE TYPE: DIRPPOOL_LT
>ran 27
27 VOL66X68          THREE_VOLUME_TABLE
TYPE IS THREE_VOLUME_TABLE TABLE OF 3 VECTORS OF UP TO 8 CHAR'S
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
POOLNAME: MEGAPOOL
>
POOLTYPE: REGULAR
>
DEVTYPE: DISK
>
VOL00X02: D000CDR D000CDR1  D000AMA
>$ D000CDR1 D000AMA
VOL03X05: D000OCC1        $        $
>
VOL06X08: $        $        $
>
VOL09X11: $        $        $
>
VOL12X14: $        $        $
>
VOL15X17: $        $        $
>
VOL18X20: $        $        $
>
VOL21X23: $  F17LAMA  F02LAMA
>
VOL24X26: $        $        $
>
VOL27X29: $        $        $
>
VOL30X32: $        $        $
>
```

```
VOL33X35: $         $         $
>
VOL36X38: $         $         $
>
VOL39X41: $         $         $
>
VOL42X44: $         $         $
>
VOL45X47: $         $         $
>
VOL48X50: $         $         $
>
VOL51X53: $         $         $
>
VOL54X56: $         $         $
>
VOL57X59: $         $         $
>
VOL60X62: $         $         $
>
VOL63X65: $         $         $
>
VOL66X68: $         $         $
>
VOL69X71: $         $         $
>
TUPLE TO BE CHANGED:
14 MEGAPOOL REGULAR DISK $ D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
WARNING - ALL DIRPHOLD FILES FOR VOLUME D000CDR DELETED
FROM TABLE DIRPHOLD, AND ARE THE USERS' RESPONSIBILITY
Regular Volume D000CDR will be taken out of DIRP as soon as possible.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>lis
POOLNO POOLNAME POOLTYPE DEVTYPE VOL00X02 VOL03X05 VOL06X08 VOL09X11
VOL12X14 VOL15X17 VOL18X20 VOL21X23 VOL24X26 VOL27X29 VOL30X32 VOL33X35
VOL36X38 VOL39X41 VOL42X44 VOL45X47 VOL48X50 VOL51X53 VOL54X56 VOL57X59
VOL60X62 VOL63X65 VOL66X68 VOL69X71
--------------------------------------------------------------------------
14 MEGAPOOL REGULAR DISK $ D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
>cha VOL00X02
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
VOL00X02: $         $         $
>D000CDR D000CDR1 D000AMA
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE CHANGED:
14 MEGAPOOL REGULAR DISK D000CDR D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

```
Regular volume D000CDR allocated.
WARNING : This POOL has a mixture of device
          types which is not recommended.
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

49.4.2.1.6 Table release history update

Each individual volume field in table DIRPPOOL is now replaced with a field that contains three volume names. The new field name represents the 3 volume names. For example, VOL24X26 represent volumes 24, 25, and 26. Table control will require 3 volume names be entered for each new volume range field. “$” is still used for no volume name. Changing volume names with a one line command is not recommended. In order to change a specific range of volumes perform a change on the range and be prompted for the new volumes.

SOC is used to limit provisioning of more than 24 volumes per pool in table DIRPPOOL. If more than 24 volumes are attempted to be provisioned in table DIRPPOOL and the SOC state is IDLE, an error message is produced indicating the SOC limitation, and the volumes are not provisioned. The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

49.4.2.1.7 Supplementary information

Volumes can be provisioned via table control or through the use of the MNT and DMNT commands at the MAPCI DIRP level. MNT and DMNT usage to provision volumes remains unchanged with this feature.

49.4.2.1.8 Translation verification other tools

The following example shows the output from MAPCI DIRP QUERY when it is used to verify the provisioned volumes in table DIRPPOOL for a specific subsystem.

```
>mapci nodisp;mtc;iod;dirp;query ama all
MAPCI:
MTC:
IOD:
DIRP:
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
AMA       3     1       0     14  NONE    ***YES***

REGULAR
FILE(S)  STATE VOLUME   RECCOUNT BLOCK E  V V_B VLID FNUM FRN#
ACTIVE   AVAIL F02LAMA          1     1 0 23 NO  8482 0036 3184
STANDBY1 AVAIL F17LAMA          0     0 0 22 NO  84C2 007F 6188

PARALLEL
FILE              STATE VOLUME   BLOCK E  V V_B VLID FNUM FRN#
                   NONE
```

```
REGULAR VOLUME(S)
VOL# VOLNAME  STATE          IOC CRD PORT VOL FSEG ROOM VLID FILES
   0 D000CDR  READY            1   8 N/A    5   28   28 2805
   1 D000CDR1 READY            1   8 N/A    6   29   29 2806
   2 D000AMA  READY            1   8 N/A    1   19   19 2801
   3 D000OCC1 READY            1   8 N/A    3   77   77 2803
  22 F17LAMA  READY          N/A N/A N/A    2  120  120 84C2 S1
  23 F02LAMA  READY          N/A N/A N/A    2  114  114 8482 A

REGULAR SPACE
VOL# VOLNAME  STATE          SEGS   EXP UNEXP TOTAL
   0 D000CDR  READY            28     0     0    28
   1 D000CDR1 READY            29     0     0    29
   2 D000AMA  READY            19     0     0    19
   3 D000OCC1 READY            77     0     0    77
  22 F17LAMA  READY           120     0     0   120
  23 F02LAMA  READY           114     0     0   114
```

49.4.2.2 Name: DIRPOOL2

49.4.2.2.1 Functional description

Feature Bridge SBB28 introduced table DIRPOOL2 in SNNCSH04. Table DIRPOOL2 links three DIRP pools in table DIRPPOOL for a subsystem listed in table DIRPSSYS. The three pools provide 72 volumes of storage capacity per subsystem.

Table DIRPOOL2 is created in feature A00003905 solely for the purpose of providing information needed to consolidate linked pools when moving to a load that now has 72 volumes per pool in table DIRPPOOL. The table is created at IPL. Its data is transferred during DART (if applicable). The table data is used during POSTSWACT to consolidate volumes in DIRPPOOL. At the end of POSTSWACT, table DIRPOOL2 is rendered inert in the switch.

Basic table functionality is provided during the duration of the ONP, but no data verification is done. Valid data is assumed from the old load (pre-SNNCSH07).

49.4.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

DIRPPOOL

DIRPSSYS

DIRPOOL2

49.4.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DIRPOOL2	0	24	Memory is allocated only during ONP and is freed afterwards.

49.4.2.3.1 Fields/OIDs

The following table lists fields for DIRPOOL2.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ssysname	new	none	ssnamesr	DIRP subsystem name
poolnam1	new	none	poolname sr	DIRP pool name
poolnam2	new	none	poolname sr	DIRP pool name
poolnam3	new	none	poolname sr	DIRP pool name

49.4.2.3.2 Datafill example

The following example shows sample datafill for table DIRPOOL2 which was transferred from feature bridge SBB28 data in SNNCSH04.

```
Mate>table dirpool2
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DIRPOOL2
Mate>lis all
TOP
SSYSNAME POOLNAM1 POOLNAM2 POOLNAM3
---------------------------------
     AMA  AMAPOOL MEGAPOOL MCKYPOOL
BOTTOM
```

49.4.2.3.3 Table release history update

Table DIRPOOL2 is introduced by feature A00003905 solely for consolidating pool volumes linked via feature bridge SBB28. SBB28 introduced table DIRPOOL2 to link up to three DIRP pools to one DIRP subsystem allowing for a maximum of 72 recording volumes. Table DIRPOOL2 is used during ONP to consolidate the linked pool volumes under the main pool that is datafilled against the subsystem in table DIRPSSYS. Post-ONP, table DIRPOOL2 is rendered inert in the system, and SOC for

feature A00003905 is used to provision more than 24 and up to 72 volumes per pool in table DIRPPOOL.

49.4.2.3.4 Supplementary information

None.

49.4.2.3.5 Translation verification other tools

Table DIRPOOL2 data can be verified post-RESTORE by listing the table on the inactive side during an ONP.

Consolidation can be verified by checking table DIRPPOOL after POSTSWACT to ensure that all linked pool volumes were moved under the main pool provisioned against the subsystem in table DIRPSSYS.

49.5 Software optionality control (SOC)

Table 6 SOC

SOC option name:	BASE DIRP enh to 72 vol
SOC option title:	Yes
SOC option control type:	State
New SOC option?	Yes
SOC option order code	BASE0014
Option defined in DRU:	BASE
Affected products:	DIRP

SOC state IDLE limits the number of provisionable volumes per pool in table DIRPPOOL to 24. SOC state ON increases the total number of volumes per pool to 72.

49.6 Command interface changes

49.6.1 Directory: MAPCI;MTC;IOD;DIRP

49.6.1.1 Directory description

DIRP provides the ability to perform a variety of commands against DIRP subsystems.

49.6.1.2 Accessing directory: DIRP

49.6.1.2.1 Access to directory or MAP level and return to CI

MAPCI;MTC;IOD;DIRP

QUIT ALL

49.6.2 Command: MNT

49.6.2.1 Command type: MENU

49.6.2.2 Command target: All

49.6.2.3 Command availability: RES

49.6.2.4 Command description

MNT mounts a specific volume to a specific DIRP subsystem.

49.6.2.5 Command syntax

MNT <DIRP subsystem> <volume name>

49.6.2.6 Qualifications and warnings

Feature A00003905 SOC limits the number of volumes provisionable per DIRP subsystem if the SOC state is IDLE. If the state is IDLE, only 24 volumes can be provisioned per DIRP pool in table DIRPPOOL. If more than 24 volumes are attempted to be provisioned with SOC state IDLE, an error message is produced, and the volume is not mounted against the subsystem.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

49.6.2.7 Responses

49.6.2.7.1 DIRP Volume Expansion SOC is not ON. Cannot mount more than 24 VOLUMES per POOL.

The user is trying to allocate more than 24 volumes per pool with the SOC state for feature A00003905 IDLE.

Table 7 MAP outputs with associated meanings and actions

Command: DIRP MNT
DIRP Volume Expansion SOC is not ON. Cannot mount more than 24 VOLUMES per POOL. **Meaning:** Cannot mount more than 24 volumes per pool in table DIRPPOOL **System or user actions:** The user needs to purchase functionality under feature A00003905 if they want to provision more that 24 volumes per pool in table DIRPPOOL.

50: Configuration (CN): A00003923

50.1 Hardware and Software Requirements

There is no specific hardware requirement for this feature. The basic ICM software package is needed to use this feature.

50.2 Initial Configuration

The required configuration for this feature is detailed in the DS section of this document.

50.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

50.4 Upgrade Impact

50.4.1 Dump and Restore

No manual action is required. A reformat Procedure will be used as the software solution.

50.4.2 Element Management Upgrade

N/A

50.5 Data schema (DS) (CM, MIBS, RDB)

50.5.1 New/modified tables, MIBs, or Database Schema

Impacted tables are listed below in Table 1

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IBNFEAT	Changed	Unchanged
KSETFEAT	Changed	Unchanged

50.5.2 Table/MIB/Remote Database Schema information

50.5.2.1 Name: IBNFEAT

Integrated Business Network Features Table

50.5.2.1.1 Functional description

N/A

50.5.2.1.2 Usage sequence and implications (CM Only)

50.5.2.1.3 Current datafill order unchanged.
Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNFEAT	0	N/A	Dynamically Allocated

50.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IBNFEAT.

The IBNFEAT fields are being shown for informational purposes only, functionality for this actvity is only assignable via SERVORD.

The new sub-option SCAIRDIR is identified on the line via a Y or N entry under the ECM option. If the sub-option SCAIRDIR is 'Y' then the MSGTO subfield is presented.

For this activity, if field 3 (DF) is ECM and field 4 (FEATURE) is ECM, then the sub-option SCAIRDIR will be presented as one of the field 5 (DATA) Area Refinements. If SCAIRDIR is set to 'Y' then a further refinement of MSGTO (Message Timeout) will be presented which will have a range of 1 to 60 seconds. (See **BOLD** in tuple example below).

Table IBNFEAT fields:

```
1   LEN         EXT_LEN
2   DNN         DNNO_RANGE
3   DF          DATA_FEATURE
4   FEATURE     DATA_FEATURE
5   DATA        AREA REFINEMENTS
```

Table IBNFEAT Tuple example:

```
LEN
            DNNO        DF    FEATURE
                                                DATA
-------------------------------------------------------------------------------
HOST  05 0 00 05
                0       ECM       ECM Y Y Y Y Y Y Y Y 60
```

50.5.2.1.5 Datafill example
Datafill for this activity is performed via SERVORD only.

50.5.2.1.6 Table release history update
Added a sub-option named SCAIRDIR to the ECM option. If SCAIRDIR is set to ‘Y’ a sub-field named MSGTO is also presented.

50.5.2.2 Name: KSETFEAT

Key Set Features Table

50.5.2.2.1 Functional description
N/A

50.5.2.2.2 Usage sequence and implications (CM Only)

50.5.2.2.3 Current datafill order unchanged.
Size

Table 3 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
KSETFEAT	0	N/A	Dynamically Allocated

50.5.2.2.4 Fields/OIDs
The following table lists fields/OIDs for KSETFEAT.

The KSETFEAT fields are being shown for informational purposes only, functionality for this actvity is only assignable via SERVORD.

The new sub-option SCAIRDIR is identified on the line via a Y or N entry under the ECM option. If the sub-option SCAIRDIR is ‘Y’ then the MSGTO subfield is presented.

For this activity, if field 2 (FEATURE) is ECM, then the sub-option SCAIRDIR will be presented as one of the field 3 (KVAR) Area Refinements. If SCAIRDIR is set to ‘Y’ then a further refinement of MSGTO (Message Timeout) will be presented which will have a range of 1 to 60 seconds. (See **BOLD** in tuple example below).

TableKSETFEAT fields:

```
1   FEATKEY     KSETFEAT_KEY
2   FEATURE     KEY_SET_FEATURE
3   KVAR        AREA REFINEMENTS
```

TableKSETFEAT Tuple example:

```
FEATKEY     FEATURE
                                                    KVAR
-------------------------------------------------------------------------------
HOST  00 0 19 16  1     ECM         ECM Y Y Y Y Y Y Y Y 60
```

50.5.2.2.5 Datafill example

Datafill for this activity is performed via SERVORD only.

50.5.2.2.6 Table release history update

Added a sub-option named SCAIRDIR to the ECM option. If SCAIRDIR is set to 'Y' a sub-field named MSGTO is also presented.

50.6 Service Orders (SO) (CM & SESM)

This activity is adding a new sub-option named SCAIRDIR to the existing ECM line option. The SCAIRDIR sub-option will also have a sub-field named MSGTO which will be available when the SCAIRDIR sub-option is set to 'Y'.

50.6.1 Service order change details

50.6.1.1 LCC and options

The new sub-option SCAIRDIR will be applicable to the same sets as the ECM Line Option (reference AR0046 - ECM / SCAI Support for Non-ACD). This includes sets that are Meridian Business Set (MBS), 500/2500 IBN and Meridian Feature Transparency (MFT) sets, including EtherSets.

Only single DN apperance per line will be supported by this activity. Lines with features such as Multiple Appearance Directory Number (MADN), Hunt Groups, UCD etc. are not supported

50.6.2 New commands

No new SERVORD commands are introduced by this activity.

50.6.2.1 How service order commands are presented - IBN

50.6.2.1.1 Description

The existing SERVORD ADO (Add Option) command will be used to assign the sub-option SCAIRDIR (via the ECM option) to an existing IBN line.

50.6.2.1.2 Example

Example of the SCAIRDIR sub-option in prompt mode

```
CI:
>servord
SO:
>ado
SONUMBER:    NOW   3 10 24 AM
>
DN_OR_LEN:
>5 0 0 5
OPTION:
>ecm
CALL_EVENTS:
>y
MAKECALL:
>y
CONF_XFER:
>y
MSG_WAIT:
>y
SCAICC:
>y
CHKLOPT:
>y
NETICM:
>y
SCAIRDIR:
>y
MSGTO:
>60
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 10 24 AM HOST 05 0 00 05 ( ECM Y Y Y Y Y Y Y Y 60) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Example of the SCAIRDIR sub-option in no-prompt mode

```
CI:
>servord
SO:
>ado $ 5 0 0 5 ecm y y y y y y y y 60 $
COMMAND AS ENTERED:
ADO NOW 3 10 24 AM HOST 05 0 00 05 ( ECM Y Y Y Y Y Y Y Y 60) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

50.6.2.2 How service order options are presented - KSET

50.6.2.2.1 Description

The existing SERVORD ADO (Add Option) command will be used to assign the sub-option SCAIRDIR (via the ECM option) to an existing KSET line.

50.6.2.2.2 Example

Example of the SCAIRDIR sub-option in prompt mode

```
CI:
>servord
SO:
```

```
>ado
SONUMBER:    NOW   3 10 24 AM
>
DN_OR_LEN:
>0 1 9 4
OPTKEY:
>1
OPTION:
>ecm
CALL_EVENTS:
>y
MAKECALL:
>y
CONF_XFER:
>y
MSG_WAIT:
>y
SCAICC:
>y
CHKLOPT:
>y
NETICM:
>y
SCAIRDIR:
>y
MSGTO:
>60
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 10 24 AM HOST 00 1 09 04( 1 ECM Y Y Y Y Y Y Y Y 60 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Example of the SCAIRDIR sub-option in no-prompt mode

```
CI:
>servord
SO:
>ado $ 0 1 9 4 1 ecm y y y y y y y y 60 $
COMMAND AS ENTERED:
ADO NOW 3 10 24 AM HOST 00 1 09 04 ( 1 ECM Y Y Y Y Y Y Y Y 60) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

50.6.3 Option prerequisites

50.6.3.1 Notes

SCAIRDIR is a sub-option of the ECM line option. The ECM is therefore required on the line in order for the SCAIRDIR sub-option to be presented.

50.6.3.2 Feature identification

This activity A00003923 - CTX / RES SCAI Redirection is activatable via SOC ICM00080 which requires ICM00001, PCID 00037570

50.7 Software optionality control (SOC)

Order code ICM00080, CTX / RES SCAI Redirection provides SCAI Redirection support for CENTREX and Residental lines that have the ECM option assigned. When ICM00080 SOC is in the IDLE state, calls to the affected line will not generate a ICM Call-Received-C message.

The following warning message is displayed when the CTX / RES SCAI Redirection SOC ICM00080 is toggled from ON to IDLE state (the warning message indicates that state transition disables the associated Call-Received-C messaging and CTX/RES SCAI Redirection functionality).

SERVICE AFFECTING: This transition will disable the CTX / RES SCAI Redirection functionality for all current and future subscribers.

Table 4 SOC

SOC option name:	ICM
SOC option title:	CTX / RES SCAIRDIR
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	ICM00080
Option defined in DRU:	CCM
Affected products:	LEC00020, LET00020, LLT00020, SN07, ISN07

51: Configuration (CN): A00003933

51.1 Hardware and Software Requirements

The Gateway Controller's (GWC's) software load must be upgraded to receive SIPLINK before CM SIPLINK is datafilled.

51.2 Initial Configuration

There is no initial configuration.

51.3 Office/Subnet parameters (OP/SP) (CM & CS2M)

Not Applicable

51.4 Upgrade Impact

SIPLINK is a new table.

51.5 Data schema (DS) (CM, MIBS, RDB)

51.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SIPLINK	NEW	NEW

51.5.2Table/MIB/Remote Database Schema information

51.5.2.1 SIPLINK

Session Internet Protocol Communication Link

51.5.2.1.1 Functional description

New table SIPLINK creates an association between CS 2000 agents (e.g., ISUP trunks) and a SIP link name.

The SIPLINK table is downloaded to GWCs datafilled as DPT SIPT in table SERVSINV.

51.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

TRKOPTS with SIPT

DPTRKMEM with DPTRKKEY.CLLI and SIPT signaling

SIPLINK with SIPTTRK already datafilled in TRKOPTS:OPTKEY.CLLI and in DPTRKMEM.

51.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SIPLINK	0	400	Memory allocated in increments for 64 tuples (each 6 bytes)

51.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SIPLINK.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LINKNAME	new	key	VECTOR OF UP TO 16 CHARS	alpha numerical name of the siplink
CONNTYPE	new		CS2CS or CS2AS	a connection type indicates CallServer to CallServer or CallServer to ApplicationServer

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AGNTDATA	new	selector	ISUPTRK	currently only ISUPTRK is implemented
SIPTTRK	new	refinement	VECTOR OF UP TO 16 CHARS	alpha numerical name of the trunk (CLLI)

51.5.2.1.5 Datafill example

The following example shows a sample datafill for tables TRKOPTS, DPTRKMEM and SIPLINK.

- **TABLE TRKOPTS (after Trimodal restructuring - SN07)**

OPTKEY OPTINFO

SIP_LOOP_1 DPT DPT SIPT NET_IP Y

- **TABLE DPTRKMEM**

DPTRKKEY RANGEINF MAXCALLS

SIP_LOOP_1 SIPT 100

- **TABLE SIPLINK**

LINKNAME CONNTYPE AGNTDATA

ACCESS_LINK_2 CS2CS ISUPTRK **SIP_LOOP_1**

51.5.2.1.6 Table release history update

This is new table for SN07 (patchable into SN06.0)

51.5.2.1.7 Supplementary information

None

51.5.2.1.8 Translation verification other tools

None

51.6 Service Orders (SO) (CM & CS2M)

Not Applicable.

51.7 Software optionality control (SOC)

There are two new core usage SOC options that are used to limit the maximum number of simultaneous calls that are allowed through the Session Server Manager at any given time. Without one or both of the new SOC options, no call processing can take place using the Session Server Manager.

These usage SOCs do not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

51.7.1SOC CS2B0008

Table 4 SOC CS2B0008

SOC option name:	CS to CS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0008
Option defined in DRU:	MSH
Affected products:	SN07

51.7.1.1 SOC limitations

The usage-controlled CS2B0008 SOC added by this activity applies to calls that meet the following criteria:

— the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,

— a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK,

— the CONNTYPE field of the tuple in table SIPLINK is set to CS2CS.

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming and outgoing SIPT calls on trunk group NGSSLOOP will increment the usage counter for the CS2AS SOC.

```
TABLE: SIPLINK
        LINKNAME CONNTYPE                  AGNTDATA
-------------------------------------------------
        NGSSOUTLK    CS2AS ISUPTRK          NGSSOUT
      NGSSINLINK    CS2AS ISUPTRK          NGSSINC
     LOOPAROUND1    CS2CS ISUPTRK          NGSSLOOP
```

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0008
GROUP:CS2B
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
CS2B0008 CS to CS Calls           N     -     127     500      1VC  04/01/19
```

51.7.1.2 SOC CS2B0008 interactions:

- Calls that peg the new CS2B0008 count will always peg the CS2B0005 count as well.
- If the SOC limit set for CS2B0008 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.
- Feature A00004271 SIP App Server SOC introduces new OM group NGSSOM for tracking the effects of the CS2B0008 SOC limit setting on CS2CS calls.

51.7.2SOC CS2B0009

Table 5 SOC CS2B0009

SOC option name:	CS to AppS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0009
Option defined in DRU:	MSH
Affected products:	SN07

51.7.2.1 SOC limiting

The usage-controlled CS2B0009 SOC added by this activity applies to calls that have the following characteristics:

— the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,

— a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK,

— the CONNTYPE field of the tuple in table SIPLINK is set to CS2AS

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming SIPT calls on trunk group NGSSINC and outgoing calls on trunk group NGSSOUT will increment the usage counter for the CS2AS SOC.

```
TABLE: SIPLINK
        LINKNAME CONNTYPE                  AGNTDATA
-------------------------------------------------
         NGSSOUTLK    CS2AS ISUPTRK          NGSSOUT
       NGSSINLINK    CS2AS ISUPTRK          NGSSINC
     LOOPAROUND1    CS2CS ISUPTRK         NGSSLOOP
```

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0009
GROUP:CS2B
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS  LAST_CHG
------    ----                 --- -----   -----   -----    -----  --------
CS2B0009 CS to AppS Calls          N     -    127     500      1VC  04/01/19
```

51.7.2.2 SOC limitations

- Calls that peg the new CS2B0009 count will always peg the CS2B0005 count as well.
- If the SOC limit set for CS2B0009 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

51.8 Element Management

Not Applicable.

51.9 Security

Not Applicable.

51.10 Configuration Information

This feature allows the craftsperson to provision a number of fields on a remote-server basis, as per customer requirements. The following section captures the provisioning information for specific configurations. The different configurations discussed include:

- NGSS - NGSS
- NGSS - SN07 VRDN
- NGSS - SN06.2 VRDN
- NGSS - SN06 VRDN
- NGSS - MCS

Please refer to the FN section for detailed information on provisionable fields.

Table 6 Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
IP Address	x.x.x.x	x.x.x.x	x.x.x.x
Port	5060	5060	5060[a]
Protocol	UDP	UDP	UDP or TCP

Table 6 Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
Optional IP (1-6)	none	none	none
Methods	INVITE, CANCEL, BYE, OPTIONS, INFO, PRACK	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO, UPDATE[b], REFER
URI Parameters Supported	none	cic	all
SIP Headers supported	Content-Disposition, **one of** Remote-Party-ID or P-Asserted-ID/ Privacy	Content-Disposition, **one of** Remote-Party-ID or P-Asserted-ID/ Privacy, Diversion	Content-Disposition, **one of** Remote-Party-ID or P-Asserted-ID/Privacy, Reason, Replaces, Referred-By, Diversion
ISUP to SIP Cause Map[c]	Default	Default	Default
SIP to ISUP Cause Map[d]	Default	Default	Default
SIP Redirection Map[e]	Default	Default	Default
ISUP Variant to SIP Version Map[f]	Default	Default[g]	Default
NOA/NPI to Phone Context Map	None	None	Default[h]
SIP Cause Precedence Priority	Default (OR) Encap: Third Retry: Second CauseCode: First	Default	Any
APN Information	Not Applicable	Not Applicable	Applicable[i]

(I)SN07 Release Change Reference Manual Standard 01.02 December 2004

Table 6 Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
Backward Call Indicator (BCI) Data	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN
Forward Call Indicator (FCI) Data	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN
SIP Header format	Compact or Long	Compact or Long	Compact or Long
Options for Heartbeat	yes	yes	yes
Telephony Profile	yes	yes	yes or no
Use Info for Long Call Audit	yes	yes	yes or no
Map non-screened RPI to Calling#	yes	yes	yes
Accepts Early SDP	no	yes	yes or no
Accept Invite without SDP	yes	yes	yes
E.164 Format Allowed[j]	no	no	yes[k]

Table 6 Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
Enforce Code-Compatibility[l]	no	no	yes or no[m]
Accepts Encapsulated ISUP	no	yes	yes or no[n]
CountryCode Support[o]	no	no	yes or no
Hop-Counter	2[p]	7	7
Out of Band DTMF	vnd.nortelnetworks.digits	telephone-event	telephone-event
Agent	ISUP	ISUP	ISUP
Unknown Header	any string	any string	anystring
Anonymous Header	any string	any string	any string

a. The port can be configured to a number of choice. Ensure the port number is consistent across the communicating NGSSs.

b. Either all the nodes in a call should support UPDATE, or none of them should. Otherwise, undesired behavior may occur.

c. A custom ISUP - SIP cause map can be added by clicking on "*ISUP and SIP Mappings*" tab and adding a new mapping under "*ISUP to SIP Map*".

d. A custom SIP - ISUP cause map can be added by clicking on "*SIP and ISUP Mappings*" tab and adding a new mapping under "*SIP to ISUP Map*".

e. A custom SIP Redirection Map can be added by clicking on "*ISUP and SIP Mappings*" tab and a new mapping under *"SIP Redirection"*.

f. This maps ISUP *Protocol/Version/Variant* <--> *SIP base and Version* fields. See FN section for instructions on how to add a new mapping. Also, See Appendix for base/version for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.

g. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)

h. Nature Of Address/Numbering Plan Identifier <--> Phone-Context Mapping table. For incoming SIP calls, this table is used to determine the NOA/NPI values to be used in the ISUP message. Similarly, for outgoing calls, this table is used to determine the 'phone-context' parameter to be added to Request-URI. The button "**Phone-Context**" (under URI-Parameters) must be turned ON for this functionality to take effect. New mapping entries can be added by following the procedure described in FN section.

i. This is used to setup handling of Action Point Number (APN), Private Numbering Plan type calls. There are three different types this can be configured as shown in the pull-down menu. **1.** *Use Prefix* ---> requires datafill of Prefix field. **2.** *Use Prefix and Phone Context* --> requires datafill of both Prefix and Phone-Context fields. **3.** *Phone Context Only* --> requires datafill of Phone Context Field.

j. Marking this field 'Y' requires datafill of Country Code Supported to be set to 'Y' and entry of valid Country Code in the provided field.

k. Marking this field 'Y' requires datafill of Country Code Supported to be set to 'Y' and entry of valid Country Code in the provided field.

l. Marking this field 'Y' requires selection of at least one applicable codec in the 'Config Data' section.

m. Marking this field 'Y' requires selection of at least one applicable codec in the 'Config Data' section.

n. Marking this field "N" requires marking "Accepts Early SDP" to "N". Marking both of these field "N" means supporting SIP (without ISUP payload) between session server and session server.

o. Must be marked 'Y' and valid Country code datafilled, if '*e.164 supported*' is set to 'Y'.

p. This value should be configured based on the MCS configuration. Please check the MCS's Initial Maximum Hop Value, and then set the Hop-Counter according to the formula as explained in the FN section of this document.

Table 7 Default Provisioning Information Various Configuration

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
IP Address	x.x.x.x	x.x.x.x
Port	5060	5060
Protocol	UDP	UDP
Optional IP (1-7)	none	none
Methods:	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, PRACK, INFO
URI Parameters Supported	cic	none
SIP Headers supported	One of Remote-Party-ID or P-Asserted-ID/Privacy, Diversion	Remote-Party-ID
ISUP to SIP Cause Map[a]	Default	Default

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
SIP to ISUP Cause Map[b]	Default	Default
SIP Redirection Map[c]	Default	Default
ISUP Variant to SIP Version Map[d]	Default[e]	Default[f]
NOA/NPI to Phone Context Map	None	None
SIP Cause Precedence Priority[g]	Default	Default
APN Information	Not Applicable	Not Applicable
Backward Call Indicator (BCI) Data	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN
Forward Call Indicator (FCI) Data	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN
SIP Header format	Compact or Long	Compact or Long
Options for Heartbeat	yes	yes
Telephony Profile	yes	yes
Use Info for Long Call Audit	yes	yes

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
Map non-screened RPI to Calling#	yes	yes
Accepts Early SDP	yes	yes
Accept Invite without SDP	yes	yes
E.164 Format Allowed[h]	no	no
Enforce Code-Compatibility[i]	no	no
Accepts Encap-sulated ISUP	yes	yes
CountryCode[j] Support	no	no
Hop-Counter	7	7
Out of Band DTMF	telephone-event	Not Applicable
Agent	ISUP	ISUP
Unknown Header	any string	any string
Anonymous Header	any string	any string

a. A custom ISUP - SIP cause map can be added by clicking on "*ISUP and SIP Mappings*" tab and adding a new mapping under "*ISUP to SIP Map*".

b. A custom SIP - ISUP cause map can be added by clicking on "*SIP and ISUP Mappings*" tab and adding a new mapping under "*SIP to ISUP Map*".

c. A custom SIP Redirection Map can be added by clicking on "*ISUP and SIP Mappings*" tab and a new mapping under *"SIP Redirection"*.

d. This maps ISUP *Protocol/Version/Variant <--> SIP base and Version* fields. See FN section for instructions on how to add a new mapping. Also, See Appendix for base/version for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.

e. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)

f. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)
g. You can change the precedence setting for testing purposes and select different precedence for different interworkings
h. Marking this field 'Y' requires datafill of Country Code Supported to be set to 'Y' and entry of valid Country Code in the provided field.
i. Marking this field 'Y' requires selection of at least one applicable codec in the 'Config Data' section.
j. Must be marked 'Y' and valid Country Code datafilled, if 'e.164 Supported' is set to 'Y'

Table 8 Default Configuration Data Settings

Field	Default Value
general Linger Timer	5000
Invite Linger Timer	5000
local TCP Port	5060[a]
local UDP Port	5060[b]
maxCallLegs	1000[c]
maxSipMsgSize	1536
maxSubscriptions	1000
provisionalTimer	180000
retransmission T1	2000
retransmission T2	4000
retransmission T4	5000
retry Count	6
codec G729 Allowed	N[d]
codecPCMUAllowed	N[e]
codecPCMAAllowed	N[f]
enableOnBoardBilling	N[g]
enableAccessControl[h] List	N

Table 8 Default Configuration Data Settings

Field	Default Value
mgcHostName	Must Correspond to table ofceng ‘mgc_hostname’ parameter in the core
susAutoRefresh	N
supportedExtensionList	100rel

a. This can be configured for NGSS-NGSS calls
b. This can be configured for NGSS-NGSS calls
c. Max value of 40000
d. Must be set if ‘codec-enforcement’ is turned on for the server
e. Must be set if ‘codec-enforcement’ is turned on for the server
f. Must be set if ‘codec-enforcement’ is turned on for the server
g. Billing is MCI specific
h. If this turned ON, please ensure ALL the IP Addresses the NGSS box communicates with are part of the Access Control List. (IP Addresses that are datafilled in Remote Server Page area automatically part of the list.) For example, when communicating with VRDN implementation, ensure the IP Addresses of all the communicating SIP GWCs are part of the list. Otherwise, call processing will not work.

51.11 Appendix

The following mapping will be used for NGSS to communicate with VRDN configuration.

Table 9 NGSS to VRDN / VRDN to NGSS mapping

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
BTUP				gb_iup
Q764			gr394	gr394
UCP			ansi88	ucp_ansi88
MCI			ansi88	mci_ansi88
Australian ISUP			ansi88	au_ansi88
Q767	100_blue	FTUP		fr_ssutr2
Q767	100_blue	Base V1	etsi121	etsi121
Q767	100_blue	Italy	etsi121	it_etsi121

Table 9 NGSS to VRDN / VRDN to NGSS mapping

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_blue	Spain	etsi121	es_etsi121
Q767	100_blue	Norway	etsi121	no_etsi356
Q767	100_blue	New Zealand	etsi121	nz_etsi121
Q767	100_blue	Brazil	etsi121	br_etsi121
Q767	100_blue	Mexico	etsi121	mx_etsi121
Q767	100_blue	Turkey	etsi121	tr_etsi121
Q767	100_blue	Portugal	etsi121	pt_etsi121
Q767	100_blue	Denmark	etsi121	dk_etsi121
Q767	100_blue	Czech	etsi121	cz_etsi121
Q767	100_white	Base V2	etsi356	etsi356
Q767	100_white	Australia	etsi356	au_etsi356
Q767	100_white	Germany	etsi356	de_etsi356
Q767	100_white	Belgium	etsi356	be_etsi356
Q767	100_white	Sweden	etsi356	se_etsi356
Q767	100_white	Israel	etsi356	il_etsi356
Q767	100_white	Papua New Guinea	etsi356	pg_etsi356
Q767	100_white	Chile	etsi356	cl_etsi356
Q767	100_white	Costa Rica	etsi356	cr_etsi356
Q767	100_white	Ethiopia	etsi356	et_etsi121
Q767	100_white	Georgia	etsi356	ge_etsi356
Q767	100_white	Myanamar	etsi356	mm_etsi356
Q767	100_white	Vietnam	etsi356	vn_etsi356
Q767	100_white	Israeli Defence Force	etsi356	il_df_etsi356
Q767	100_white	Saudi Arabia	etsi356	sa_etsi356
Q767	100_white	Hungary	etsi356	hu_etsi356
Q767	100_white	Peru	etsi356	pe_etsi356

Table 9 NGSS to VRDN / VRDN to NGSS mapping

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_white	Argentina	etsi356	ar_etsi356
Q767	100_white	China	etsi356	cn_etsi356
Q767	100_white	Spain	etsi356	es_etsi356
Q767	100_white	Turkey	etsi356	tr_etsi356
Q767	100_white	HongKong	etsi356	hk_etsi356
Q767	100_white	RUSSIA	etsi356	ru_etsi356
Q767	100_EIV3	Base V3	etsi356	etsi356
Q767	100_EIV3	UK-ISUP	etsi356	gb_etsi356
Q767	100_EIV3	France SPIROU	etsi356	fr_etsi356
Q767	CCITT7_White		etsi356	etsi356
Q767	CCITT7_Blue		etsi121	etsi121

52: Configuration (CN): A00003947

52.1 Hardware and Software Requirements

None

52.2 Initial Configuration

52.3 Office/Subnet parameters (OP/SP) (CM & SESM)

CM

52.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	MULTINET_DISPLAY_ACTIVE	NEW	CM

52.3.2 Parameter information

52.3.2.1 MULTINET_DISPLAY_ACTIVE

Multiple Networks Display Active

52.3.2.1.1 Functional description

This is a new office parameter associated with Trimodal Call Server that activates the new and changed OMs/Logs and MAP screens. This allows the customer the flexibility of enabling multiple packet networks (likely for testing purposes only) prior to having the back-office system (i.e., OSS systems) ready to support the new OMs/Logs/MAP screens. This is an YES-NO type parameter. This parameter would be part of OFCVAR table. The default would be set to 'NO'.

52.3.2.1.2 Provisioning rules

52.3.2.1.2.1 Behavior when the parameter is set to ‘YES’

- First time change from ‘NO’ to ‘YES’ using table control or using Table transfer.
  - — The tuples in the new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are displayed.
  - — Pegging of the OM group registers in IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group is displayed.
  - — The display of bridge pool in IWBM 800 series of LOGS is enabled.
- Second time change from ‘NO’ to ‘YES’ using table control
  - — The tuples in the new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are displayed.
  - — Pegging of the OM group registers in IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group would be displayed.
  - — The display of bridge pool in IWBM 800 series of LOGS is enabled.

52.3.2.1.2.2 Behavior when the parameter is set to ‘NO’

- Change from ‘YES’ to ‘NO’ using table control
  - — A warning message would be displayed “All OM and LOGs data pertaining to Trimodal call server will be lost.”.
  - — The tuples in the new OM groups would not be displayed.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group would not be displayed.
  - — All the counters for the registers of the new OM groups would be set to zero.
  - — The counters of the registers of the new OM groups would not be pegged.
  - — The display of bridge pool in IWBM 800 series of LOGS would be disabled.
  - — The OMSHOW command would display the OM groupsIWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

52.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
YES-NO	YES-NO	NO

52.3.2.1.4 Activation
Immediate

52.3.2.1.5 Dependencies

None
None

52.3.2.1.6 Consequences

None

52.3.2.1.7 Verification
To verify that the MULTINET Display is active and OM groups are created, use the CI command OMSHOW DPTOFCP. This command should display the OM group files and its tuples

52.3.2.1.8 Memory requirements
No memory impact.

Units per memory block = <10>

Words per memory block = <510>

If the parameter value = <25>

words required = (((parameter value - 1)/units per block) + 1) *words per block = <>

52.3.2.1.9 Parameter release history update
N/A

52.4 Upgrade Impact

52.5 Data schema (DS) (CM, MIBS, RDB)

52.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
OFRT	CHANGED	NEW
OFR2	CHANGED	NEW
OFR3	CHANGED	NEW
OFR4	CHANGED	NEW
IBNRTE	CHANGED	NEW
IBNRT2	CHANGED	NEW
IBNRT3	CHANGED	NEW
IBNRT4	CHANGED	NEW
HNPACONT$RTEREF	CHANGED	NEW

52.5.2 Table/MIB/Remote Database Schema information

52.5.2.1 Name: OFRT

Office Routing Table

52.5.2.1.1 Functional description

52.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

OFRT

52.5.2.1.3 Size

Not Changed

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DDPACDEV	0	8 000 000	Memory is automatically allocated for 16 DPC devices.

52.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for OFRT.

<conditional information>

Table 5 OFRT Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,PKT, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.

Table 5 OFRT Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,PKT, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	UNDEF[a], ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
NETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

a. No trunk and line agent can belong to an network with fabric as “UNDEF”. Hence “UNDEF” fabric selector is blocked form being datafilled.

52.5.2.1.5 Datafill example

The following examples shows sample datafill for table OFRT.

Figure 1 CND BEARNET

```
TABLE OFRT
POS 99
100 (CND BEARNET DFLTTDM ST 901)
(CND BEARNET DFLTIP ST 902)
(CND BEARNET DFLTATM ST 903) $ $
```

Figure 2 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901)
   (CND FABRIC IP ST 902)
   (CND FABRIC AAL1 ST 903)
   (CND FABRIC AAL2 ST 904) $ $
```

52.5.2.1.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support ATM and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name.

52.5.2.1.7 Supplementary information

The above mentioned changes are applicable to all the routing tables OFR2, OFR3, OFR4, IBNRTE, IBNRT2, IBNRT3, IBNRT4 and HNPACONT$RTEREF that have CND and NOT bound in as the route selector.

52.5.2.1.8 Translation verification other tools

The following example shows the output from Traver when it is used to verify OFRT.

<abbreviated name of table> does not use translation verification tools.

Figure 3 Traver example: with BEARNET Option

```
traver tr isupicitt 7211001 BEARNET MyAAL1NW b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
.  .  . SAME TABLE
 .  .  . 1002 S D ISUPITOG
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

52.6 Service Orders (SO) (CM & SESM)

52.7 Software optionality control (SOC)

52.8 Element Management

52.9 Command interface changes

52.9.1 Command: TRAVER

52.9.1.1 Command type: NON-MENU

52.9.1.2 Command target: All

52.9.1.3 Command availability: RES

52.9.1.4 Command description

Traver is a Translations Verification Tool.

- Traver enhancements
  - — New Traver option BEARNET to input the network name of the incoming trunk agent to support FABRIC and BEARNET conditional selector routing
  - — Traver TRKMEM option is enhanced to derive the originating trunk bearer network/fabric. The bearer network/fabric is used to support FABRIC and BEARNET conditional selector routing

52.9.1.5 Command syntax

Table 6 Tarver command parameters and variables

Command	Parameters and variables
TARVER	Parms: <ORIG> {MX <OPTION> {MOBORIG} <PROFNAME> STRING [<CENTREX> {CTX <ORIGMIN> STRING}] [<ORIGMIN> {ORIGMIN <ORIGMIN> STRING}] [<CELL> {CELL <CELLSTR> STRING}], ... TR <CLLI> STRING [<CLLIOPT> {SAT <BOOL> "TRUE" or "FALSE"}] [<MBGOPTS> {MBG <TYPE> {LOCAL, NATL} <ID> {0 TO 4294967295} <LP> {0 TO 255} <GAP> STRING}] [<TRIGOPT> {TRIG <PIC> {ALL, ORIG, COLLECT} .. .. .. [<TRKMEM> {TRKMEM <TRKMEM> {0 TO 9999}}]} .. .. .. <BEARNET> {BEARNET <NETWORK NAME DATAFILLED IN TABLE BEARNETS> STRING} <TRACE> {T, NT, B} .. .. .. [<TABIDX> {TABIDX <MSG_INDEX> {0 TO 1000} <PTS_INDEX> {0 TO 1000}}]

Table 6 Tarver command parameters and variables

Command	Parameters and variables
BEARNET	Bearer Network Defined in Table BEARNETS
TRKMEM	Trunk Member number

52.9.1.6 Qualifications and warnings

None.

52.9.1.7 Responses

52.9.1.7.1 <response>

Table 7 Traver outputs

Command: TRAVER

```
traver tr isupicitt 7211001 BEARNET MyAAL1NW b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
..
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
.  .  . SAME TABLE
 .  .  . 1002 S D ISUPITOG
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Table 7 Traver outputs

Command: TRAVER

```
traver tr isupicitt 7211001 TRKMEM 1001 b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .  . TABLE OFRT
 .  . 1001 CND BEARNET TDM_ENET ST 1002
 .  .      CND BEARNET MYAAL1NW ST 1003
.  .  . SAME TABLE
 .  .  . 1003 S D ATMTRK1
 .  .  . EXIT SAME TABLE
 .  .      CND BEARNET MYIP4NW ST 1004
 .  . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

52.9.1.8 Example

Table 8 Usage examples for <CommandName> command

Description of task:	

Table 8 Usage examples for <CommandName> command

Description of task	Synchronize the two CPUs of the CM without matching memory after synchronization and without displaying any warnings regarding possible side effects beforehand.
Command: MAP response:	Example: SYNC Nomatch Noprompt Example: SYNCHRONIZATION SUCCESSFUL

52.10 Security

52.11 Configuration Walkthrough

53: Configuration (CN): A00003948

53.1 Hardware and Software Requirements

53.1.1 Hardware

No additional hardware is required in order to upgrade to a load capable of supporting multiple packet networks (support limited to IP interworking with AAL2 for SN07). All exisiting TDM/Packet configurations will continue to be supported, including:

- UA-AAL1
- PT-AAL1
- Ultralite AAL1
- UA-IP
- PT-IP
- PT-IP Compact (includes AAL2 via the PVG)
- AAL2 Wireless

In addition, the following new office configuration are supported:

- UA-AAL1/IP
- PT-AAL2/IP
- New hardware will be required for the addition of the second packet network.

53.1.2 Software

The software reconfiguration to use the new networking tables (BEARNETS, NETBRDGE, NETPATH, NET2NET) will occur automatically to include default datafill dictated by the value of a new office parameter. This parameter, PRE_SN07_DUMPSIDE_PACKET_FABRIC, must be set by the engineering team and applied to the office prior to the table transfer.

SESM will align with the standard SESM requirements.

In order to provision a second packet network, the customer will have to provision the new network, any bridging resources for that network, and the connectivity supported between the networks via the bridging resource paths.

53.2 Initial Configuration.

53.2.1 Office parameters

53.2.1.1 NETWORK_ACTIVE

The network_active office parameter will be set to EXTENET when upgraded to the SN07 Succession load, even if it had been previously set to ENET.

If it had been set to JNET, the value will remain as JNET. In these offices, there will be no default network datafill in the new network tables.

Note: If the value of the network_active office parameter is set to JNET, the packet connectivity function is not available.

53.2.1.2 PRE_SN07_DUMPSIDE_PACKET_FABRIC

Will be set to one of {NONE, AAL1, AAL2, IP}. Once the ONP is complete, there is no need to change this office parameter.

53.2.1.3 MULTINET_DISPLAY_ACTIVE = 'N'

The display control for the new OMs and Logs introduced by this activity is initially off.

53.2.1.4 ECAN_EDGE_STRATEGY

The existing ECAN_EDGE_STRATEGY office parameter will be deleted following the ONP. By default, the ECAN strategy will be EDGE for the office and applies to all IP and AAL2 networks. AAL1 networks will have the ECAN_REGION_STRATEGY option added to them during the ONP if the office parm ECAN_EDGE_STRATEGY was FALSE on the from side.

53.2.2 New Network Tables - initial datafill

The examples that follow are the default tuples that will be in the new network tables after the ONP is complete. Note that the initial value of the NET 1 FABRIC field will be determined by the new office parameter PRE_SN07_DUMPSIDE_PACKET_FABRIC.

Figure 1 ENET on from side (ENET)

```
TABLE BEARNETS:
NETIDX  NETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET            $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET            $
```

Figure 2 ENET & AAL1 on from side (UA-AAL1 & PT-AAL1)

```
TABLE BEARNETS:
NETIDX  NETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET            $
NET 1   NET_AAL1        ATM             AAL1            (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    725             0                       ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_AAL1    CORE_BRDG       E-A1                    (TDM_ENET NET_AAL1) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       (ENET_TO_AAL1) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_AQAL1 0) $
NET_AAL1                (TDM_ENET 0) $

NOTE: BEARNETS tuple NET 1 will also have the ECAN_REGION_STRATEGY option if the
office parameter ECAN_EDGE_STRATEGY transferred as 'F'.
```

Figure 3 AAL1 on from side (Ultralite-AAL1)

```
TABLE BEARNETS:
NETIDX  NETNAME          DISPLAY          FABRIC           OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET         ENET             ENET             $
NET 1   NET_AAL1        ATM             AAL1           (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI             ADNUM            TRKGRSIZ                  ADMININF
-------------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI         BRDGTYPE         DISPLAY                   ADMININF
-------------------------------------------------------------------

TABLE NETPATH
PATHIDX                  NETPATH
--------------------------------------

TABLE NET2NET
BNETNAME                 CONNNETS
--------------------------------------
TDM_ENET                 $
NET_AAL1                 $

NOTE: BEARNETS tuple NET 1 will also have the ECAN_REGION_STRATEGY option if
the office parameter ECAN_EDGE_STRATEGY transferred as 'F'.
```

Figure 4 ENET & IP on from side (UA-IP and PT-IP)

```
TABLE BEARNETS
NETIDX  NETNAME         DISPLAY         FABRIC          OPTIONS
-------------------------------------------------------------------
NET 0   TDM_ENET        ENET            ENET            $
NET 1    NET_IP         IP              IP             (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-------------------------------------------------------------------
ENET_TO_IP      725             0                       ENET_TO_IP_BRIDGE_POOL

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-------------------------------------------------------------------
ENET_TO_IP      CORE_BRDG       E-IP                    (TDM_ENET NET_IP) $

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------
0                       (ENET_TO_IP) $

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
TDM_ENET                (NET_IP 0) $
NET_IP                  (TDM_ENET 0) $
```

Figure 5 IP on from side (PT-IP Compact)

```
TABLE BEARNETS
NETIDX  NETNAME         DISPLAY          FABRIC          OPTIONS
-----------------------------------------------------------------
NET 1   NET_IP          IP               IP              (PACKET_NETWORK_DEFAULT) $


TABLE CLLI
CLLI            ADNUM           TRKGRSIZ                ADMININF
-----------------------------------------------------------------

TABLE NETBRDGE
BRDGCLLI        BRDGTYPE        DISPLAY                 ADMININF
-----------------------------------------------------------------

TABLE NETPATH
PATHIDX                 NETPATH
-------------------------------------

TABLE NET2NET
BNETNAME                CONNNETS
-------------------------------------
NET_IP                  $
```

53.2.3 New fields in existing tables

53.2.3.1 MNNODE

- IW SPM: will include new field BRDGCLLI set to key of only entry in table NETBRDGE.
- IW DPT: will include a new field BEARNETS set to (<name of NET 1> Y) $.
- MG4K: will include a new field BEARNETS set to (NET_AAL1 Y) $

53.2.3.2 TRKOPTS

- DPT tuples will be pulled out of the DYNAMIC option as an application type and moved into it's own option area.
- DPT tuples will contain a new BEARNETS field, that will contain (<name of NET 1> Y) $

53.2.3.3 SERVRINV

- Will contain a new BEARNETS field, which will be set to:
  - (<name of NET 1> Y) $ if GWC is not a DPT GWC
  - $ if a DPT GWC

53.2.3.4 Routing tables: CND PKT selector

The existing CND PKT routing selector will be converted to CND FABRIC in all of the applicable routing tables.

53.2.4 SESM

Each non DPT GWC provisioned will have a network codec profile associated with it, using the existing network codec profile that is configured for the office.

DPT GWC's will not have a network codec profile associated with them.

53.3 Office/Subnet parameters (OP/SP) (CM & SESM)

53.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCOPT	network_active	Unchanged	CM
OFCENG	ecan_edge_strategy	Deleted	CM
OFCVAR	multinet_display_active	New	CM
OFCENG	pre_sn07_dumpside_packet_fabric	New	CM

53.3.2 Parameter information

53.3.2.1 OFCOPT::NETWORK_ACTIVE

- The parameter itself is not really changing in SN07. It will simply be used to aid in the detection of an upgrade to a Succession call server capable of supporting multiple packet networks.
- As of SN04, any ENET offices upgrading to a packet capable Succession load will have this office parameter converted to EXTENET automatically during the upgrade.
- The value EXTENET is now expanded to include the ability to support mutiple packet networks.
- The use of the network tables (BEARNETS, NETBRDGE, NETPATH, and NET2NET) is enforced in connectivity for interworking the various networks, even when only a single packet network exists.

53.3.2.1.1 Functional description
This parameter controls various aspects of call processing, most importantly the network connectivity capabilities that are supported by the system.

53.3.2.1.2 Provisioning rules
For JNET call processing, set the value of this parameter to JNET.

For ENET call processing, set the value of this parameter to ENET (non-Succession loads only).

For Succession (single or multiple packet networks), the value should be set to EXTENET. “Succession” includes all cases where the load is packet capable, such that it includes the MSH DRU. This includes offices that currently only have an ENET provisioned.

53.3.2.1.3 Range information
Unchanged.

53.3.2.1.4 Activation
Unchanged.

53.3.2.1.5 Dependencies
No additional dependencies.

53.3.2.1.6 Consequences
Unchanged.

Note: The update mentioned under activation was put in place because this office parameter requires a restart for activation, and packet network connectivity is not available unless the office parm is set to EXTENET for Succession loads.

53.3.2.1.7 Verification
Not applicable.

53.3.2.1.8 Memory requirements
No memory impact.

53.3.2.1.9 Parameter release history update
Office parm value EXTENET also applies to the Trimodal Succession Call Server.

Note: The current SN06 NTP documentation does not reflect that this parameter will be changed on an ONP to EXTENET, if the from side is currently set at “ENET” and the to load contains the MSH DRU. The update that does this was submitted in TL16.

53.3.2.2 OFCENG::ECAN_EDGE_STRATEGY

Echo cancellation provisioning strategy on a packet network.

Potential issue: This office parm still needs to transfer in order to properly set the BEARNETS ECAN_REGION_STRATEGY option. It should be deleted from the system only after the table transfer of BEARNETS.

53.3.2.2.1 Functional description

This is a Succession related parameter that indicates whether a given load is using an edge or region strategy to control echo cancellation.

This parameter will be deleted in SN07.

53.3.2.2.2 Provisioning rules

Not applicble.

53.3.2.2.3 Range information

Unchanged.

Table 2 Range Information

Minimum	Maximum	Default
Y/N	Y/N	N

53.3.2.2.4 Activation

Not applicable.

53.3.2.2.5 Dependencies

Not applicable.

53.3.2.2.6 Consequences

Not applicable.

53.3.2.2.7 Verification

Not applicable.

53.3.2.2.8 Memory requirements

No additional memory required.

53.3.2.2.9 Parameter release history update

As of SN07, the ECAN strategy is moved to the individual packet network tuples in table BEARNETS, as option ECAN_REGION_STRATEGY. When this option is not present in the tuple, the ECAN strategy will default to the edge strategy for that network. Refer to the FN section for more information.

On an ONP, the AAL1 packet network tuples in the new table BEARNETS will automatically have the ECAN_REGION_STRATEGY added to them if the ECAN_EDGE_STRATEGY was F (false).

53.3.2.3 OFCOPT::MULTINET_DISPLAY_ACTIVE

Multiple Networks Display Active

53.3.2.3.1 Functional description

This is a new office parameter associated with Trimodal Call Server that activates the new and changed OMs and logs. This allows the customer the flexibility of enabling multiple packet networks (likely for testing purposes only) prior to having the back-office system (i.e., OSS systems) ready to support the new OMs and log fields. This is an Y/N type parameter. This parameter would be part of OFCVAR table. The default would be set to 'N'.

53.3.2.3.2 Provisioning rules

This office parameter cannot be turned on unless NETWORK_ACTIVE = EXTENET.

There are no restrictions for setting it to 'N'.

53.3.2.3.2.1 Behavior when the parameter is set to 'Y'

- Change from 'N' to 'Y' using table control.
  - — The tuples in the new OM groups IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are created (if non-existing) and displayed.
  - — Pegging of the OM group registers in IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
  - — The signaling type for the DPT node tuple in the DPTNODE OM group is displayed. The bearer network is also displayed for DPTNODE OMs if the DPT node is SPM based. The bearer network will not be displayed for GWC hosted DPT.
  - — The display of the bridge pool in IWBM 800 series of LOGS is enabled.
  - — Automatic creation of additional tuples via the table provisioning interfaces is turned on.

53.3.2.3.2.2 Behavior when the parameter is set to 'N'

- Change from 'Y' to 'N' using table control
  - — A warning message would be displayed "All OM and LOGs data pertaining to Trimodal call server will be lost.".
  - — The tuples in the new OM groups would not be displayed.

— The signaling type and bearer network for the DPT node tuple in the DPTNODE OM group would not be displayed.

— All the counters for the registers of the new OM groups would be set to zero.

— The counters of the registers of the new OM groups would not be pegged.

— The display of bridge pool in IWBM 800 series of LOGS would be disabled.

— The OMSHOW command would display the OM groupsIWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

— Automatic creation of addtional tuples via the table provisioning interfaces is turned off.

53.3.2.3.3 Range information

Table 3 Range Information

Minimum	Maximum	Default
Y/N	Y/N	N

53.3.2.3.4 Activation

Immediate

53.3.2.3.5 Dependencies

This parameter cannot be set to Y unless NETWORK_ACTIVE = EXTENET.

53.3.2.3.6 Consequences

None

53.3.2.3.7 Verification

To verify that the MULTINET Display is active and OM groups are created, use the CI command OMSHOW DPTOFCP. This command should display the OM group files and its tuples.

53.3.2.3.8 Memory requirements

Refer to the EI section for final details.

Enabling this office parameter will create store allocation for the following OM groups:

IWBMNODE OM group: Protected store of 10.5K bytes.

TRK2NET1 and TRK2NET2 combined:

— 48Kbytes of protected store, assuming only one network provisioned in table BEARNETS.

— Each additional tuple requires an additional 8Kbytes of store, for a maximum of 160Kbytes.

53.3.2.3.9 Parameter release history update

New in SN07.

53.3.2.4 OFCENG::PRE_SN07_DUMPSIDE_PACKET_FABRIC

SN07 Dumpside Packet Fabric prior to Trimodal upgrade.

53.3.2.4.1 Functional description

This office parameter is set by the Nortel engineering team in an office parm changes flat file prior to the night of ONP. It is to be applied after the transfer of the office parameters and prior to the TABXFER.

The purpose of the parameter is to identify the FABRIC type of the single packet fabric supported on the from side prior to the upgrade, in order for the proper network tuples to be created in tables BEARNETS, CLLI, NETBRDGE, NETPATH, and NET2NET, as well as allow the new network related fields in tables MNNODE, TRKOPTS, and SERVRINV to be assigned the proper default values.

It is very important that this parameter be set correctly.

Note: Let's talk about what to call this office parameter. The current name is a placeholder.

53.3.2.4.2 Provisioning rules

This parameter has the following range: {UNDEF, NONE, AAL1, AAL2, IP}. It will be defaulted to UNDEF at IPL, and should be set to one of the other values on all upgrades to Succession loads. Although present in non Succession loads, it does not need to be set for these loads. Once an office is already on an SN07 or later load, it does not need to be set again.

A warning will be output on all changes except "UNDEF" to one of the other values that this parameter impacts the automatic creation of the network data on ONP, and should be changed with care.

Once a packet tuple is provisioned in table BEARNETS, changes will not be allowed.

In order to properly set the value, datafill will be required from the dump side from the following tables: MNNODE, MNCKTPAK, TRKOPTS, LGRPINV.

Explanation of parameter values:

- UNDEF: Default value at IPL. Indicates that the engineering team has not looked at the data.
- NONE: The engineering team has analyzed the from side data and detected that no packet nodes are provisioned. Indications that a packet node existed would include:
  - — MNNODE: IW SPM, DPM SPM, or MG4K SPMs are provisioned.
  - — SERVRINV: any tuple provisioned.
  - — Although one could argue that datafill in tables SERVSINV or LGRPINV also indicates a packet node, it cannot be added without a GWC first.
- AAL1: The from side packet datafill contained one of the following:
  - — MNNODE contained an SMG4 (MG4K). Prior to SN07.1, MG4K IP did not exist.
  - — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is ATM RM.
- AAL2:
  - — Cannot be detected based on table datafill. Hopefully the engineering team knows if the PVG is using AAL2 or IP/AAL5.
- IP:
  - — MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is GEM RM.
  - — Table LGRPINV contains tuples whose GRPTYPE field is ‘M’ or ‘C’. indicating IAD devices or CICM.
  - — The parm should also be set to IP if dumpside was using IP/AAL5. This will not be distinguished as a seperate bearer network.

53.3.2.4.3 Range information

Office parm is deleted.

Table 4 Range Information

Minimum	Maximum	Default
{UNDEF, NONE, AAL1, AAL2, IP}	{UNDEF, NONE, AAL1, AAL2, IP}	UNDEF

53.3.2.4.4 Activation

Not applicable. This office parameter is only used during the TABXFER of data to a new load. It should be set to the correct fabric PRIOR to the night of ONP, and not changed thereafter. It is not used by call processing.

53.3.2.4.5 Dependencies

The following tables rely on the proper provisioning of this parameter:

- BEARNETS
- NETBRDGE
- NETPATH
- NET2NET
- MNNODE
- TRKOPTS
- SERVRINV

53.3.2.4.6 Consequences

- There are no consequences of incorrect provisioning if there are no packet nodes currently supported at the site. If the parameter is set to a packet fabric in a site that does not have a packet network, then network tuples will automatically be created in tables BEARNETS, NETBRDGE, NETPATH, NET2NET.
- If a packet network was supported, and the parameter is provisioned incorrectly, tuple transfer errors could occur in the following tables:

  — TABXFER data errors in MNCKTPAK, TRKOPTS, LGRPINV.

53.3.2.4.7 Verification

Not applicable.

53.3.2.4.8 Memory requirements

Minimal. Just need to store the fabric type in a protected variable. Does not control the allocation of any additional memory.

53.3.2.4.9 Parameter release history update

New in SN07.

53.4 Upgrade Impact

53.4.1 Dump and Restore

Callp functionality should not be affected over an upgrade from pre-SN07 to post-SN07. In order to maintain this, the new/changed tables need to be datafilled over the ONP. It is required that this upgrade has minimum impact

to the customer. Aside from the traditional issues with type specific reformats, we have the additional issue of determining what the FABRIC type was on the from side, in order to properly create default tuples in the new network tables. Since call processing will start depending on this data to make inter-network connections, it is vital that this data is correct after the transfer is ONP.

Given the importance of a proper transfer, the need for user input, and the complexity of the data involved, the design team held a meeting with the upgrade team. This chosen alternative was suggested during this meeting, and was unanimously agreed upon by all who were present.

Once the data transfer is complete, the goal is to have the correct network representation for the currently configured networks, such that only new network information is required for when the customer wishes to add additional networks.

The ONP strategy must handle the following information:

53.4.1.1 Office Parameters

- OFCOPT::NETWORK_ACTIVE - If ENET, convert to EXTENET, and ensure that appropriate datafill is created to handle the existing networks.
- OFCOPT::MULTINET_DISPLAY_ACTIVE - Ensure the new office parameter is defaulted to ‘N’.
- OFCENG::ECAN_EDGE_STRATEGY - Move the information currently provided on an office-wide level via the office parameter into the individual packet network tuples in table BEARNETS as the option ECAN_REGION_STRATEGY. Obsolete the office parameter.
- OFCENG::PRE_SN07_DUMPSIDE_PACKET_FABRIC: the new office parameter *must be set by the upgrade engineering team* to indicate the default packet fabric on the from side network. This is set in a flat file that is applied after the office parameters have been transferred and before the tables are transferred. The engineering team is responsible for setting the correct values, and the application team is responsible for applying the changes at the proper point. Note that this is simply a new parameter included in the existing office parameter process. No changes are required to the process. This parameter applies only to alternative 1.

53.4.1.2 ONP Creation of Default Network Tuples

Tuples will be created automatically during the TABXFER for the following tables. For more information see “New Network Tables - initial datafill” on page 3128.

- BEARNETS
  - — Create a NET 0 tuple representing the ENET if ENET is present.

— Create an appropriate NET 2 tuple representing the existing packet network. The FABRIC should be set to either AAL1, AAL2, or IP as appropriate.

- CLLI
  - — Create the appropriate CLLI used as the index to table NETBRDGE.
- NETBRDGE
  - — If there is currently an IW SPM provisioned in the office, create a default bridge group representing it.
- NETPATH
  - — If there is currently an IW SPM provisioned in the office, create a path from the NET 0 ENET to the NET 1 packet network using the bridge group available in table NETBRDGE.
- NET2NET
  - — For each network in table BEARNETS, create a tuple in NET2NET.
  - — If there is an IW SPM, assume that both the ENET and the packet network can be connected to the other using the single path index defined in table NETPATH.
  - — Ensure that the NET 1 packet network detected is assigned the PACKET_NETWORK_DEFAULT option.
  - — If the packet network has an AAL1 fabric, and the office parameter ECAN_EDGE_STRATEGY = F, then assign the ECAN_REGION_STRATEGY to the NET 1 packet tuple.

53.4.1.3 Initialization of new fields in existing tables

- MNNODE:
  - — IW SPM: Initialize the new BRDGCLLI field to the single bridge group defined in table NETBRDGE.
  - — DPT SPM: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
  - — MG4K: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
- TRKOPTS:
  - — Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the DPT trunk group.
- SERVRINV:
  - — If not a DPT GWC, initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the GWC.
  - — If this is a DPT GWC, initialize the new BEARNETS field to $.

53.4.1.4 Type reformats on existing tables

- TRKOPTS: Remove DPT trunk groups as an application under the DYNAMIC trunk option, and create a DPT trunk option.
- OFRn, IBNRTn, HNPACONT::RTEREF, FNPACONT::RTEREF:
  - Convert the CND PKT conditional selector to CND FABRIC in all of the applicable routing tables.

53.4.2 Element Management Upgrade

53.5 Data schema (DS) (CM, MIBS, RDB)

53.5.1 New/modified tables, MIBs, or Database Schema

Table 5 New or modified tables

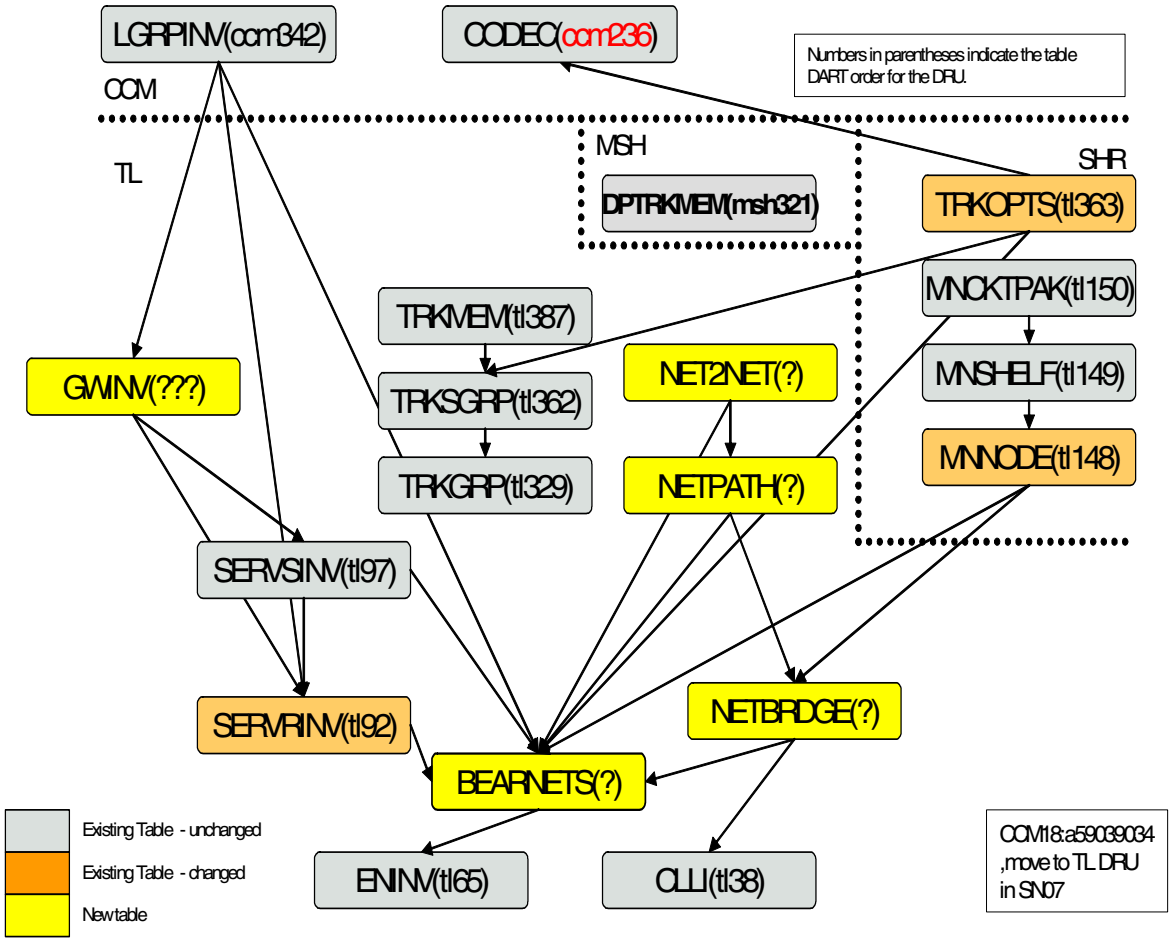
Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Core Tables:		
BEARNETS	NEW	NEW
NETBRDGE	NEW	NEW
NETPATH	NEW	NEW
NET2NET	NEW	NEW
MNNODE	Changed	Unchanged
SERVRINV	Changed	Unchanged
SERVSINV	Changed	Unchanged.
TRKOPTS	Changed	Unchanged
MNCKTPAK	n/a	Unchanged
OFRn	Changed	Unchanged
IBNRTn	Changed	Unchanged
HNPACONT:RTEREF	Changed	Unchanged
FNPACONT:RTEREF	Changed	Unchanged
SESM/GWCEM		
GWC_NETWORK_CODEC_PROFILE	New	New
GWCNode	Changed	Old

Table 5 New or modified tables

Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GWCPROFILE	Changed	Old
GATEWAYPROFILE	Changed	Old

53.5.2 Table/MIB/Remote Database Schema information

53.5.2.1 Core Table Dependencies



53.5.2.2 Core Table BEARNETS

Bearer networks

53.5.2.2.1 Functional description

On a Succession Call Server, this table identifies the bearer networks supported by the server and the network options that apply to the packet networks.

The overall default packet network for the office is determined by the assignment of the packet_network_default option to a single tuple in the table. If no packet network is detected in the provisioning hierarchy for a packet agent, this default packet network will be used.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

53.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

ENINV

BEARNETS

NETBRDGE, NET2NET, MNNODE, SERVRINV, TRKOPTS

53.5.2.2.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
BEARNETS	0	8	Memory not allocated unless tuples are provisoned. (Required if NETWORK_ACTIVE = EXTENET).

53.5.2.2.4 Fields/OIDs

The following table lists fields for BEARNETS.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETIDX	New	No	0-7	Key to the table. Will be displayed as “NET 0” - “NET 7”.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	Vector of up to 32 characters.	Identifies the name of the bearer network.This will be used in other tables to reference the associated bearer network and its characteristics. Making the name a field of the tuple rather than the index allows the customer to make name changes to the networks defined. The 32 character name of the network must be unique across the table.
DISPLAY	New	No	Vector of up to 4 characters.	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control.
FABRIC	New	No	UNDEF, ENET, AAL1, AAL2, IP	Identifies the bearer network fabric type.
OPTIONS	New	Refinements	Vector of {pkt_network_default, ecan_region_strategy}	Vector of options against the bearer network.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
pkt_network_default	New	OPTIONS refinement (not a field)	n/a	Indicates that this tuple is the packet bearer network default for the office. Primarily used in initializing dependant tables during an ONP. Restrictions: Only one tuple in the table can have this option. Cannot be added to tuples where the FABRIC is UNDEF or ENET.
ecan_region_strategy	New	OPTIONS refinement (not a field)	n/a	Indicates that calls on this network will use the region strategy to govern their echo cancellation. Restrictions: Can only be added to AAL1 networks.

53.5.2.2.5 Datafill example

The following example shows sample datafill for table BEARNETS.

```
TABLE: BEARNETS
NETIDX NETNAME      DISPLAY FABRIC OPTIONS
----------------------------------------
NET 0  TDM_ENET     ENET    ENET   $
NET 1  NET_AAL1     ATM     AAL1   (PKT_NETWORK_DEFAULT)$
NET 2  NET_IP       IP      IP     $
NET 3  NET_AAL2     AAL2    AAL2   $
```

53.5.2.2.6 Table release history update

New in SN07.

53.5.2.2.7 Supplementary information

Table BEARNETS, along with tables NETBRDGE, NETPATH, and NET2NET) is required to be provisioned in all Succession sites supporting bridged calls from a TDM network to a packet network.

On an ONP, this table will be automatically provisioned with both TDM and packet networks tuples where they exist.

— If the from side datafill contained an ENET, the NET 0 tuple from the datafill example will be automatically provisioned.

— If the from side supported packet nodes (as indicated by the setting of the PRE_SN07_DUMPSIDE_NETWORK_FABRIC), the NET 1 tuple will be provisioned and marked as the PKT_NETWORK_DEFAULT.

Datafill restrictions and limitations:

- Additions of packet networks to the table will not be allowed unless the Office Parm NETWORK_ACTIVE is EXTENET.
- Table BEARNETS is a counted table. Tuple deletes are not be allowed when other tables reference it.
- Only one packet network can have the packet_network_default option. If this option is added to another network tuple, the option will be removed from the existing network tuple. Determine the restrictions for doing this.
  — Do not change unless all GWCs (except DPT) have a default network provisioned?
  — Allow changes, but first search for and assign all GWCs the existing default network?
- The FABRIC field cannot be changed.

Refer to the supplementary information for table NET2NET for additional information.

53.5.2.2.8 Translation verification other tools

BEARNETS does not use translation verification tools.

53.5.2.3 Core Table NETBRDGE

Network bridging resources.

53.5.2.3.1 Functional description

This table defines the network bridging resources for interconnecting networks. Bridges provide the ability to connect one network to another without regard to the call type. Bridges typically have two connectivity endpoints, one for each of the networks that it inter-connects.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

53.5.2.3.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

CLLI, BEARNETS

NETBRDGE

NETPATH, NET2NET, MNNODE

53.5.2.3.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	64	Refer to the EI section after DSUM.

53.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BRDGCLLI	New	No	CLLI common_language_name	Identifies the name of the bridge resource group.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TYPE OR BRDGTYPE?	New	No	CORE_BRDG	The type of the bridging resource. For SN07, this is limited to core bridges, but could be expanded in the future.
DISPLAY	New	No	Vector of up to 4 characters	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control.
BEARNETS	New	Structure	BNETNAME, BNETNAME	Identifies the two networks that can be bridged with this bridging resource group.

53.5.2.3.5 Datafill example

The following example shows sample datafill for table NETBRDGE.

```
TABLE: NETBRDGE
BRDGCLLI       TYPE         DISPLAY BEARNETS
-----------------x-------------------------
ENET_TO_AAL1   CORE_BRDG    E-A1     (TDM_ENET NET_AAL1) $
ENET_TO_IP     CORE_BRDG    E-IP     (TDM_ENET NET_IP)   $
```

53.5.2.3.6 Table release history update

New in SN07.

53.5.2.3.7 Supplementary information

- In SN07, the only TYPE supported is CORE_BRDG. It is possible that other bridge types may be added in the future.
- Table NETBRDGE shall be a counted table. Tuple deletes shall not be allowed when other tables reference it.

- The following tuple fields cannot be changed unless the tuple is not referenced by any other tables:
  - — TYPE
  - — BEARNETS

53.5.2.3.8 Translation verification other tools

NETBRDGE does not use translation verification tools.

53.5.2.4 Core Table NETPATH

Interconnecting network path.

53.5.2.4.1 Functional description

Tuples in this table identify the list of bridging resource groups (the bridge path) that can be used to interconnect two networks. In SN07, two bridges are required to connect an AAL1 agent and an IP agent, so the path consists of a bridge resource from each of those NETBRDGE's.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

53.5.2.4.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

NETBRDGE

NETPATH

NET2NET

53.5.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETPATH	0	256	Refer to the EI section of this document following the DSUM.

53.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for NETPATH.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PATHIDX	New	New	0 to 255	The key to the table.
NETBRDGE	New	New	Vector of BRDGCLLI	A list of the bridge pools that are required to go from one network to another.

53.5.2.4.5 Datafill example

The following example shows sample datafill for table NETPATH

```
TABLE: NETPATH
PATHIDX       NETBRDGE
----------------------------------------
  0           (ENET_TO_AAL1)  $
  1           (ENET_TO_IP)    $
  2           (ENET_TO_AAL1), (ENET_TO_IP)$
  3           (AAL1_TO_IP)    $

NOTE: PATHIDX 3 is not supported in SN07.
```

53.5.2.4.6 Table release history update

New table in SN07.

53.5.2.4.7 Supplementary information

Network paths are used dynamically during call processing. If a user changes a network path currently in use via table NET2NET, new connection requests between the 2 networks will begin using the new path.

Restored connections will continue to use the old path.

53.5.2.4.8 Translation verification other tools

NETPATH does not use translation verification tools.

53.5.2.5 Core Table NET2NET

Network interconnection.

53.5.2.5.1 Functional description

Tuples in this table define the allowable interconnections between networks, and the network path used to interconnect them.

Call processing will assume that any agents on the same network can be connected with one another.

Once the normal translations have occurred, a request will be made to connectivity to connect the agents.

- If the agents are on the same network, the connection request will proceed.
- If the agents are provisioned on seperate networks, connectivity will check table NET2NET to see if the connection is allowed.
  - — If the two networks are provisioned as connecting in the table, the NETPATH and associated bridge resources will be retrieved and the connection request will continue. If there are no idle members in the bridge groups, the connection request will then fail.
  - — If the two networks are not provisioned as connecting in the table, the connection request will fail immediately.
- In SN07, no mechansim is provided for choosing an alternate bridging path if the bridging resources are unavailable in the provisioned path.

53.5.2.5.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS, NETPATH

NET2NET

53.5.2.5.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NET2NET	0	7	Allocated upon first tuple entry.

53.5.2.5.4 Fields/OIDs

The following table lists fields/OIDs for NET2NET.

Each CONNNETS vector entry consists of:

- NET2NET - the interconnecting network
- NETPATH - reference to tuple in table NETPATH definining the path by which the two networks interconnect.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	BNETNAME defined in table BEARNETS	Identifies the name of the bearer network. Must be datafilled in Table BEARNETS first.
CONNNETS	New	No	Vector of connecting_network	Identifies a list of other bearer networks that are allowed to interconnect to this bearer network.
NET2NET	New	Field of connecting_network	BNETNAME provisioned in table BEARNETS	The interworking bearer network. Must be provisioned in Table BEARNETS first.
NETPATH	New	Field of connecting_network	Key to table NETPATH 0 - 255	Index into Table NETPATH.

53.5.2.5.5 Datafill example

The following example shows sample datafill for table NET2NET.

Figure 6 ENET/AAL1/IP NET2NET DatafillI

```
TABLE BEARNETS
NETIDX  NETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $

TABLE CLLI
-----------------------------------------------
CLLI          ADNUM   TRKGRPSIZ    ADMININF
ENET_TO_IP    725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724      0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----------------------------------------------
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
ENET_TO_AAL1  CORE_BRDG    E-A1         (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
-----------------------------------------------
PATHIDX          NETPATH
0                (ENET_TO_AAL1) $
1                (ENET_TO_IP) $
2                (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----------------------------------------------
BNETNAME        CONNNETS
TDM_ENET        (NET_ATM 0) (NET_IP  1) $
NET_ATM         (TDM_ENET 0) (NET_IP  2) $
NET_IP          (TDM_ENET 1) (NET_ATM 2) $
```

Figure 7 Enterprise/Carrier DatafilII

```
TABLE BEARNETS
NETIDX  NETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
-----------------------------------------------
CLLI          ADNUM   TRKGRPSIZ    ADMININF
ENET_TO_IP    725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724      0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----------------------------------------------
BRDGCLLI      BRDGTYPE     DISPLAY       BEARNETS
ENET_TO_AAL1  CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
-----------------------------------------------
PATHIDX          NETPATH
0                (ENET_TO_AAL1) $
1                (ENET_TO_IP) $
2                (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----------------------------------------------
BNETNAME        CONNNETS
TDM_ENET        (NET_ATM 0) (NET_IP  1) $
NET_ATM         (TDM_ENET 0) (NET_IP  2) $
NET_IP          (TDM_ENET 1) (NET_ATM 2) $
NET_IPE         $
```

Note taht NET_IPE does not connect to NET_IP, even though they have the same FABRIC.

This is the SN07 configuration example to support Carrier Hosted Services (i.e. H.323 and Media Call Server 5200) via PVG looparounds.

Figure 8 Differet Networks, same Fabric

```
TABLE BEARNETS
NETIDX  NETNAME    DISPLAY     FABRIC    OPTIONS
-----------------------------------------------
NET 0   TDM_ENET   ENET        ENET      $
NET 1   NET_ATM    ATM         AAL1      $
NET 2   NET_IP     IP          IP        $
NET 3   NET_IPE    IPE         IP        $

TABLE CLLI
-------------------------------------------------
CLLI          ADNUM   TRKGRPSIZ    ADMININF
ENET_TO_IP    725     0            ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724      0            ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-------------------------------------------------
BRDGCLLI       BRDGTYPE     DISPLAY       BEARNETS
ENET_TO_AAL1   CORE_BRDG    E-A1          (TDM_ENET NET_AAL1) $
ENET_TO_IP     CORE_BRDG    E-IP          (TDM_ENET NET_IP) $

TABLE NETPATH
-------------------------------------------------
PATHIDX          NETPATH
0                (ENET_TO_AAL1) $
1                (ENET_TO_IP) $
2                (ENET_TO_AAL1) (ENET_TO_IP) $
3                $

TABLE NET2NET
-------------------------------------------------
BNETNAME        CONNNETS
TDM_ENET        (NET_ATM 0) (NET_IP  1) $
NET_ATM         (TDM_ENET 0) (NET_IP  2) $
NET_IP          (TDM_ENET 1) (NET_ATM 2) (NET_IPE 3)$
NET_IPE         (NET_IP 3) $
```

To interconnect two different networks on the same fabric, define a NETPATH that requires no bridges, and put entries in NET2NET using that path.

53.5.2.5.6 Table release history update

New in SN07.

53.5.2.5.7 Supplementary information

- When a new interconnection is made from one network to another using a given NETPATH index, the reverse network connection tuple will also be updated to add the connectivity in the other direction using the same NETPATH index. Conversely, if a network connection path is removed from a tuple, it will also be removed in the reverse direction.
- It is recommended that if a network can connect only with itself, that a tuple is still provisioned with a '$' in the CONNNETS field. During the ONP, this will be the standard default datafill. However, if a tuple is deleted

that has a “$” for the CONNNETS field, connections will still be allowed among agents on the same network.

- Changes to NET2NET tuples take effect immediatly upon the change for all new connection requests. They do not impact the path of restored connections. Note that this can impact some active service interworking, if the service moves agents around in new connection configurations, such as Call Hold (CHD).
- A given network may only appear once is the CONNNETS list against another network. It is not permissable to provision network connectivity using two different NETPATH entries.

53.5.2.5.8 Translation verification other tools

NET2NET does not use translation verification tools.

53.5.2.6 Core Table MNNODE

Maintenance node table used to provision Spectrum nodes.

53.5.2.6.1 Functional description

Unchanged.

53.5.2.6.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

All existing dependencies, plus BEARNETS, NETBRDGE

MNNODE

All existing dependant tables.

53.5.2.6.3 Size

Table 14 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNNODE	Unchanged	Unchanged	Refer to the EI section of this document after DSUM complete.

53.5.2.6.4 Fields/OIDs

The following table lists fields/OIDs for MNNODE.

The following nodes provisioned in table MNNODE are impacted by these changes:

- Interworking bridges (NODEKEY=IW, DPT_INFO = BRDG_ONLY)

- DPT SPM (NODEKEY = IW, DPT_INFO = DPT_ONLY)
- MG4K (NODEKEY = SMG4)

Each of the applicable node type change is broken into it's own table below.

Table 15 Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	**IW**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	**BRDG_ONLY**	Refinements created based on this field.
BRDGCLLI	**New**	**New subfield when DPT_INFO = BRDG_ONLY**	**List of BRDGCLLI (common_language_identifier) provisioned in table NETBRDGE**	**List of the supported bridge groups the bridges belong to.**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 16 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged

Table 16 Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEINFO	Changed	IW refinement	**IW**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	**DPT_ONLY**	Refinements created based on this field.
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 17 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	**SMG4**	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
EXECTAB	Unchanged	Unchanged	Unchanged	Unchanged
DPT	Unchanged	Unchanged	Unchanged	Unchanged
DPT_NUM_REQ	Unchanged	Unchanged	Unchanged	Unchanged
SLINK_THRESHOLD_DATA	Unchanged	Unchanged	Unchanged	Unchanged
BOOTP_SUPPRESS	Unchanged	Unchanged	Unchanged	Unchanged
REMOTE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.**

Table 17 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**

53.5.2.6.5 Datafill example

The following examples show sample datafill for the affected nodetypes in table MNNODE.

Figure 9 Example Datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-------------------------------------------------
SPM  1 SPM_1  IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $(SYSB CR RPT)  (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT)(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

Figure 10 Example Datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM 1   SPM_1   IW   1   SYNCH   INTERNAL   15   (DTMF 60)  (ECAN
60) (TONESYN 60) $ (SYSB CR RPT)  (MANB MJ RPT)  (ISTB MN RPT)
(SYSBNA CR RPT)(MANBNA MJ RPT)  (DTMFLOW MN RPT)  (ECANLOW MN RPT)
(TONESLOW MN RPT)  (PATCHFAIL MJ RPT)  (ATMBCN CR RPT)(SMCHLD MF
RPT)  (SMCHLD24 CR RPT)  $DPT_ONLY  (NET_AAL1 Y) $
(SPMECIDX 0)$
```

Figure 11 Example Datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS     NODEINFO
-------------------------------------------------
SPM  1              SPM_1          SMG4   0   SYNC   LINE   50
(COT 60)  (DTMF 60)  (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT)  (MANB MJ RPT)  (ISTB MN RPT)  (SYSBNA CR RPT)(MANBNA MJ
RPT)  (COTLOW MN RPT)  (DTMFLOW MN RPT)(ECANLOW MN RPT)  (MFLOW
MN RPT)  (CMRLOW MN RPT)(TONESLOW MN RPT)  (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT)(ATMBCN CR RPT)  (STE3HLD MJ RPT)  (STE3HLD24
CR RPT)(SMCHLD MF RPT)  (SMCHLD24 CR RPT)  (SPMSRMNTD MN RPT)
(LOCUR MJ RPT)  (TMCFAIL CR RPT)  $ $  N  0  $  N  N  (NET_AAL1 Y) $
```

53.5.2.6.6 Table release history update

In SN07, The following mandatory fields were added:

- BEARNETS field added to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node.
- BRDGCLLI field added to IW BRDG_ONLY nodes to indicate the list of bridge groups the particular SPM node contributes to.

53.5.2.6.7 Supplementary information

- MNNODE is the bearer network provisioning point for the following SN07 nodes:
  - IW SPM
  - DPT SPM
  - MG4K
- As of SN07, in order for interworking bridges to be utilized, the BRDGCLLI for the IW must be included in a NETPATH used to interconnect two networks in table BEARNETS.
- Terminations to DPT will dynamically match the network of the DPT SPM to the network provsioned against the terminating trunk group in table TRKOPTS to properly select a DPT “terminal” on the correct network.
- In order to change the BEARNETS field of a DPM SPM node or a MG4K DPT, the node must be “Installtion Busy.” Additional restrictions/checks are being investigated.
- Checks for changing the BRDGCLLI are being investigated.
- IW SPM must be OOS (MANB, OFFL, SYSB) before changing the
  - MNNODE first, must either crosscheck that correct card is provisioned in MNCKTPAK or put something in the RTS code to block RTS unless the other data agrees.
  - MNCKTPAK change

— Datafill must be complete before the IW SPM can be RTS'd.

53.5.2.6.8 Translation verification other tools

MNNODE does not use translation verification tools.

53.5.2.7 Core Table SERVRINV

Server Inventory

53.5.2.7.1 Functional description

A new field, BEARNETS is added to the SERVRINV table to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default.

In addition, DPT GWCs should not be provisioned with a bearer network, as it is a signalling only network element.

53.5.2.7.2 Usage sequence and implications (CM Only)

The following provisioning dependencies is added :

BEARNETS

SERVRINV

53.5.2.7.3 Size

Table 18 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	Unchanged	Unchanged	tbd

53.5.2.7.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 19 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SERVRNAME	Unchanged	Unchanged	Unchanged	Unchanged
SERVRADDR	Unchanged	Unchanged	Unchanged	Unchanged
SERVREXEC	Unchanged	Unchanged	Unchanged	Unchanged
SERVRTONE	Unchanged	Unchanged	Unchanged	Unchanged

Table 19 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARNETS	**New**	**New subfield when DPT_INFO = DPT_ONLY**	**Vector of (BNETNAME and DEFAULT)**	**List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node.** **In SN07, only 1 network can be added, and it will be the default.** **DPT GWC's should not be provisioned with a bearer network.**
BNETNAME	**New**	**Subfield of BEARNETS.**	**BNETNAME provisioned in table BEARNETS.**	**Name of the bearer network from table BEARNETS.**
DEFAULT	**New**	**Subfield of BEARNETS**	**{Y, N}**	**Indicates whether the particular bearer network is the default network**
SERVROPTS	Unchanged	Unchanged	Unchanged	Unchanged

53.5.2.7.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Figure 12 Example Datafill

```
TABLE: MNNODE
SERVRNAME SERVRADDR SERVREXEC SERVRTONE BEARNETS SERVROPTS
---------------------------------------------------------
GWC 0     IP  47 192 48 24 (POTS POTSEX)  (KEYSET  KSETEX)  $
NORTHAA (PACKET_DEFAULT Y) $ $
```

53.5.2.7.6 Table release history update

Added BEARNETS field in SN07.

53.5.2.7.7 Supplementary information

- SERVRINV is the bearer network provisioning point for the following nodes, if the BEARNETS field contains a default network. If the GWC does not have a BEARNETS entry, the office default (the tuple in table BEARNETS with the default_packet_network option assigned) will be taken as the bearer network for the following agents.
  - IP trunking gateways (PVG, Audiocodes)
  - Logical groups
  - ABI lines and trunks
  - H.323 & Media Call Server 5200
  - UAS (for CALEA)
- DPT GWCs do not have a bearer network provisioning against them, as the DPT TIDs against the GWC do not have associated hardware. If a network is provisioned against DPT GWC, it will have no effect on call processing. DPT trunk groups get their bearer network from table TRKOPTS.
- Changes to the BEARNETS field in table SERVRINV should be made only via the GWC-EM GUI, although this will not be enforced in table control. Instead, the usual warning will be output from the table control interface when changes are attempted in this table: ‘Warning: Changes must be done via SESM node provisioning to avoid data corruption.”. The GWC itself has knowledge of the bearer fabric and the codecs supported on the fabric, so changing the bearer network through table control can have unpredictable results.
- Restrictions for changing the bearer network, where the FABRIC remains the same:
  - Impacts trunking queues only.
  - Take GWC OOS or make change and swact?
- Restrictions for changing the bearer network, where the FABRIC also changes:
  - Impacts trunks and lines that are already allocated.
  - Not allowed.
- In order for the BEARNETS field to be changed, all p-side nodes must be in an OOS state:
  - GWC trunk members.
  - Logical line groups - pathends associated dynamically.
  - ABI lines - pathends associated dynamically
  - ABI trunks - pathends associated dynamically

53.5.2.7.8 Translation verification other tools

SERVRINV does not use translation verification tools.

53.5.2.8 Core Table SERVSINV

Subtending Server Inventory

53.5.2.8.1 Functional description

A hook is added to the table control write code so that during an upgrade, if a DPT terminal group is added, the code will go into SERVRINV physical data and remove the default BEARNET that was added during the initial provisioning.

Under normal conditions, table SERVRINV is provisioned via the SESM or OSSDI interface, and is not provisioned via the MAP for a customer, so the BEARNETS information in SERVRINV will be correct the first time. On an ONP, we will assign all GWCs the default network, and then remove it for DPT groups, since the GWC cannot host both DPT and actual gateways, and the data does not apply to DPT GWCs.

53.5.2.8.2 Usage sequence and implications (CM Only)

The datafill order for table SERVSINV is unchanged

53.5.2.8.3 Size

Table 20 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVSINV	Unchanged	Unchanged	Unchanged

53.5.2.8.4 Fields/OIDs

The fields and field values for table SERVSINV are unchanged..

53.5.2.8.5 Datafill example

Unchanged.

53.5.2.8.6 Table release history update

Added ONP checks such that during TABXFER on a Trimodal upgrade, when a DPT group is added, the BEARNETS will be removed from the host GWC.

This check will not be enforced during normal provisioning sequence.

53.5.2.8.7 Supplementary information

DPT terminal groups are signalling only, and do not have any physical hardware associated. The DPT trunk group, via provisioning in table TRKOPTS, contains the bearer network information, and DPT "terminals" can be associated with any bearer network provisioned against the trunk group, as long as the signalling type matches.

53.5.2.8.8 Translation verification other tools

SERVSINV does not use translation verification tools.

53.5.2.9 Core Table TRKOPTS

Trunk Options.

53.5.2.9.1 Functional description

Unchanged.

53.5.2.9.2 Usage sequence and implications (CM Only)

The following dependency is added to the existing provisioning order:

BEARNETS

TRKOPTS

53.5.2.9.3 Size

Table 21 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	Unchanged	Unchanged	Refer to EI section after DSUM.

53.5.2.9.4 Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

```
>range
 1 OPTKEY            TRKOPTS_KEY
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
LOGICAL TUPLE TYPE: TRKOPTS_LOGICAL_TUPLE
>range 2
 2 OPTINFO           TRKOPTS_OPTINFO_VAR_AREA
TYPE IS TRKOPTS_OPTINFO_VAR_AREA   MULTIPLE WITH
        OPTION                     TRKOPTS_OPTION REFINEMENTS:
{DYNAMIC}                    MULTIPLE WITH
             SIGNALING             {ISUP,ISUPPLUS,SIPT}
             SIGNALING_NETWORK     {IP,SS7,STRK}
             BEARER_NETWORK        {IP,ATM,STRK}
             APPLICATION           {OC,POS,DPT,RAS,SIPBCPT,STRK}
             SIGNALING             REFINEMENTS:
             {SIPT}                MULTIPLE WITH
                  DEST_MGCNAME     MGCINV_KEY
                  TPROFILE         TPROFILE_KEY
                  ALT_HOST_MGCNAME VECTOR OF UP TO 32 CHAR'S
                  INTER_DOMAIN     {N,Y}
             {ISUPPLUS}            MULTIPLE WITH
                  CAPABILITY_SET   {1 TO 2}
             OTHERWISE             DEFAULT_DYN_SEL_AREA
{DPT}                   MULTIPLE WITH
             PROTOCOL         {BICC,SIPT}
           BEARER_NETWORK      VECTOR OF UP TO 32 CHAR'S
             PROTOCOL REFINEMENTS:
             {SIPT}                MULTIPLE WITH
                  DEST_MGCNAME     MGCINV_KEY
                  TPROFILE         TPROFILE_KEY
                  ALT_HOST_MGCNAME VECTOR OF UP TO 32 CHAR'S
                  INTER_DOMAIN     {N,Y}
             {BICC}            MULTIPLE WITH
                  CAPABILITY_SET   {1 TO 2}
```

Table 22 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Unchanged	No	Unchanged	Unchanged
OPTINFO	**Changed**	**No**	**Add DPT to list of valid OPTIONs**	**Add DPT to list of valid OPTIONs**
OPTION	**Changed**	**Selector subfield of OPTINFO**	**DYNAMIC**	**Added new DPT option and refinement.**

Table 22 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SIGNALING	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
SIGNALING_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
BEARER_NETWORK	Unchanged	Subfiled of DYNAMIC option	Unchanged	Unchanged
APPLICATION	**Changed**	**Subfiled of DYNAMIC option**	**{OC, POS, RAS, SPBCPT, STRK}**	**DPT Removed from valid entry range. Should now be provisioned as a DPT option.**
SIGNALING	Unchanged	Subfiled of DYNAMIC option	SIPT	Unchanged
DEST_MGCNAME	Unchanged	Subfield of SIPT signaling	Unchanged	Unchanged
TPROFILE	Unchanged	Subfield of SIPT signaling	Unchanged	Unchanged
ALT_HOST_MGCNAME	Unchanged	Subfield of SIPT signaling	Unchanged	Unchanged
INTER_DOMAIN	Unchanged	Subfield of SIPT signaling	Unchanged	Unchanged
SIGNALING	Unchanged	Subfiled of DYNAMIC option	ISUPPLUS	Unchanged (Should this be BICC now?)
CAPABILITY_SET	Unchanged	Subfield of ISUPPLUS signaling	Unchanged	Unchanged
SIGNALING	Unchanged	Subfiled of DYNAMIC option	OTHERWISE	Unchanged

Table 22 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	Selector subfield of OPTINFO	DPT	Remove DPT from list of valid APPLICATIONs
PROTOCOL	New	Subfiled of DPT option	{BICC, SIPT}	The DPT signalling protocol.
BEARER_NETWORK	New	Subfiled of DPT option	BNETNAME from table BEARNETS	The BNETNAME of a bearer network provisioned in table BEARNETS.
PROTOCOL	New	Subfiled of DPT option	SIPT	Subfields when protocol = SIPT.
DEST_MGCNAME	New	Subfield of SIPT protocol	MGCINV_KEY	Same as under the dynamic option.
TPROFILE	New	Subfield of SIPT protocol	TPROFILE_NAME	Same as under the dynamic option.
ALT_HOST_MGCNAME	New	Subfield of SIPT protocol	Vector of up to 32 chars.	Same as under the dynamic option.
INTER_DOMAIN	New	Subfield of SIPT protocol	N, Y	Same as under the dynamic option.
PROTOCOL	New	Subfiled of DPT option	BICC	Subfields when protocol = BICC (old ISUPPLUS)
CAPABILITY_SET	New	Subfield of ISUPPLUS protocol	{1 to 2}	Same as under the dynamic option.

53.5.2.9.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

Figure 13 Example Datafill

```
TABLE: TRKOPTS
OPTKEY          OPTINFO
----------------------------------------
DPTTRK DPT      DPT BICC NET_AAL1 1 (100 200) (300 400) $ 200
SIPTRK DPT      DPT SIPT NET_IP $ 200
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC $
```

53.5.2.9.6 Table release history update

- DPT is removed from APPLICATION field under the DYNAMIC option.
- DPT is added as a new OPTION.

53.5.2.9.7 Supplementary information

The signaling network field is not required for DPT. The signaling protocol implies the signaling network: BICC implies SS7, and SIPT implies IP.

The bearer_fabric provisioned for DPT in table TRKOPTS indicates the bearer fabric for a specific DPT trunk group, and a given DPT trunk group can only have one bearer fabric.

GWC DPT trunk “agents” (provisioned in table SERVSINV) will be associated with the DPT trunk group during call processing based on the signaling protocol only. Bearer fabric is not provisioned against DPT GWCs in table SERVRINV.

SPM DPT trunk “agents” (proavisioned in table MNNODE) will be associated with the DPT trunk group during call processing based on both the signaling protcol and the bearer network provisioned in table MNNODE.

53.5.2.9.8 Translation verification other tools

The following example shows the output from <ToolName> when it is used to verify <abbreviated name of table>.

<abbreviated name of table> does not use translation verification tools.

53.5.2.10 Core Table MNCKTPAK

Management Network Node Table

No sematice changes have been made to this table.

Additional validation checking has been added for when the GWM RM and ATM RM card provisioning, to ensure that the network implies by the card agrees with the bearer network provisioned against the node.

53.5.2.10.1 Functional description

Unchanged.

53.5.2.10.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

53.5.2.10.3 Size

Table 23 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNCKTPAK	Unchanged	Unchanged	Unchanged

53.5.2.10.4 Fields/OIDs

The following table lists fields/OIDs for MNCKTPAK.

Table 24 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CPKKEY	Unchanged	Unchanged	Unchanged	Unchanged
CPKINFO	Changed	CPKTYPE	GEM or ATM	Additional checking added to compare to the bearer network in table MNNODE.
PEC	Unchanged	Unchanged	Unchanged	Unchanged
RELEASE	Unchanged	Unchanged	Unchanged	Unchanged
LOAD	Unchanged	Unchanged	Unchanged	Unchanged

53.5.2.10.5 Datafill example

The following example shows sample datafill for table MNCKTPAK.

Figure 14 Example Datafill

```
SPM 0 0 9 ATM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
(PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $ NTLX73BA 01 ATC20AW
```

53.5.2.10.6 Table release history update

Additional network card validation checks added in SN07.

53.5.2.10.7 Supplementary information
When adding a network card, ensure that if a GEM card is being added, the SPM supports either a BEARNETS with FABRIC = IP or a BRDGCLLI that bridges a network with an IP FABRIC. Similarly, if adding an ATM RM, the network should be AAL1.

53.5.2.10.8 Translation verification other tools

MNCKTPAK does not use translation verification tools.

53.5.2.11 Core Tables OFRT, OFR2, OFR3, OFR4
Office Routing Tables

Same change applies to each

53.5.2.11.1 Functional description
Unchanged.

New CND/NOT selector condition of BEARNET, to allow conditional routing based on the originator's bearer network.

Changed the name of the PKT conditional selector to FABRIC, and increased the allowable FABRIC range from {ENET} to {ENET, AAL1, AAL2, IP}.

53.5.2.11.2 Usage sequence and implications (CM Only)
Tables must be datafilled in the following sequence:

BEARNETS

OFRT

53.5.2.11.3 Size
Not Changed

Table 25 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFRT	unchanged	unchanged	unchanged
OFR2	unchanged	unchanged	unchanged
OFR3	unchanged	unchanged	unchanged
OFR4	unchanged	unchanged	unchanged

53.5.2.11.4 Fields/OIDs
The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for PKTSEL.

If CND/NOT condition is BEARNET, will be prompted for NETSEL.

Table 26 OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT,**~~ TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT**~~, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	UNDEF[a], ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS

Table 26 OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

a. No trunk and line agent can belong to an network with fabric as “UNDEF”. Hence “UNDEF” fabric selector is blocked form being datafilled.

53.5.2.11.5 Datafill example

The following examples shows sample datafill for table OFRT.

Figure 15 CND BEARNET

```
TABLE OFRT
POS 99
100 (CND BEARNET DFLTTDM ST 901)
(CND BEARNET DFLTIP ST 902)
(CND BEARNET DFLTATM ST 903) $ $
```

Figure 16 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901)
   (CND FABRIC IP ST 902)
   (CND FABRIC AAL1 ST 903)
   (CND FABRIC AAL2 ST 904) $ $
```

53.5.2.11.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

53.5.2.11.7 Supplementary information

The above mentioned changes are applicable to all the routing tables OFR2, OFR3, OFR4, IBNRTE, IBNRT2, IBNRT3, IBNRT4 and

HNPACONT$RTEREF that have CND and NOT bound in as the route selector.
The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

53.5.2.11.8 Translation verification other tools

The following example shows the output from Traver when it is used to verify OFRT.

Figure 17 Traver example: with BEARNET Option

```
traver tr isupicitt 7211001 BEARNET MyAAL1NW b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
 . SUBTABLE STDPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 721 721 LRTE 1001
 . SUBTABLE RTEREF
 . 1001 T OFRT 1001
 .   . TABLE OFRT
 .   . 1001 CND BEARNET TDM_ENET ST 1002
 .   .      CND BEARNET MYAAL1NW ST 1003
 .   .   . SAME TABLE
 .   .   . 1002 S D ISUPITOG
 .   .   . EXIT SAME TABLE
 .   .      CND BEARNET MYIP4NW ST 1004
 .   . EXIT TABLE OFRT
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

53.5.2.12 Core Tables IBNRTn (IBNRTE, IBNRT2, IBNRT3, IBNRT4)

IBN Routing Table

53.5.2.12.1 Functional description

Unchanged

53.5.2.12.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

IBNRTE, IBNRT2, IBNRT3, IBNRT4

53.5.2.12.3 Size

Table 27 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNRTE	Unchanged	Unchanged	Unchanged
IBNRT2	Unchanged	Unchanged	Unchanged
IBNRT3	Unchanged	Unchanged	Unchanged
IBNRT4	Unchanged	Unchanged	Unchanged

53.5.2.12.4 Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for PKTSEL.

If CND/NOT condition is BEARNET, will be prompted for NETSEL.

Table 28 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			

Table 28 IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CNDSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT,**~~ TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS, RND,SNPA,EA,TOD,MIGRATE,NARS, COSMAP, NRR,SITE,CALLCHR,INTERLATA,~~**PKT**~~, TOPEAALT,TOPEAXFR,TOPEACLS,STS,**FABRIC,BEARNET**	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	UNDEF[a], ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
NETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

a. No trunk and line agent can belong to an network with fabric as “UNDEF”. Hence “UNDEF” fabric selector is blocked form being datafilled.

53.5.2.12.5 Datafill example

Similar to the above examples.

53.5.2.12.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

53.5.2.12.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

53.5.2.12.8 Translation verification other tools

Refer to TRAVER information under table OFRT.

53.5.2.13 Core Tables HNPACONT::RTEREF and FNPACONT::RTEREF

Subtable Route Reference from the Home Numbering Plan Area

Subtable Route Reference from the Foreign Numbering Plan Area

Changes are the same as for OFRn and IBNRTn.

53.5.2.13.1 Functional description

Refer to OFRn.

53.5.2.13.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

HNPACONT::RTEREF & FNPACONT::RTEREF (order between these is unchanged)

53.5.2.13.3 Size

Table 29 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
HNPACONT::RTEREF	Unchanged	Unchanged	Unchanged
FNPACONT::RTEREF	Unchanged	Unchanged	Unchanged

53.5.2.13.4 Fields/OIDs

Same changes as table OFRn.

53.5.2.13.5 Datafill example

Refer to table OFRn.

53.5.2.13.6 Table release history update

— CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.

— New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

53.5.2.13.7 Supplementary information

The bearer network of the originiator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

53.5.2.13.8 Translation verification other tools

Refer to OFRn.

53.5.2.14 GWC_NETWORK_CODEC_PROFILE

53.5.2.14.1 Functional description

This new table is used to store network codec profiles that created by customer. The profiles will be used when customer add GWC node. Please refer to DID document for details.

53.5.2.14.2 Fields

The following table lists fields of this table.

Table 30 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
~~Profile_Id~~	~~New~~	~~VARCHAR~~	~~This field is the primary key of this table. It is not allow to be NULL.~~
profilename	New	VARCHAR2 (32)	The name of the profile. It is not allow to be NULL. This field is the primary key of this table.
bearerpath	New	NUMBER	Indicates the bearer network fabric type. Refer to table “BEARERPATH_MAP“. The default value is “0”.
defaultcodec	New	NUMBER	Indicate the default codec. Refer to table “CODEC_MAP“. The default value is “0”.
preferredcodec	New	NUMBER	Indicate the preferred codec. Refer to table “CODEC_MAP“. The default value is “0”.
alternativecodec	New	NUMBER	Indicate the alternative codec. Refer to table “CODEC_MAP“. The default value is “0”.
packetizationinteger	New	NUMBER	Indicate the packetization rate. Refer to table “PACKETIZATION_MAP“. The default value is “0”.

Field	New/ Changed	Entry	Explanation and action
t38	New	NUMBER(1)	Indicate whether the T38 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
rfc2833	New	NUMBER(1)	Indicate whether the RFC2833 setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
comfortnoise	New	NUMBER(1)	Indicate whether the comfort noise setting is enabled. Available values are “0” and “1”. Number “0” indicates disabled, number “1” indicates enabled. The default value is “0”.
bearertypedefault	New	CHAR(1)	Indicate whether this profile is a default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is default profile for this bearer network type, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 default profile every bearer network fabric type.
networkdefault	New	CHAR(1)	Indicate whether this profile is network default profile. Available values are “Y” and “N”. Char “Y” indicates this profile is the default profile in network, char “N” indicates this profile is not the default one. This field can not be NULL. The default value is “N”. Please note that there will be up to 1 network default profile totally.

53.5.2.15 GWCNode

53.5.2.15.1 Functional description

This table is used to store attributes of GWC node. Two new fields will be added into this table. Please refer to DID document for details.

53.5.2.15.2 Fields

The following table lists fields of this table.

Table 1 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
Network_Instance	New	VARCHAR2 (32)	Indicates the name of the associated network instance.
Network_Codec_Profile_Name	New	VARCHAR2 (32)	Indicates the associated network codec profile. Refer to table “GWC_NETWORK_CODEC_PROFILE“.

53.5.2.16 GWCPROFILE

53.5.2.16.1 Functional description

This table is used to store attributes of Gateway Controller profile. One new field will be added into this table, which is used to indicate whether network instance is needed to be associated to this GWC or not.

53.5.2.16.2 Fields

The following table lists the new field of this table.

Table 2 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_INSTANCE_REQUIRED	New	CHAR(1)	Indicate whether network instance is needed to be associated to this GWC or not. Available values are “Y” and “N”. Char “Y” indicates need, char “N” indicates not need. The default value is “Y”. This field can not be NULL.

53.5.2.17 GATEWAYPROFILE

53.5.2.17.1 Functional description

This table is used to store attributes of Gateway profile. One new field will be added into this table, which is used to support the fabric type check when customer associate gateway to GWC node. Please refer to DID document for details.

53.5.2.17.2 Fields

The following table lists fields of this table.

Table 3 Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_FABRIC_RESTRICTION_LIST	New	Embedded table of "RestrictList_NT" type	The Name of this field is: Bearer fabric restriction list. This field can be NULL. This field would list the bearer fabrics to which the gateway is restricted. In most cases, this list will be empty and there will be no restriction. But for some special gateway (e.g. MG9000IP and ATM versions), the values would be provided.

53.6 Service Orders (SO) (CM & SESM)

Not applicable.

53.7 Software optionality control (SOC)

Not applicable.

53.8 Element Management

Prior to SN07, the SESM server could support only one bearer network fabric type (IP/AAL1/AAL2) at one time. As of SN07, each GWC will be associated with a beaer network instance, which defines the associated bearer network fabric type. This information will be provided by the customer as they add the GWC through the GWC-EM. In addition to the beaer fabric instance, GWC-EM will allow the cutomer to define multiple network codec "profiles" in the system and will allow the customer to select the desired profile as they add the GWC to the network.

53.8.1 New/modified GUIs

Table 31 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC-EM	Changed

53.8.2 GUI information

53.8.2.1 GWC-EM GUI

Gateway Controller Element Manager Graphical User Interface

53.8.2.1.1 Functional description

The GWC-EM database will be changed to include a new MIB table: GET_NETWORK_CODEC_PROFILE.

The following functionality is added to the GWC-EM:

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
   - — Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
   - — Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
   - — Change the associated network codec profile of one GWC node from GWC-EM GUI.

53.8.2.1.2 GUI usage and implications

GUIs must be used in the following sequence:

Current datafill order unchanged.

53.8.2.1.3 GUI size

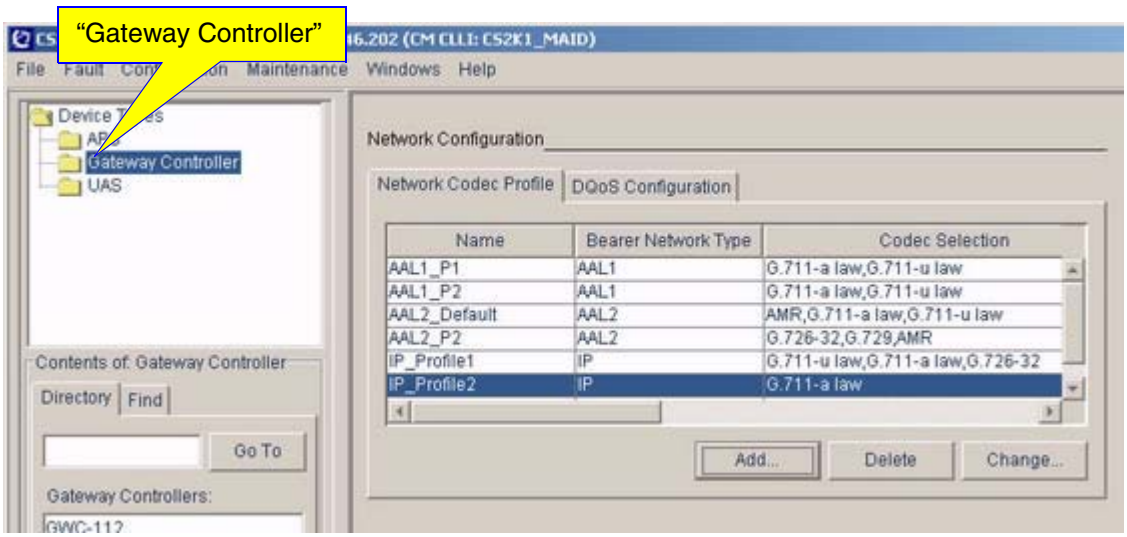
Table 32 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWC-EM	Unchanged	Unchanged	Unchanged

53.8.2.1.4 Usage Example: Display network codec profile

When customer click the “Gateway Controller” type from the device type tree at the left side, all network codec profiles will be displayed on the right side. (Please refer to “Figure 1 Network codec profile display panel”)

Figure 1 Network codec profile display panel



All existing codec profiles will be displayed in a table, each profile includes following parameters:

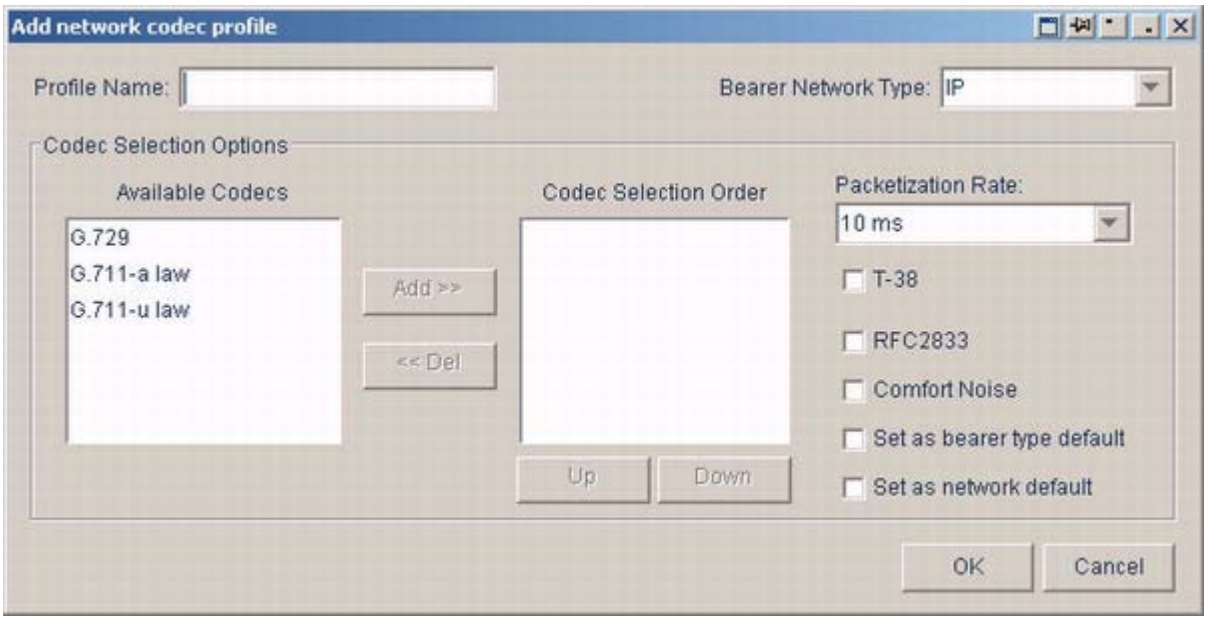
Table 4 Parameters of network codec profile

Parameter name	Description	Notes
Name	The name of the profile.	
Bearer Network Type	Indicates the bearer network fabric type.	
Codec Selection	Indicate the codecs used in this profile.	
Packetization rate	Indicate the packetization rate.	For IP bearer type only.
T-38	Indicate whether the T38 setting is enabled.	For IP bearer type only.
RFC2833	Indicate whether the RFC2833 setting is enabled.	For IP bearer type only.
Comfort noise	Indicate whether the comfort noise setting is enabled.	For IP bearer type only.
Default Profile	Indicate whether this profile is a default profile. Please note that there will be up to 1 default profile every bear network fabric type.	

53.8.2.1.5 Usage Example: Add network codec profile

Customer will be able to add one new network codec profile just by clicking the “Add” button, then a dialog “Add network codec profile” will be popped up. (Please refer to “Figure 2 Add network codec profile dialog”)

Figure 2 Add network codec profile dialog

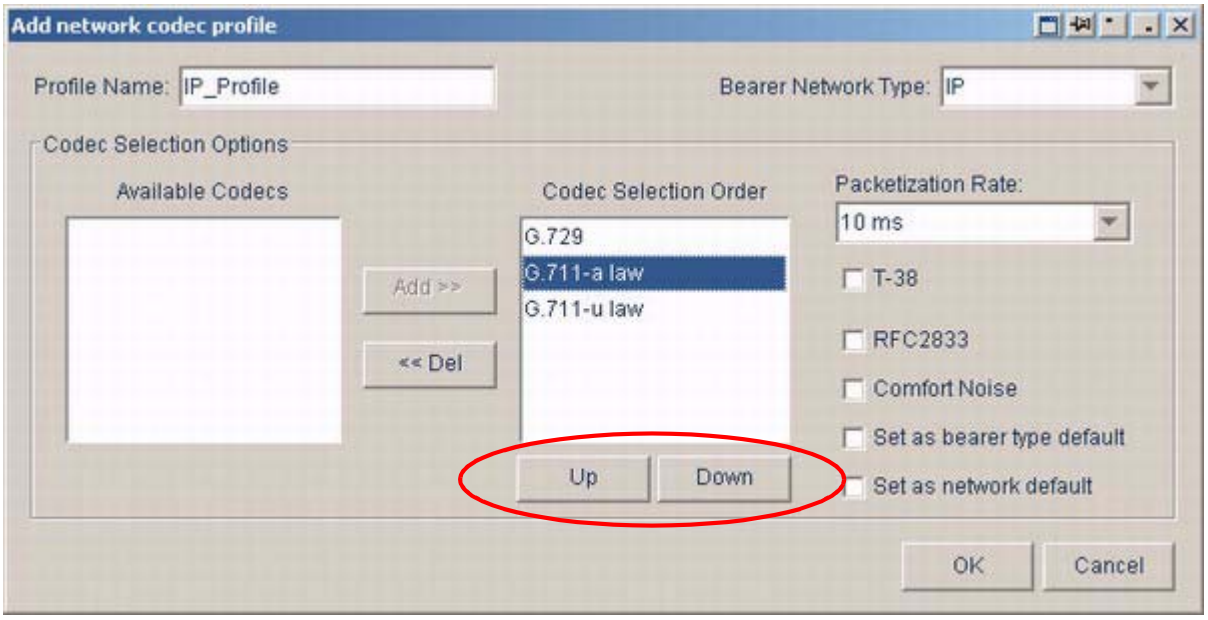


When customer select a bearer network type from the droplist box, the corresponding available codecs will be displayed below in the left list box. The available codec list may be different for different bearer network type.

Please note that the codec selecting is different from SN06 version. Customer won't select different codec for “Compression codec”, “Default codec” and “Alternative Codec” one by one. The available codecs will be listed at left side, customer should be able to select them just by highlighting codec item and clicking the “Add >>” button. Then the selected codec will be added into codec selection. Contrarily, customer could delete some codec from the selection by highlighting the codec item and clicking the button “<< Del”.

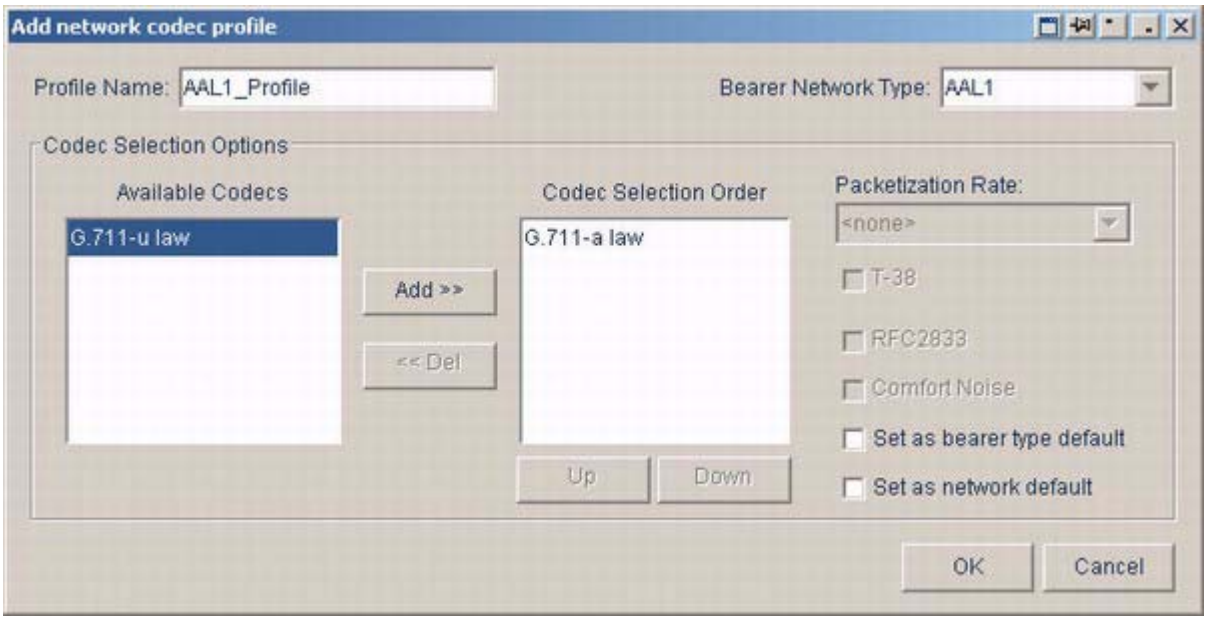
In the codec selection, the order of the codec determines how the device will treat them. For example, the first one will be mapped to “Compression codec”, the second one will be mapped to “Default Codec”, and the last one will be mapped to “Alternative Codec”. Additional, customer could change the order of codecs by highlighting the codec item and clicking the “Up” and “Down” buttons.

Figure 3 Change the order of codecs in the selection



Please note that parameters “Packetization Rate” and LCO options (T38, RFC2833, and Comfort Noise) are settings for IP bearer type only. If customer select “AAL1” or “AAL2” as the bearer network fabric type, these settings will be disabled.

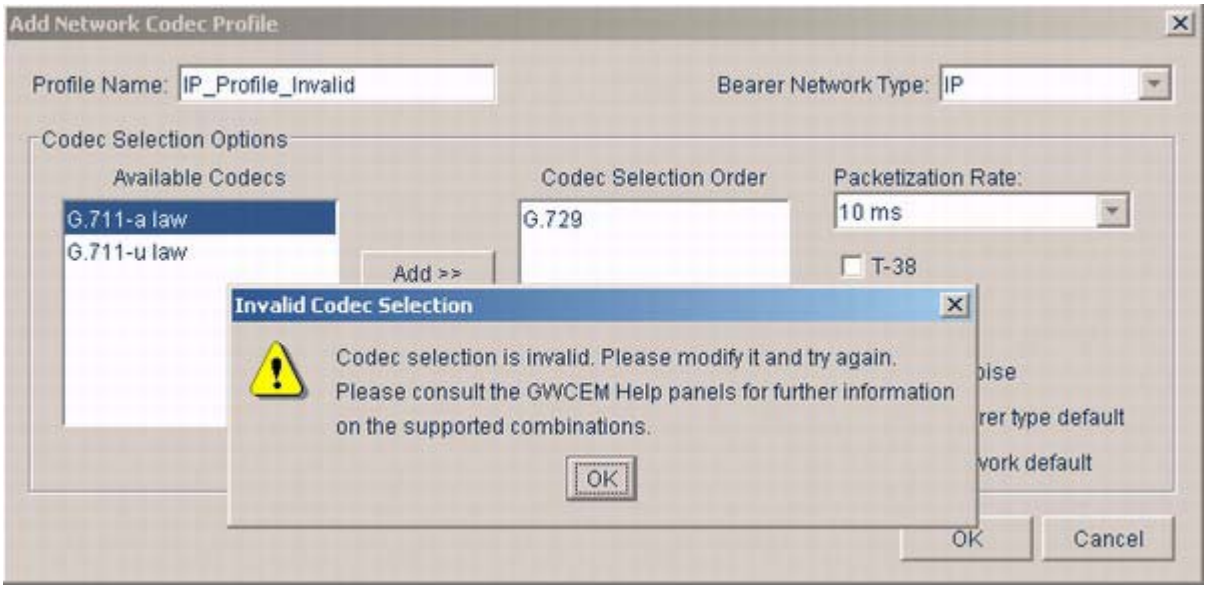
Figure 4 Select “AAL1” as the bearer network fabric type



Customer will be able to use the recommended codec setting by clicking the button “Recommended Codec Setting”, then the recommended setting will be restored into the dialog. Note that the recommended codec setting will be different for different bearer network type.

If customer select an invalid codec selection, alert dialog will be popped up. (Please refer to “Figure 5 Alert dialog for invalid codec selection”)

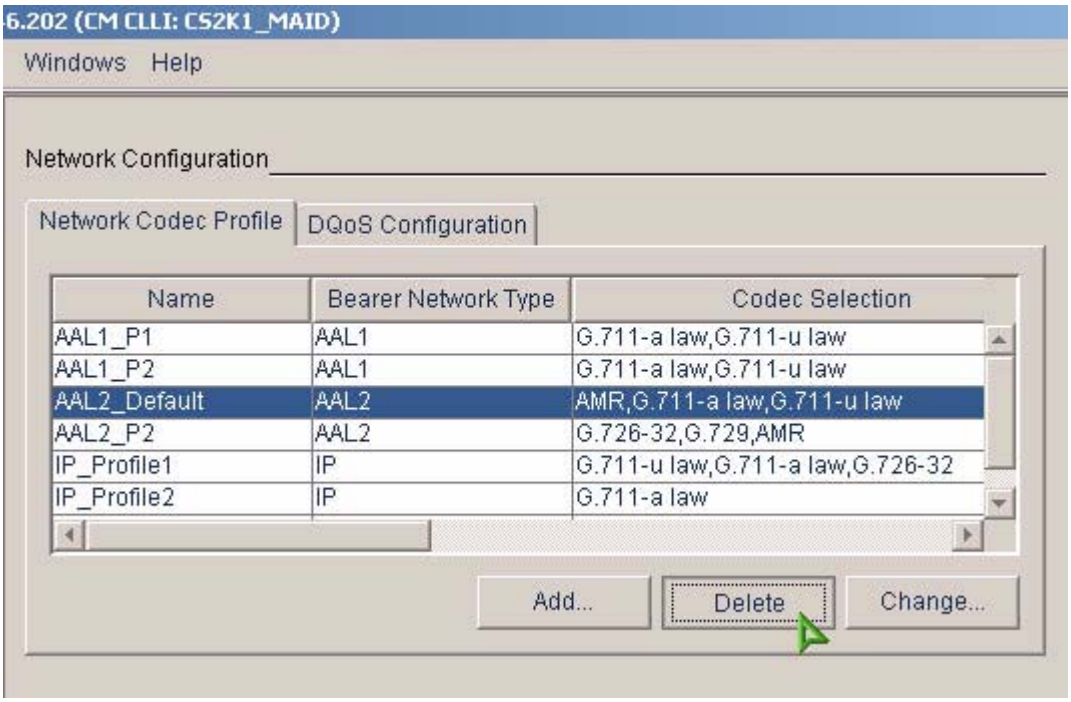
Figure 5 Alert dialog for invalid codec selection



53.8.2.1.6 Usage Example: Delete network codec profile

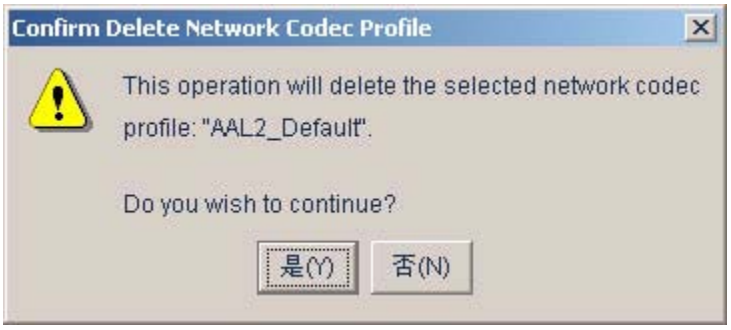
Customer will be able to delete one existing network codec profile just by highlighting the profile row from the table, and click the “Delete” button. (Please refer to “Figure 6 Delete existing network codec profile”)

Figure 6 Delete existing network codec profile



Once customer click the “Delete” button, one confirmation dialog will be popped up.

Figure 7 Delete network codec profile confirmation dialog

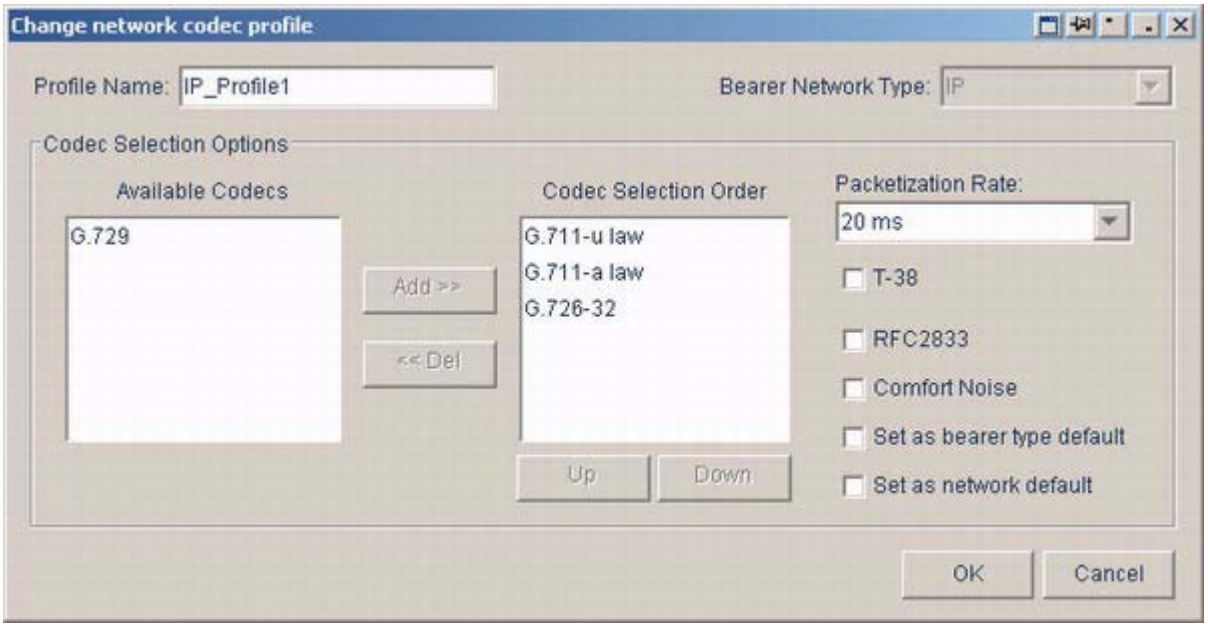


The operation result will be displayed in a pop-up dialog, and the codec profile table will be updated according to the result. Please note that if any GWC using this profile, the delete operation will be failed.

53.8.2.1.7 Usage Example: Change network codec profile

Customer will be able to change one existing network codec profile just by highlighting the profile row from the table, and click the “Change” button. Then the dialog “Change network codec profile” will be popped up. All parameters of the profile will be filled in the dialog. (Please refer to “Figure 8 Change existing network codec profile”)

Figure 8 Change existing network codec profile

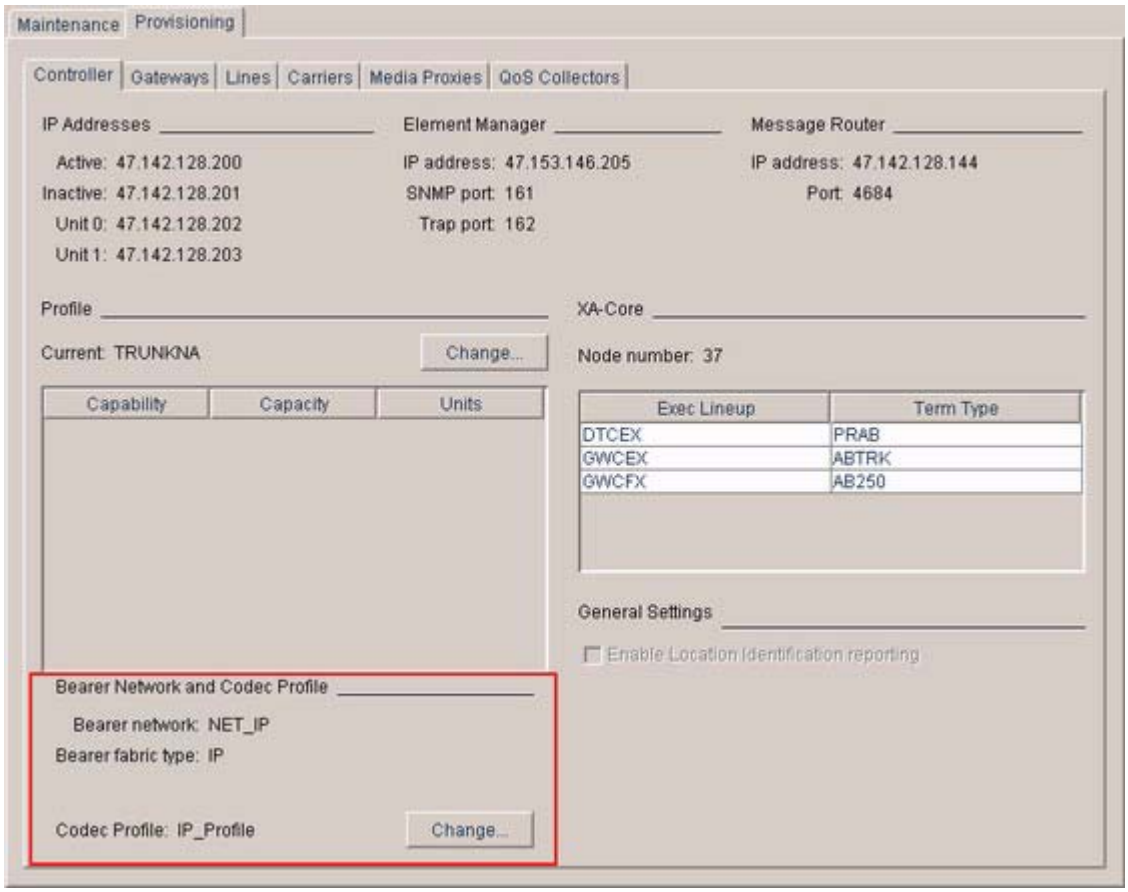


Note that the bearer network type of the profile is not allowed to be changed. Please refer to "53.8.2.1.5 Usage Example: Add network codec profile" section for how to change other parameters. Once the profile was updated successfully, these parameters will be updated into all GWCs using this profile.

53.8.2.1.8 Usage Example: Display GWC node

A new section will be added to the GWC provisioning panel to indicate the bearer network and codec profile configuration for the selected GWC.

Figure 9 Display GWC node



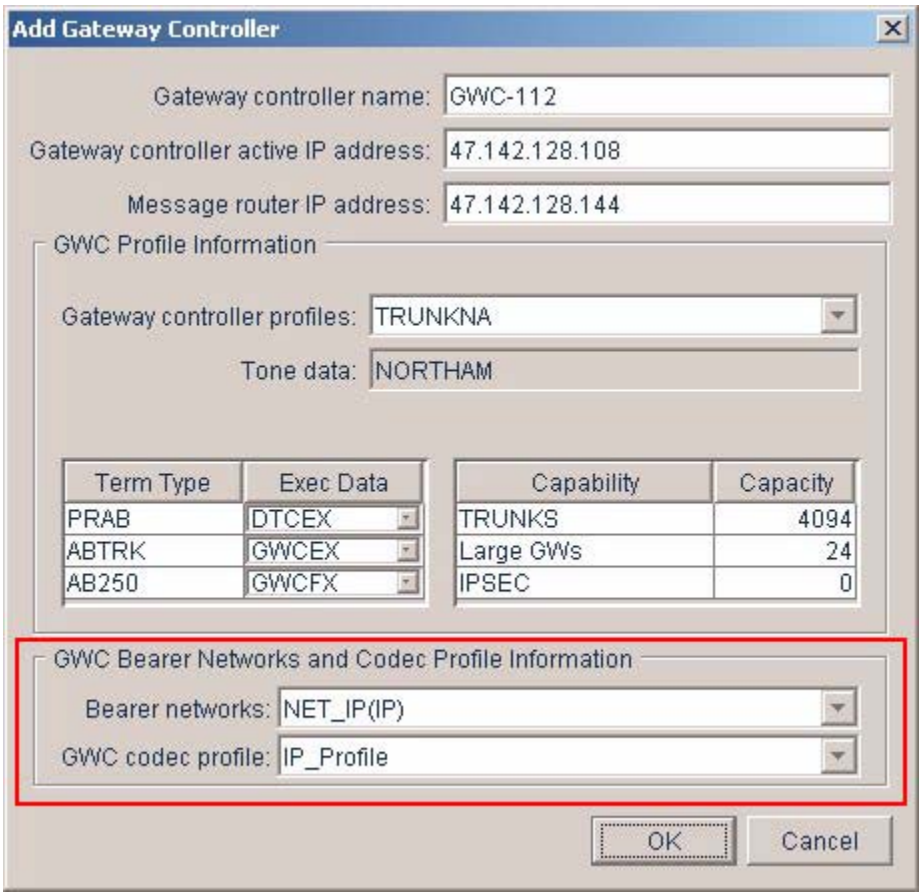
The new section includes two part, one is bearer network area and another is codec profile area. A “Change...” button will be added to the right of the codec profile fields to allow customer to change the codec configuration for the GWC.

This information will be displayed on the GUI with other GWC’s informations together while customer select a GWC from the GWC device list tree.

53.8.2.1.9 Usage Example: Add GWC node

Two new list boxes will be added to the “Add GWC Node” dialog to allow customers to select a specific bearer network instance and codec profile while a GWC is adding to the system.

Figure 10 Add GWC node



One of these two new box contains the bearer network list, another contains the codec profile list. The codec profile list must match the bearer network, that means, if customers select a bearer network instance belonging to “IP” bearer type, then the codec profile box will only contain the names of “IP” codec profiles; if customer select a “AAL1” bearer network instance, the codec profile box will be changed to only contain the “AAL1” codec profile names.

And if customers leave the codec profile box not selected, a default codec profile based on the bearer network type will be selected automatically.

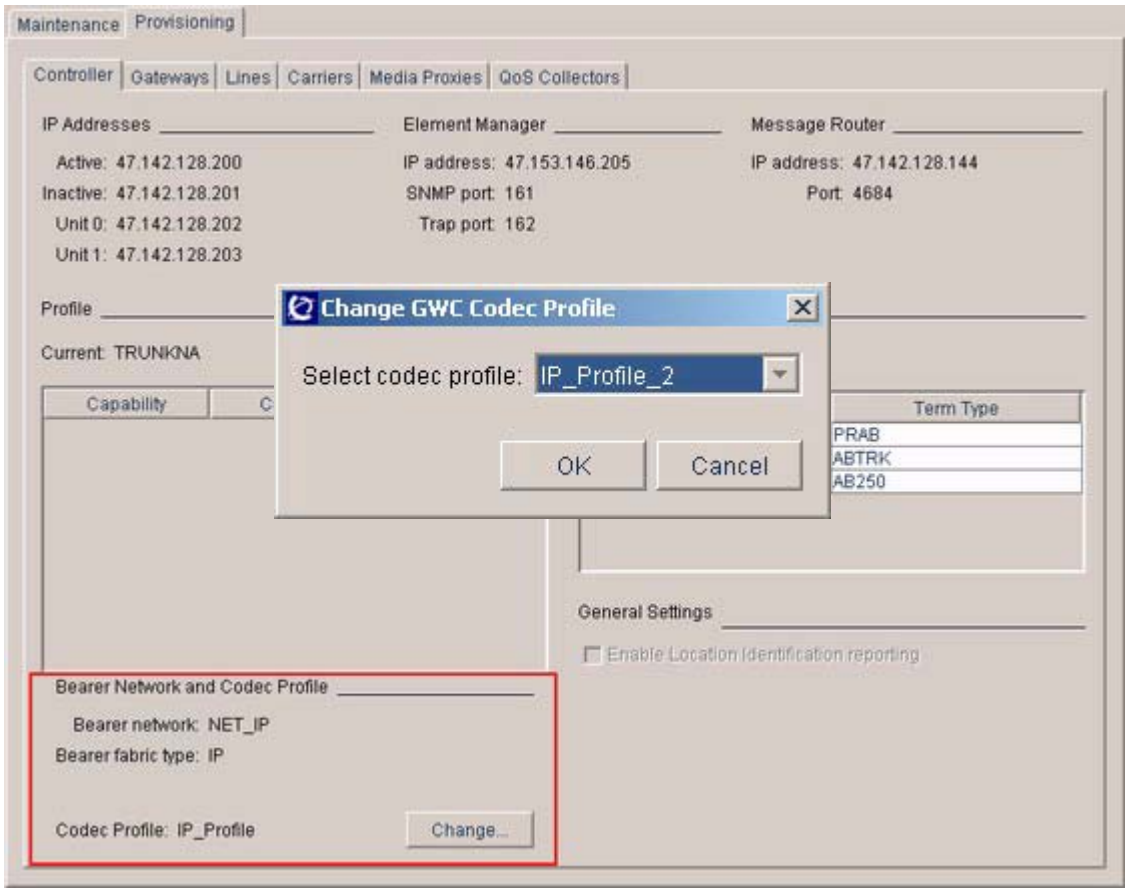
Once the addition operation has been performed successfully, a dialog like following will be pushed to the customer to indicate that the GWC was added to the system without errors.

Figure 11 Add GWC node result dialog

53.8.2.1.10 Usage Example: Change GWC network codec profile

When customers click the “Change...” button on the right of the codec profile fields on the GWC provisioning panel, a “Change Codec Configuration” dialog will be created like the following figure.

Figure 12 Change GWC's network codec profile



From this dialog, customers can select a different codec profile for the specific GWC even after the GWC has been provisioned already and a dialog with successful information will be displayed for customers if the operation has been performed without errors. Otherwise, a error message will be returned to the customers.

53.8.2.1.11 GUI release history update

1. Support the provisioning of multiple network codec profiles.
   - — Display network codec profile on GWC-EM GUI.
   - — Add network codec profile from GWC-EM GUI.
   - — Delete network codec profile from GWC-EM GUI.
   - — Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.

— Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.

— Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.

— Change the associated network codec profile of one GWC node from GWC-EM GUI.

53.8.2.1.12 Supplementary information

53.9 Command interface changes

53.9.1 Directory: TRAVER

53.9.1.1 Directory description

TRAnslations VERification.

53.9.1.2 Accessing directory: TRAVER

53.9.1.2.1 Access to directory or MAP level and return to CI

CI> TRAVER <traver options>

Traver is a single command interface rather than an envirnment that is entered. You are automatically returned to the CI level after execution of the command.

53.9.2 Command: TRAVER TR

53.9.2.1 Command type: unchanged

53.9.2.2 Command target: unchanged

53.9.2.3 Command availability: unchanged

53.9.2.4 Command description

Traver an originating trunk based with the digits provided. The originating trunk (TRAVER TR) command is changed as follows:

When encountering a CND FABRIC or CND BEARNET selector in the translations route, three options are created for determining the originator's bearer fabric or network in order to determine how to interprete the CND route selection.

- TRKMEM option: The fabric or network of the member specified will be used.

- NEW FABRIC option: Allows the user to specify the bearer fabric {ENET, AAL1, AAL2, or IP} of the specified trunk group.
- NEW BEARNET option: Allows the user to specify the bearer network (32 char vector identifying a BNETNAME provisioned in table BEARNETS) of the specifified trunk group.
- If none of the above options is specified, the TDM network will be assumed for the specified trunk group for non-DPT trunk groups.
- For DPT trunk groups, where none of the above options is specified, the bearer fabric or network will be obtained from table TRKOPTS.

53.9.2.5 Command syntax

Table 33 <CommandName> command parameters and variables

Command	Parameters and variables
TRAVER **TR**	Next par is: <CLLI> STRING Enter: <CLLI> [<CLLIOPT>] [<MBGOPTS>] [<TRIGOPT>] **[<TRKMEM>] [<FABRIC>] [<BEARNET>]** <DIGITS OR N FOR NO DIGITS> [<CDNIE>] [<NSF>] [<TNSIE>] [<OSAIE>] [<BC>] [<SR>] [<PI>] [<TRI>] [<NETINFO>] [<FINFO>] [<RPOAP>] [<RPOAS>] [<NOA>] [<AIN_OPTIONS>] [<AIN_INFO>] [<SCAIIN>]
Parameters and variables	Description
[<TRKMEM>}	Existing option. Input is unchanged. Will now be used to obtain the bearer network and bearer fabric to be used when making conditional translations decisions CND FABRIC or CND BEARNET.
[<FABRIC>]	New option. Allows user to specify the FABRIC (ENET, AAL1, AAL2, or IP) to be used in making conditional routing decisions based on FABRIC. This fabric will be used in making these decisions, even if the trunk group does not currently have members on the fabric specified.
[<BEARNET>]	New option. Allows user to specify the bearer network (up to 32 character BNETNAME provisioned in table BEARNETS) to use as the originating bearer network. This will also imply the FABRIC, since the FABRIC is a field in table BEARNETS. Both of these will be used when making conditional routing decsions based on FABRIC or BEARNET (CND selectors). The network specified will be used, even if the trunk group does not have members on that network.

53.9.2.6 Qualifications and warnings

- Non-DPT trunk groups can have members that are spread across the varioius networks. During call processing, an effort will be made to match the originator's network to a trunk member of a like network. Traver will not be enhanced to show this selection process.
- Line group originations (eg: HUNT, MDN, ACD) will use the network fabric of the primary member of the group to determine the network fabric.
- If the FABRIC or BEARNET option is used to specify the bearer network information of a trunk group, this information will be used in TRAVER to determine the routing, even if the trunk group does not have members in that network. This allows users to test the translations before adding members, but also allows for verification to pass when during call processing it could actually fail.
- If a user enters the FABRIC option, and a CND BEARNET is encountered in the translations, the FABRIC specified will be used for the CND FABRIC, and the TDM network will be used for CND BEARNET.

53.9.2.7 Responses

53.9.2.7.1 Undefined BEARNET specified

Since the user will be prompted for a 32 character string rather than a list of tuples provisioned in table BEARNET, an invalid entry should be met with a response indicating where to look for the valid information.

Table 34 MAP outputs with associated meanings and actions

Command TRAVER TR <trunk group CLLI> <digits> BEARNET <BNETNAME>
<RESPONSE>: <description> **Meaning:** The BEARNET name entered does not exist in table BEARNETS. **System or user actions:** Choose a BNETNAME of out table BEARNETS.
<RESPONSE>: <description> **Meaning:** **System or user actions:**

53.9.2.8 Example of TRKMEM option

Table 35 Usage examples for TRAVER TR command with TRKMEM option

Description of task:	traver tr isupicitt 7211001 **TRKMEM 1001** b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the trunk member data.
Command: MAP response:	WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 $. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 **. . CND BEARNET MYAAL1NW ST 1003** **. . . SAME TABLE** **. . . 1003 S D ATMTRK1** **. . . EXIT SAME TABLE** . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT ... ... AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++

Table 36 Usage examples for TRAVER TR command with BEARNET option

Description of task:	traver tr isupicitt 7211001 **BEARNET MyAAL1NW** b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the BEARNETS MyAAL1NW tuple entry.
Command: MAP response:	WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 $. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 **. . CND BEARNET MYAAL1NW ST 1003** **. . . SAME TABLE** **. . . 1002 S D ISUPITOG** **. . . EXIT SAME TABLE** . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT ... ... AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++

Table 37 Usage examples for TRAVER TR command with FABRIC option

Description of task:	traver tr isupicitt 7211001 **FABRIC AAL1** b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be the TDM BEARNET and the AAL1 FABRIC.
Command: MAP response:	WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 $. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND FABRIC AAL1 ST 1002 **. . CND FABRIC ENET ST 1003** **. . . SAME TABLE** **. . . 1002 S D ISUPITOG** **. . . EXIT SAME TABLE** . . CND FABRIC IP ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT ... ... AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++

53.10 Security

53.10.1 Network configuration

Document recommendations on confirguration of network edge devices (eg Firewalls, NATs NAPTs, Routers) as a result of this activity.

53.10.2 Key management

Not appicable.

53.10.3 Protocol

Not applicable.

53.10.4 Authentication

Not applicable.

53.11 Configuration Walkthrough

What are the provisioning steps/activities for this compoent? Include:

- Software and services
- messaging/signaling/protocols for component interaction
- provisioning routing
- other provisioning
- logical order and dependencies of component porvisioning
- SWACTS/RESTARTS.

54: Configuration (CN): A00003971

54.1 Hardware and Software Requirements

When a manual or force swact is issued on the CEM protection level MAP, if the command fails, a reason should be displayed along with the existing response.

When the RTS of a RM fails due to invalid load in the flash, a message is displayed. This existing message needs to be corrected to include a ‘have a’ to make it grammatically correct.

54.2 Command interface changes

54.2.1 Directory: <directory name/MAP level>

CEM PROT level (protection level)

54.2.1.1 Directory description

This level is used to perform a manual/forced sparing on a CEM.

54.2.1.2 Accessing directory: <directory name>

54.2.1.2.1 Access to directory or MAP level and return to CI

To access the protection level for a CEM unit, the following is used on the command interface.

mapci;mtc;pm;post spm <spm_number>;select cem <cem number>;prot

To quit and return to the CI level, the following command is used

quit mapci

54.2.2 Command: <Manual/Force>

54.2.2.1 Command description

Manual command performs a manual sparing action on the selected CEM unit.

54.2.2.2 Responses

In case of failure or refusal of the manual/force sparing command, a response is output indicating the reason for failure/refusal. The list of reason strings in the response is as shown below

No swact comment
Node not inservice
Will disrupt service
Maintenance in progress

No response from unit(s)
Data-sync blocked swact.
Clock-sync blocked swact.
Carriers not up.
Hardware failure.
Unit not active. Hence cannot switch activity.
Mate CEM blocking swact.
Mate not present. Node is in simplex mode
Mate not available. Check the state of mate unit
Unable to contact mate. Mate isolated
Mate unit's state is worse off
Mate unit has already assumed activity.
Swact in progress.

Figure 1, "MAP command response for CEM swact failure/refusal" shows the format of the response on the MAP.

Figure 1 MAP command response for CEM swact failure/refusal

```
 CM      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
 CM Flt   SysB   5 CkEr   2CSLk   2 SPM     .       .        .CS   1Crit    .
   M       M                      *C*                             *C*
 Protectn                        SysB    ManB    OffL    CBsy    ISTb    InSv
  0 Quit          PM               0       0       1       0      10       9
  2               SPM              0       0       0       0       4       0
  3                 CEM            0       0       0       0       2       0
  4
  5           SPM    4  ISTb
  6           Prot Grp: CEM          Mode: N/A              Schema: N/A
  7 Force     Sh0 U R A Stat   Sh0 U R A Stat   Sh1 U R A Stat   Sh1 U R A Stat
  8 Manual     1 -- - - ----    8  1 S A ISTb    1 -- - - ----    8 -- - - ----
  9            2 -- - - ----    9 -- - - ----    2 -- - - ----    9 -- - - ----
 10            3 -- - - ----   10 -- - - ----    3 -- - - ----   10 -- - - ----
 11            4 -- - - ----   11 -- - - ----    4 -- - - ----   11 -- - - ----
 12            5 -- - - ----   12 -- - - ----    5 -- - - ----   12 -- - - ----
 13 Select_    6 -- - - ----   13 -- - - ----    6 -- - - ----   13 -- - - ----
 14            7  0 W I ISTb   14 -- - - ----    7 -- - - ----   14 -- - - ----
 15           y
 16           SPM  4 CEM  1 Manual: Request has been submitted.
 17           SPM  4 CEM  1 SwAct: Command failed.<Failure reason string>
 18
  CMAP3
Time  19:51
```

54.2.3 Directory: <directory name/MAP level>

RM circuit pack level

54.2.3.1 Directory description

This level is used to perform maintenance commands on a RM.

54.2.3.2 Accessing directory: <directory name>

54.2.3.2.1 Access to directory or MAP level and return to CI

To access the RM level for the circuit pack, the following is used on the command interface.

mapci;mtc;pm;post spm <spm_number>;select <RM circuitpack ><RM unit number>

To quit and return to the CI level, the following command is used

quit mapci

54.2.4 Command: <RTS>

54.2.4.1 Command description

RTS command returns the circuit pack(s) to service.

54.2.4.2 Responses

In case of failure a message is displayed on the MAP.

If the failure is due to an invalid load in the flash, the following message is displayed on the MAP.

RM does not valid load in Flash**.**

This message has been changed to

RM does not have a valid load in Flash.

Figure 2, "MAP response for RTS failure due to invalid load in flash" shows the format of the response on the MAP.

Figure 2 MAP response for RTS failure due to invalid load in flash

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
AMDI     Istb   1IOCOS    .     7 SPM  4   RS    .     52CC.   1 Maj  ATM_21
 *C*              M             *C*     *C*             *C*      M      *C*
DLC                             SysB    ManB    OffL    CBsy    ISTb    InSv
 0 Quit          PM                4       0       0       0      20       5
 2               SPM               0       0       0       0       8       1
 3 ListSet         DLC             1       0       0       0       1       0
 4
 5            SPM    5 DLC   0  InAct  SysB
 6 Tst
 7 Bsy        Loc : Row B  FrPos  0 ShPos 59 ShId 1 Slot  1   Prot Grp : 1
 8 RTS       Default Load: DLC71AZ                          Prot Role: Working
 9 OffL       rts
10 LoadMod    SPM  5 DLC  0 RTS: Request has been submitted.
11            Severity:  Critical
12 Next       Problem : Restart failed, no load in Flash, please reload.
13 Select_
14 QueryMod   Action     : No Cardlist Available.
15 ListAlm    SPM  5 DLC  0 RTS: Command failed. RM does not have a valid load
16 Prot       in Flash.
17 SPERFORM
18
  MALINI
Time  04:31  >
```

55: Configuration (CN): A00003995

55.1 Upgrade Impact

55.1.1 Element Management Upgrade

This activity is responsible for handling modifications from the SN06.2 release to the SN07 release. No user interaction is required; the updates are automatically applied when the system is upgraded from SN06.2 to SN07.

Prior to the SN07 release, H.323 Endpoint Groups were listed in the Endpoint Group panel. With the updated phlosophy of adding this datafill as EPG carrier groups, previously provisioned H.323 endpoints are moved to the Carrier Panel. This is accomplished by updating the endpoint type field in the oracle database during the upgrade process and therefore no user interaction is required.

When the user provisions a H.323 GW, one of the required fields that must be datafilled is the reserved terminations. In 6.1 and 6.2, performing this action also filled in the Endpoint Groups that were assocaited with the GW. The user had the option of selecting any value as long as it was less than or equal to the maximum number of terminations allowed for that gateway type as defined by the GWs profile. A side affect of this was that more terminations then were requested would be provisioned if the user did not pick a multiple of 24/32 (North America/International). For example, a user had the option of filling in 34. If the user chose this number, the system would automatically provision 48/64 terminations. The count for the number of terminations listed in the gateway panel and stored internally was the value input by the user, not the actual count of terminations auto-generated. Because of unwanted side affects that are realized with the new “change” features provided by this activity, this value is converted to the actual number of terminations provisioned and will be updated internally and in the gateways display panel after an upgrade to SN07.

55.2 Data schema (DS) (CM, MIBS, RDB)

N/A

55.3 Service Orders (SO) (CM & SESM)

N/A

55.4 Element Management

55.4.1 New/modified GUIs and Functionality

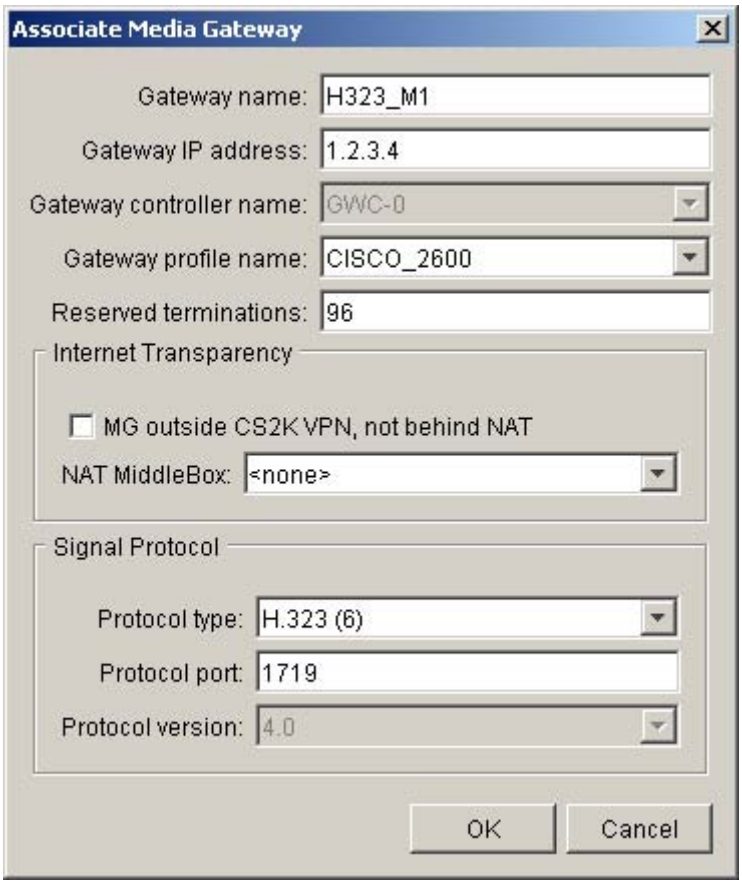
This section describes the Updates to GUIs affected by H.323 provisioning as a result of this activity. It lists dialogs that have cosmetic changes and the new functionality associated with them. For some cases, existing dialogs have not been changed but new functionality has been modified to accommodate updated H.323 provisioning. These dialogs are listed in this section too as a means to describe the new functionality.

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, DELETED
Associate Media Gateway	Changed functionality in SN07
GWC Provisioning Panel Endpoint Group Component	Deleted in SN07
Add Carrier	New for H.323 in SN07
GWC Provisioning Panel Carrier Component	New for H.323 in SN07
Trunks Associated with EPG Dialog	New for H.323 in SN07
Change Gateway	Changed in SN06.2, propped into SN07
Change Gateway IP address and Port Dialog	New in SN06.2, propped into SN07 by this activity
Change Gateway Capacity Dialog	New for H.323 in SN07
Disassociate Gateway	Changed functionality in SN07
Delete Carrier	New for H.323 in SN07

55.4.2 GUI information

55.4.2.1 GUI name: Associate Media Gateway



55.4.2.1.1 Functional description

The Associate Media GW dialog is displayed by using the configuration menu from the main CMT GUI or by selecting the “Associate” button from the GW panel of a GWC. This dialog is used to add H.323 GWs to the CMT which in turn populates the GWC device. The fields that are available with this dialog have not been updated in the SN07 release, however, functionality has been updated.

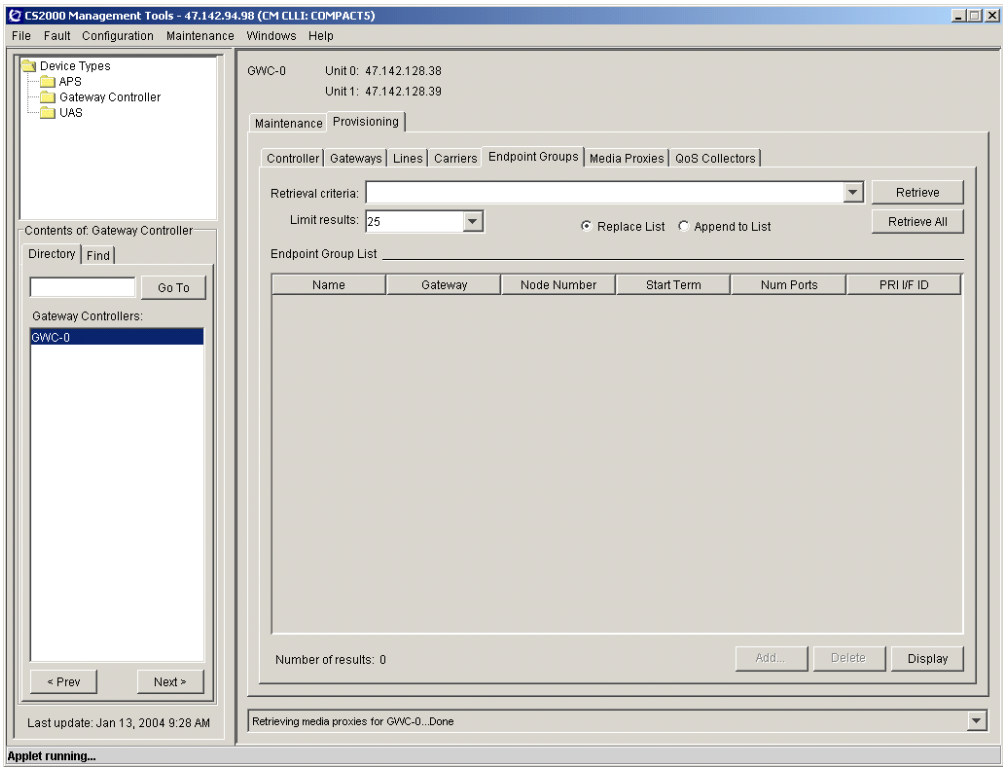
55.4.2.1.2 GUI usage and implications

Prior to the SN07 release, adding a H.323 GW to the system had unique functionality for H.323 GWs in that EPGs were automatically created and added to the system. The size of the EPGs (24 or 32) is dependent upon configuration options selected when the CMT product is initially installed. For North American systems, 24 is used, International systems, 32. As well, the number of EPGs provisioned was automatically calculated by the system so

that the appropriate number of groups were added as dictated by the mandatory "Reserved terminations" field. With pre-SN07 functionality, the location of the TIDs allocated was under system control.

In SN07, this behavior has been altered. EPGs are no longer automatically added. Because of this, a separate and additional step of adding the EPGs is required using the "Add carrier" operation. Details concerning the the add carrier operation are described in a later section of this document. In other words, adding a GW does not give the system terminations capability, it is only used as a means of adding a GW which must then be filled with terminations. Profiles for H.323 gateways have not been altered by this activity and the maximum capacities implemented in pre-SN07 releases are still applicable.

55.4.2.2 GUI name: EndpointGroup Panel



55.4.2.2.1 Functional description

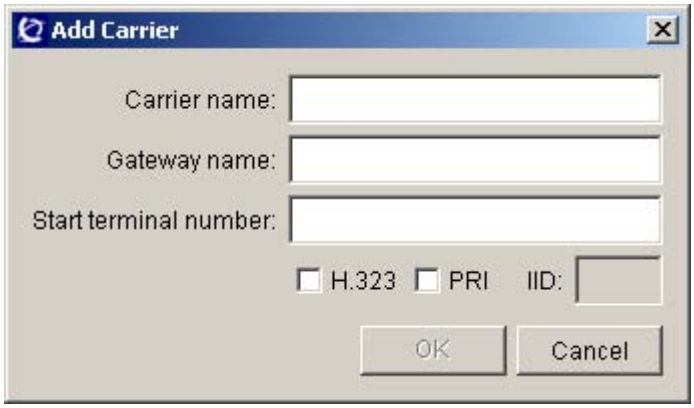
In pre-SN07 releases the Endpoint Groups panel was used to display the Endpoint Groups and attributes for H.323 GWs. Because of the updated philosophy of adding the EPGs using the carrier dialogs and logic, this panel is removed in the SN07 release and replaced by the Carriers Panel.

55.4.2.2.2 GUI usage and implications

Deleted in SN07.

Note: The GUI listed in this document shows the Endpoint Groups tab. This is a temporarily GUI depiction used for discussion purposes only. For the released version of the SN07 product the GWC tabs will not include this panel.

55.4.2.3 GUI name: Add Carrier



55.4.2.3.1 Functional description

The Add Carrier dialog is an existing dialog that is now available for provisioning H.323 EPGs. This dialog is displayed when the user selects the "add" button from the "Carriers Panel" and is used to add EPGs to H.323 GWs. As in previous releases, the size for the EPG is dependent upon the configuration set when installing the CMT. For North American systems, 24 is used, for International systems, 32 is used.

55.4.2.3.2 GUI usage and implications

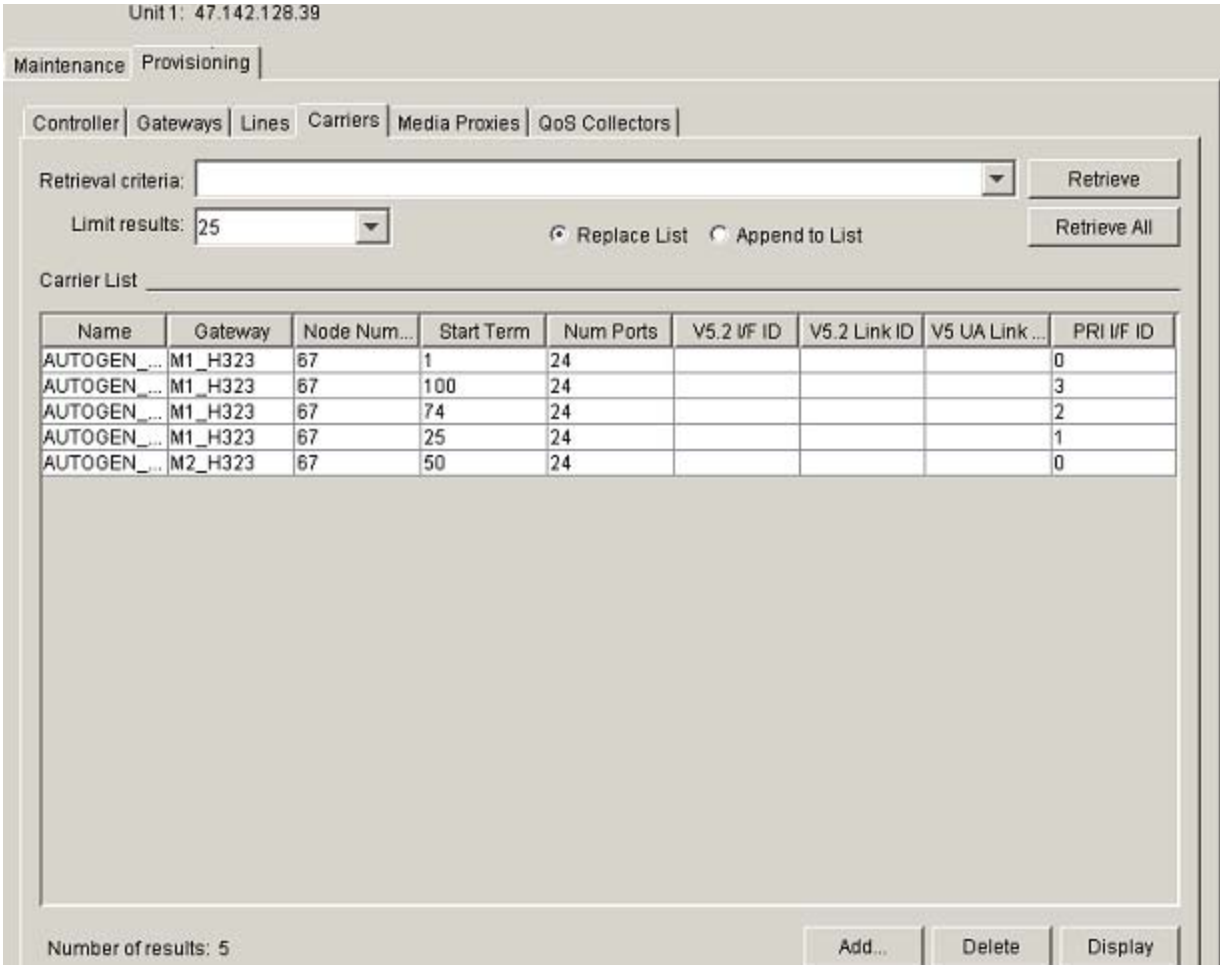
H.323 EPGs are added to the system as PRI groups and mimic the provisioning behavior of PRI carriers. However, in order to provision H.323 GW's, the H.323 checkbox should be selected. Selecting this checkbox causes the IID values to be auto generated by the system and are not required to be input by users. The naming convention "EPG" (described below) is unique to H.323 GWs and selection of the H.323 check box mandates that this convention is followed.

The Carrier name field is used to input the name of the EPG and this name must be unique within the GW. Naming conventions for these EPGs are fairly simple and should be input as follows; EPG_XXX where XXX represents an integer value between 000 and 999. The integer part must be zero padded and must be preceeded by the "_" character. Example datafill might be: EPG_000. Having duplicate EPGs names on different GWs is allowed.

The “Gateway name” field is used to indicate which GW the EPG is added to. In order for the operation to succeed, the GW specified must already exist within the system. Multiple EPGs can be added to a GW up to the maximum capacity as dictated by the reserved capacity that is provisioned for the GW. For example, a GW on a North American system that has a reserved capacity of 240 can have up to 10 EPGs added to it (10 EPGs x 24 EPs = 240 EPs).

The “Start terminal number” field is a new optional field made available in the SN07 release for all carrier service types. If this field is left blank the system will automatically pick which TIDs are used and how they map to the EPs. These values and mappings can be displayed using the Carrier Panel and Trunks Associated Dialog described later in this document. As well, the listAllCarriers XML interface (described later in this document) can be used to view these values. If the user puts a value in for the “Start terminal number” field, a contiguous block of 24 or 32 endpoints are created at the specified starting location. If a Contiguous range of TID locations following the starting location is not available, the operation will fail.

55.4.2.4 GUI name: Carrier Panel



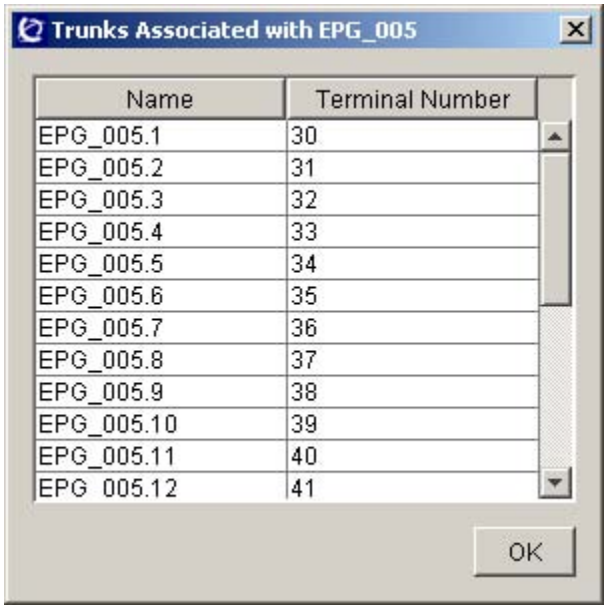
55.4.2.4.1 Functional description

The Carrier Panel is an existing panel that is now used for display of H.323 EPGs. This panel is made available by selecting the Carrier tab from the GWC Provisioning panel. In order to display H.323 EPGs provisioned, the "Retrieve" and "Retrieve All" buttons should be selected. Information such as the EPG name, associated GW, Node Number and Start Term, Number of Ports are pertinent to H.323 EPGs listed.

55.4.2.4.2 GUI usage and implication

This panel should be used to view attributes of EPGs associated with H.323 GWs. It replaces the Endpoint Group panel that was used to display this information prior to the SN07 release. In order to expand a EPG and see EP/TN mappings a EPG should be selected and the "Display" button should be selected. Details concerning this functionality are listed below.

55.4.2.5 GUI name: Trunks associated with EPG Expansion Dialog



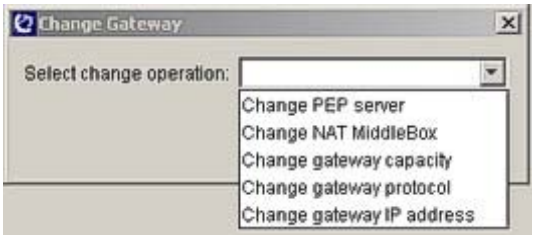
55.4.2.5.1 Functional description

The Trunks Associated dialog is an existing dialog that is now available for viewing H.323 EPG mappings in the SN07 release. This dialog is generated by selecting a EPG within the carriers panel and selecting the “display” button.

55.4.2.5.2 GUI usage and implications

This dialog is used to view EP/TN mappings for a H.323 EPG. It can be used to view system or user defined starting TN mappings. The naming conventions for individual EPs is EPG_XXX.xx where xx is an integer between 1 and 32.

55.4.2.6 GUI name: Change GW



55.4.2.6.1 Functional description

The Change GW dialog is used as a starting point to change attributes of an existing GW. A user picks the attribute they want to change from the combo box and the dialog is expanded to display appropriate fields. The Change GW dialog is a existing dialog that has been amended to include the “Change

gateway IP address" pick. This update was introduced in SN06.2 release and this activity is responsible for moving this functionality into the SN07 product.

In addition to the IP address pick update, new functionality of supporting "Change gateway capacity" is now supported for H.323 GWs.

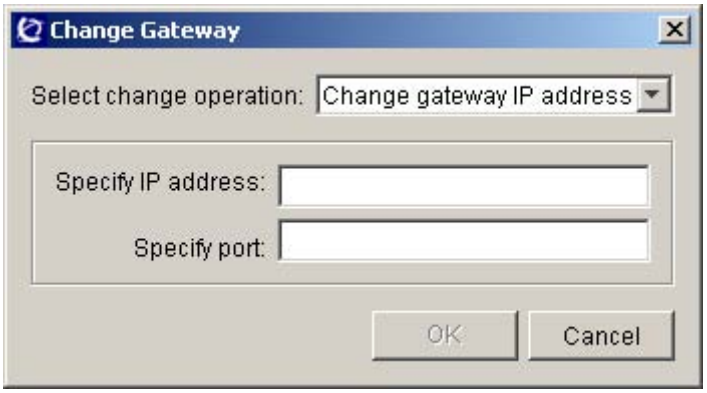
This dialog is rendered by selecting a GW from the GWs panel and selecting the "change" button. Once the dialog is display the combo box arrow is selected to display the pick.

55.4.2.6.2 GUI usage and implications

The change IP address and Port ability is restricted to updating H.323 GWs that are assocaited with a NAT. If an attempt is made to change the IP address of a GW type other than H.323, the operation will fail. In addition, only 1 GWs IP address or Port can be updated at a time using this operation. If multiple GWs are selected in the GWs panel the "Change gateway IP address" pick is not rendered.

> ***Note:*** The ability to change a small line GWs IP address to discovery is available by going to the gateways panel and selecting the "change" button with no GW rows selected. For this case, a unique change dialog is rendered that allows this operation. Changing a H.323 GWs IP address to discovery is not supported and has not been affected by this activity.

55.4.2.7 GUI name: Change GW IP address and Port



55.4.2.7.1 Functional description

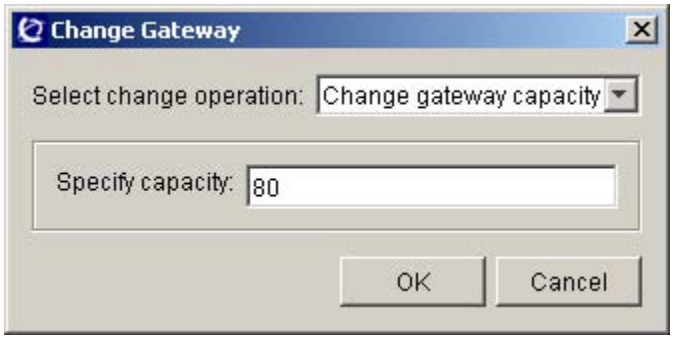
The Change GW IP address and Port dialog was newly added in the SN06.2 release and propped to SN07 by this activity. This dialog allows users to change the IP address and/or Port associated with a H.323 GW. Either the IP address, Port or both can be changed with a single transaction. However, in order to change only one of the values the other value must be input with the previously provisioned value. For example, if a user wanted to change the port

from 4721 to 4800 but leave the IP address alone they would put 4800 in the port field and the already provisioned IP address in the IP address field.

55.4.2.7.2 GUI usage and implications

This dialog allows users to change IP address and/or Ports associated with H.323 GWs. If a non-H.323 GW attempts to change the IP address to a value other than discovery, this action will fail. If a H.323 GW attempts to change the IP address to discovery, the operation will fail.

55.4.2.8 GUI name: Change GW Capacity



55.4.2.8.1 Functional description

The Change gateway capacity dialog is an existing dialog that is now available for changing the capacity of H.323 GWs in the SN07 release. This dialog is generated by selecting a GW or range of GWs within the GWs panel and selecting the “change” button. Once the dialog is rendered, select the “change gateway capacity” pick for the list made available by selecting the combo box arrow.

55.4.2.8.2 GUI usage and implications

Changing the H.323 GWs capacity in the SN07 release mirrors changing the capacity for other GW types. The capacity can be increased or decreased with the following constraints. A GWs capacity can be increased to the maximum allowed capacity for the GW type as dictated by the profile. A GWs capacity can be decreased to a smaller value as long as it is changed to a value greater than or equal to the number of EPs already allocated. If the user wants to change the capacity to a number smaller then the number of EPs provisioned, then the delete carriers operation should be used to remove EPG carrier group capacity and then the change capacity operation should be performed. Note that changing the capacity does not add or delete EPGs from the gateway. Changing the capacity only affects the potential number of EPs that can be provisioned. In order to add or remove EPGs, the “add carrier” or “delete carrier” operations should be used.

55.4.2.9 GUI name: Disassociate GW

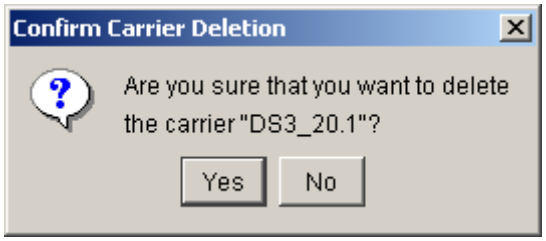
55.4.2.9.1 Functional description

The Disassociate Media Gateway is the dialog used to remove a GW from the CMT and subtending elements. It is displayed when the user selects a GW and pushes the Disassociate button on the GWs panel. The GUI for this operation has not been updated in the SN07 release, however, functionality associated with this action has.

55.4.2.9.2 GUI usage and implications

Disassociating a H.323 GW in a pre-SN07 release performed automatic deletions of EPGs and individual EPs dependent upon the EP state. In SN07, this behavior is modified so that H.323 GW deletions mirror behavior of other GW deletions in that if EPs exist for the GW, the transaction will fail. In other words, deletion of a H.323 GW requires the user to remove all EPGs from the GW prior to attempting the disassociate GW operation.

55.4.2.10 GUI name: Delete Carrier



55.4.2.10.1 Functional description

The Delete Carrier dialog is an existing dialog this is now available to remove H.323 EPGs from the system. This dialog is generated by going to the carriers panel, selecting a carrier, then pushing the “delete” button.

55.4.2.10.2 GUI usage and implications

This operation should be used to remove EPGs from a H.323 GW. In order to remove the EPG carrier group, the EPs within the group must be in an Installation Busy (INB) condition or the “unknown” state.

55.5 User Interface changes

55.5.1 OSSGate User Interface

This activity modifies support for the operations listed below:

- **changeMG capacity (updated functionality for H.323)**
- **changeMG IP address and port (new parameters)**
- **associateMG (updated functionality for H.323)**
- **addCarrier (updated functionality for H.323)**
- **queryEndpointGroup (deleted in SN07)**
- **listAllCarriers (updated functionality for H.323)**
- **disassociateMG (updated functinality for H.323)**
- **deleteCarrier (updated functinality for H.323)**

55.5.2 Terminology & Description of New Method Parameters

55.5.2.1 changeMG Capacity

This feature introduces the ability to change the EPG provisioning capacity of a previously provisioned GW. Although this capability currently exists for GWs using other protocols, it is now supported for GWs using the H.323 protocol.

55.5.2.2 changeMG IP address and Port

This feature introduces the ability to change the IP address and/or Port address associated with an existing GW. This capability is only supported for H.323 gateways that have a NAT associated with them and will be rejected if a GW with a protocol other than H.323 attempts the change IP/Port operation. Support for this operation allows a user to change the IP address, Port, or both with a single transaction.

55.5.2.3 assocMG

Associate MG is the OSSGate XML interface used to datafill new Media Gateways. The interface to associate a GW using XML was available with the introduction of H.323 functionality in the SN06.1 release. This interface has not been modified from the previous release. However, it is important to realize that functionality provided for this action is changed in SN07 in that EPGs are no longer automatically provisioned. In order to add EPGs to a GW, an additional step of adding a EPG carrier group or groups is required.

55.5.2.4 addCarrier

The addCarrier interface is an existing interface that is now used to provision H.323 EPGs. This command will add a EPG of size 24 or 32 endpoints to a

GW dependent upon market configuration. CMT systems that were configured as “North America” will provision EPGs of size 24, and systems configured as “International” will provision EPGs of size 32. In order to provision a GW with multiple EPGs, this command should be called repeatedly with a unique EPG.

This command will automatically grab the first available block of contiguous TID space TNs available on the GWC if the optional “FirstTN” tag is not used. The user can also specify the starting TID location if this field is included. This option gives users the ability to assign EPs to specific TID locations if they desire. If a firstTN tag is included, the system will assign a contiguous group of 24 or 32 EPs (system specific depending upon North American or International configuration) starting at the given location. If any of the TNs in the range are unavailable the command will fail.

55.5.2.5 queryEndpointGroup

This interface is removed in the SN07 release. In order to retrieve EP/TID mappings for H.323 GWs, the listAllCarriers interface should be used.

55.5.2.6 listAllCarriers

The list all carriers XML command is an existing command that should be used starting in SN07 to retrieve EP/TID mappings for H.323 GWCs. This command replaces the queryEndpointGroup command. Several filters (FILTER_ALL, FILTER_GWC, FILTER_MG, and FILTER_CARRIER) are available to limit the range of mappings to return. For details concerning use of these filter please refer to the XML examples and schema listings below.

55.5.3 XML - Example Commands and Responses

Listed below are syntax examples of the XML commands affected by the H.323 work in this activity. For some cases, new functionality is introduced. For others, new optional tags in reference to H.323 are highlighted. The XML in these examples are formatted for ease of understanding.

55.5.3.1 XML command examples for Change MG command

The following are examples of the enhanced change MG XML commands and the corresponding response messages for each operation supported by this activity. This activity introduces three new attributes that can be changed on an existing H.323 GW, the capacity, the IP address, and the Port. The capacity change is a stand alone operation while the IP address and Port changes can be combined.

Example format of **changeMG** IP address and/or Port

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
      <Command>
            <Interface>cs2kCfgMgrIf</Interface>
            <Methods>
                  < changeMG usn="1" version="1.0" >
                        <Parameters>
                              <mgUIName>H323_M1</mgUIName>
                              <mgIpAddr>22.44.66.88</mgIpAddr>
                              <mgProtocolPort>88</mgProtocolPort>
                        </Parameters>
                  </assocMG>
            </Methods>
      </Command>
</CommandList>
```

Example format of successful **changeMG** response to change IP address and Port:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
      <Response>
            <Interface>cs2KCfgMgrIf</Interface>
            <Methods>
                  <changeMG usn="1" version="1.0">
                        <RC>0</RC>
                        <mgUIName>H323_M1</mgUIName>
                        <MsgTxt>H323_M1 Change MG Successful.
                        All Change MG requests have been processed.</MsgTxt>
                  </changeMG>
            </Methods>
      </Response>
</CommandList>
```

Example format of failed **changeMG** response to change IP address and Port:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
      <Response>
            <Interface>cs2KCfgMgrIf</Interface>
            <Methods>
                  <changeMG usn="1" version="1.0">
                        <RC>43</RC>
                        <MsgTxt>* H323_M1 Change MG Failed - Invalid MG Name
                        All Change MG requests have been processed.</MsgTxt>
                  </changeMG>
            </Methods>
      </Response>
</CommandList>
```

Example format of **changeMG** Capacity

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
        <Command>
                <Interface>cs2kCfgMgrIf</Interface>
                <Methods>
                        < changeMG usn="1" version="1.0" >
                                <Parameters>
                                        <mgUIName>H323_M1</mgUIName>
                                        <reservedTerminations>500</reservedTerminations>
                                </Parameters>
                         </assocMG>
                </Methods>
        </Command>
</CommandList>
```

Example format of successful **changeMG** response to change Capacity :

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Response>
                <Interface>cs2KCfgMgrIf</Interface>
                <Methods>
                        <changeMG usn="1" version="1.0">
                                <RC>0</RC>
                                <mgUIName>H323_M1</mgUIName>
                                <MsgTxt>H323_M1 Change MG Successful.
                                All Change MG requests have been processed.</MsgTxt>
                        </changeMG>
                </Methods>
        </Response>
</CommandList>
```

Example format of failed **changeMG** response to change Capacity

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Response>
                <Interface>cs2KCfgMgrIf</Interface>
                <Methods>
                        <changeMG usn="1" version="1.0">
                                <RC>43</RC>
                                <MsgTxt>* H323_M1 Change MG Failed - Invalid MG Name
                                All Change MG requests have been processed.</MsgTxt>
                        </changeMG>
                </Methods>
        </Response>
</CommandList>
```

55.5.3.2 Command Examples for Associate MG command

The command syntax for assocMG command has not changed from prior releases in reference to adding H.323 GWs. The syntax is listed here as a convenience.

Example format of an **assocMG** command

```
<?xml version="1.0" encoding="UTF-8"  ?>
<CommandList>
  <Command>
   <Interface>cs2kCfgMgrIf</Interface>
   <Methods>
   <assocMG usn="1" version="1.0">
      <Parameters>
            <mgUIName>H323_M1</mgUIName>
            <mgProfileName>CISCO_2600</mgProfileName>
            <mgIpAddr>47.49.23.43</mgIpAddr>
            <mgProtocolType>6</mgProtocolType>
            <mgProtocolVersion>4.0</mgProtocolVersion>
            <mgProtocolPort>2427</mgProtocolPort>
            <gwcUIName>GWC-0</gwcUIName>
            <reservedTerminations>200</reservedTerminations>
      </Parameters>
   </assocMG>
  </Methods>
 </Command>
</CommandList>
```

55.5.3.3 Command Examples for Add Carrier command

The addCarrier command is an existing XML interface that is now used to provision H.323 EPGs. After adding a H.323 GW this command should be used to populate the terminations. The firstTN tag is optional and is used to dictate the starting location of a contiguous block of 24 or 32 EPs.

Example format of an **addCarrier** command **with optional firstTN** tag**:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
      <Command>
            <Interface>EndptGrpProvIf</Interface>
            <Methods>
                  <addCarrier usn="1" version="1.0" >
                        <Parameters>
                              <mgName>H323_M1</mgName>
                              <carrierName>EPG_001</carrierName>
                              <svcData>
                                 <H323 />
                              </svcData>
                              <firstTN>649</firstTN>
                        </Parameters>
                  </assocMG>
            </Methods>
      </Command>
</CommandList>
```

Example format of an **addCarrier** command **without optional firstTN** tag

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
        <Command>
                <Interface>EndptGrpProvIf</Interface>
                <Methods>
                        <addCarrier usn="1" version="1.0" >
                                <Parameters>
                                        <mgName>H323_M1</mgName>
                                        <carrierName>EPG_001</carrierName>
                                        <svcData>
                                           <H323 />
                                        </svcData>
                                </Parameters>
                        </assocMG>
                </Methods>
        </Command>
</CommandList>
```

Example format of successful **addCarrier** response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Response>
                <Interface>EndptGrpProvIf</Interface>
                <Methods><addCarrier usn="1" version="1.0">
                        <ReturnData>
                                <Row><firstTID>649</firstTID>
                                <numberOfTids>24</numberOfTids></Row>
                                <RC>0</RC>
                                <MsgTxt>Add CARRIER operation was successful</MsgTxt>
                        </ReturnData>
                </Methods>
        </Response>
</CommandList>
```

Example format of failed **addCarrier** response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Response>
                <Interface>EndptGrpProvIf</Interface>
                <Methods><addCarrier usn="1" version="1.0">
                        <MethodName>queryMG</MethodName>
                        <RC>4</RC>
                        <MsgTxt>EGP> The mgName does not have corresponding MG UI
name <MsgTxt>
                </Methods>
        </Response>
</CommandList>
```

55.5.3.4 Command Examples for List All Carriers command

The list all carriers command is an existing command that is now used to view mappings for H.323 EPGs. This command replaces the queryEndpointGroup command that was used in pre-SN07 releases. Several different tag filters are available to determine the scope of listings. For more details concerning other filters, refer to the schema later in this document.

Example format of **listAllCarriers** command with GWC filter**:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
        <Command>
            <Interface>EndptGrpProvIf</Interface>
            <Methods>
                    <listAllCarriers usn="1" version="1.0">
                    <Parameters>
                            <FILTER_GWC>
                               <gwcName>GWC-6</gwcName>
                            </FILTER_GWC>
                    </Parameters>
                    </listAllCarriers>
            </Methods>
        </Command>
</CommandList>
```

Example format of successful **listAllCarriers** response

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
<Response>
<Interface>EndptGrpProvIf</Interface>
<Methods>
<listAllCarriers usn="1" version="1.0">
<ReturnData>
<gwc name="GWC-6">
        <mg name="H323_M1">
<carrier name="EPG_001">
<svcData>
<service>PRI</service>
<IID>7</IID>
</svcData>
<endptList>
<endPt name="EPG_001.1"><tid>36 1</tid></endPt>
<endPt name="EPG_001.2"><tid>36 2</tid></endPt>
:
:
<endPt name="EPG_001.22"><tid>36 22</tid></endPt>
<endPt name="EPG_001.23"><tid>36 23</tid></endPt>
<endPt name="EPG_001.24"><tid>36 24</tid></endPt>
</endptList>
</carrier>
<carrier name="EPG_002">
<svcData>
<service>ISUP</service>
</svcData>
<endptList>
<endPt name="EPG_002.1"><tid>36 1401</tid></endPt>
<endPt name="EPG_002.2"><tid>36 1402</tid></endPt>
<endPt name="EPG_002.3"><tid>36 1403</tid></endPt>
:
:
<endPt name="EPG_002.22"><tid>36 1422</tid></endPt>
<endPt name="EPG_002.23"><tid>36 1423</tid></endPt>
<endPt name="EPG_002.24"><tid>36 1424</tid></endPt>
</endptList>
</carrier>
</mg>
</gwc>
<RC>0</RC>
<MsgTxt>
Retrieval of Carriers Successfully Completed. </MsgTxt>
</ReturnData>
</listAllCarriers>
</Methods>
</Response>
</CommandList>
```

Failed response to **listAllCarriers** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
      <Response>
            <Interface>EndptGrpProvIf</Interface>
            <Methods>
                <listAllCarriers usn="1" version="1.0">
                    <MethodName>listAllCarriers</MethodName>
                    <RC>4</RC>
                    <MsgTxt> The gwcName does not have corresponding Gateway
Controller</MsgTxt>
                </listAllCarriers>
            </Methods>
      </Response>
</CommandList>
```

55.5.3.5 Command examples of Disassociate MG

Tags values for the disAssocMG XML command are not changed in the SN07 release. Functionality for issuing this command has changed, however. Command syntax is listed here as a convenience to the reader.

Example format of **disAssocMG** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
      <Command>
          <Interface>cs2kCfgMgrIf</Interface>
          <Methods>
                  <disAssocMG usn="1" version="1.0">
                  <Parameters>
                        <mgUIName>H323_M1</mgUIName>
                  </Parameters>
                  </listAllCarriers>
          </Methods>
      </Command>
</CommandList>
```

55.5.3.6 Command examples of Delete Carrier

Tags values for the delete carrier XML command are not changed in the SN07 release. Functionality for issuing this command has changed, however. Command syntax is listed here as a convenience to the reader.

Example format of **Delete Carrier**

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
        <Command>
            <Interface>EndptGrpProvIf</Interface>
            <Methods>
                    <deleteCarrier usn="1" version="1.0">
                    <Parameters>
                            <mgName>H323_M1</mgName>
                            <carrierName>EPG_000</carrierName>
                    </Parameters>
                    </listAllCarriers>
            </Methods>
        </Command>
</CommandList>
```

55.5.4 XML Schema Listings for affected H.323 commands

55.5.4.1 Change MG

The XML tags for the changeMG have been changed in the SN07 release. In SN06.2 and prior releases, the choice of “profile” or “capacity” was listed. Underlying server code did not support “profile” changes using this command so this tag has been removed. New tags “mgIpAddr” and “mgProtocolPort” have been added as optional parameters. With the new schema, the user has the ability to include the reserved termination choice or the IP address and/or Port choice, but, cannot list both choices within a single transaction. Since the IP address and Port tags have been made optional, the user can include either or both within a single transaction. Note that failure to include any of the choice tags will result in a failed operation.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!--
*****************************************************************************
*************** -->
 <!-- * Define changeMG Method Parameters -->
 <!--
*****************************************************************************
*************** -->
 <xsd:complexType name="changeMGMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="changeMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="changeMGParamsType">
  <xsd:sequence>
    <xsd:sequence>
     <xsd:element name="mgUIName" type="NoSpaceNameType" />
    </xsd:sequence>
<xsd:choice >
      <xsd:element name="reservedTerminations" type="ReservedTerminationsType" />
      <xsd:sequence>
```

```
          <xsd:element name="mgIpAddr" type="IPAddressType" minOccurs="0"  />
          <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" minOccurs="0" />
        </xsd:sequence>
</xsd:choice>
   </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

55.5.4.1.1 Tag value definitions listed in cs2kcfgbase:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
              version="1.0"
              xml:lang="en" >
  <!--
*************************************************************************************
*************** -->
  <!-- ** Global Attribute Groups Used by all schemas  -->
  <!--
*************************************************************************************
*************** -->

  <!-- ********************************************************************** -->
  <!-- * Define Common Usn_Version Attribute Group-->
  <!-- ********************************************************************** -->
  <xsd:attributeGroup name="Usn_VersionAttrbGroup" >
    <xsd:attribute name="usn" type="xsd:integer" use="required" />
    <xsd:attribute name="version" type="xsd:decimal" default="1.0" use="optional" />
  </xsd:attributeGroup>
  <!--
*************************************************************************************
*************** -->
  <!-- ** Global Complex Types Used by all schemas -->
  <!--
*************************************************************************************
*************** -->
  <!--
*************************************************************************************
*************** -->
  <!-- * Global Simple Types Used or Useable by all schemas follows: -->
  <!--
*************************************************************************************
*************** -->
  <!--
*************************************************************************************
*************** -->
  <!-- * Define No Space Name Type -->
  <!--
*************************************************************************************
*************** -->
  <xsd:simpleType name="NoSpaceNameType">
    <xsd:restriction base="xsd:token">
      <xsd:minLength value="1" />
      <xsd:pattern value="\S{1,32}" />
    </xsd:restriction>
  </xsd:simpleType>
  <!--
*************************************************************************************
*************** -->
  <!-- * Define IPAddressType-->
  <!--
*************************************************************************************
*************** -->
  <xsd:simpleType name="IPAddressType">
    <xsd:restriction base="xsd:string">
```

```
    <xsd:pattern value="\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}"/>
   </xsd:restriction>
  </xsd:simpleType>
  <!--
*****************************************************************************************
*************** -->
  <!-- * Define MGProtocolType-->
  <!--
*****************************************************************************************
*************** -->
  <xsd:simpleType name="MGProtocolType">
   <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="6" />
    <xsd:pattern value="\d{1}" />
   </xsd:restriction>
  </xsd:simpleType>
  <!--
*****************************************************************************************
*************** -->
  <!-- * Define GWCNameType-->
  <!--
*****************************************************************************************
*************** -->
  <xsd:simpleType name="GWCNameType">
   <xsd:restriction base="xsd:string">
    <xsd:pattern value="GWC-\d\d?\d?" />
   </xsd:restriction>
  </xsd:simpleType>
  <!--
*****************************************************************************************
*************** -->
  <!-- * Define ReservedTerminationsType -->
  <!--
*****************************************************************************************
*************** -->
  <xsd:simpleType name="ReservedTerminationsType">
   <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="6400" />
   </xsd:restriction>
  </xsd:simpleType>
   <!--
*****************************************************************************************
*************** -->
  <!-- * Define IpPortTypeType-->
  <!--
*****************************************************************************************
*************** -->
  <xsd:simpleType name="IpPortType">
   <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="65535" />
   </xsd:restriction>
  </xsd:simpleType>
   <!--
*****************************************************************************************
*************** -->
  <!-- * Define MGSiteNameType-->
  <!--
*****************************************************************************************
*************** -->
  <xsd:simpleType name="MGSiteNameType">
   <xsd:restriction base="NoSpaceNameType">
    <xsd:maxLength value="4" />
   </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

55.5.4.2 Assoc MG

No changes have been made to this schema. This interface should be used in a similar manner as it was in prior releases, however, automatic addition of EPGs will not be realized.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!--
*****************************************************************************
**************** -->
 <!-- * Define AssocMG Method Parameters -->
 <!--
*****************************************************************************
**************** -->
 <xsd:complexType name="assocMGMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="assocMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="assocMGParamsType">
  <xsd:sequence>
   <xsd:element name="mgUIName" type="NoSpaceNameType" />
   <xsd:element name="mgProfileName" type="NoSpaceNameType" />
   <xsd:element name="mgIpAddr" type="IPAddressType" />
   <xsd:element name="mgProtocolType" type="MGProtocolType" />
   <xsd:element name="mgProtocolVersion" type="xsd:decimal" />
   <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" />
   <xsd:element name="mgSiteName" type="MGSiteNameType" minOccurs="0" />
   <xsd:element name="gwcUIName" type="GWCNameType" minOccurs="0" />
   <xsd:element name="reservedTerminations" type="ReservedTerminationsType" minOccurs="0" />
   <xsd:choice minOccurs="0">
    <xsd:element name="pepServerName" type="xsd:token" />
    <xsd:element name="NATname" type="xsd:token" />
   </xsd:choice>
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

55.5.4.3 Add Carrier

The add carrier operation is now used to datafill H.323 EPG carrier groups. To datafill this type of carrier group, the H.323 service type should be used. For H.323 EPG carrier groups, the IID value should not be entered because it is auto-generated by the system.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!-- ********************************************************************** -->
 <!-- * Define AddCarrier Method Parameters -->
 <!-- ********************************************************************** -->
 <xsd:complexType name="addCarrierMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="addCarrierParamsType" />
  </xsd:all>
```

```
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addCarrierParamsType">
    <xsd:sequence>
      <xsd:element name="mgName" type="CarMGNameType" />
      <xsd:element name="carrierName" type="CarrierNameType" />
      <xsd:element name="svcData" type="svcDataType" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="firstTN" type="firstTNType" minOccurs="0" maxOccurs="1" />
    </xsd:sequence>
  </xsd:complexType>
<!-- ********************************************************************** -->
<!-- * Define svcDataType -->
<!-- ********************************************************************** -->
  <xsd:complexType name="svcDataType">
    <xsd:choice>
      <xsd:element name="PRI" type="PRISvcType" />
      <xsd:element name="V5.2" type="V5.2SvcType" />
      <xsd:element name="ISUP" type="xsd:string" fixed="" />
      <xsd:element name="H323" type="xsd:string" fixed="" />
    </xsd:choice>
  </xsd:complexType>
<!-- ********************************************************************** -->
<!-- * Define PRISvcType -->
<!-- ********************************************************************** -->
  <xsd:complexType name="PRISvcType">
    <xsd:sequence>
      <xsd:element name="IID" type="firstTNType" />
    </xsd:sequence>
  </xsd:complexType>
<!-- ********************************************************************** -->
<!-- * Define V5.2SvcType -->
<!-- ********************************************************************** -->
  <xsd:complexType name="V5.2SvcType">
    <xsd:sequence>
      <xsd:element name="v5.2IId" type="firstTNType" />
      <xsd:element name="v5.2LinkId" type="firstTNType" />
      <xsd:element name="v5.2UALinkId" type="firstTNType" />
    </xsd:sequence>
  </xsd:complexType>

<!-- ********************************************************************** -->
<!-- * Define firstTNType -->
<!-- ********************************************************************** -->
  <xsd:simpleType name="firstTNType">
    <xsd:restriction base="xsd:integer">
      <xsd:minInclusive value="1" />
      <xsd:maxInclusive value="4094" />
    </xsd:restriction>
  </xsd:simpleType>

</xsd:schema>
```

55.5.4.4 List All Carriers

The list all carriers schema is an existing interface that should be used to view Endpoint/TID mappings. This interface replaces the SN06.1 and SN06.2 queryEndpointGroup interface. No changes have been made to this interface for SN07, but, since it is now a required interface to list mappings for H.323 GWs it is listed here as a convenience.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
            version="1.0"
            xml:lang="en" >
 <!-- ********************************************************************** -->
 <!-- * Define listAllCarriers Method Parameters  -->
 <!-- ********************************************************************** -->
 <xsd:complexType name="listAllCarriersMethodType">
  <xsd:sequence>
   <xsd:element name="Parameters" type="listAllCarParamsType" />
  </xsd:sequence>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="listAllCarParamsType">
  <xsd:choice>
   <xsd:element name="FILTER_ALL" type="xsd:string" fixed="" />
   <xsd:element name="FILTER_GWC" type="filterGWCType" />
   <xsd:element name="FILTER_MG" type="filterMGType" />
   <xsd:element name="FILTER_CARRIER" type="filterCarType" />
  </xsd:choice>
 </xsd:complexType>
 <xsd:complexType name="filterMGType">
  <xsd:sequence>
   <xsd:element name="mgName" type="CarMGNameType" />
  </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="filterCarType">
  <xsd:sequence>
   <xsd:element name="mgName" type="CarMGNameType" />
   <xsd:element name="carrierName" type="CarrierNameType" />
  </xsd:sequence>
 </xsd:complexType>

</xsd:schema>
```

55.5.4.5 Disassocate MG

Tags values for the disAssocMG XML command are not changed in the SN07 release. Schema's is listed here as a convenience to the reader.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!--
*****************************************************************************
*************** -->
 <!-- * Define disAssocMG Method Parameters  -->
 <!--
*****************************************************************************
*************** -->
 <xsd:complexType name="disAssocMGMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="disAssocMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="disAssocMGParamsType">
  <xsd:sequence>
   <xsd:element name="mgUIName" type="NoSpaceNameType" />
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

55.5.4.6 Delete Carrier

Tags values for the Delete Carrier XML command are not changed in the SN07 release. Schema's are listed here as a convenience to the reader.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!--
*****************************************************************************
**************** -->
 <!-- * Define deleteCarrier Method Parameters  -->
 <!--
*****************************************************************************
**************** -->
 <xsd:complexType name="deleteCarrierMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="delCarrierParamsType"/>
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="delCarrierParamsType">
  <xsd:sequence>
   <xsd:element name="mgName" type="CarMGNameType" />
   <xsd:element name="carrierName" type="CarrierNameType" />
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

55.6 Configuration Walkthrough

As previously mentioned, H.323 provisioning rules have changed from the 6.2 to the SN07 release. The following sections give a quick overview of operations used for provisioning and highlight the differences in the 2 releases. The operations are supported using either the CMT GUI or the XML interfaces except where indicated.

55.6.1 Adding a H.323 EPG

- SN06.2
  - — Add a H.323 GWC to the system
  - — Associate GW with the GWC
    - Adds GW to GWC
    - Adds EPG to GW
    - Picks starting TID automatically
    - Requires query to identify TID information for table TRKMEM
- SN07
  - — Add a H.323 GWC to the system
  - — Associate GW with the GWC

- Adds a GW to GWC
- Reserves TID space for EPGs

— Add EPGs to GW using Add Carrier command

- Allows users to specify starting TID
- Consistent with PVG trunking
- Repeat this step for the desired number of EPs and EPGs
- Query can be used to identify TID information if desired

55.6.2 Deleting a H.323 GW

- SN06.2
  - — Ensure EPs on the GW are in an Out Of Service state
  - — Select the GW to delete and issue disassociate MG command
    - Deletes EPGs from the GW
    - Deletes GW

- SN07
  - — Ensure EPs on the GW are in an Out Of Service state
  - — Delete EPGs from GW using Delete Carriers command
    - Repeat this step until all EPGs are removed
  - — Delete GW using Disassociate MG command

55.6.3 Increasing the Reserved Capacity for a H.323 GW

- SN06.2
  - — Not available

- SN07
  - — Select the GW from the GW GUI and issue change operation
    - Change value must be less than or equal to maximum value as dictated by GWs profile
    - GWC must have enough TID locations unreserved to accommodate change as dictated by the GWCs profile
  - — Add additional EPGs to GW using Add Carrier command
    - Allows users to specify starting TID
    - Consistent with PVG trunking

- Repeat this step for the desired number of EPs and EPGs
- Query can be used to identify TID information if desired

55.6.4 Decreasing the Reserved Capacity for a H.323 GW

- SN06.2
  - — Not available

- SN07
  - — Select and remove EPGs that are over the new lower limit if necessary using the Delete Carrier operation
  - — Select the GW from the GW GUI and issue change operation
    - Decreases TID reserve capacity allocated for GWC
    - Does not remove any EPs

56: Configuration (CN): A00004005

56.1 Hardware and Software Requirements

There is no pre-configuration assumptions/criteria.

56.2 Initial Configuration

There is no initial configuration. However, when replacing the session Server chassis with a spare in order to replace the motherboard and when the unit will not boot properly or when there is a need to verify that the BIOS is properly set up use this procedure: as soon as the server comes up with the HP Invent intro screen, hit F2 to go to BIOS When the BIOS screen eventually comes up, arrow over to Boot and change the 1st Boot Priority to be CDROM. F10 to save and exit. The Session Server will reboot again and will eventually go to the prompt that will boot the server.

56.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

56.4 Upgrade Impact

56.4.1 Dump and Restore

Not Applicable.

56.4.2 Element Management Upgrade

Not Applicable.

56.5 Data schema (DS) (CM, MIBS, RDB)

Not Applicable.

56.6 Service Orders (SO) (CM & SESM)

Not Applicable.

56.7 Software optionality control (SOC)

Not Applicable.

56.8 Element Management

The Session Server element manager is not used to perform or change configuration procedures, instead it is used to view the status of the system and to perform maintenance actions. Please refer to the FN section for snap shots of various GUI panels.

56.9 Command interface changes

On the Session Server there is a new command line interface tool developed to get system status and perform maintenance actions from command line as well as to facilitate the web based GUI implementation.

56.9.1 <mtccli Link Commands>

The mtccli tool supports the following link maintenance actions: lock, unlock, and swlnk.

56.9.1.1 Command syntax

Table 1 <mtccli lock> command parameters and variables

Command	Parameters and variables
mtccli lock	0|1
Parameters and variables	Description
lock	lock the inactive link

Table 2 <mtccli unlock> command parameters and variables

Command	Parameters and variables
mtccli unlock	0|1
Parameters and variables	Description
unlock	Unlock the inactive link.

Table 3 <mtccli swlnk> command parameters and variables

Command	Parameters and variables
mtccli swact	
Parameters and variables	Description
swlnk	Switch link activity.

Table 4 MTCCLI Link Command outputs with associated meanings and actions

Command: mtccli lock 0|1
mtccli lock 0|1 Reason: link already locked. **Meaning:** This response warns users that the link is already in a locked state **System or user actions:** You should unlock the link first before attempting to lock it. Use mtccli status to check link status, before attempting this command.
mtccli unlock 0|1 Reason: link already unlocked. **Meaning:** This response warns users that the link is already unlocked. **System or user actions:** You should lock the link first before attempting to unlock it. Use mtccli status to check link status, before attempting this command.
mtccli swlnk Reason: inactive link is locked Reason: inactive link is locked. the command fails due to attempting to switch link activity when inactive link is locked **Meaning:** This response warns users that the inactive link is locked. **System or user actions:** You should unlock the inactive link first before attempting to lock it. Use mtccli status to check link status, before attempting this command.

56.9.2 <mtccli Node Commands>

The mtccli tool supports the following node maintenance actions: swact, jam, and unjam.

56.9.2.1 Command syntax

Table 5 <mtccliswact|jam|unjam> command parameters and variables

Command	Parameters and variables
mtccli swact	<force>
Parameters and variables	Description

Table 5 <mtccliswact|jam|unjam> command parameters and variables

Command	Parameters and variables
swact	Performs unit switch of activity. This command supports the force option. It can be executed from the active unit only.

Table 6 <mtccli jam> command parameters and variables

Command	Parameters and variables
mtccli jam	
Parameters and variables	Description
jam	Performs jam of the inactive unit.This command can be executed from the active unit only.

Table 7 <mtccli unjam> command parameters and variables

Command	Parameters and variables
mtccli unjam	
Parameters and variables	Description
unjam	Performs unjam of the inactive unit. This command can be executed from the active unit only. There is one condition where the unjam action can be executed from the inactive unit: If the inactive is in a jammed state, and the active unit is unavailable, then the unjam command can be executed from the inactive unit.

Table 8 MTCCLI swact Command outputs with associated meanings and actions

Command: mtccli swact
mtccli swact Please wait this action may take up to 130 sec. Command passed. **Meaning:** This response gives users the estimated time it could take to execute the swact command as well as report that the command status. **System or user actions:** no action is required, command passed.

Table 8 MTCCLI swact Command outputs with associated meanings and actions

Command: mtccli swact
mtccli swact Error: Command failed. Reason: Mate not available. **Meaning:** This response warns users that the mate unit is unavailable. **System or user actions:** You should have both units booted and in enabled state before attempting the swact command.
mtccli swact Command failed. Reason: Not active unit. **Meaning:** This response warns users that the command is issued on the inactive unit. **System or user actions:** You should login to the active unit before issuing the swact command.
mtccli swact Error: Command failed. Reason: Application is out-of-sync. **Meaning:** This response warns users that the command failed because the mate unit operation state is diabled. **System or user actions:** You should wait until the mate operation state is enabled before attempting the swact command. Use mtccli status command to check mate operation status.
mtccli swact Please wait this action may take up to 130 sec. Error: Command failed. Reason: PRECHECK FAILED: application rejected request. **Meaning:** This response warns users that application rejected the swact request. **System or user actions:** You should check the design logs to find out the name of the application rejecting the request. Then try the command again, if the problem persists then contact your next level of support.

Table 9 MTCCLI jam Command outputs with associated meanings and actions

Command: mtccli jam
mtccli jam Reason: Not active unit. **Meaning:** This response warns users that the command is issued on the inactive unit. **System or user actions:** You should login to the active unit before issuing the jam command.

Table 10 MTCCLI unjam Command outputs with associated meanings and actions

Command: mtccli unjam
mtccli unjam Reason: already unjammed. **Meaning:** This response warns users that unit is not in a jam state or the command is issued on the inactive unit. **System or user actions:** You should jam the unit before attempting to the unjam command. Or if the command is issued on the inactive unit then, log to the active unit before issuing the unjam command.

56.9.3 <mtccli Reboot and Halt Commands>

The mtccli tool supports reboot and halt maintenance actions for both units from the active unit. In order to reboot the inactive unit the “mtccli rebootmate” command should be used, and to halt the inactive unit the “mtccli haltmate” command should be used.

56.9.3.1 Command syntax

Table 11 <mtccli reboot> command parameters and variables

Command	Parameters and variables
mtccli reboot	force
Parameters and variables	Description
reboot	reboot the active unit. This command can be executed from the active unit only.

Table 12 <mtccli halt> command parameters and variables

Command	Parameters and variables
mtccli halt	force
Parameters and variables	Description
halt	halt the active unit. This command can be executed from the active unit only.Warrning: after halting the system you have to physically be in front of the unit and press the rest button to recover the unit.

Table 13 <mtccli rebootmate> command parameters and variables

Command	Parameters and variables
mtccli rebootmate	force
Parameters and variables	Description
rebootmate	rebootmate command is used to reboot the inactive unit. This command can be executed from the active unit only.

Table 14 <mtccli haltmate> command parameters and variables

Command	Parameters and variables
mtccli haltmate	force
Parameters and variables	Description
haltmate	haltmate command is used to halt the inactive unit. This command can be executed from the active unit only. Warning: after halting the system you have to physically be in front of the unit and press the rest button to recover the unit.

Table 15 MTCCLI reboot Command outputs with associated meanings and actions

Command: mtccli reboot
mtccli reboot Reason: Not active unit. **Meaning:** This response warns users that the command was issued on the inactive unit. **System or user actions:** You should issue the reboot command from the active unit. Use mtccli status command to check units activity, before attempting this command.
mtccli reboot Reason: Mate is available. **Meaning:** This response warns users that the inactive unit is still available. **System or user actions:** You can not reboot the active unit if the inactive is still available. You should reboot the inactive unit first using rebootmate, then switch activity before attempting to reboot.

Table 16 MTCCLI halt Command outputs with associated meanings and actions

Command: mtccli halt
mtccli halt Reason: Not active unit. **Meaning:** This response warns users that the command was issued on the inactive unit. **System or user actions:** You should issue the halt command from the active unit. Use mtccli status command to check units activity, before attempting this command.
mtccli halt Reason: Mate is available. **Meaning:** This response warns users that the inactive unit is still available. **System or user actions:** You can not halt the active unit if the inactive is still available. You should reboot the inactive unit first using rebootmate, then switch activity before attempting to halt.

Table 17 MTCCLI rebootmate Command outputs with associated meanings and actions

Command: mtccli rebootmate
mtccli rebootmate Command failed. Reason: Not active unit. **Meaning:** This response warns users that the command was issued on the inactive unit. **System or user actions:** You should issue the rebootmate command from the active unit. Use mtccli status command to check units activity, before attempting this command.
mtccli reboot Reason: Mate is available. **Meaning:** This response warns users that the inactive unit is still available. **System or user actions:** You can not reboot the active unit if the inactive is still available. You should reboot the inactive unit first using rebootmate, then switch activity before attempting to reboot.
mtccli rebootmate Please wait this action may take up to 230 sec. Error: Command failed. Reason: PRECHECK FAILED: application rejected request. **Meaning:** This response warns users that the reboot mate command can not be executed because application failed precheck request. **System or user actions:** You should check design logs to find out the name of the application rejecting the request. Then try the command again, if the problem persists, then contact your next level of support.

Table 18 MTCCLI haltmate Command outputs with associated meanings and actions

Command: mtccli haltmate
mtccli haltmate Reason: Not active unit. **Meaning:** This response warns users that the command was issued on the inactive unit. **System or user actions:** You should issue the halt command from the active unit. Use mtccli status to check activity status, before attempting this command.

Table 18 MTCCLI haltmate Command outputs with associated meanings and actions

Command: mtccli haltmate
mtccli haltmate Reason: Mate is available. **Meaning:** This response warns users that the inactive unit is still available. **System or user actions:** You can not halt the active unit if the inactive is still available. You should reboot the inactive unit first using rebootmate, then switch activity before attempting to halt.
mtccli haltmate Please wait this action may take up to 230 sec. Error: Command failed. Reason: PRECHECK FAILED: application rejected request. **Meaning:** This response warns users that the halt mate command can not be executed because application failed precheck request. **System or user actions:** You should check design logs to find out the name of the application rejecting the request. Then try the command again, if the problem persists, then contact your next level of support.

56.9.4 <mtccli Query Commands>

The mtccli tool supports the following system query commands: qrycpu, qryzmb, qrymem, qryntp, qrycputl, qryoper, qrymateoper and queryip.

56.9.4.1 Command syntax

Table 19 <mtccli qrycpu> command parameters and variables

Command	Parameters and variables
mtccli qrycpu	
Parameters and variables	Description
qrycpu	Displays CPU load average and 1 minute load average thresholds

Table 20 <mtccli qryzmb> command parameters and variables

Command	Parameters and variables
mtccli qryzmb	
Parameters and variables	Description
qryzmb	Displays number of zombie processes and the alarm thresholds

Table 21 <mtccli qrymem> command parameters and variables

Command	Parameters and variables
mtccli qrymem	
Parameters and variables	Description
qrymem	Displays system memory report and the alarm thresholds based on the amount of avail memory remaining.

Table 22 <mtccli qryntp> command parameters and variables

Command	Parameters and variables
mtccli qryntp	
Parameters and variables	Description
qryntp	Displays NTP servers report.

Table 23 <mtccli qrycputl> command parameters and variables

Command	Parameters and variables
mtccli qrycputl	
Parameters and variables	Description
qrycputl	Displays CPU utilization report and the CPU utilization alarm thresholds average.

Table 24 <mtccli queryip> command parameters and variables

Command	Parameters and variables
mtccli queryip	
Parameters and variables	Description
queryip	Displays server IP addresses.

Table 25 <mtccli qryoper> command parameters and variables

Command	Parameters and variables
mtccli qryoper	
Parameters and variables	Description
qryoper	Displays server operation state.

Table 26 <mtccli qrymateoper> command parameters and variables

Command	Parameters and variables
mtccli qrymateoper	
Parameters and variables	Description
qrymateoper	Displays mate operation state.

56.9.4.2 Example

```
mtccli qrycpu
CPU Load Average report retrieved on Thu Apr 22 13:56:54 2004:

      1 min Load Avg: 1.04
      5 min Load Avg: 1.07
     15 min Load Avg: 0.83

 Number of Processes: 68

   Alarm Description: 1 minute load average
     Minor threshold: 10.00
     Major threshold: 20.00
  Critical threshold: 40.00

mtccli qryzmb
Zombie process report retrieved on Thu Apr 22 13:57:15 2004:

 Number of Zombie Processes: 0

  Alarm Description: Number of zombie processes
    Minor threshold: 5
    Major threshold: 10
 Critical threshold: 15

mtccli qryntp
NTP report retrieved on Thu Apr 22 13:57:30 2004:

  Total number of time servers: 2
  Number of accessible servers: 2
Number of synchronized servers: 2
Time Offset from server 10.40.4.101: 8(ms)
```

```
mtccli qrycputl
CPU Utilization report retrieved on Thu Apr 22 13:57:47 2004:

      5 min Util Avg: 4.18
     20 min Util Avg: 5.05
     30 min Util Avg: 0.00
   Alarm Description: cpu utilization average
     Minor threshold: over 95.00% for 5 minutes
     Major threshold: over 99.00% for 20 minutes
  Critical threshold: over 99.00% for 30 minutes

mtccli queryip
Query IP Address report for unit 0:
Description     IP Address
localptp        192.168.1.1
localport0      10.40.5.57
localport1      10.40.5.58
localblade      10.40.5.59
activeip        10.40.5.64
inactiveip      10.40.5.63
mateptp         192.168.1.2
mateport0       10.40.5.60
mateport1       10.40.5.61
mateblade       10.40.5.62

mtccli qryoper
Enabled

mtccli qrymateoper
Disabled
```

56.9.5 <mtccli System Status and Alarms Commands>

In addition to the query commands the mtccli tool supports the status and alarms commands.

The status command displays both Session Servers units status.

```
mtccli status
Unit 0 Status:
              Jam:  Link0:  Link1:  PTPLink:  OperationState:
Unit0  Inact  no    . Inact . Act    .        Enabled
Unit1  Act    no    . Act   . Inact  .        Enabled
```

The alarms command displays the overall system alarms

```
mtccli alarms
 SessServer      SYS      CON      APPL             Unit: 1
  simplx        NTP      MatCon   simplx
    M                      M        M
```

The status/alarms commands have support the -c option to display a continues system status/alarms. To exit the continues mode enter Ctrl-c.

56.9.5.1 Command syntax

Table 27 <mtccli status> command parameters and variables

Command	Parameters and variables
mtccli status	-c option
Parameters and variables	Description
status	Displays both units status. The -c option can be used to run the command in continues mode. To exit -c option, enter Ctrl-c

Table 28 <mtccli alarms> command parameters and variables

Command	Parameters and variables
alarms	-c option
Parameters and variables	Description
alarms	Displays overall alarms status. The -c option can be used to run the command in continues mode. To exit -c option, enter Ctrl-c

56.10 Security

Not applicable.

56.11 Configuration Walkthrough

57: Configuration (CN): A00004036

57.1 Hardware and Software Requirements

57.2 Initial Configuration

57.3 Office/Subnet parameters (OP/SP) (CM & SESM)

57.4 Upgrade Impact

57.5 Data schema (DS) (CM, MIBS, RDB)

57.6 Service Orders (SO) (CM & SESM)

57.7 Software optionality control (SOC)

Table 1 SOC

SOC option name:	Off-board Service Control
SOC option title:	Yes
SOC option control type:	state
New SOC option?	Yes
SOC option order code	AIN00321 SVC MGR Basic AIN00322 SVC MGR List Editing AIN00323 SVC MGR Speed Call AIN00324 SVC MGR Call Forward AIN00325 SVC MGR Privacy Control AIN00326 SVC MGR COT and CCW AIN00327 SVC MGR SIMRING

Table 1 SOC

Option defined in DRU:	CNA
Affected products:	SNNCSH07

57.8 Element Management

57.9 Command interface changes

57.10 Security

57.11 Configuration Walkthrough

58: Configuration (CN): A00004045

58.1 Hardware and Software Requirements

In order to perform CLIDN call tracing on the DMS-250, SOC UTRS0012 must be ON and the desired termination number(s) must be datafilled in table CLIDN.

58.2 Initial Configuration

This feature impacts EANT, PRI, DAL, ONAL, ONAT and IMT trunks.

This feature creates a section for existing table CLIDN (see Section 13.5.1).

58.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

58.4 Upgrade Impact

58.4.1 Dump and Restore

If ACTPATCH KGL03 (UCS19)is active on Dump side, then UTRS0012 will be set to RTU "Y" and "ON" on ONP to the sourced release (restore side UCS20 and above).

58.4.2 Element Management Upgrade

N/A

58.5 Data schema (DS) (CM, MIBS, RDB)

58.5.1 New table

Table CLIDN is new to the UCS DRU, but currently exists in DMS-100/200.

Table 1 New table

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CLIDN	NEW	UNCHANGED

58.5.2 Table/MIB/Remote Database Schema information

58.5.2.1 Name: CLIDN

Calling Line Identification Directory Number

58.5.2.1.1 Functional description

Table CLIDN allows for a maximum of 67 ten-digit directory number (DN) (area code + office code + DN) tuples for which CLI call tracing is provided.

These DNs are external to the switching unit. The ten-digit DNs include an area code + office code + directory number or a service code.

For a service code (i.e., 411, 911, 0, etc.) or a seven-digit DN, the letter N must be prefixed to make the total digit count equal to 10. The system internally translates the letter N to 0.

Table CLIDN is associated with the TRK605 log on the DMS-250 switch. When the called number is datafilled in table CLIDN, UTRS0012 SOC option is ON and the incoming trunk type is supported (trunk types: EANT, PRI, DAL, ONAL, ONAT or IMT), the TRK605 log is generated.

The TRK605 log report contains the following fields:

- the incoming trunk group and number
- the outgoing trunk group and number
- the called party number
- the originating party number
- the date and time

58.5.2.1.2 Usage sequence and implications (CM Only)

No other tables need to be datafilled prior to entering data into table CLIDN.

58.5.2.1.3 .Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CLIDN	0	67	

58.5.2.1.4 Fields

The following table lists field description for table CLIDN.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIGITS	N/A		numeric digits 0-9 and N	*Digits.* The entry is equal to the ten-digit DN of a line external to the switching unit. The letter N must prefix service codes like 411, 911 and 0. This action makes the total digit count equal to 10. The system translates the letter N internally to 0.

58.5.2.1.5 Datafill example

The Figure 1 shows an example of datafill for table CLIDN. The example contains a service code, 7-digit DN and 10-digit DN.

Figure 1 MAP example for table CLIDN

```
TABLE: CLIDN

DIGITS
----------
NNNNNNN411
NNN8765000
2018213456
```

58.5.2.1.6 Table release history update

Design activity A00004045 (CLIDN for DMS-250) introduced log report TRK605 to the UCS DRU in SN07.

Design activity AN1658 (Inter-Switch Call Trace) introduced log report TRK605 in CNA05.

58.5.2.1.7 Supplementary information

N/A

58.5.2.1.8 Translation verification other tools

Table CLIDN does not use translation verification tools.

58.6 Service Orders (SO) (CM & SESM)

N/A

58.7 Software optionality control (SOC)

Table 4 SOC

SOC option name:	CLIDN for DMS-250
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	UTRS0012
Option defined in DRU:	UCS
Affected products:	SN07

58.8 Element Management

N/A

58.9 Command interface changes

N/A

58.10 Security

N/A

58.11 Configuration Walkthrough

In order to perform CLIDN call tracing on the DMS-250, SOC UTRS0012 must be ON and the desired called number(s) must be datafilled in table CLIDN.

59: Configuration (CN): A00004046

59.1 Initial Configuration

Customers must consider the ECAN requirements of trunk members that will comprise trunk groups within the network. The inability to set more than two simultaneous SPMECIDX values within a trunk group is the source of this constraint.

The SPMECIDX field identifies a particular ECAN configuration tied to trunk members within a trunk subgroup. The existing TRKSGRP table only allows two tuples within the same trunkgroup. Therefore, for SPM based trunks coexisting with ENET based trunks, there are only 2 possible ECAN alternatives available.

59.2 Office parameters (CM)

The ECAN_EDGE_STRATEGY office parameter's role is changing slightly in SN07. This change impacts the role of this office parameter for determining ECAN implementation strategy within the network.

59.2.1 Modified office parameters

Table 1 Modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	ECAN_EDGE_STRARTEGY	CHANGED	CM

59.2.2 Parameter information

59.2.2.1 ECAN_EDGE_STRATEGY

ECAN_EDGE_STRATEGY in table OFCENG.

59.2.2.1.1 Functional description

The ECAN_EDGE_STRATEGY is used to determine ECAN resource allocation strategy within the network. The role of this parameter is changing in SN07 to only impact AAL1 networks. The assumption is that all other packet networks are EDGE strategy by default.

59.2.2.1.2 Provisioning rules

No Change

59.2.2.1.3 Range information

No Change

59.2.2.1.4 Activation

No Change

59.2.2.1.5 Dependencies

No Change

59.2.2.1.6 Consequences

No Change

59.2.2.1.7 Verification

No Change

59.2.2.1.8 Memory requirements

No Change

59.2.2.1.9 Parameter release history update

ECAN_EDGE_STRATEGY in table OFCENG in SN07 and beyond will only apply to AAL1 bearer networks. All other packet network type such as IP will assume the edge ECAN strategy.

59.3 Upgrade Impact

59.3.1 Dump and Restore

There is no impact to upgrades.

59.3.2 Element Management Upgrade

Not applicable.

60: Configuration (CN): A00004126

60.1 Hardware and Software Requirements

It is assumed that all basic provisioning is complete up to and including Table SPMECAN.

60.2 Initial Configuration

Not Applicable.

60.3 Upgrade Impact

60.3.1 Dump and Restore

All tuples in Table SPMECAN will contain the new IGNOREEC field as they are transferred from the old BCS side to the new. The new field will be set FALSE as a default value. There is no preparation that must be done by the customer until after the dump and restore has completed.

If the customer wishes to change the field afterwards then they must use standard Table Control mechanisms to set the IGNOREEC bool to Y.

60.3.2 Element Management Upgrade

Not Applicable.

60.4 Data schema (DS) (CM, MIBS, RDB)

60.4.1 New/modified tables, MIBs, or Database Schema

Adding a new IGNOREEC field to the existing table definition of SPMECAN.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SPMECAN	CHANGED	NEW

60.4.2 Table/MIB/Remote Database Schema information

60.4.2.1 Name: SPMECAN

SPM Echo Cancellation Table

60.4.2.1.1 Functional description

Table SPMECAN provides entries which define the attributes of specific ECAN setup. Tuples in Table TRKSGRP can assign (as an option) an index into Table SPMECAN to that subgroup. All trunks which use this subgroup

will also use the specific SPMECAN setup as defined in the SPMECAN tuple associated to the index used by subgroup tuple.

60.4.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- Current datafill order unchanged.

60.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SPMECAN	0	256	new field adds 1 bool (bit) to overall size of physical store. Since the store is word aligned there is actually no additional memory usuage.

60.4.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SPMECAN.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IGNOREEC	NEW	NA	Y/N	Long Name: ignoreec Default Value: N For rules on setting this bool see “60.5 Configuration Walkthrough” on page 3262

60.4.2.1.5 Datafill example

The following example shows sample datafill for table SPMECAN:

```
>table spmecan
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

TABLE: SPMECAN
>lis
TOP
ECINDEX TONDS TONMG TONEDMOD S56KB AUTON NLP NSMAT SOS TDINC  MDLA MERL ACOM
FAREC BK2BK IGNOREEC S2COMPAT ECBYTE1 ECBYTE2 ECBYTE3 ECBYTE4
---------------------------------------------------------------------------
```

```
1     Y     Y     G165     Y     Y   Y     Y   Y     Y  32MS  6DB 33DB
N     Y     N    S2C_NORM      00      00      00      00
```

60.4.2.1.6 Table release history update

A new field is added to Table SPMECAN called IGNOREEC. This field (if set to Y) is used to instruct CEM Callp if it should use the FAREC and BK2BK fields in the SPMECAN tuple to set up ECANs for individual calls. If the field is set N, then ECANs are set up using the EC bits in the ACM/ANS and ANI callp messages in the CEM.

60.4.2.1.7 Supplementary information

Not Applicable

60.4.2.1.8 Translation verification other tools

None.

60.5 Configuration Walkthrough

The walkthrough or datafill order for this table has not changed. The IGNOREEC field can be set Y or N depending on the use of the SPMECAN tuple in table TRKSGRP. The following rule apply:

- When changing the IGNOREEC bit from N to Y, it cannot be set Y if there are existing TRKSGRP tuples that use this SPMECAN index (tuple) and support any signaling type other than CCS7.

  The following string is output at the MAP table control when this error occurs (where nnn = range of datafilled trksgrp tuples):

  ```
  "Non-CCS7 tuple(s) in Table TRKSGRP are using this ECAN index."
  "See SGRP Index:nnnn in Table TRKSGRP."
  ```

- When changed to Y, the new setting of the IGNOREEC bit will apply to all TRKSGRP CCS7 tuples that use the SPMECAN index.
- When changing the IGNOREEC bit from Y to N, it can be set N even if there are tuples in Table TRKSGRP that use this SPMEC index. The setting of the bit to N will be applied to all Trunk Subgroups that use this SPMECAN index.
- When changing a tuple in Table TRKSGRP to use an existing SPMECAN index that has the IGNOREEC bool set to Y, the TRKSGRP tuple must only support ISUP. If it supports any other signaling type the following error messages appear (depending on whether the load is a CNA or UCS load):

  CNA:

  ```
  "SPMECIDX IS NOT SUPPORTED ON THIS TRUNK"
  "TYPE FOR MG4K NA100 PTS."

  "SPMECIDX IS NOT SUPPORTED ON THIS TRUNK"
  "TYPE FOR MG4K NA100 ISDN."
  ```

  UCS:

```
"SPMECIDX IS NOT SUPPORTED ON THIS TRUNK"
"TYPE FOR MG4K UCS PTS."

"SPMECIDX IS NOT SUPPORTED ON THIS TRUNK"
"TYPE FOR MG4K UCS  ISDN."
```

61: Configuration (CN): A00004131

61.1 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

61.2 Initial Configuration

Standard configuration applies.

61.3 Office/Subnet parameters (OP/SP) (CM & SESM)

61.3.0.0.1 Activation

BCH negotiation functionality applies only when SOC option TRKGRP:OLISCRN is set to ‘1’ and is set to ‘ON’.’.

61.4 Upgrade Impact

NONE.

61.5 Data schema (DS) (CM, MIBS, RDB)

61.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKSGRP	changed	unchanged

61.5.2 Table/MIB/Remote Database Schema information

61.5.2.1 Name: TRKSGRP

Trunk Subgroup

61.5.2.1.1 Functional description

This feature allows setting field BCHNEG to ‘Y’ for PRI trunks using N449PRI variant. Prior to this feature, setting BCHNEG to Y for trunks supporting the N449PRI protocol variant was not supported.

61.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

61.5.2.1.3 Size

No change.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKSGRP	unchanged	unchanged	No change

61.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for TRKSGRP

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BCHNEG	Changed	Subfield	Y/N	Controls whether B-Channel negotiations is allowed for the trunk group.

61.5.2.1.5 Datafill example

The following example shows sample datafill for table TRKSGRP.

SGRPKEY CARDCODE SGRPVAR SGRPVAR

PRI925DRN5 0 DS1SIG ISDN 15 15 87Q931 2 **Y STAND** NETWORK PT_PT PVTNET N UNEQ 10 N SNTK SPM 1 61 1 64K HDLC $ $

61.5.2.1.6 Table release history update

SN07 allows setting field BCHNEG to ‘Y’ for PRI trunks using N449PRI variant.

61.5.2.1.7 Supplementary information

None.

61.5.2.1.8 Translation verification other tools

N/A

61.6 Service Orders (SO) (CM & SESM)

N/A.

61.7 Software optionality control (SOC)

Table 4 SOC

SOC option name:	NPRI
SOC option title:	NPRI N449 B-Channel Negot
SOC option control type:	state
New SOC option?	Yes
SOC option order code	NPRI0003
Option defined in DRU:	UCS
Affected products:	DMS-250

61.8 Element Management

N/A

61.9 Command interface changes

N/A

61.10 Security

N/A.

61.11 Configuration Walkthrough

N/A

62: Configuration (CN): A00004137

62.1 Hardware and Software Requirements

Not applicable

62.2 Initial Configuration

Not applicable.

62.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

62.4 Data schema (DS) (CM, MIBS, RDB)

62.4.1 New/modified tables, MIBs, or Database Schema

A new value is added to the ISUPDIX field of Table TRKGRP.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKGRP	Changed	Unchanged

62.4.2 Table/MIB/Remote Database Schema information

62.4.2.1 Name: TRKGRP

Trunk Group (TRKGRP) Table

62.4.2.1.1 Functional description

A new value, UCS2FE, is added to the ISUPIDX field of table TRKGRP.

62.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

62.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKGRP	0	32767	unchanged

62.4.2.1.4 Fields/OIDs

The following table lists the changed field for table TRKGRP.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ISUPIDX	Changed	None	UCS2FE	When ISUPIDX field is set to UCS2FE and the UTRS0014 SOC is on, a FAR message will be sent on the originating trunk per requirements outlined in the FN section of feature A00004137.

62.4.2.1.5 Datafill example

The following example shows sample datafill for table TRKGRP:

```
>table trkgrp
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
EAN821C7DR02 EANT 50 NPDGP NCOF 0 2W EAN MIDL 16 7 16 16 EAPT 10
4 214 UCS2FE NIL 214 111 MANUAL 0 RTE18 0 1 VOICE_DATA 160 (MCCS
) (OHQ)(TMANIDLV ALWAYS) (REORGVAL ) (ID24_ON ) (CAIN ) (DEFCIC
601 N N Y N N)(INCDNIS $) $
BOTTOM
>.
```

62.4.2.1.6 Table release history update

Added the UCS2FE value to field ISUPIDX in table TRKGRP.

62.4.2.1.7 Supplementary information

Not applicable.

62.4.2.1.8 Translation verification other tools

Not applicable.

62.5 Service Orders (SO) (CM & SESM)

Not applicable.

62.6 Software optionality control (SOC)

The UTRS0014 SOC is added for this feature.

Table 4 SOC

SOC option name:	UTRS
SOC option title:	PRI Enhanced ANI Delivery
SOC option control type:	state
New SOC option?	Yes
SOC option order code	UTRS0014
Option defined in DRU:	UCS
Affected products:	DMS-250

62.7 Element Management

Not applicable.

62.8 Command interface changes

Not applicable.

62.9 Security

Not applicable.

62.10 Configuration Walkthrough

Not applicable.

63: Configuration (CN): A00004260

63.1 Hardware and Software Requirements

Only requires SN07 load in Core. Will be patched back to SN06.

The parameter and log names are different between SN06 and SN07. In SN06, there will be ATM606, ATM806, and ATM807 logs. In SN07, these logs have been replaced with XPKT301, XPKT806, and XPKT807, respectively. Versions of this DDOC prior to issue AA24 will show the names used in SN06, while issue AA24 and later will show the names used in SN07.

63.2 Initial Configuration

At the CI prompt, enter these commands:

- ENGWRITE ON
- TABLE OFCENG
- POS XPKT806_SMG4_RAISE_CLEAR

which positions on the first of the four new tuples.

63.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Introducing three new office parameters for Table OFCENG in the CM.

63.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	XPKT806_SMG4_RAISE_CLEAR	New	CM
OFCENG	XPKT806_IW_RAISE_CLEAR	New	CM
OFCENG	XPKT806_DPT_RAISE_CLEAR	New	CM
OFCENG	XPKT806_SUPPRESSES_XPKT301	New	CM

63.3.2 Parameter information

63.3.2.1 XPKT806_SMG4_RAISE_CLEAR

SMG4 node threshold parameters for raising and clearing XPKT806 alarm.

63.3.2.1.1 Functional description

This parameter controls the raising of an XPKT806 major alarm for SMG4 nodes due to the number of XPKT301 hits against the SMG4 nodes. It also controls clearing the alarm via an XPKT807 log.

There are four subfields for this tuple:

1. RAISE_THRESHOLD - when the number of XPKT301 logs against the SMG4 node crosses (i.e. reaches or exceeds) this number during the raise cycle, then generate an XPKT806 log with major alarm, update “nn PKT” display under the APPL banner, and change the node to a clear cycle. Range is 0 to 32767. Default is 0, which disables this feature for all SMG4 nodes. Recommended value is 2.
2. RAISE_CYCLE - number of minutes in the “raise cycle” where we count the number of XPKT301 logs against the SMG4 node to see if XPKT806 needs to be generated. Range is 1 to 1440, where 1440 = 60 minutes per hour times 24 hours in a day. So we can go as fast as every minute, or as slow as every day. Default is 15, which is also the recommended value.
3. CLEAR_THRESHOLD - when the number of XPKT301 logs against the SMG4 node meets (or falls below) this number during the clear cycle, then generate an XPKT807 log, update “nn PKT” display under the APPL banner, and change the node to a raise cycle. Range is 0 to 32767. Default is 0, meaning there must be no XPKT301 failures against the node during the clear cycle to generate the XPKT807 log. Recommended value is 0.
4. CLEAR_CYCLE - number of minutes in the “clear cycle” where we count the number of XPKT301 logs against the SMG4 node to see if XPKT807 needs to be generated. Range is 1 to 1440. Default is 5, which is also the recommended value.

63.3.2.1.2 Provisioning rules

It is recommended (but not enforced) that RAISE_THRESHOLD should be greater than or equal to CLEAR_THRESHOLD. When this situation is encountered, the user will be warned with:

Warning: CLEAR_THRESHOLD should not exceed
RAISE_THRESHOLD.

If RAISE_THRESHOLD is set to a zero value (i.e. disabling the feature), then this message will be seen instead:

Note: Disabled reporting of XPKT806 alarms for all SMG4 nodes.

If the feature is disabled (i.e. RAISE_THRESHOLD = 0) and the user attempts to change the other fields, then this warning will be generated:

Warning: Altering these fields will have no effect since the feature is disabled (i.e. RAISE_THRESHOLD = 0).

63.3.2.1.3 Range information

Since this tuple has subfields, we will show 4 numbers for each table entry. The

Table 2 Range Information

Minimum	Maximum	Default
0, 1, 0, 1	32767, 1440, 32767, 1440	0, 15, 0, 5 Setting RAISE_THRESHOLD to 0 disables this feature for all SMG4 nodes.

numbers correspond to the subfields described above in the Functional Description.

63.3.2.1.4 Activation

Activation is immediate and will be conveyed to the user with this message whenever the parm values are changed while RAISE_THRESHOLD is non-zero (i.e. feature is enabled):

Note: This office parm change takes effect immediately for all SMG4 nodes by resetting the detection cycles with the updated parameter values.

If any XPKT806 alarms are present when the feature becomes disabled, then the alarms will be cleared immediately.

If any XPKT806 alarms are present when the parameters are changed while the feature is enabled, then the alarms will remain raised.

63.3.2.1.5 Dependencies

None

63.3.2.1.6 Consequences

None

63.3.2.1.7 Verification

To check that the office parameter changes are working, go to the MAPCI;MTC;APPL;PKT;SPM_ATM level and enter the PARMS command.

To actually see the XPKT806 alarm raised, you will need to cause XPKT301 logs via ATM call connection failures. Do NOT cause these failures in a live switch.

63.3.2.1.8 Memory requirements

No memory impact.

63.3.2.1.9 Parameter release history update

Introduced new XPKT806_SMG4_RAISE_CLEAR parameter for Table OFCENG that controls raising XPKT806 alarm for SMG4 nodes.

63.3.2.2 XPKT806_IW_RAISE_CLEAR

IW node threshold parameters for raising and clearing XPKT806 alarm.

63.3.2.2.1 Functional description

This parameter controls the raising of an XPKT806 major alarm for IW nodes due to the number of XPKT301 hits against the IW nodes. It also controls clearing the alarm via an XPKT807 log.

There are four subfields for this tuple:

1. RAISE_THRESHOLD - when the number of XPKT301 logs against the IW node crosses (i.e. reaches or exceeds) this number during the raise cycle, then generate an XPKT806 log with major alarm, update “nn PKT” display under the APPL banner, and change the node to a clear cycle. Range is 0 to 32767. Default is 0, which disables this feature for all IW nodes. Recommended value is 2.
2. RAISE_CYCLE - number of minutes in the “raise cycle” where we count the number of XPKT301 logs against the IW node to see if XPKT806 needs to be generated. Range is 1 to 1440, where 1440 = 60 minutes per hour times 24 hours in a day. So we can go as fast as every minute, or as slow as every day. Default is 15, which is also the recommended value.
3. CLEAR_THRESHOLD - when the number of XPKT301 logs against the IW node meets (or falls below) this number during the clear cycle, then generate an XPKT807 log, update “nn PKT” display under the APPL banner, and change the node to a raise cycle. Range is 0 to 32767. Default is 0, meaning there must be no XPKT301 failures against the node during the clear cycle to generate the XPKT807 log. Recommended value is 0.
4. CLEAR_CYCLE - number of minutes in the “clear cycle” where we count the number of XPKT301 logs against the IW node to see if XPKT807 needs to be generated. Range is 1 to 1440. Default is 5, which is also the recommended value.

63.3.2.2.2 Provisioning rules

It is recommended (but not enforced) that RAISE_THRESHOLD should be greater than or equal to CLEAR_THRESHOLD. When this situation is encountered, the user will be warned with:

Warning: CLEAR_THRESHOLD should not exceed RAISE_THRESHOLD.

If RAISE_THRESHOLD is set to a zero value (i.e. disabling the feature), then this message will be seen instead:

Note: Disabled reporting of XPKT806 alarms for all IW nodes.

If the feature is disabled (i.e. RAISE_THRESHOLD = 0) and the user attempts to change the other fields, then this warning will be generated:

Warning: Altering these fields will have no effect since the feature is disabled (i.e. RAISE_THRESHOLD = 0).

63.3.2.2.3 Range information

Since this tuple has subfields, we will show 4 numbers for each table entry. The

Table 3 Range Information

Minimum	Maximum	Default
0, 1, 0, 1	32767, 1440, 32767, 1440	0, 15, 0, 5 Setting RAISE_THRESHOLD to 0 disables this feature for all IW nodes.

numbers correspond to the subfields described above in the Functional Description.

63.3.2.2.4 Activation

Activation is immediate and will be conveyed to the user with this message whenever the parm values are changed while RAISE_THRESHOLD is non-zero (i.e. feature is enabled):

Note: This office parm change takes effect immediately for all IW nodes by resetting the detection cycles with the updated parameter values.

If any XPKT806 alarms are present when the feature becomes disabled, then the alarms will be cleared immediately.

If any XPKT806 alarms are present when the parameters are changed while the feature is enabled, then the alarms will remain raised.

63.3.2.2.5 Dependencies
None

63.3.2.2.6 Consequences
None

63.3.2.2.7 Verification
To check that the office parameter changes are working, go to the MAPCI;MTC;APPL;PKT;SPM_ATM level and enter the PARMS command.

To actually see the XPKT806 alarm raised, you will need to cause XPKT301 logs via ATM call connection failures. Do NOT intentionally cause these failures in a live switch!

63.3.2.2.8 Memory requirements
No memory impact.

63.3.2.2.9 Parameter release history update
Introduced new XPKT806_IW_RAISE_CLEAR parameter for Table OFCENG that controls raising XPKT806 alarm for IW nodes.

63.3.2.3 XPKT806_DPT_RAISE_CLEAR
DPT node threshold parameters for raising and clearing XPKT806 alarm.

63.3.2.3.1 Functional description
This parameter controls the raising of an XPKT806 major alarm for DPT nodes due to the number of XPKT301 hits against the DPT nodes. It also controls clearing the alarm via an XPKT807 log.

There are four subfields for this tuple:

1. RAISE_THRESHOLD - when the number of XPKT301 logs against the DPT node crosses (i.e. reaches or exceeds) this number during the raise cycle, then generate an XPKT806 log with major alarm, update “nn PKT” display under the APPL banner, and change the node to a clear cycle. Range is 0 to 32767. Default is 0, which disables this feature for all DPT nodes. Recommended value is 2.
2. RAISE_CYCLE - number of minutes in the “raise cycle” where we count the number of XPKT301 logs against the DPT node to see if XPKT806 needs to be generated. Range is 1 to 1440, where 1440 = 60 minutes per hour times 24 hours in a day. So we can go as fast as every minute, or as slow as every day. Default is 15, which is also the recommended value.

3. CLEAR_THRESHOLD - when the number of XPKT301 logs against the DPT node meets (or falls below) this number during the clear cycle, then generate an XPKT807 log, update “nn PKT” display under the APPL banner, and change the node to a raise cycle. Range is 0 to 32767. Default is 0, meaning there must be no XPKT301 failures against the node during the clear cycle to generate the XPKT807 log. Recommended value is 0.
4. CLEAR_CYCLE - number of minutes in the “clear cycle” where we count the number of XPKT301 logs against the DPT node to see if XPKT807 needs to be generated. Range is 1 to 1440. Default is 5, which is also the recommended value.

63.3.2.3.2 Provisioning rules

It is recommended (but not enforced) that RAISE_THRESHOLD should be greater than or equal to CLEAR_THRESHOLD. When this situation is encountered, the user will be warned with:

Warning: CLEAR_THRESHOLD should not exceed RAISE_THRESHOLD.

If RAISE_THRESHOLD is set to a zero value (i.e. disabling the feature), then this message will be seen instead:

Note: Disabled reporting of XPKT806 alarms for all DPT nodes.

If the feature is disabled (i.e. RAISE_THRESHOLD = 0) and the user attempts to change the other fields, then this warning will be generated:

Warning: Altering these fields will have no effect since the feature is disabled (i.e. RAISE_THRESHOLD = 0).

63.3.2.3.3 Range information

Since this tuple has subfields, we will show 4 numbers for each table entry. The

Table 4 Range Information

Minimum	Maximum	Default
0, 1, 0, 1	32767, 1440, 32767, 1440	0, 15, 0, 5 Setting RAISE_THRESHOLD to 0 disables this feature for all DPT nodes.

numbers correspond to the subfields described above in the Functional Description.

63.3.2.3.4 Activation

Activation is immediate and will be conveyed to the user with this message whenever the parm values are changed while RAISE_THRESHOLD is non-zero (i.e. feature is enabled):

> Note: This office parm change takes effect immediately for all DPT nodes by resetting the detection cycles with the updated parameter values.

If any XPKT806 alarms are present when the feature becomes disabled, then the alarms will be cleared immediately.

If any XPKT806 alarms are present when the parameters are changed while the feature is enabled, then the alarms will remain raised.

63.3.2.3.5 Dependencies

None

63.3.2.3.6 Consequences

None

63.3.2.3.7 Verification

To check that the office parameter changes are working, go to the MAPCI;MTC;APPL;PKT;SPM_ATM level and enter the PARMS command.

To actually see the XPKT806 alarm raised, you will need to cause XPKT301 logs via ATM call connection failures. Do NOT cause these failures in a live switch.

63.3.2.3.8 Memory requirements

No memory impact.

63.3.2.3.9 Parameter release history update

Introduced new XPKT806_DPT_RAISE_CLEAR parameter for Table OFCENG that controls raising XPKT806 alarm for DPT nodes.

63.3.2.4 XPKT806_SUPPRESSES_XPKT301

Suppress XPKT301 logs while XPKT806 alarm is raised against SPM node impacted by the XPKT301.

63.3.2.4.1 Functional description

This parameter controls the suppression of XPKT301 logs for SPM nodes that are already in an XPKT806 alarm condition. Possible values are Y and N, with default of N and recommended value of Y. This parameter is “off” (N) by default, so it must be turned “on” (Y) to suppress XPKT301 logs.

63.3.2.4.2 Provisioning rules

None

63.3.2.4.3 Range information

Table 5 Range Information

Minimum	Maximum	Default
N	Y	N

63.3.2.4.4 Activation

Activation is immediate. When value is changed from N to Y, the customer will see this informational message:

> Note: XPKT301 logs are now being suppressed for SPM nodes with the XPKT806 alarm raised.

When values is changed from Y to N, the customer will see this informational message:

> Note: No longer suppressing XPKT301 logs.

63.3.2.4.5 Dependencies

None

63.3.2.4.6 Consequences

None

63.3.2.4.7 Verification

Only way to verify operation is to cause a flood of XPKT301 failures that result from ATM call connection failures, then verify the XPKT301 logs are suppressed as XPKT806 alarms occur. Do NOT cause these failures in a live switch.

63.3.2.4.8 Memory requirements

No memory impact.

63.3.2.4.9 Parameter release history update

Introduced new XPKT806_SUPPRESSES_XPKT301 office parameter in Table OFCENG to suppress XPKT301 logs while XPKT806 alarm is raised.

63.4 Upgrade Impact

63.4.1 Dump and Restore

No impact.

63.4.2 Element Management Upgrade

N/A.

63.5 Data schema (DS) (CM, MIBS, RDB)

No impact.

63.6 Service Orders (SO) (CM & SESM)

No impact.

63.7 Software optionality control (SOC)

No impact.

63.8 Element Management

No impact.

63.9 Command interface changes

63.9.1 Map Level: MTC

63.9.1.1 Level description

Modify the APPL banner in the existing/resident Map MTC level so a new alarm will be displayed whenever one of the SMG4/IW/DPT nodes have an XPKT806 alarm present. The new alarm is “nn PKT” with major severity, where “nn” is the number of SMG4/IW/DPT nodes with the alarm and “PKT” is Packet. The precedence of “nn PKT” with respect to existing APPL alarms is that “nn PKT” is higher than a SDM billing alarm but lower than a SysB SDM alarm.

Here’s how the Map banner will appear if two nodes have the XPKT806 alarm:

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
   .       .       .       .       .       .       .       .       .    2 PKT
                                                                        M
   MTC         MTC:
  0 Quit
  2
  3 MTCNA
  4 SRSTATUS
  5 BERP
  6 CAPACITY
  7
  8
  9 XAC
 10 MS
 11 IOD
 12 Net
 13 PM
 14 CCS
 15 Lns
 16 Trks
 17 Ext
 18 APPL
   RLYNCH2
 Time  19:10  >
```

63.9.1.2 Accessing Map level: MTC

63.9.1.2.1 Access to MAP level and return to CI

To access the MTC level from CI, enter “mapci;mtc”
To return to CI, enter “quit all”

63.9.2 Map Level: APPL

63.9.2.1 Level description

Modifying the existing/resident Map APPL level to add a “PKT” display column and new menu command to enter the PKT level. Here’s how the new Map will appear when there are two ATM nodes with XPKT806 alarms:

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
   .       .       .       .       .       .       .       .       .     2 PKT
                                                                          M
 APPL             OAMAP  ATMFW   SDM   SPMCP  SWMTC  SDMBIL   PKT  TOPSIP
  0 Quit            .      .      .      .      .      .     2 PKT   .
  2                                                          M
  3
  4 OAMAP
  5 ATMFW
  6 SDM
  7 SPMCP
  8 SWMTC
  9 SDMBIL
 10 PKT
 11 TOPSIP
 12
 13
 14
 15
 16
 17
 18
   RLYNCH
 Time  14:25  >
```

63.9.2.2 Accessing Map level: APPL

63.9.2.2.1 Access to MAP level and return to CI

To access the APPL level from CI, enter “mapci;mtc;appl”

To return to CI, enter “quit all”.

63.9.3 Command: PKT

63.9.3.1 Command type: Listed MENU

63.9.3.2 Command target: All

63.9.3.3 Command availability: RES

63.9.3.4 Command description

New command under APPL level that allows entry to the new PKT level described below.

63.9.3.5 Command syntax

Table 6 PKT command parameters and variables

Command	Parameters and variables
PKT	(none)

63.9.3.6 Qualifications and warnings

If switch is running a MTXP/MSH20 Combo load, then the PKT command will be rejected with this error message:

Error: PKT command not supported in MTXP/MSH Combo loads.

63.9.3.7 Responses

If non-Combo load, then only response is to take user to the PKT level described below.

63.9.4 Map Level: PKT

63.9.4.1 Level description

Added new/resident Map PKT (for "Packet") level to show a dynamic summary of nodes contributing to the "nn PKT" alarm, and provide a new SPM_ATM command.

Here's how the Map will appear at the new PKT level when there are two SPM nodes with an XPKT806 alarm. The "SPM_ATM = 2" is the dynamic status that shows the number of ATM SPM (MG4K, IW, DPT) nodes that are contributing to the current "nn PKT" alarm. When there are no nodes with the XPKT806 alarm, a dot will be shown instead of a number (e.g. "SPM_ATM = .").

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
   .        .        .        .        .        .        .        .        .      2 PKT
                                                                                   M
PKT                OAMAP  ATMFW    SDM    SPMCP   SWMTC   SDMBIL   PKT    TOPSIP
  0 Quit              .      .      .       .       .       .     2 PKT     .
  2                                                                  M
```

```
 3
 4 SPM_ATM        SPM_ATM = 2
 5            PKT:
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
  RLYNCH4
Time  10:29  >
```

63.9.4.2 Accessing Map level: PKT

63.9.4.2.1 Access to MAP level and return to CI

To access the PKT level from CI, enter “mapci;mtc;appl;pkt”

To return to CI, enter “quit all”.

63.9.5 Command: SPM_ATM

63.9.5.1 Command type: Listed MENU

63.9.5.2 Command target: All

63.9.5.3 Command availability: RES

63.9.5.4 Command description

New command under PKT level that allows entry to the new SPM_ATM level described below.

63.9.5.5 Command syntax

Table 7 PKT command parameters and variables

Command	Parameters and variables
SPM_ATM	(none)

63.9.5.6 Qualifications and warnings

None

63.9.5.7 Responses

Only response is to take user to the SPM_ATM level described below.

63.9.6 Map Level: SPM_ATM

63.9.6.1 Level description

Added new/resident Map SPM_ATM level to display the dynamic XPKT806 alarm status on all 86 possible SMG4/IW/DPT nodes, and provide commands to troubleshoot the XPKT806 alarm on a node. Here's how the SPM_ATM level will appear when SPMs 62 and 65 have the XPKT806 alarm. Note that the dynamic PKT status is also shown (e.g. "SPM_ATM = 2" in the example below).

```
XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
   .        .        .        .        .        .        .        .        .      2 PKT
                                                                                   M
SPM_ATM            OAMAP   ATMFW    SDM    SPMCP   SWMTC   SDMBIL   PKT    TOPSIP
  0 Quit              .       .       .       .       .       .     2 PKT     .
  2                                                                   M
  3
  4 Status_          SPM_ATM = 2
  5 SumAll           Status of SPMs with XPKT806 alarms:
  6 SumFail                     1111111111222222222233333333333444
  7 Parms               0123456789012345678901234567890123456789012
  8 Clear_              ----------------------------------------
  9 Zero_               4444444555555555566666666667777777777888888
 10                     3456789012345678901234567890123456789012345
 11                     -----------------..*..*...-...------------
 12              KEY: '.' = OK   '*' = XPKT806 alarm   '/' = Disabled   '-' = N/A
 13              SPM_ATM:
 14
 15
 16
 17
 18
   RLYNCH4
 Time  10:35  >
```

Per the key above:

- "." indicates a supported SPM node class (e.g.SMG4) that has the feature enabled (via Table OFCENG) but does not currently have an XPKT806 alarm.
- "*" indicates a supported SPM node class that currently has an XPKT806 alarm raised (and, of course, the feature is enabled).
- "/" indicates a supported SPM node class that has the feature disabled so XPKT806 alarms will be ignored.
- "-" indicates an unsupported SPM node class (e.g. Legacy TDM SPM).

63.9.6.2 Accessing Map level: SPM_ATM

63.9.6.2.1 Access to MAP level and return to CI

To access the PKT level from CI, enter "mapci;mtc;appl;pkt;spm_atm"

To return to CI, enter "quit all".

63.9.7 Command: STATUS

63.9.7.1 Command type: Listed MENU

63.9.7.2 Command target: All

63.9.7.3 Command availability: RES

63.9.7.4 Command description

New command under ATM level that shows the XPKT806 statistics for a specified SPM node.

63.9.7.5 Command syntax

Table 8 <CommandName> command parameters and variables

Command	Parameters and variables
STATUS	<SPMNO> (0 to 85)
Parameters and variables	Description
<SPMNO>	Displays the XPKT806 statistics for the given SPM.

63.9.7.6 Qualifications and warnings

None

63.9.7.7 Responses

63.9.7.7.1 Command output

Table 9 MAP outputs with associated meanings and actions

STATUS Command
SPM: <SPMNUM> Class: <SPM Class> XPKT806 alarm: <stat> Which Cycle XPKT301 Thresh Time Cycle Cycle Type Hits Limit Elpsd Max ----- ------ ------ ------ ----- ----- Prev <CyTy> <Hits> <Thrs> <Time> <Max> Curr <CyTy> <Hits> <Thrs> <Time> <Max>
Meaning: Shows the statistics for processing XPKT806 alarms on the given SPM, where each parameter is described below: <stat> is “Raised” or “Clear” depending on the current **STAT**us of the XPKT806 alarm for the SPM. <SPMNUM> is the **NUM**ber of the **SPM**. <SPM Class> is the **SPM Class**, which is one of “SMG4”, “IW” (for BRDG_ONLY IW), or “DPT” (for DPT_ONLY IW). <CyTy> is the **CY**cle **TY**pe, which can be “Raise” or “Clear”. If “raise”, then raise cycle is determining whether XPKT806 alarm should be raised. If “clear”, then clear cycle is determining whether XPKT806 alarm should be cleared. <Hits> is the number of XPKT301 **HITS** (i.e. logs) against the node during the cycle. <Thrs> is the value of **THR**e**S**hold Limit in the cycle that must be reached to raise or clear the XPKT806 alarm. If the SPM class is SMG4 and the Cycle Type is “raise” cycle, then <Thrs> will be the value of RAISE_THRESHOLD in the XPKT806_SMG4_RAISE_CLEAR tuple in Table OFCENG. <Time> is the **TIME** Elapsed in the cycle. <Max> is the **MAX** time in the cycle. For a clear cycle on a IW node, this is the value of the CLEAR_CYCLE in the XPKT806_IW_RAISE_CLEAR parameter. **Note1:** if the feature is disabled for the SPM, then only the first line above is shown and the second line will be “Feature disabled - see PARMS command.” An example is shown below. **Note2:** if the first cycle is still running after a restart or enabling of the feature, then “Prev” info will not be valid. In this case, the entire “Prev” info line is replaced with “**Init**” until the initial current cycle completes. An example is shown below. **System or user actions:** If the XPKT806 alarm is present, you should analyze the XPKT301 logs and determine what ATM network problem is causing this node to raise the XPKT806 alarm. If the XPKT301 failures are acceptable, then consider raising the RAISE_THRESHOLD and/or RAISE_CYCLE sub-parameters in Table OFCENG for the particular SPM node class type.

63.9.7.8 Example

If the XPKT806 alarm is present on SPM 62, then the user enters “STATUS 62” at the SPM_ATM level and will see output like this:

```
SPM: 62  Class: SMG4  XPKT806 alarm: Raised
Which  Cycle  XPKT301 Thresh Time  Cycle
Cycle  Type    Hits   Limit Elpsd  Max
-----  ------ ------ ------ ----- -----
 Prev  Raise      3      3     4    15
 Curr  Clear      1      2     2     5
```

In this example, the alarm was raised on SPM 62 during the previous cycle when 3 XPKT301 failures were detected at 4 minutes into the 15 minute raise cycle. The RAISE_THRESHOLD was 3. The current cycle shows that we have had 1 XPKT301 failure at 2 minutes into the 5 minute clear cycle. If the cycle ends with less than 2 XPKT301 failures, then the XPKT806 alarm will automatically be cleared.

If the first cycle is running after a restart or after enabling the feature, then the output of STATUS will appear as:

```
SPM: 64  Class: IW  XPKT806 alarm: Clear
Which  Cycle   XPKT301  Thresh  Time   Cycle
Cycle  Type     Hits   Limit   Elpsd   Max
-----  ------  ------  ------  -----  -----
 Prev   Init
 Curr   Raise       0       2      2      5
```

If the feature is disabled for the SPM, then the output will appear as:

```
SPM: 64  Class: IW  XPKT806 alarm: Clear
Feature disabled - see PARMS command.
```

63.9.8 Command: SUMALL

63.9.8.1 Command type: Listed MENU

63.9.8.2 Command target: All

63.9.8.3 Command availability: RES

63.9.8.4 Command description

New command under the SPM_ATM level that shows the XPKT806 status for all SPMs that support this alarm (i.e. SMG4/IW/DPT).

63.9.8.5 Command syntax

Table 10 <CommandName> command parameters and variables

Command	Parameters and variables
SUMALL	(none)

63.9.8.6 Qualifications and warnings

None

63.9.8.7 Responses

63.9.8.7.1 Command output

Table 11 MAP outputs with associated meanings and actions

SUMALL Command

```
SPM Clas Cycle XPKT301 Thresh Time  Cycle
Num Type Type   Hits   Limit Elpsd  Max
--- ---- ----- ------ ------ ----- -----
<n><Clas><CyTy><Hits> <Thrs> <Time> <Max>
 .
 .
<n><Clas><CyTy><Hits> <Thrs> <Time> <Max>
```

Meaning: SUMALL lists the XPKT806 status for every supported SPM, where each parameter is described below. Supported SPMs are SMG4, IW, and DPT.

<SPM Num> is the **NUM**ber of the **SPM**.

<Clas>: **CLAS**s **TYPE** of the SPM node - can be “SMG4”, “IW”, or “DPT”.

<CyTy> is the **CY**cle **TY**pe, which can be “Raise”, “Clear”, or “Disabled”. If “Raise”, then raise cycle is determining whether XPKT806 alarm should be raised. If “Clear”, then clear cycle is determining whether XPKT806 alarm should be cleared. So don’t get confused: a “Clear” in this column means the XPKT806 alarm is raised for the node and we are looking to clear it. If “Disabled”, then the feature is currently disabled for this SPM node class and the other fields on this row will be blank. Run the “PARMS” command to see how to enable the feature for a SPM node class.

<Hits> is the number of XPKT301 **HITS** (i.e. logs) against the node during the current cycle.

<Thrs> is the value of **THR**e**S**hold Limit in the current cycle that must be reached to raise or clear the XPKT806 alarm. If the SPM class is SMG4 and the Cycle Type is “raise” cycle, then <Thrs> will be the value of RAISE_THRESHOLD in the XPKT806_SMG4_RAISE_CLEAR tuple in Table OFCENG.

<Time> is the **TIME** Elapsed in the current cycle.

<Max> is the **MAX** time in the current cycle. For a clear cycle on a IW node, this is the value of the CLEAR_CYCLE in the XPKT806_IW_RAISE_CLEAR parameter.

System or user actions: Useful for showing the XPKT301 hits across all SPMs in the ATM network.

Table 11 MAP outputs with associated meanings and actions

SUMALL Command

63.9.8.8 Example

Output of SUMALL command when there are only 5 ATM SPM nodes:

```
SPM Clas Cycle XPKT301 Thresh Time  Cycle
Num Type Type   Hits   Limit Elpsd  Max
--- ---- ----- ------ ------ ----- -----
 60 SMG4 Raise     0      3    12    15
 61 SMG4 Clear     1      3     4     5
 62 DPT  Raise     0      4    12    15
 63 DPT  Raise     0      4    12    15
 64 IW   Disabled
```

In this example, only one of the nodes (SPM 61) has the XPKT806 alarm raised. So SPM 61 is currently 4 minutes into a 5 minute “Clear” cycle, during which it has had one XPKT301 log (i.e. “hit”) against it. If three more XPKT301 hit occurs during this cycle (for a total of 4), then the alarm will not clear since the CLEAR_THRESHOLD is 3. If no more XPKT301 hits occur, then the alarm will automatically clear. Note that the feature is disabled for the IW class.

63.9.9 Command: SUMFAIL

63.9.9.1 Command type: Listed MENU

63.9.9.2 Command target: All

63.9.9.3 Command availability: RES

63.9.9.4 Command description

New command under the SPM_ATM level that shows the XPKT806 status for only those SPMs that currently have the XPKT806 alarm raised.

63.9.9.5 Command syntax

Table 12 <CommandName> command parameters and variables

Command	Parameters and variables
SUMFAIL	(none)

63.9.9.6 Qualifications and warnings

None

63.9.9.7 Responses

63.9.9.7.1 Command output

Table 13 MAP outputs with associated meanings and actions

SUMFAIL Command
SPM Clas Cycle XPKT301 Thresh Time Cycle Num Type Type Hits Limit Elpsd Max --- ---- ----- ------ ------ ----- ----- <n><Clas><CyTy><Hits> <Thrs> <Time> <Max> . . <n><Clas><CyTy><Hits> <Thrs> <Time> <Max> **Meaning:** SUMFAIL lists the status for every SPM that currently has the XPKT806 alarm raised. <SPM Num> is the **NUM**ber of the **SPM**. <Clas>: **CLAS**s **TYPE** of the SPM node - can be “SMG4”, “IW”, or “DPT”. <CyTy> is the **CY**cle **TY**pe, which can be “Raise” or “Clear”. If “raise”, then raise cycle is determining whether XPKT806 alarm should be raised. If “clear”, then clear cycle is determining whether XPKT806 alarm should be cleared. So don’t get confused: a “Clear” in this column means the XPKT806 alarm is raised for the node and we are looking to clear it. <Hits> is the number of XPKT301 **HITS** (i.e. logs) against the node during the current cycle. <Thrs> is the value of **THR**e**S**hold Limit in the current cycle that must be reached to raise or clear the XPKT806 alarm. If the SPM class is SMG4 and the Cycle Type is “raise” cycle, then <Thrs> will be the value of RAISE_THRESHOLD in the XPKT806_SMG4_RAISE_CLEAR tuple in Table OFCENG. <Time> is the **TIME** Elapsed in the current cycle. <Max> is the **MAX** time in the current cycle. For a clear cycle on a IW node, this is the value of the CLEAR_CYCLE in the XPKT806_IW_RAISE_CLEAR parameter. **System or user actions:** Useful for showing the XPKT301 hits across all SPMs in the ATM network that have an XPKT806 alarm raised.

63.9.9.8 Example

Output of SUMFAIL command when only 1 ATM SPM node in the office currently has the XPKT806 alarm raised:

```
SPM Clas Cycle XPKT301 Thresh Time  Cycle
Num Type Type   Hits   Limit Elpsd  Max
--- ---- ----- ------ ------ ----- -----
61 SMG4 Clear     1      3     4     5
```

In this example, only one of the nodes (SPM 61) has the XPKT806 alarm raised. So SPM 61 is currently in a clear cycle, during which it currently has had one XPKT301 hit. If three more XPKT301 hit occurs during this cycle (for

a total of 4 hits), then the alarm will not clear since the CLEAR_THRESHOLD is 1. If no more XPKT301 hits occur, then the alarm will automatically clear.

63.9.10 Command: PARMS

63.9.10.1 Command type: Listed MENU

63.9.10.2 Command target: All

63.9.10.3 Command availability: RES

63.9.10.4 Command description

New command under the SPM_ATM level that shows the office parameter values that control the reporting of XPKT806 alarms for the supported ATM SPMs. Also shows the parameter controlling XPKT301 suppression while the XPKT806 alarm is raised.

63.9.10.5 Command syntax

Table 14 <CommandName> command parameters and variables

Command	Parameters and variables
PARMS	(none)

63.9.10.6 Qualifications and warnings

None

63.9.10.7 Responses

63.9.10.7.1 Command output

Table 15 MAP outputs with associated meanings and actions

PARMS Command
Table OFCENG parameters that control threshold reporting: OFCENG Parameter Name — Raise Thrhld — Raise Cycle — Clear Thrhld — Clear Cycle XPKT806_SMG4_RAISE_CLEAR <x1> <y1> <a1> <b1> XPKT806_IW_RAISE_CLEAR <x2> <y2> <a2> <b2> XPKT806_DPT_RAISE_CLEAR <x3> <y3> <a3> <b3> Table OFCENG parameter that suppresses XPKT301 logs: XPKT806_SUPPRESSES_XPKT301 = <YES/NO> **Meaning:** PARMS command lists the current value of every office parameter that controls the threshold reporting of the XPKT806 alarm. Note that there are a set of values for every support ATM SPM class. Also shows the parameter that control suppressing XPKT301 logs while an XPKT806 alarm is raised against any SPM node impacted by the XPKT301. **System or user actions:** Shows user where to go in Table OFCENG to change the way XPKT806 is handled. Note that setting the RAISE_THRESHOLD to zero will disable reporting XPKT806 for that ATM SPM class.

63.9.10.8 Example

Output of PARMS command:

```
Table OFCENG parameters that control threshold reporting:
                         Raise   Raise  Clear   Clear
OFCENG Parameter Name    Thrhld  Cycle  Thrhld  Cycle
-----------------------  ------  -----  ------  -----
XPKT806_SMG4_RAISE_CLEAR      1      5       0      3
XPKT806_IW_RAISE_CLEAR        1      5       0      3
XPKT806_DPT_RAISE_CLEAR       1      5       0      3

Table OFCENG parameter that suppresses XPKT301 logs:
  XPKT806_SUPPRESSES_XPKT301 = NO
```

Note that XPKT806 reporting is currently disabled for all DPT nodes.

63.9.11 Command: CLEAR

63.9.11.1 Command type: Listed MENU

63.9.11.2 Command target: All

63.9.11.3 Command availability: RES

63.9.11.4 Command description

New command under SPM_ATM level that manually clears the XPKT806 alarm for a specified SPM node.

63.9.11.5 Command syntax

Table 16 <CommandName> command parameters and variables

Command	Parameters and variables
CLEAR	<SPMNO> (0 to 85)
Parameters and variables	Description
<SPMNO>	Manually clears the XPKT806 alarm for the given SPM.

63.9.11.6 Qualifications and warnings

If the alarm is raised, user will be prompted to confirm the action before proceeding. Here's the prompt that will appear:

Warning: confirm clearing XPKT806 alarm on SPM <nn> : (Y/N)>

where <nn> is the same number given as the option for the CLEAR command.

63.9.11.7 Responses

63.9.11.7.1 Command output

Table 17 MAP outputs with associated meanings and actions

CLEAR Command
XPKT806 alarm cleared for SPM <SPMNO> **Meaning:** Confirms that the XPKT806 alarm was manually cleared for the given SPM, where <SPMNO> is the number of the SPM. **System or user actions:** Helpful for user to manually clear an XPKT806 alarm without waiting for the clear interval to complete.

63.9.11.8 Example

If the XPKT806 alarm is present on SPM 63, then here's what is seen when the user manually clears the alarm:

```
clear 63
Warning: confirm clearing XPKT806 alarm on SPM  63 : (Y/N)>
y
Successful - XPKT806 alarm cleared for SPM 63
```

In this example, the alarm is successfully cleared so the SPM is reset into a fresh raise cycle with the XPKT301 hit counter cleared for that SPM.

If the SPM does not currently have the XPKT806 alarm present when CLEAR is run, then the output will appear as:

```
clear 63
No action taken - XPKT806 alarm is not present for SPM 63
```

63.9.12 Command: ZERO

63.9.12.1 Command type: Listed MENU

63.9.12.2 Command target: All

63.9.12.3 Command availability: RES

63.9.12.4 Command description

New command under SPM_ATM level that zero's the XPKT301 hit counter in the current cycle for a specified SPM node. See STATUS command for display of the XPKT301 hit counter in the current cycle.

63.9.12.5 Command syntax

Table 18 <CommandName> command parameters and variables

Command	Parameters and variables
ZERO	<SPMNO> (0 to 85)
Parameters and variables	Description
<SPMNO>	Manually zero's XPKT301 hit counter for the given SPM.

63.9.12.6 Qualifications and warnings

None

63.9.12.7 Responses

63.9.12.7.1 Command output

Table 19 MAP outputs with associated meanings and actions

ZERO Command
XPKT301 hit counter reset to 0 in current cycle for SPM <SPMNUM> **Meaning:** Confirms that the XPKT301 hit counter was reset to zero in the current cycle, where <SPMNO> is the number of the SPM. **System or user actions:** Helpful for user to manually zero the XPKT301 hit counter in the current cycle without waiting for the clear cycle to complete.

63.9.12.8 Example

Here's what is seen when the user manually zero's the XPKT301 hit counter for SPM 62:

```
>status 62
XPKT806 alarm: Raised   SPM: 62  Class: SMG4

Cycle  XPKT806  XPKT301  Time  Raise   Clear
       Alarm    Hits   Left  Thresh  Thresh
-----  ------  ------  ----  ------  ------
 Prev  Clear       3    11       3       2
 Curr  Raised      1     3       3       2
> zero 62
XPKT301 log hits reset to 0 for SPM 62
>status 62
XPKT806 alarm: Raised   SPM: 62  Class: SMG4

Cycle  XPKT806  XPKT301  Time  Raise   Clear
       Alarm    Hits   Left  Thresh  Thresh
-----  ------  ------  ----  ------  ------
 Prev  Clear       3    11       3       2
 Curr  Raised      0     2       3       2
```

In this example, the XPKT301 hit counter was 1 as shown by the first STATUS command. After the ZERO command, the second STATUS command confirms the counter was zeroed.

63.10 Security

No impact.

63.11 Configuration Walkthrough

This feature is "off" by default, so start by enabling the feature for each node type (SMG4, IW, DPT) with the appropriate office parameter in Table OFCENG (described above). Once enabled, the feature will run autonomously without user intervention to raise XPKT806 major alarms for any node that exceeds its XPKT301 threshold, then automatically clear the alarm with the clear threshold is met.

64: Configuration (CN): A00004271

64.1 Hardware and Software Requirements

N/A

64.2 Initial Configuration

N/A

64.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

64.4 Upgrade Impact

N/A

64.5 Data schema (DS) (CM, MIBS, RDB)

N/A

64.6 Service Orders (SO) (CM & SESM)

N/A

64.7 Software optionality control (SOC)

Table 1 SOC

SOC option name:	CS to AppS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0009
Option defined in DRU:	MSH
Affected products:	SN07

64.8 Element Management

N/A

64.9 Command interface changes

N/A

64.10 Security

N/A

64.11 Configuration Walkthrough

N/A

65: Configuration (CN): A00004391

65.1 Hardware and Software Requirements

Not applicable.

65.2 Initial Configuration

Not applicable.

65.3 Office parameters (OP)

65.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCOPT	MAX_NUMBER_ACD_AGENTS_PER_SWITCH	CHANGED	CM

65.3.2 Parameter information

65.3.2.1 MAX_NUMBER_ACD_AGENTS_PER_SWITCH

Maximum Number of Automatic Call Distribution Agents Per Switch

65.3.2.1.1 Functional description

This is a pre-existing office parameter which specifies the maximum number of ACD agent positions that the operating company can assign on the switching unit.

The purpose of this parameter will not be changed by this activity.

The range of this parameter will be increased to have a maximum value of 30,000 agents. The ability to assign a new value to this parameter will be restricted. A new value can only be assigned by changing the limit of the feature SOC.

When the SOC usage limit is increased or decreased, the value stored in the office parameter will be automatically updated to reflect the new limit. See section 13.7 for SOC information.

65.3.2.1.2 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	30000	0

This activity increases the maximum value of the office parameter.

65.3.2.1.3 Memory requirements

No memory impact.

65.3.2.1.4 Parameter release history update

The maximum value is being increased from 9999 to 30000 for SN07.

65.4 Upgrade Impact

65.4.1 Dump and Restore

This feature requires no operating company intervention during dump/restore or any other phase of ONP.

65.4.2 Element Management Upgrade

Not applicable.

65.5 Data schema (DS)

65.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ACDGRP	CHANGED	UNCHANGED

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
KSETLINE	CHANGED	UNCHANGED
KSETFEAT	CHANGED	UNCHANGED
IBNFEAT	CHANGED	UNCHANGED
ACDLOGIN	CHANGED	UNCHANGED
ACDENLOG	CHANGED	UNCHANGED

65.5.2 Table/MIB/Remote Database Schema information

65.5.2.1 Name: ACDGRP

ACD Group Info

65.5.2.1.1 Functional description

ACDGRP is an existing table. This table defines ACD groups. A new field is introduced by this activity to specify the size (number of digits) of the Login ID. The size is either 4 or 5 digits. Default value is 4 digits.

65.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.1.3 Size

The size of table ACDGRP is not impacted by this activity.

65.5.2.1.4 Fields

The following table lists fields for ACDGRP.

A new field IDSIZE is added to this table. All other fields of this table are unchanged.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IDSIZE	New	None	4 or 5	Size of the Login ID in number of digits.

65.5.2.1.5 Datafill example

The following example shows sample datafill for table ACDGRP. In this example, group ACDTEST1 is using 5 digit login IDs while the other 2 groups are using 4 digit login IDs.

Figure 1 Example tuples from table ACDGRP

```
ACDNAME        CUSTGRP ACDRNGTH              THROUTE
            NSROUTE PRIOPRO DBG MAXCQSIZ MAXWAIT
                                                    ACDMIS
                                MSQS DISTRING OBSWTONE
                  FRCNGTSV    IDSIZE
                                                    OPTIONS

-----------------------------------------------------------------------------------------
ACDGRP2             CGA             12              OFR3    1
            OFR3    1       0   N       12      20
                                                            N
                                N       NONE            N
                    N               4
                                                            $
ACDTEST1            IBNTST              0               OFRT    41
            OFRT    43      0   N       1       256
                                                            N
                                N       NONE            N
                    N               5
                                    (  VARWRAP 100) (   ACDCPK N )$
ACD1CGA             CGA             12              OFR3    1
            OFR3    1       0   N       12      20
                                                N
                                N       NONE                    N
                    N               4
                                                            $
```

65.5.2.1.6 Table release history update

Since BCS18.

65.5.2.1.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDGRP due to the new field IDSIZE introduced by this activity. The reformat procedures will default the value of this field to 4 during ONP.

65.5.2.1.8 Translation verification other tools

ACDGRP does not use translation verification tools.

65.5.2.2 Name: KSETLINE

Key Set Line Information table

65.5.2.2.1 Functional description

KSETLINE is an existing table. This table defines INCALLS KEY to key number 1 on ACD set. This activity changes the field POSID, which is the ACD position ID associated with the INCALLS KEY. The POSID will be changed to a 5 digit number.

65.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.2.3 Size

The size of table KSETLINE is not impacted by this activity.

65.5.2.2.4 Fields

The following table lists fields for KSETLINE.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the INCALLS key.

65.5.2.2.5 Datafill example

The following example shows sample datafill for table KSETLINE. Note the 5 digit POSIDs.

Figure 2 Example tuples from table KSETLINE

```
          KSETKEY
                FORMAT
                                                          DNRESULT
                KSFMTID
                                                  KSFMTARE
-------------------------------------------------------------------------------------------
HOST  05 0 00 06  1
                      ACD    Y          7502338
                        CGA    2          0  909
           INCALLS    CGAACD3   1 Y  00332
                                    (      3WC) (      MSB) (     ACDNR)$
                        MBS
HOST  05 1 00 06  1
                      ACD    Y          7502339
                        CGA    2          0  909
           INCALLS    CGAACD4   1 Y  00443
                                         (      MSB) (     ACDNR)$
                        MBS
SRCM  04 0 01 01  1
                      ACD    Y          7502331
                        CGA    2          0  909
           INCALLS    CGAACD1   1 Y  00112
                                    (      PRK) (      MSB) (     ACDNR)$
                        MBS
```

65.5.2.2.6 Table release history update

Since BCS10.

65.5.2.2.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table KSETLINE due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all ACD Position IDs upgraded during ONP.

65.5.2.2.8 Translation verification other tools

KSETLINE does use translation verification tools but are not impacted by this activity.

65.5.2.3 Name: KSETFEAT

Key Set Feature Information table

65.5.2.3.1 Functional description

KSETFEAT is an existing table. This table defines SUPR feature data when assigned to a keyset feature key. This activity changes the field POSID, which is the ACD position ID associated with the supervisor feature. The POSID will be changed to a 5 digit number.

65.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.3.3 Size

The size of table KSETFEAT is not impacted by this activity.

65.5.2.3.4 Fields

The following table lists fields for KSETFEAT.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the SUPR key.

65.5.2.3.5 Datafill example

The following example shows sample datafill for table KSETFEAT. Note the 5 digit POSIDs.

Figure 3 Example tuples from table KSETFEAT

```
                FEATKEY     FEATURE
                                                    KVAR
-------------------------------------------------------------------------------
HOST  00 0 19 02  1    SUPR       SUPR   ACDTEST2   1 Y 01111
HOST  00 1 08 01  1    SUPR       SUPR   ACDTEST2   1 Y 02222
HOST  01 0 00 14  1    SUPR       SUPR    CGAACD5   1 Y 05555
HOST  01 1 01 24  1    SUPR       SUPR    CGAACD2   1 Y 07777
HOST  05 1 00 06  1    SUPR       SUPR    CGAACD4   1 Y 04444
```

65.5.2.3.6 Table release history update

Since BCS10.

65.5.2.3.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table KSETFEAT due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all SUPR Position IDs upgraded during ONP.

65.5.2.3.8 Translation verification other tools

KSETFEAT does use translation verification tools but are not impacted by this activity.

65.5.2.4 Name: IBNFEAT

IBN Line Feature Information table

65.5.2.4.1 Functional description

IBNFEAT is an existing table. This table defines ACD and SUPR feature data when assigned to IBN sets. This activity changes the field POSID which is the ACD position ID associated with the ACD or SUPR options on the set. The POSID will be changed to a 5 digit number.

65.5.2.4.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.4.3 Size

The size of table IBNFEAT is not impacted by this activity.

65.5.2.4.4 Fields

The following table lists fields for IBNFEAT.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the ACD or SUPR option.

65.5.2.4.5 Datafill example

The following example shows sample datafill for table IBNFEAT. Note the 5 digit POSIDs.

Figure 4 Example tuples from table IBNFEAT

```
          LEN
            DNNO        DF      FEATURE
                                                                    DATA
-------------------------------------------------------------------------------
HOST  01 1 02 00
              0             ACD             ACD     CGAACD2   1 Y 00020
       (ACDNR )$
HOST  05 1 01 05
              0             ACD             ACD     ACDTEST1  1 Y 05115
             $
HOST  05 1 01 05
              0             SUPR            SUPR    ACDTEST1  1 Y 05225
```

65.5.2.4.6 Table release history update

Since BCS10.

65.5.2.4.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table IBNFEAT due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all ACD Position IDs upgraded during ONP.

65.5.2.4.8 Translation verification other tools

IBNFEAT does use translation verification tools but are not impacted by this activity.

65.5.2.5 Name: ACDLOGIN

ACD Login Table

65.5.2.5.1 Functional description

ACDLOGIN is an existing table. This table maps ACD Login IDs to a corresponding password, if needed. This table also maps Customer groups to the corresponding ACD Login ID, if requested. This table is indexed by Login ID.

65.5.2.5.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.5.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDLOGIN	0	30,000	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512. Two words of protected store is needed per tuple.

65.5.2.5.4 Fields

The following table lists fields for ACDLOGIN.

A range of the LOGINID field is changed by this activity. Remaining fields of this table are not changed.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	Changed	None	5-digit number between 00001 and 30000	The range of ACD Login ID is expanded to accommodate 30,000 Login IDs.

65.5.2.5.5 Datafill example

The following example shows sample datafill for table ACDLOGIN. Note the 5 digit LOGINIDs.

Figure 5 Example tuples from table ACDLOGIN

```
LOGINID CUSTGRP PSWD OPTIONS
-------------------------------------------------------------------------------
00551 Y CGA N (VARWRAP 100) $
01001 N N $
01002 Y IBNTST Y 1234 $
01003 Y IBNTST Y 1234 (VARWRAP 60) (PAQ 1) $
02001 N N $
02002 Y COMKODAK Y 1234 $
02003 Y COMKODAK Y 1234 (VARWRAP 60) (PAQ 1) $
04120 Y CGA N (VARWRAP 100) $
```

65.5.2.5.6 Table release history update

Since BCS18.

65.5.2.5.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDLOGIN due to change in field LOGINID made by this activity. The reformat procedures will prefix a digit 0 to all Login Ids upgraded during ONP.

65.5.2.5.8 Translation verification other tools

ACDLOGIN does not use translation verification tools.

65.5.2.6 Name: ACDENLOG

ACD Enhanced Login

65.5.2.6.1 Functional description

Table ACDENLOG is an existing table. It allows multiple customer groups the full range of Login IDs for their ACD agents. This table is indexed by a two-part key, made up of the Partition Number (PARTNO) and Login ID (LOGINID). The table format is same as table ACDLOGIN with one additional field, ACTIVATE.

65.5.2.6.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

65.5.2.6.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDENLOG	0	30,000	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512. Two words of protected store is needed per tuple.

65.5.2.6.4 Fields

The following table lists fields for ACDENLOG.

The range of the LOGINID field is changed by this activity. Remaining fields of this table are not changed.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	Changed	None	5-digit number between 00001 and 30000	The range of ACD Login ID is expanded to accommodate 30,000 Login IDs.

65.5.2.6.5 Datafill example

The following example shows sample datafill for table ACDENLOG. Note the 5 digit LOGINIDs.

Figure 6 Example tuples from table ACDENLOG

```
 PARTNO LOGINID ACTIVATE  CUSTGRP  PSWD OPTIONS
-------------------------------------------------------------------------------
121 00551 N Y CGA N (VARWRAP 100) $
121 01001 N N N $
124 00551 N Y IBNTST Y 1234 $
125 01003 N Y IBNTST Y 1234 (VARWRAP 60) (PAQ 1) $
131 02001 N N N $
133 02002 N Y COMKODAK Y 1234 $
205 02002 N Y COMKODAK Y 1234 (VARWRAP 60) (PAQ 1) $
212 04120 N Y CGA N (VARWRAP 100) $
```

65.5.2.6.6 Table release history update

Since BCS20.

65.5.2.6.7 Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDENLOG due to change in field LOGINID made by this activity. The reformat procedures will prefix a digit 0 to all Login Ids upgraded during ONP.

65.5.2.6.8 Translation verification other tools

ACDENLOG does not use translation verification tools.

65.6 Service Orders (SO)

This activity does not introduce any new Service Order commands, LCCs, or options.

65.6.1 Service order change details

When the ACD option is added to a line (ADO, NEW, NEWACD commands), or when ACD option data is changed (CHF command), one of the prompts offered by Servord is POSID. Currently, any value between 0001 and 9999 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be a 5 digit value in the range of 00001 to 30000.

65.6.1.1 How service order commands are presented

65.6.1.1.1 Description

The range of valid input for the POSID prompt has changed. Previously, the POSID was entered as a 4 digit value in the range of 0001 to 9999. It will now be entered as a 5 digit value in the range of 00001 to 30000.

65.6.1.1.2 Applicability

The POSID prompt is applicable to Servord commands ADO, NEW, NEWACD, and CHF only when they are used to manipulate the data associated with the ACD or SUPR line option.

65.6.1.1.3 Example

The following figures show an example of adding the ACD option to an existing business set using the ADO command. Note that when the system prompts for POSID, the user must now provide a 5 digit value in the range of 00001 to 30000. Previously, a 4 digit value would have been accepted.

Figure 7 Example of the ADO command in prompt mode

```
SO:
>ado
SONUMBER:    NOW   3 11  6 AM
>
DN_OR_LEN:
>6218000
OPTKEY:
>1
OPTION:
>acd
ACDGROUP:
>acdtest1
ACDSGRP:
>0
IDNUM:
>y
POSID:
>00018
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 11 6 AM 6218000 ( 1 ACD ACDTEST1 0 Y 0009 ( ) ( ) ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Figure 8 Example of the ADO command in no-prompt mode

```
SO:
>ado $ 6218000 1 acd acdtest1 0 y 00018 $
```

The NEW, NEWACD, and CHF commands also offer the POSID prompt when used to manipulate ACD data. Examples of these commands are not provided because the effect of this change is identical to the ADO example shown above. POSID must now be input as a 5 digit value.

65.6.1.1.4 Command prompts

The valid input has changed for system prompt POSID.

Table 12 Valid input for POSID

Prompt	Valid input	Description	Areas affected by prompt
POSID	00001 to 30000	ACD agent position ID.	Affects Servord commands ADO, NEW, NEWACD, and CHF when used to manipulate ACD option data.

65.7 Software optionality control (SOC)

This feature will be controlled by a standard usage based SOC. The usage limit will define the maximum number of ACD agents in the switch.

The default usage limit will be 0 ACD agents. During ONP from previous loads, the SOC usage limit will be set to match the value of office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH. Thus there will be no impact to existing customers who do not purchase this SOC.

The SOC usage limit will control the maximum number of ACD agents in the switch. The office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH will automatically be updated to match the SOC usage limit anytime the SOC usage limit is changed (increased or decreased).

The other aspects of this feature including 5 digit login optionality, ability to use login IDs between 10000 and 30000, and mandatory use of 5 digit POSIDs are not controlled in anyway by the SOC.

Table 13 SOC

SOC option name:	ACD00101
SOC option title:	ACD Agent Expansion
SOC option control type:	USAGE
New SOC option?	YES
SOC option order code	00037650
Option defined in DRU:	CCM
Affected products:	NA100, SL100

65.8 Element Management

Not applicable.

65.9 Command interface changes

65.9.1 Command: ACDDEBUG

65.9.1.1 Command type: NON-MENU

65.9.1.2 Command target: All

65.9.1.3 Command availability: RES

65.9.1.4 Command description

ACDDEBUG is a CI tool created to display ACD data structures in both dynamic and static environments.

The available commands are:

QUERY - Allows display of ACD data structures

CPIDTOAGT - Displays LEN and DN for entered line cpid or CLLI and member number for an entered trunk cpid.

QUIT - Quits from ACDDEBUG environment

Currently, the Query command uses a 4 digit positionID as an index in order to display ACD agent data. This activity will extend the command so that the data structures of an ACD agent with a 5 digit position will be displayed.

65.9.1.5 Command syntax for changed parameters

Table 14 ACDDEBUG command parameters and variables

Command	Parameters and variables
QUERY AGENTDATA	ALL, GROUP, POSID

Table 14 ACDDEBUG command parameters and variables

Command	Parameters and variables
Parameters and variables	**Description**
ALL	Displays all agent data on the switch
GROUP	Displays agent data in a particular ACDGROUP
POSID	Displays agent data for a particular position ID. The positionID must be 5 digits.

65.9.1.6 Qualifications and warnings

NA

65.9.1.7 Responses

65.9.1.7.1 Wrong type

Table 15 CI outputs with associated meanings and actions

ACDDEBUG
Wrong type: <ACD_posid?> {1 TO 30,000} Enter: <ACD_posid?> [<Form?>]   **Meaning:** The user has input an invalid position ID. **System or user actions:** Input a valid position ID from 1 to 30,000

65.9.1.8 Example

Table 16 Usage examples for ACDDEBUG Query command

Description of task:	Display the ACD agent data
Command: MAP response:	QUERY agentdata posid 12300 ACD GROUP NUMBER 5 (“ACDTEST1”) - - ACD AGENT DATA Protected Data - Index 22 Address 59443834 Incalls Cp_id: HOST 01 0 06 04 DN 6136212200 KEY 1 Agent Position ID: 12300 SCAI agent: NO Unprotected Data - Index 22 Address 4EC906E0 ECM_ASSOCIATED: N ECM_USER_DATA_PTR: FFFF0000 ECM_IDX_IN_AGT_LIST: -515 ECM_NETNODEID: 4261281277 Agent Login ID: 11300 Agent Login Partition NO.: 0 Status: ACDIDLE Not Ready Active: N

65.9.2 Command: ACDSHOW

65.9.2.1 Command type: NON-MENU

65.9.2.2 Command target: All

65.9.2.3 Command availability: RES

65.9.2.4 Command description

ACDSHOW is a CI tool that displays specific information concerning a current ACD configuration such as the a list of agent positions in a ACD group and agent information for a given user login ID. Currently, ACDSHOW commands use a 4 digit positionID as an index in order to display information concerning an ACD configuration. This activity will extend the command so that the information of an ACD agent with a 5 digit position will be displayed.

The available commands are:

ACDSHOW		
ACDDNS	HELP	QUIT
ACDSHOW	LOADMGMT	STATUS
ADMINGROUP	LOGINID	SUPERVISOR
AGTPOS	MODE	TABENTRY
AUDIOGROUP	NSAUDGRP	THRESHOLD
COUNTS	NSROUTE	THROUTE
GROUPINFO	OVFLROUTE	VALIDAUDIO
GROUPNAME	PASSWORD	VALIDROUTES
FIAUDGRP	FOAUDGRP	CLRROUTE
RENQTOUT	RENQRTE	RENQAUD

65.9.2.5 Command syntax for changed parameters

Table 17 ACDSHOW command parameters and variables

Command	**Parameters and variables**
AGTPOS	ALL, GROUP, POSID, LEN, DN, CLLI,
LOGINID	ID
Parameters and variables	**Description**
ALL	Displays all agent data on the switch.
GROUP	Displays agent data in a particular ACDGROUP.

Table 17 ACDSHOW command parameters and variables

Command	Parameters and variables
POSID	Displays agent data for a particular position ID. The positionID will be 5 digits.
LEN	Displays agent data for a particular LEN.
DN	Displays agent data for a particular DN.
CLLI	Displays agent data for a particular CLLI.
ID	Displays agent data for a particular login ID.The loginID will be 5 digits.

65.9.2.6 Qualifications and warnings

NA

65.9.2.7 Responses

65.9.2.7.1 Wrong type

Table 18 CI outputs with associated meanings and actions

ACDSHOW
Wrong type: <ACD_posid?> {1 TO 30,000} Enter: <ACD_posid?> [<Form?>]   **Meaning:** The user has input an invalid position ID. **System or user actions:** Input a valid position ID from 1 to 30,000

65.9.2.8 Example

Table 19 Usage examples for ACDSHOW AGTPOS command

Description of task:	Show ACD information by ACD agent positionID

Table 19 Usage examples for ACDSHOW AGTPOS command

Command:	AGTPOS POSID 12300
MAP response:	Agent: HOST 01 0 06 04 DN 6136212200 KEY 1 Agent Login ID: 11300 Status: IDLE Loginid Partition: 0

Table 20 Usage examples for ACDSHOW LOGINID command

Description of task:	Show ACD information by ACD agent loginID
Command:	LOGINID 11300 brief ibntst
MAP response:	Agent Position ID: 12300 Agent Login ID: 11300 Status: IDLE Loginid_Partition: 000
Command:	LOGINID 11300 full ibntst
Map response:	Agent Position ID: 12300 Agent Login ID: 11300 Status: IDLE Loginid_Partition: 000 Agent: HOST 01 0 06 04 DN 6136212200 KEY 1 ACD Group: ACDTEST1 ACD Subgroup: 0 SCAI Agent: NO

65.10 Security

Not applicable

65.11 Configuration Walkthrough

Not applicable

66: Configuration (CN): A00004414

66.1 Hardware and Software Requirements

N/A

66.2 Initial Configuration

N/A

66.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

66.4 Upgrade Impact

N/A

66.5 Data schema (DS) (CM, MIBS, RDB)

N/A

66.6 Service Orders (SO) (CM & SESM)

N/A

66.7 Software optionality control (SOC)

Table 1 SOC

SOC option name:	CS to CS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0008
Option defined in DRU:	MSH
Affected products:	SN07

66.8 Element Management

N/A

66.9 Command interface changes

N/A

66.10 Security

N/A

66.11 Configuration Walkthrough

N/A

67: Configuration (CN): A00004500

67.1 Hardware and Software Requirements

NONE

67.2 Initial Configuration

NONE

67.3 Office/Subnet parameters (OP/SP) (CM & SESM)

NONE

67.4 Upgrade Impact

NONE

67.5 Data schema (DS) (CM, MIBS, RDB)

67.5.1 New/modified tables, MIBs, or Database Schema

New table IPAPPL will be created to store data on each SCTP instance.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPAPPL	NEW	NEW
TRIGITM	Changed	NEW
TRIGINFO	Changed	NEW

67.5.2 Table/MIB/Remote Database Schema information

67.5.2.1 Name: IPAPPL - Internet Protocol Appliction

67.5.2.1.1 Functional description

Table IPAPPL defines the IP Application instance that data will be transmitted over for a given service. This table is being created for the AIN on SCTP/IP project but it is being designed so that it could be used by other applications (ie. ACB/AR, NMS) that may want to use IP as a transport in the future. The table will contain the connection information for controlling the communications processes associated with the transport.

67.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

IPAPPL

TRIGITM

OR

TRIGINFO

Tables TRIGITM and TRIGINFO use the INST (sctp instance) that is datafilled in table IPAPPL.

67.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IPAPPL	0	64	Memory is automatically allocated for 64 Intelligent Network SCTP instances.

67.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for Table IPAPPL.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INSTKEY	NEW	subfield	0-64	Defines the SCTP instance number.
INSTNAME	NEW	subfield	8 character vector	Defines the SCTP instance name.
TRANSPRT	NEW	subfield	SCTP	Defines the transport to be used by the application.
IPDEVICE	NEW	subfield	EIU/HIOP	Specifies the device that the instance will use.
IPADDRS	NEW	subfield	Vector of up to 4 IPV4 IP addresses	Specifies the remote IP addresses to be used for the instance.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IPPORT	NEW	subfield	UNSIGNEDINT	Specifies the IP port to be used.
OPTLIST	NEW	subfield	VECTOR of IP_OPTION_LIST	Specifies optional data associated with the instance.
Application	NEW	refinement of optlist	Service {AIN}	Defines the service that is using the insctance.
Multihoming	NEW	refinement of optlist		Specifies if the insctance supports multihoming.
Mode	NEW	refinement of optlist	Client, Server	Specifies if the insctance is a client or server.
Setprime	NEW	refinement of optlist	1 to 4	Specifies which of the IP address in the IPADDRS field is the primary.

67.5.2.1.5 Datafill example

The following example shows sample datafill for table IPAPPL

TABLE IPAPPL

INSTKEY INSTNAME TRANSPRT IPDEVICE IPADDRS IPPORT OPTLIST

---

0 SS SCTP EIU (IPV4 47 142 160 173) $ 4977 (APPLICATION AIN R02)

(SETPRIME 1) (MODE SERVER) $

67.5.2.1.6 Fields/OIDs

The following table lists fields/OIDs for Table TRIGITM/TRIGINFO.

Table 4 Table field descriptions TRIGITM/TRIGINFO

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AIN_TRANSPORT	Changed	refinement	SCTP INST {0 to 64}	Adding SCTP as a valid AIN transport.

67.5.2.1.7 Datafill example

The following example shows sample datafill for table TRIGITM and TRIGINFO.

TABLE TRIGITM

TDP TINAME TRIGGER TRIGDATA CRITERIA STATE ACTION SLHR OPTIONS

---

20 SSTAT TERMATT $ ULK EVENT R02 SCTPIP 0 $

TABLE TRIGINFO

KEY ACTION OPTIONS

AININFO EVENT TCAP R02 SCTPIP 0 $

67.5.2.1.8 Table release history update

NONE

67.5.2.1.9 Supplementary information

NONE

67.5.2.1.10 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify TRIGITM.

>traver l 7502511 95505555 b

TABLE IBNLINES

HOST 00 0 00 22 0 DT STN IBN 7502511 CGA 0 0 909 (CDC) (CNDB) $

TABLE DNATTRS

909 750 2511

(PUBLIC (NAME ASTN1CGA0) $)

(PRIVATE (NAME PASTN1CGA0) $)$ $

TABLE DNGRPS

909 750 2511 2511

(PUBLIC (NAME CGA) $)

(PRIVATE (NAME PCGA) $)$

TABLE IBNFEAT

TUPLE NOT FOUND

TABLE CUSTSTN

TUPLE NOT FOUND

TABLE OFCVAR

AIN_OFFICE_TRIGGRP TIID

AIN Orig Attempt TDP: no subscribed trigger.

TABLE NCOS

CGA 0 0 0 CGA0 (IDDDARS N)$

TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL

CGA CGAXLA CGXXLA STARXLA 1 CGXCOL

TABLE DIGCOL

CGXCOL 9 POTS Y

TABLE IBNXLA: XLANAME CGAXLA

CGAXLA 9 NET Y Y 1 Y POTS N N GEN (LATTR 42 909_EAEO_42 L909_LATA1_42) (EA C541 Y 0)$ $

TABLE DIGCOL

POTS specified: POTS digit collection

TABLE LINEATTR

42 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 909_EAEO_42 L909_LATA1_42 $

LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

909_EAEO_42 NSCR 909 EAEO RTE4 Y RGA 0 0 $ $

TABLE RATEAREA

L909_LATA1_42 L909 NIL LATA1 $

TABLE STDPRTCT

EAEO (1) (1) 6

. SUBTABLE STDPRT

WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE

BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO

DOCUMENTATION.

. 550 5551211 N NP 0 NA

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE HPCPATTN

TUPLE NOT FOUND

TABLE HNPACONT

909 Y 949 8 (133) (1) (0) (0) 2 $

. SUBTABLE HNPACODE

. 550 550 DN 909 550

TABLE TOFCNAME

909 550 $

TABLE DNINV

909 550 5555 D BLDN

TABLE DNFEAT

TUPLE NOT FOUND

TABLE DNATTRS

TUPLE NOT FOUND

TABLE DNGRPS

TUPLE NOT FOUND

TABLE TMTCNTL

LNT (148)

. SUBTABLE TREAT

. BLDN Y S T120

LNP Info: Called DN is not resident.

LNP Info: HNPA results are used.

TABLE LCASCRCN

909 L909 (10) OPTL N N Y

. SUBTABLE LCASCR

. 550 551

TABLE PFXTREAT

OPTL NP Y NP UNDT

AIN Info Collected TDP: no subscribed trigger.

Checking AIN SDS Trigger Items as SDS is compatible with current call

. . TABLE OFCTIID

. . 4 SSSDS ON

. . TABLE TRIGITM

. . 4 SSSDS SDS (DG 9095505555) $ ULK EVENT R02 SCTPIP 0 $

AIN Info Analyzed TDP: trigger criteria met.

Querying the database would occur now.

Use the AINMQG option to save the query to a file for use in TstQuery.

Use the AINRES option for further information

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

AIN Info Analyzed TDP: trigger criteria met.

Querying the database would occur now.

Use the AINMQG option to save the query to a file for use in TstQuery.

Use the AINRES option for further information

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

67.6 Service Orders (SO) (CM & SESM)

Not impacted.

67.7 Software optionality control (SOC)

A new usage/limit SOC INW00003 will be created by this activity to control the allocation of IN SCTP links in table IPAPPL. If the limit has not been met the the user will be allowed to add entries to table IPAPPL.

Table 5 SOC

SOC option name:	IN Messages Over IP
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	INW00003
Option defined in DRU:	SHR
Affected products:	All

67.8 Element Management

Not Impacted.

67.9 Command interface changes

67.9.1 Command: TSTQUERY

The AIN TSTQUERY command will be changed to support SCTPIP as a valid transport.

67.9.1.1 Command type: Listed MENU

The setrnsp MENU command will be modified to allow for SCTPIP prompting.

67.9.1.2 Command target: All

67.9.1.3 Command availability: RES

67.9.1.4 Command description

The setrnsp command is used to specify which AIN transport the TSTQUERY message should be sent over.

67.9.1.5 Command syntax

Help setrnsp

Command to set the Transport

Parms: <Transport> {SS7 <GttName> STRING

<GttSource> {DEFAULT,

CHARGE,

CALLED},

TCPIP <Application Instance Number> {0 TO 3},

SCTPIP <Application Instance Number> {0 TO 64}

67.9.1.6 Qualifications and warnings

NONE

67.9.1.7 Responses

NONE

67.9.1.8 Example

Setrnsp sctpip 0

67.10 Security

67.11 Configuration Walkthrough

68: Configuration (CN): A00004872

The SN07 services contained in this activity are assigned similar to current legacy methods. These services are ACD OBS/FOBS, ACD EMK, MBSCAMP, MOH, EBO/EBX, and DCBI. For more general information on these services, see the FN section of this document.

68.1 Hardware and Software Requirements

These services are configured in Succession as they are in Legacy. The tones provided by these services for a pure Succession network are provided by a gateway (GW), and therefore the physical characteristics of those tones are a product of the GW playing the tone. Information pertaining to this tones must be configured before the tone can be provided for Legacy offices where the tones are provided by the MTM. For Succession lines, since the tone is provided by the GW, no tone datafill is required.

68.2 Initial Configuration

Not applicable.

68.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

68.4 Upgrade Impact

68.4.1 Dump and Restore

Not applicable.

68.4.2 Element Management Upgrade

Not applicable.

68.5 Data schema (DS) (CM, MIBS, RDB)

68.5.1 New/modified tables, MIBs, or Database Schema

Datafill in Table STN is not required for a pure Succession office.

68.5.2 Table/MIB/Remote Database Schema information

68.5.2.1 Name: Table STN

Special Tones

68.5.2.1.1 Functional description

Table STN is used to provision the hardware associated with special tones, typically played from a MTM circuit pack. With this activitiy, datafill is not required to support a purely Succession switch. If Legacy lines exist on the

switch, this datafill is still required as it exists today in order to provide tones from the MTM..

68.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

68.5.2.1.3 Size

There is no change to the size limits to Table STN.

68.5.2.1.4 Fields/OIDs

There are no new fields for Table STN.

68.5.2.1.5 Datafill example

The following example shows sample datafill for table STN for Legacy, which is not required for Succession.

STN EBOT 1 MTM 5 14 3X68AC 10 0

68.5.2.1.6 Table release history update

Not applicable.

68.5.2.1.7 Supplementary information

The services of this activity that require special tones to be configured must now state that the tone can be provisioned via Table STN for Legacy lines, but this is no longer a requirement for packet lines. Also, the “typical” tone characteristics can be stated but if the tone is played by the GW, these characteristics are a product of the GW providing the tone.

The following table lists examples of current documentation and notes on the changes required.

Table 1 Changes required for special tones via Table TONES

Document type	Current information	Modification needed
Data Schema for Table TONES description (volume 10 in LEC017)	Functional description states: The special tones listed below are generated on cards located on a trunk module (TM) or maintenance trunk module (MTM), and defined in table STN instead of table TONES: *BVTONE: IBN busy verification tone *CWT: call waiting tone *DISTCWT: distinctive call waiting tone *EBOT: executive busy override tone *ERWT: expensive route warning tone *OHQT: offhook queuing tone *ROH: receiver offhook tone	It should be noted that these tones may exist in Table STN when the tone is played by the TM/MTM device for Legacy/TDM lines.
Translations Guide for DCBI feature (volume 11 in LEC017)	Description states: Both parties of the current call can receive an optional warning tone before the barging-in of the activating station occurs. The application of this tone is a customer group option. The DCBI tone contains 440 Hz at 13dbm. Datafill sequence show Table STN as a table requiring datafill for feature, stating: You must enter data in table STN to define the special tones used with DCBI.	It is suggested that the actual tone be stated as “typically” 440hz at 13dbm (since the characteristics can now be dependent on the GW configuration). It should be noted that the DCBITONE is not required for packet lines
Data Schema for Table CUSTSTN DCBITIONE (volume 3 in LEC017)	CUSTSTN option DCBITIONE states : Tone circuits in table STN with the code EBOT supply the warning tones	The TONE EBOT may be provided from a GW so that Table STN datafill is not required
Translations Guide for MBS Busy Override (volume 14 in LEC017)	Operation of feature states that when the calling party presses the EBO key, the called party and the party connected to the called party hears 500 ms of EBO warning tone. The translations table flow mentions defining EBOT in table STN for this feature. Datafilling table STN describes the provisioning required.	The “typical” tone length is 500 ms. The EBOT tone datafill is not a requirement for packet lines.
Translations Guide for Station camp on for Meridian Business Set (volume 15 in LEC017)	Translations table flow states: Table STN is required for tones that require trunk cards and allows MBSCAMP to work to another MBS. A 3X68AC... is required along with CWT datafill. The summary of table flow defines table STN and gives datafill for CWT tone.	The CWT tone is no longer needed for MBSCAMP to a Succession pphone (standard CWT buzz is now supplied). However it is still required of a Legacy pphone.

Table 1 Changes required for special tones via Table TONES

Document type	Current information	Modification needed
Translations Guide for ACD OBS (volume 16 in LEC017)	Description states “If OBSWTONE is set to Y,make an entry in table STN. Refer to the data schema section of this document for additional information on table STN.”	An entry is not required in table STN for a packet line.

68.5.2.1.8 Translation verification other tools

Table STN does not use translation verification tools.

68.6 Service Orders (SO) (CM & SESM)

Not applicable

68.7 Software optionality control (SOC)

Not applicable.

68.8 Element Management

Not applicable

68.9 Command interface changes

Not applicable

68.10 Security

Not applicable

68.11 Configuration Walkthrough

In order to configure the SN07 services ACD OBS, EBO, and DCBI to play tones from the GWs, if the office is a legacy office which plays the tone through the MTM, the current TABLE STN provisioning is still used. For provisioning these services on packet lines using audio servers for conferencing, no tones datafill is required.

69: Configuration (CN): A00005007

69.1 Hardware and Software Requirements

Not Applicable to the activity A00005007.

69.2 Initial Configuration

Not Applicable to the activity A00005007

69.3 Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	REPORT_ISUP _CI_TO_CM	NEW	CM

69.3.1 Parameter information

69.3.1.1 Name: REPORT_ISUP_CI_TO_CM

Reporting of Cause Indicator to CM.

69.3.1.1.1 Functional description

This parameter will enable sending of supervision to GWC for reporting of the cause indicator of Relase message to CM. The cause indicator will be attached to the Clear Forward or Clear Back Message.
This implementation of this parameter is being done in ISN07 (SNWCSH07).

69.3.1.1.2 Provisioning rules

This parameter enables sending of supervision when set to TRUE and disables when set to FALSE.

69.3.1.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
Boolean {N,Y}	n/a.	N

69.3.1.1.4 Activation

Any changes are activated immediately.

69.3.1.1.5 Dependencies

None.

69.3.1.1.6 Consequences

None

69.3.1.1.7 Verification

No verification required for this parameter.

69.3.1.1.8 Memory requirements

No memory impact.

69.3.1.1.9 Parameter release history update

Creating Office Parameter REPORT_ISUP_CI_TO_CM in table OFCENG.

69.4 Upgrade Impact

Not Applicable to the activity A00005007.

69.5 Data schema (DS) (CM, MIBS, RDB)

Not Applicable to the activity A00005007.

69.6 Service Orders (SO) (CM & SESM)

Not Applicable to the activity A00005007.

69.7 Software optionality control (SOC)

Not Applicable to the activity A00005007.

69.8 Element Management

Not Applicable to the activity A00005007.

69.9 Command interface changes

Not Applicable to the activity A00005007.

69.10 Security

Not Applicable to the activity A00005007.

69.11 Configuration Walkthrough

Not Applicable to the activity A00005007.

70: Configuration (CN): A00005016

70.1 Hardware and Software Requirements

NA

70.2 Initial Configuration

NA

70.3 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

70.4 Upgrade Impact

NA

70.5 Data schema (DS) (CM, MIBS, RDB)

70.5.1 New/modified tables, MIBs, or Database Schema

As part of this feature the following modification was made to the UEMG Megaco Enterprise MIB:

The previous definition of nnMegacoFaultType had only one type in it:

```
nnMegacoFaultType OBJECT-TYPE
    SYNTAX     INTEGER
               {
                 rootTermStatusChange     (1)
               }
    MAX-ACCESS accessible-for-notify
    STATUS     current
    DESCRIPTION
       "Type of Megaco Fault"
::= { nnMegacoNotifObjects 1 }
```

This has been replaced by the following definition:

```
nnMegacoFaultType ::= TEXTUAL-CONVENTION
    STATUS     current
    DESCRIPTION
       "Enumeration of Fault Types Megaco Maintenance will throw."
    SYNTAX     INTEGER
               {
                 rootTermStatusChange     (1),          -- generic reason
                vMGAdminStatusOutOfService (2),  - VMG was administratively set
to out of service

                 cardLocked (3),          -- card is locked
                 cardDisabled (4),        -- card is disabled
                 cardInitializing (5),        -- card is initializing
                   lineMtceOnPairNotReady (8),    -- Line maintenance is not ready
              megacoMtceOnPairNotReady (9),    -- Megaco maintenancec is not ready
```

```
                gwcLinkStatusDown (51), -- first hop layer 2 down
                edgeRouterUnreachable(52),  -- pings to reach first hop failed
                gWCUnreachable (53),      -- pings to reach GWC failed
                noGWCReply (54),          -- GWC didn't reply to ServiceChange
                bearerSubsystemOnPairNotReady (55),
                aal1BearerSubsystemOnPairNotReady (56),
                ipBearerSubsystemOnPairNotReady (57),
                                --- skip 58
            carrier NotProvisioned (59), -- physical interface not provisioned
                carrierNotReady (60), -- physical interface not ready
             networkInterfaceNotProvisioned (61),   -- layer 2 not provisioned
                networkInterfaceNotReady (62),    -- layer 2 not ready
                messagingInterfaceNotProvisioned  (63),  -- call control not
provisioned
                messagingInterfaceNotReady (64),  -- call control not ready
                                --- skip 65 and 66
                bearerInterfaceNotProvisioned  (67),  -- bearer subnet not
provisioned
          bearerInterfaceNotReady (68), -- bearer subnet not ready
                .
                .  (more types)

             }
```

The new MIB definition can be found at the following location:

http://triweb/smg5000/mibDir/mibTxt/NORTEL-UEMG-MEGACO.mib

70.6 Service Orders (SO) (CM & SESM)

NA

70.7 Software optionality control (SOC)

NA

70.8 Element Management

The Switched Line Services Screen will now have a new field on the GW Status Config tab “Fault status”. This field will show what, if any, faults have been raised against the VMG.

70.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GW Status Config Tab under the Switched Line Services screen	CHANGED

70.8.2 GUI information

70.8.2.1 GUI name: GW Status Config

GateWay Status Configuration tab.

70.8.2.1.1 Functional description

A new field will be added to the Gateway Status Configuration tab to show what alarms have been raised against the VMG.

The status screen will in most cases automatically be updated when alarms are raised against the VMG. In addition, when the user presses the Refresh button, the correct fault status will be displayed, based on what VMG alarms have been raised to the EM.

70.8.2.1.2 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GW Status Config	1	1 per MG9000	NA

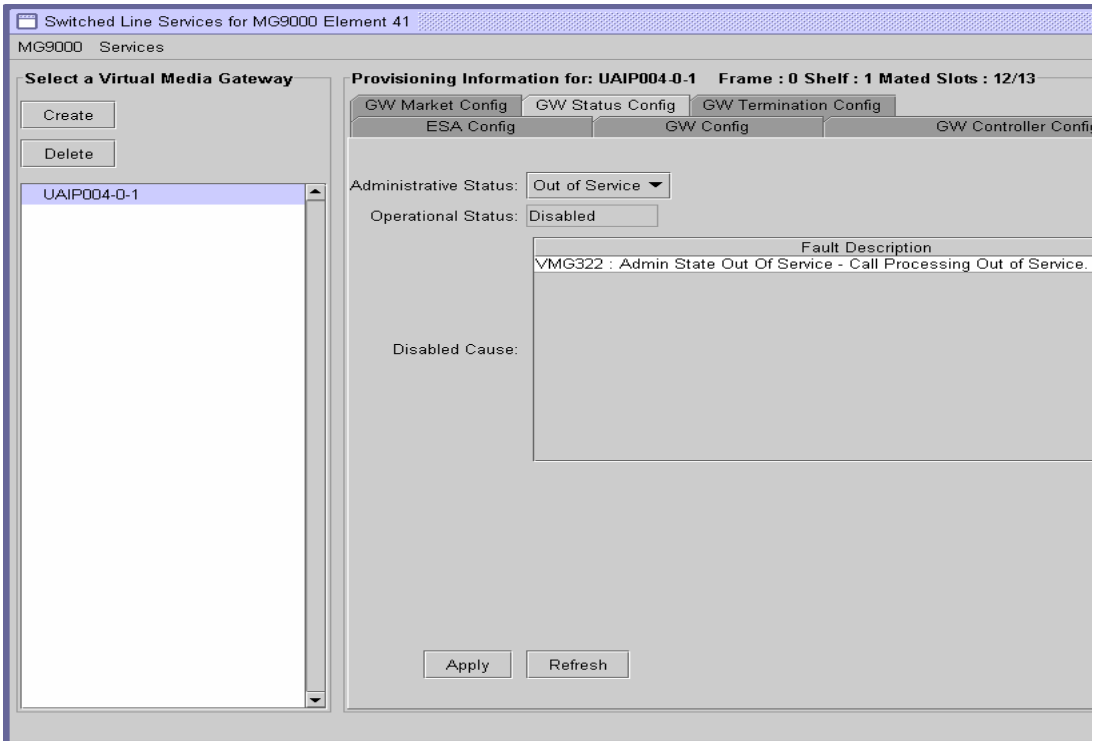
70.8.2.1.3 GUI fields

The following table lists the new field for GUI GW Status Config.

Table 3 GUI field descriptions

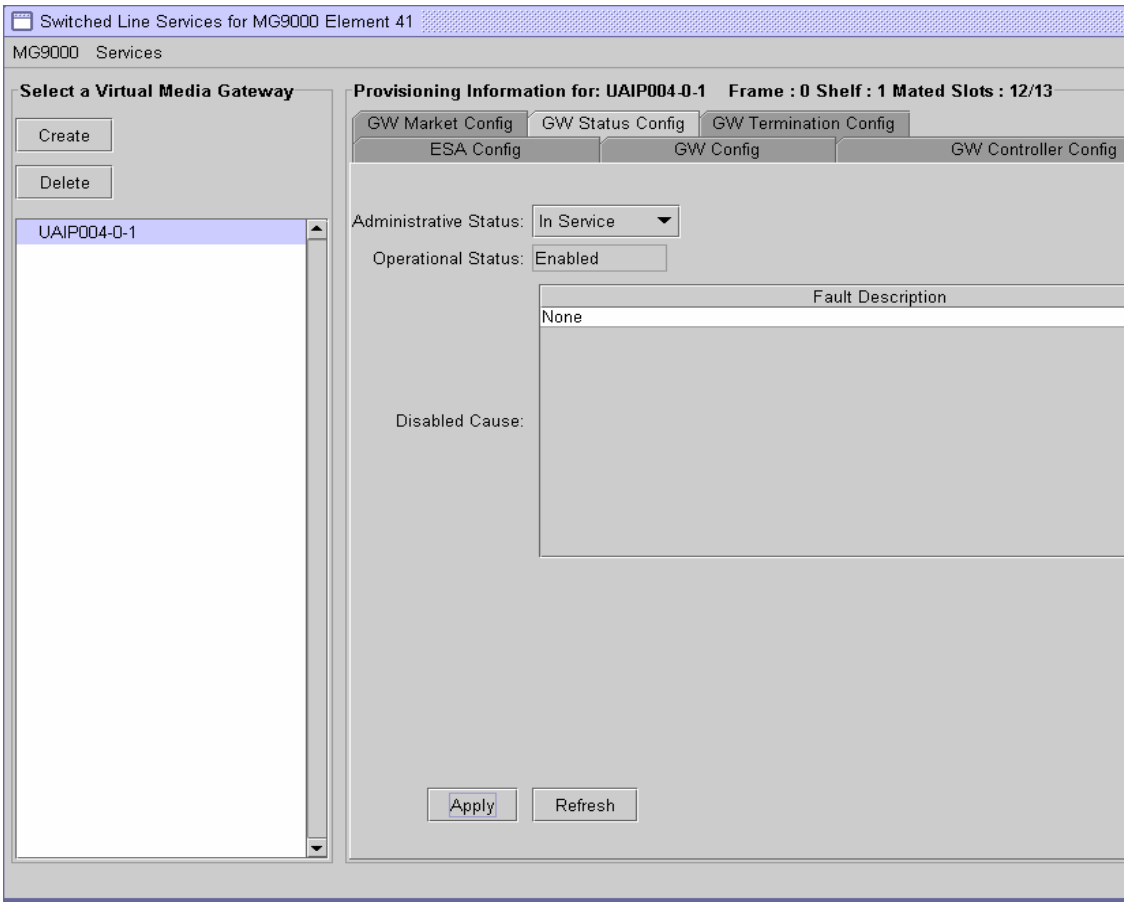
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
outOfService State	New	No	Fault Status for VMG	Displays the VMG faults raised for this VMG. If there are no faults, then this field will display “None”	None

70.8.2.1.4 Usage example



This example shows a VMG with Administrative Status Out of Service. In this state, the Disabled Cause field will show one alarm as show above.

The example below shows a VMG that is in an Enabled state.



70.8.2.1.5 GUI release history update

None

70.8.2.1.6 Supplementary information

This should provide more detail on the appearance of the fault information.

70.8.2.1.7 CLUI Interface

NA

70.9 Command interface changes

NA

70.10 Security

NA

70.11 Configuration Walkthrough

NA

71: Configuration (CN): A00005073

71.1 Hardware and Software Requirements

- OpenSSH installed on SDM/CBM.
  SBA SFTPW does not function if OpenSSH software is missing.
- SDM/CBM Private Data Manager installed and running
- SBA installed and InSv

71.2 Initial Configuration

- Configure and activate a SBA stream

71.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

71.4 Upgrade Impact

N/A

71.5 Data schema (DS) (CM, MIBS, RDB)

N/A

71.6 Service Orders (SO) (CM & SESM)

N/A

71.7 Element Management

N/A

71.8 Command interface changes

N/A

71.8.1 Command: <command name>

71.9 Security

71.9.1 Secure Data Transfer to OSS with OpenSSH sftp

This feature provides optional secure outbound file transfer using OpenSSH sftp client. The sftp client protects all data including sensitive user s' password by encrypting the data before it leaves SDM/CBM and decrypting the data after it arrives the downstream OSS. The sftp also provides data integrity check to ensure that no one has tampered the data during the transfer.

The SBA user can configure the secure file transfer by adding or changing an existing schedule tuple in billmtc. For SN07, the user has to manually accept the downstream host key for each destintation before configuring secure outbound file transfer to the destintation. The actual configuration details are documented in the configuration section.

71.9.2 Downstream OSS password protection

This feature also enhances SBA password protection scheme by using SDM/CBM private data manager (documented in A00005074) to store all the passwords for OSS access. The private data manager is responsible for storing the data in an encrypted form.

71.10 Configuration Walkthrough

71.10.1 Host key acceptance for downstream OSS

Figure 1 Host key acceptance

```
In AIX
> login: root
> root's Password: xxxx
> su - maint
> /usr/bin/ssh -l maint wcary2p3
The authenticity of host 'wcary2p3 (47.135.213.53)' can't be established.
RSA key fingerprint is ef:f8:b9:b5:4e:15:71:66:09:82:0d:93:fa:ce:58:ff.
Are you sure you want to continue connecting (yes/no)? yes
```

71.10.2 SBA specific configuration

SBA secure outbound file transfer can be configured by adding or changing an existing schedule tuple after the user has done a host key acceptance. The following shows an example on how a user can configure secure outbound file transfer. The text in bold indicate the field values that are different from FTPW

Figure 2 Prompts for schedule add

Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream: occ

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Destination can have between 1 and 15 alphanumeric characters.
Enter Destination: OOS

Valid protocols are {'FTPW', 'RFTPW' 'SFTPW}.
Press Enter to accept 'FTPW'.
Enter Protocol: SRTFPW

Primary destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Primary_Destination: 47.135.213.53

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

Alternate destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Alternate_Destination: 47.135.213.53

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Alternate_Port: 22

... (con't on next figure)

Figure 3 Prompts for Schedule add (con't)

```
Start time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Start_Time: 00:00

Stop time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Stop_Time: 23:00

Interval can be between 5 and 1440 minutes.
Press Enter to accept '120'.
Enter Interval: 5

Remote storage directory can have between 1 and 255 characters.
Enter Remote_Storage_Directory: /billing

Remote login can have between 1 and 20 characters.
Enter Remote_Login: test

Remote password can have between 1 and 20 characters.
Enter Remote_Password:
Re-enter Remote_Password:

Maximum retries can be between 0 and 10.
Press Enter to accept '3'.
Enter Maximum_Retries:

Retry wait time can be between 1 and 60 seconds.
Press Enter to accept '1'.
Enter Retry_Wait_Time:

File extension can have between 0 and 3 characters.
Enter 'Blank' for no file extension.
Press Enter to accept 'Blank'.
Enter File_Extension:

Field separator can have 1 character.
Press Enter to accept '.'.
Enter Field_Separator:

WARNING: Billing files associated with this tuple will not
transfer downstream when Active is set to No.

Valid active values are {'No', 'n', 'Yes', 'y'}.
Press Enter to accept 'No'.
Enter Active: y
```

After schedule tuple configuration is completed, the user can run the sftp client manually to verify that the downstream OSS is ready for file transfer using SFTPW protocol. In other words, ready for accepting connection from a sftp client.

It should also be noted that the SFTPW protocol will be in effect in the next interval once you make the tuple active.

Figure 4 Steps to run sftp manually to verify downstream availability for SFTP

1. logon to SDM/CBM as root

2. Run sftp command to connect to the downstream OSS

sftp -oPreferredAuthentications=password <loginId>@<IP> -oPort=<port#>
e.g. sftp -oPreferredAuthentications=password test@47.135.213.53 -oPort=22

3. If you get back a password prompt: “test‘s password:” , then the downstream is ready for SFTPW otherwise please refer to the required software component and configuration sections for more details.

72: Configuration (CN): A00005074

72.1 Hardware and Software Requirements

OMDD application running on the SDM/CBM is InSv. OpenSSH is installed on the SDM/CBM.

72.2 Initial Configuration

The initial configuration of OMDD is not changed by this activity.

72.3 Element Management

72.3.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
OMUI	Changed

72.3.2 GUI information

The OMUI “Add File Transfer Destination” and “Modify File Transfer Destination” menus are modified by this activity.

72.3.2.1 GUI name: OMUI

OMDD User Interface

72.3.2.1.1 Functional description

The “Add File Transfer Destination” menu in OMUI enables the user to configure a destination where OMDD can transfer OM reports. The “Modify File Transfer Destination” menu enables the user to modify an already configured file transfer destination.

This activity modifies the Add and Modify File Transfer Destination menus of OMUI. From now on, when a user adds or modifies a file transfer destination, he/she will be asked to select the type of file transfer for the destination in addition to the already existing parameters. The choices for the type of file transfer will be “Standard” and “Secure” .

If the user chooses “Secure”, a warning message will be printed along with the confirmation prompt. This warning message informs the user that secure file transfer would fail if OpenSSH was not installed on the SDM/CBM.

Figure 1 shows an example configuration of file transfer destination using the modified menu. The same changes are made in the “Modify File Transfer Destination” menu also.

Figure 1 OMUI File Transfer Destination menu

Add File Transfer Destination (for a secure file transfer destination)

File Transfer Destination name > ftd1
Destination IP Address > 1.1.1.1
Type of File Transfer: Standard/Secure > Secure
Destination Port [22] >
Destination Login > user1
Destination Password >
WARNING: File Transfer to this destination will fail if OpenSSH is not installed.
Please install OpenSSH if it is not already installed.
Add File Transfer Destination(Y/N)?

Add File Transfer Destination (for a standard file transfer destination)

File Transfer Destination name > ftd2
Destination IP Address > 1.1.1.2
Type of File Transfer: Standard/Secure > Standard
Destination Port [21] >
Destination Login > user1
Destination Password >
Add File Transfer Destination(Y/N)?

SDM/CBM output - black
User input - blue
Step newly added by this activity - red

72.4 Configuration Walkthrough

This activity introduces an additional step in the add and modify file transfer destination menus of OMUI. This does not change the existing configuration methods of OMDD.

73: Configuration (CN): A00005160

73.1 Hardware and Software Requirements

A data network must be engineered and commissioned to enable UDP and ICMP echo messaging between OSSAIN/OSAC switches and OSSAIN service nodes. Refer to "73.10 Security" on page 3372 for information relevant to configuring the data network. Refer to the FN section of this DDOC for more information about capacity engineering.

XA-Core Ethernet interface cards should be commissioned on the switch before attempting to convert OSSAIN nodes to use them.

OSSAIN service nodes, provided either by Nortel Networks or by a third party vendor, must be in place.

73.2 Initial Configuration

For overall information about configuring OSSAIN, refer to the *OSSAIN User's Guide* (297-8403-901) and to SN-specific documentation.

If this feature is being commissioned on a switch that does not already have XA-Core Ethernet interfaces, it is important to develop an overall IP address plan that will last when the switch begins to use Succession functionality. Refer to Nortel Networks system engineering documentation for more information.

Also refer to engineering documentation for specific information about commissioning XA-Core Ethernet interface cards. Existing CI XAIPTOOL may be useful in working with XA-Core Ethernet interfaces.

An SN must not be on the same subnet as a core Ethernet interface unless it is intended that the core use that interface, and its associated core IP address, when sending messages to that SN. A local subnet check in the core routing software will select the core interface rather than the EIU router if a local subnet match is found. This applies both to XA-Core Ethernet interfaces and to EIUs that are configured as interfaces instead of routers, although whether a local subnet match is found for the XA-Core Ethernet interface depends on interactions with other features.

Migration from EIU to XA-Core Ethernet interface at a switch can be done gradually, on a per far-end node basis. OSAC hosts and remotes do not have to be converted at the same time. For example, an OSAC remote can send messages via its EIU to the host's XA-Core Ethernet interface IP address, and the host responds using its XA-Core Ethernet interface to the IP address that the remote uses with its EIU. Also, an OSAC host or remote can use XA-Core Ethernet interface for messaging with some service nodes, and EIU for

messaging with others. A service node can communicate with some switches that use XA-Core Ethernet interface and with others that use EIU.

See "73.11 Configuration Walkthrough" on page 3373 for the steps in converting a switch to use XA-Core Ethernet interface rather than EIU for messaging with a specific far-end node (SN or OSAC switch).

73.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

73.4 Upgrade Impact

73.4.1 Dump and Restore

No customer action is required. On an ONP from pre-SN07 to SN07 or later, OSSAIN nodes are automatically datafilled in table OANODINV to use the EIU data path.

73.4.2 Element Management Upgrade

Not applicable.

73.5 Data schema (DS)

73.5.1 New/modified tables

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Table OANODINV	changed	unchanged
Table CMIPADDR	changed	unchanged
Table QMSMIS	changed	unchanged

73.5.2 Table information

73.5.2.1 Name: Table OANODINV

Operator Services System Advanced Intelligent Network Node Inventory

73.5.2.1.1 Functional description

This table maps an OSSAIN node identifier to a unique node name. It defines the transport layer protocol used for messaging to the given node and specifies protocol related network address information. This table also allows datafilling OSSAIN node specific information.

73.5.2.1.2 Usage sequence and implications (CM Only)

The following tables must be datafilled before OANODINV:

- ENSITES
- ENTYPES
- OANODNAM
- CMIPADDR, for OANODINV tuples with field DATAPATH = XAETHR

Current datafill sequence is unchanged for tables that are datafilled after table OANODINV.

73.5.2.1.3 Size

This activity increases the store for each OANODINV tuple by 4 bytes.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OANODINV	0	768 (unchanged)	Approximately 1038 bytes per tuple. Refer to the Engineering (EI) section of this DDOC for more information.

Note: The amount of store used by table OANODINV depends on the NODEID values that are datafilled in table OANODNAM. To avoid wasting store, avoid datafilling higher NODEID values than needed.

73.5.2.1.4 Fields

The following table shows the top-level fields for table OANODINV.

Table 3 Table OANODINV field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODENAME	unchanged			
NODEAREA	refinements changed	This field consists of subfield ONPMTYPE and refinements		
ONPMTYPE	unchanged	This is a selector field.	OSN, OSNM, or OSAC (unchanged)	unchanged
AUDTRIES	unchanged			
AUDRTIMR	unchanged			
AUDFREQ	unchanged			

ONPMTYPE = OSN

If the entry in subfield ONPMTYPE is OSN, datafill refinements as shown in the following table.

Table 4 OSN refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ENNODENO	unchanged			
PROTOCOL_ AREA	unchanged			
ADDRESS_ AREA	unchanged			
DATAPATH_ AREA	New	This field consists of subfield DATAPATH and refinements		
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSN is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSN is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.
CMIPADDR	New	This is a refinement field, present only if selector DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
HOSTNAME	unchanged			
FAIL_DET	unchanged			
ONODTYPE	unchanged			
ONODLOC	unchanged			
ONODSITE	unchanged			
ONODINFO	unchanged			

ONPMTYPE = OSNM

If the entry in subfield ONPMTYPE is OSNM, datafill refinements as shown in the following table.

Table 5 OSNM refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ENNODENO	unchanged			
PROTOCOL_ AREA	unchanged			
ADDRESS_ AREA	unchanged			
NMTCPORT	unchanged			
DATAPATH_ AREA	New	This field consists of subfield DATAPATH and refinements		
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSNM is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSNM is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.
CMIPADDR	New	This is a refinement field, present only if selector DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
FAIL_DET	unchanged			
TSTTIME	unchanged			
RTSTIME	unchanged			
ONODTYPE	unchanged			
ONODLOC	unchanged			

Table 5 OSNM refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ONODSITE	unchanged			
ONODINFO	unchanged			

ONPMTYPE = OSAC

If the entry in subfield ONPMTYPE is OSAC, datafill refinements as shown in the following table.

Table 6 OSAC refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RELATION_ AREA	A refinement of this field is changed	This field consists of subfield RELATION and refinements		
RELATION	unchanged	This is a selector field. If SELF is entered, there are no refinements. If OTHER is entered, datafill the refinement fields shown below.	SELF or OTHER	unchanged
ENNODENO	unchanged			
PROTOCOL_ AREA	unchanged			
ADDRESS_ AREA	unchanged			
DATAPATH_ AREA	New	This field consists of subfield DATAPATH and refinements. This field is present only if selector RELATION = OTHER.		

Table 6 OSAC refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSAC node is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSAC node is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.
CMIPADDR	New	This is a refinement field, present only if DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
ONODTYPE	unchanged			
ONODLOC	unchanged			
ONODSITE	unchanged			
ONODINFO	unchanged			

73.5.2.1.5 Datafill example

The following example shows sample datafill for table OANODINV. A bold font is used to highlight the new fields introduced by this activity.

```
NODENAME  NODEAREA                                    AUDTRIES AUDRTIMR AUDFREQ
-------------------------------------------------------------------------------
SWITCH_A  OSAC SELF                                          4        5      30
SWITCH_B  OSAC OTHER 0 UDP IPV4 172 16 10 2 XAETHR 172 16 1 108
                  SWITCH 3 B 11 CITYB REMOTEOSAC 4           5      30
SWITCH_C  OSAC OTHER 1 UDP IPV4 172 16 20 5 EIU
                  SWITCH 1 A 12 CITYC HOSTOSAC   4           5      30
BRAND_01  OSNM 0 UDP IPV4 172 16 1 200 7000 EIU
               Y 2 240 60 SN 2 BB 3 CITYA BRANDING1 4        5      60
DEBIT_01  OSNM 1 UDP IPV4 172 16 1 210 7001 XAETHR 172 16 1 109
               Y 2 240 30 SN 2 BB 8 CITYA DEBIT1    4        5      60
DAA_01    OSN 1 UDP IPV4 172 16 20 205 7000 XAETHR 172 16 1 108
              SWITCH_C Y 2 SN 1 DD 33 CITYC DAA1    4        5      60
DAA_02    OSN 0 UDP IPV4 172 16 20 206 7000 EIU
              SWITCH_C Y 2 SN 1 DD 34 CITYC DAA2    4        5      60
```

73.5.2.1.6 Table release history update

The DATAPATH_AREA field, with selector subfield DATAPATH and refinement CMIPADDR, is added for OSN, OSNM, and OSAC OTHER tuples. The CMIPADDR refinement field is present only if DATAPATH = XAETHR.

73.5.2.1.7 Supplementary information

When XAETHR is entered as the data path, the IP address in the OANODINV CMIPADDR refinement field must be used by the far-end node as the destination address for OSSAIN messages. This same IP address will be the source IP address for OSSAIN messages sent to the far-end node.

The XAETHR data path cannot be datafilled in table OANODINV unless the IP address in refinement field CMIPADDR has been previously added to table CMIPADDR, as the ACTIVEIP entry in a CMHOST tuple. If an attempt is made to violate this restriction, the following error message is displayed:

```
The CMIPADDR entry in OANODINV must match an ACTIVEIP
entry in a CMHOST tuple in table CMIPADDR.
```

The XAETHR data path cannot be datafilled in table OANODINV if the node is identified in table QMSMIS as a server for OSSAIN QMS MIS. If an attempt is made to change the OSSAIN QMS MIS server's data path to XAETHR, the following error message is displayed:

```
This node is datafilled in table QMSMIS. DATAPATH XAETHR
is not supported for an OSSAIN QMS MIS server.
```

73.5.2.1.8 Translation verification tools

Table OANODINV does not use translation verification tools.

73.5.2.2 Name: Table CMIPADDR

Computing Module Internet Protocol Addresses

Note: The only changes are a new cross-check with table OANODINV and a new error message. However, because earlier releases of Nortel Networks documentation may have missed some of the details about this table, this feature goes into some detail in documenting the fields.

73.5.2.2.1 Functional description

Table CMIPADDR contains the IP addresses and subnet masks associated with the XA-Core, as well as the gateway router IP address and the edge device IP addresses and subnet masks.

73.5.2.2.2 Usage sequence and implications (CM Only)

Table CMIPADDR is datafilled during commissioning of the Ethernet interfaces in an XA-Core switch. Changing the gateway or host address information after that may cause data mismatches between various nodes in the IP network.

This activity (A00005160, OSSAIN XA-Core Data Messaging Capacity Enhancements) adds the following dependency: Table CMIPADDR must be datafilled before a tuple with DATAPATH = XAETHR can be added to table OANODINV.

73.5.2.2.3 Size

Current size unchanged.

73.5.2.2.4 Fields

The following table lists the top-level fields for table CMIPADDR.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	unchanged	This field consists of subfields KEYCLASS and ENTRYNO.		
KEYCLASS	unchanged		GATEWAY, CMHOST, AMDIHOST, ETHRLNK	Key class. Indicates the class of tuple being datafilled. Enter GATEWAY to datafill the IP address of a gateway router. There can be only one GATEWAY tuple. Enter CMHOST to datafill an active IP address for the XA-Core. There can be two CMHOST tuples (total two active host IP addresses). Enter ETHRLNK to datafill a physical Ethernet link. There can be up to 8 ETHRLNK tuples, with each tuple corresponding to a physical link. AMDIHOST was added to allow datafill of an IP address to be used with an AMDI link for CLIP (Classical IP) over ATM. This value cannot be datafilled in SN07 or ISN07.
ENTRYNO	unchanged		0 to 7	Entry number. This is used to create a unique key. The KEYCLASS limits the ENTRYNO values that can be datafilled: GATEWAY: 0 to 0 CMHOST: 0 to 1 AMDIHOST: N/A ETHRLNK: 0 to 7
DATA	unchanged	This field consists of selector field SELCLASS and refinements.		
SELCLASS	unchanged	This is a selector field	GW, HOST, AMDI, ETHR	Selector class. The KEYCLASS in the key must match the SELCLASS entry as follows: GATEWAY: GW CMHOST: HOST AMDIHOST: AMDI ETHRLNK: ETHR

SELCLASS = GW

If the entry in subfield SELCLASS is GW, datafill refinements as shown in the following table.

Table 8 GW refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYIP	unchanged		four numbers, each 0 to 255	Gateway IP address. Enter an address for a gateway router. This address is downloaded to the Ethernet interface card or packlet. ***Note 1:*** VRRP and similar redundancy schemes allow a pair of routers to use a single IP address. ***Note 2:*** The GTWYIP entry may be the same as an address entered for an edge device in an ETHRLINK tuple, in case there is an Ethernet LAN but no WAN. It may not be the same as any other IP address in table CMIPADDR.
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

SELCLASS = HOST

If the entry in subfield SELCLASS is HOST, datafill refinements as shown in the following table.

Table 9 HOST refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ACTIVEIP	unchanged		four numbers, each 0 to 255	Active IP address for the XA-Core. This will be one of the IP addresses used by applications and advertised outside of the core. The active IP addresses are dynamically associated with physical interfaces. If an active IP address is bound to a physical interface that suffers a failure, it will be automatically rebound to a different interface in the same subnet.
NETMASK	unchanged		1 to 30	Subnet mask. Enter the number of leading ‘1’s in the mask.

Table 9 HOST refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

SELCLASS = AMDI

This value cannot be datafilled in SN07/ISN07.

SELCLASS = ETHR

If the entry in subfield SELCLASS is ETHR, datafill refinements as shown in the following table.

Table 10 ETHR refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SLOTID	unchanged	This field consists of subfields SLOT and SIDE		
SLOT	unchanged		0 to 18	Slot. The physical slot number on the XA-Core shelf where the Ethernet interface card resides. (For EIOP, this is where the IOP resides.) ***Note:*** Refer to XA-Core engineering documentation for packfill restrictions.
SIDE	unchanged		UNKNOWN, FRONT, REAR	Side. The location on the XA-Core shelf where the Ethernet interface card resides. Enter FRONT or REAR. ***Note:*** Refer to XA-Core engineering documentation for packfill restrictions.
PACKLET	unchanged		NONE, LOWER, UPPER	Packlet. For EIOP, enter the location of the Ethernet packlet on the IOP card. For other Ethernet interfaces such as HIOP and HCMIC, enter NONE.
CARDIP	unchanged		four numbers, each 0 to 255	Card IP address. This address is used only within the interface card or packlet, and is not advertised.
CARDNETM	unchanged		1 to 30	Card subnet mask. Enter the number of leading ‘1’s in the mask.

Table 10 ETHR refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MTCIP	unchanged		four numbers, each 0 to 255	Maintenance IP address. This is used by the core for maintenance of the interface card or packlet from the core. This address is not advertised.
MTCNETM	unchanged		1 to 30	Maintenance subnet mask. Enter the number of leading ‘1’s in the mask.
EDGEIP	unchanged		four numbers, each 0 to 255	Edge device IP address. This is the address of the device to which the Ethernet interface is directly attached. This address is used by the core in performing integrity checks, using ICMP echo requests, on the point-to-point link between the Ethernet interface card or packlet and the edge device to which it is attached. Assuming the edge device is a Passport 8600, datafill the physical IP address of the CallP VLAN/subnet on the Passport 8600 that the HIOP or HCMIC subtends.
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

73.5.2.2.5 Datafill example

The following example shows sample datafill for table CMIPADDR.

```
KEY         DATA
---------------------------------------------------------
GATEWAY 0   GW (172 16 0 1) 0
CMHOST 0    HOST (172 16 14 108) 20 0
CMHOST 1    HOST (172 16 14 109) 20 0
ETHRLNK 1   ETHR 12 REAR NONE (172 16 14 104) 20
            (172 16 14 110) 20 (172 16 0 2) 0
ETHRLNK 2   ETHR 6 REAR NONE (172 16 14 106) 20
            (172 16 14 112) 20 (172 16 0 3) 0
```

73.5.2.2.6 Table release history update

Table CMIPADDR was introduced and modified in CSP16 by the following features:

- A59025829, IRM Plan B
- A59029386, CLIP on the XA-Core
- A59029980, Succession HIOP Maintenance Software

In CSP20 (SN07), new cross-checks and error messages are added by the following features:

- A00002510, LANCOMM IP over IRM - adds cross-checks with table IPNETWRK.
- A00005160, OSSAIN XA-Core Data Messaging Capacity Enhancements (this feature) - adds cross-checks with table OANODINV.

73.5.2.2.7 Supplementary information

In SN07/ISN07, only one subnet is supported for the core Ethernet interfaces. All active IP, maintenance IP, and card IP addresses must be unique, and they must all have the same netmask and the same subnet.

A GATEWAY or CMHOST tuple can be changed or deleted only if all links associated with the subnet are off-line. An ETHRLNK tuple can be changed or deleted only if the link is off-line.

Warning: Changes to the GATEWAY or CMHOST IP addresses or subnet information in this table after the initial commissioning may cause data mismatches between various nodes in the IP network.

This activity (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) adds the following error message. This message is printed if an attempt is made to delete or change a CMHOST tuple whose active IP address is datafilled in table OANODINV.

```
ERROR: The active IP address in this tuple is referenced
by table OANODINV. The tuple cannot be changed or deleted
as long as table OANODINV references it.
```

Note: Much other datafill may depend on the OANODINV tuple. To avoid having to delete and re-add all this other datafill if it is necessary to change the IP address plan, one can temporarily change the DATAPATH field in the OANODINV tuple to EIU. However, this does not imply that the CMHOST tuples can be changed without major impact on the OSSAIN application.

73.5.2.2.8 Translation verification and other tools

Table CMIPADDR does not use translation verification tools.

73.5.2.3 Name: Table QMSMIS

QMS MIS Link Definition Table

Note: The only changes are a new cross-check and a new error message.

73.5.2.3.1 Functional description

Table QMSMIS defines the links used by a Queue Management System Management Information System (QMS MIS) application and also defines the audit frequency for the links.

73.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

73.5.2.3.3 Size

Current size unchanged.

73.5.2.3.4 Fields/OIDs

The following table lists the top-level fields for table QMSMIS.

Table 11 QMSMIS field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INDEX	unchanged			
DATALINK	unchanged			

73.5.2.3.5 Datafill example

The following example shows sample datafill for table QMSMIS.

```
INDEX                                                DATALINK
-----------------------------------------------------------
OSSAIN                          ETHERNET MIS_OSSAIN 24 7001
TOPS                                  MPC (3 3 1) (4 4 2) $
```

73.5.2.3.6 Table release history update

Cross-checks are added to enforce that an OSSAIN QMS MIS server cannot be datafilled in table OANODINV with data path XAETHR.

73.5.2.3.7 Supplementary information

If an attempt is made to datafill an OSSAIN tuple whose node has data path XAETHR in table OANODINV, the following error message is displayed:

```
THIS NODE HAS DATAPATH XAETHR IN TABLE OANODINV. OSSAIN
QMS MIS SERVERS MUST USE THE EIU. XA-CORE ETHERNET DATA
PATH IS NOT SUPPORTED FOR OSSAIN QMS MIS.
```

73.5.2.3.8 Translation verification and other tools

Tools unchanged.

73.6 Service Orders (SO) (CM & SESM)

Not applicable.

73.7 Software optionality control (SOC)

Table 12 SOC

SOC option name:	OSSAIN Base
SOC option title:	OSSAIN Base
SOC option control type:	state
New SOC option?	No
SOC option order code	OSAN0101
Option defined in DRU:	TOPS
Affected products:	SN0x, ISN0x

73.8 Element Management

Not applicable.

73.9 Command interface changes

73.9.1 Command: QUERYPM (in OAINPMDIR directory)

73.9.1.1 Command type: Listed MENU

73.9.1.2 Command target: All

73.9.1.3 Command availability: RES

73.9.1.4 Command description

The QUERYPM command is available in a number of different MAP levels. In general, it is used to display information about the posted peripheral module (PM).

This feature changes the output that is displayed when the QUERYPM command is issued with no arguments in the OAINPMDIR directory. The OAINPMDIR directory is entered from the MAPCI;MTC;PM level by posting an OSN, OSNM, or OSAC node. These node types are used for the TOPS OSSAIN application.

73.9.1.5 Command syntax

The command syntax is unchanged. In the OAINPMDIR directory, the QUERYPM command may be entered with no parameters or with the constant FLT parameter. This feature only changes the output when QUERYPM is entered with no parameters.

73.9.1.6 Qualifications and warnings

None.

73.9.1.7 Responses

This feature changes only the success response. It does not change the error responses.

The success response displays information about the posted node, from table OANODINV. None of the information that was displayed prior to this feature is changed in format or meaning. This feature adds a new line to the success response, corresponding to new information in table OANODINV.

The new line displays the data path used for the posted node. The data path can be EIU or XAETHR. EIU refers to the Ethernet Interface Unit. XAETHR refers to XA-Core Ethernet interface cards such as HIOP and HCMIC. If the node uses an XAETHR data path, the display also shows the active CM host IP address that the switch uses in messaging with the node.

The success response does not require any user action. It is visible on both XA-Core and BRISC. On BRISC the data path will always be EIU. On XA-Core, it can be either EIU or XAETHR.

73.9.1.8 Example

The following figure shows an example success response for a posted node with connectivity through XA-Core Ethernet cards using active host IP address 172.16.1.109. The figure uses a bold font to highlight the new line that has been added to the display.

```
NODENAME: DAA_01
NODEID:   1
PROTOCOL: UDP
IPADDR:   172.16.20.205
DATAPATH: XAETHR (172.16.1.109)
ONODTYPE: SN
ONODLOC:  1 DD 33
ONODSITE: CITYC
HOSTNAME: SWITCH_C
```

Actual data values depend on datafill in table OANODINV.

73.9.2 Command: BUFSTATS (in OSSAINCI directory)

73.9.2.1 Command type: NON-MENU

73.9.2.2 Command target: All

73.9.2.3 Command availability: RES

73.9.2.4 Command description

OSSAINCI is an existing directory that provides non-menu commands that are used primarily by Nortel Networks customer support personnel. The OSSAINCI directory is accessed by entering the directory name. Most of the commands are related to tracing of OSSAIN messages. The new BUFSTATS command is not related to tracing; it is related to buffer resources.

The BUFSTATS command allows the user to view information about the queues and buffer pools that are used for processing messages incoming to OSSAIN via an XA-Core Ethernet interface. It also allows the user to reset the low water marks associated with the free queues.

73.9.2.5 Command syntax

Table 13 BUFSTATS command parameters and variables

Command	**Parameters and variables**
BUFSTATS	DISPLAY, RESET
Parameters and variables	**Description**
DISPLAY	Displays information about buffer resources
RESET	Resets low water marks associated with free queues used by the application.

73.9.2.6 Qualifications and warnings

Low water marks are approximate. (Realtime and possible blocking involved in keeping them accurate would be counter-productive.) In-queue counts are also approximate, but are closer to accurate than low water marks.

Displaying buffer stats frequently during peak traffic hours can cause blocking.

73.9.2.7 Responses

Table 14 MAP outputs with associated meanings and actions

Response to command BUFSTATS with no parameters, or with DISPLAY parameter

The system displays information about the queues. Following is an example. The numbers will vary.
 	
`XAETHR Free Qs/Pools`
`====================`
`Bytes/buff  Alloc  Count   LWM`
`----------  -----  -----  -----`
`   64        300    270    114`
`  128        300    281     70`
`  320        150    150    147`
 	
`XAETHR Inuse Qs`
`===============`
`Use     Count`
`-----   -----`
`CallP     45`
`Mtce       3`
 	
Meaning:
 	
Bytes/buff — number of message body bytes in buffers
Alloc — number of buffers allocated
Count — approximate number of buffers currently in queue
LWM — low water mark
Use — kind of messages the queue/pool is used for
 	
User actions:
 	
No user action is required.

Table 15 MAP outputs with associated meanings and actions

Success response to command BUFSTATS with RESET parameter
`LWMs have been reset for all FreeQs` **Meaning:** The System has reset the low water marks of the free queues. **User actions:** No user action is required.

73.9.2.8 Example

Table 16 Usage example for OSSAINCI BUFSTATS command

Description of task:	Study free queue low water marks during a defined study period.
At the beginning of the study period:	
Command: MAP response: Command: MAP response: Command: MAP response:	>OSSAINCI OSSAIN: >BUFSTATS RESET LWMs have been reset for all FreeQs >LEAVE CI:
At the end of the study period:	
Command: MAP response: Command: MAP response: Command: MAP response	>OSSAINCI OSSAIN: >BUFSTATS DISPLAY *<display similar to that in Table 14 on page 3369>* >LEAVE CI:

73.9.3 Command: SCREENTAB (in OSSAINCI directory)

73.9.3.1 Command type: NON-MENU

73.9.3.2 Command target: All

73.9.3.3 Command availability: RES

73.9.3.4 Command description

OSSAINCI is an existing directory that provides non-menu commands that are used primarily by Nortel Networks customer support personnel. The OSSAINCI directory is accessed by entering the directory name. Most of the commands are related to tracing of OSSAIN messages. The new SCREENTAB command is not related to tracing; it is related to an internal table that the switch maintains.

The SCREENTAB command allows Nortel Networks support personnel to view the contents of the internal table. The internal table does not affect any functionality in the SN07/ISN07 releases. It is for possible future use.

73.9.3.5 Command syntax

Table 17 SCREENTAB command parameters and variables

Command	Parameters and variables
SCREENTAB	none

73.9.3.6 Qualifications and warnings

None.

73.9.3.7 Responses

Table 18 MAP outputs with associated meanings and actions

Response to command SCREENTAB

The system displays information about the internal table. Following is an example. The numbers will vary.
 	
`idx (hex)  entry  collisions`
`---------  --------------------------  ----------`
`00B9  2F8EE0B9  (47.142.224.185)  0`
`0201  2FF50E01  (47.245.14.1)  0`
 	
Meaning:
 	
idx — index into internal hash table
entry — data in internal hash table
collisions — number of hash collisions to access entry
 	
User actions:
 	
No user action is required.

73.9.3.8 Example

Table 19 Usage example for OSSAINCI SCREENTAB command

Description of task:	View contents of internal hash table.
Command: MAP response:	`>OSSAINCI` `OSSAIN:`
Command: MAP response:	`>SCREENTAB` *<display similar to that in Table 18 on page 3371>*
Command: MAP response	`>LEAVE` `CI:`

73.10 Security

A secure network is assumed. The risk in using OSSAIN in an insecure network is greater with XA-Core Ethernet interface cards than with the EIU. This is because the EIU can offer some protection to the core by screening out messages from unwanted IP addresses. With XA-Core Ethernet interface cards, anyone with access to the central office LAN has direct access to the core.

73.10.1 Network configuration

Firewalls and routers must allow UDP datagrams to and from the IP addresses and ports used for OSSAIN.

- IP addresses
  - — In the core, OSSAIN may use the active CMHOST IP addresses datafilled in table CMIPADDR, the IP address in the CMIPADDR tuple of table IPNETWRK, or both. Which core IP addresses OSSAIN uses is based on datafill in table OANODINV.
  - — IP addresses of OSSAIN and OSAC nodes are datafilled in the IPV4ADDR field of table OANODINV.
  - — If OSSAIN is configured to use EIUs, it uses them as routers.
- Ports
  - — OSSAIN uses UDP ports 5289 through 5293 in the core, regardless of whether it is configured to use EIUs or XA-Core Ethernet interfaces.
  - — UDP ports used in service nodes for OSSAIN messaging are datafillable in the following tables and fields:
    - – table OANODINV, field NMTCPORT in OSNM refinement
    - – table OASESNPL, fields CPPORT and MTCPORT in various refinements

  Note: Although an OSAC remote switch does not have have datafill for a centralized service node's maintenance port, it does send messages to and receive messages from this port. The centralized service node is datafilled in the OSAC remote as an OSN node, and in the OSAC host as an OSNM node. The OSAC remote sends datagrams to and receives datagrams from the centralized service node at the NMTCPORT datafilled in the OSAC host, as well as at the session pool ports datafilled in both switches.

OSSAIN also requires that the data network support ICMP echo requests and replies to and from the IP addresses used for OSSAIN nodes (both OSAC switches and service nodes).

This activity does not restrict whether the active host IP addresses in table CMIPADDR are in the same or a different subnet than the CM IP address used by the EIU.

73.10.2 Key management

N/A.

73.10.3 Protocol

N/A.

73.10.4 Authentication

N/A.

73.11 Configuration Walkthrough

This section outlines steps for converting OSSAIN to use XA-Core Ethernet interface, rather than EIU, for messaging with a single far-end node (SN or OSAC switch). This procedure has the following prerequisites:

- The secure, engineered data network must be up. Firewalls and routers must be configured to allow ICMP echo and UDP messaging between the XA-Core Ethernet interface to be used and the far-end node. (Refer to "73.10 Security" on page 3372 for information about UDP ports used for OSSAIN.)
- The XA-Core Ethernet interfaces must be commissioned.
- If an SN is involved (it will be unless it's an OSAC link being changed), the method for changing the switch IP address on the SN must be understood. This method is different for different service nodes.

Once the prerequisites are satisfied, there are several ways the change could be made. The sequence shown here is straightforward and will not cause sessions in progress to fail; however, it may cause SysB alarms in switches in the OSAC network. These alarms will clear automatically once the conversion is successfully completed. If avoiding such alarms is a priority, more steps may be needed. For example, if an OSAC host is being converted to use XA-Core Ethernet interface for messaging with a particular SN, it will need to briefly off-line the SN, and this will raise alarms in the OSAC remotes unless the SN's session pools and the SN itself have first been busied in the remotes.

1. At the switch that is to start using XA-Core Ethernet interface cards:

a. Drain all session pools datafilled against the far-end node. This is done at the SesnPool level (SESNPOOLDIR) of the DMS MAP. Wait for the session pools to transition to ManB.

Note: Drain is not supported for OSN node types. If an OSAC remote is being converted to use XA-Core Ethernet interface for an OSN, temporarily route the traffic elsewhere rather than draining.

b. Off-line all session pools datafilled against the far-end node.

c. At the OAINPMDIR directory, busy and off-line the far-end node.

d. In table OANODINV, modify the tuple for the far-end node to use XAETHR data path, and datafill the CMIPADDR field.

2. At the far-end node, change its configuration to use the new IP address for the switch.

— If the far-end node is an SN, follow SN-specific procedures for this step.

— If the far-end node is an OSAC switch, follow the steps below at that switch. These steps assume that switch A is the one being changed to use XA-Core Ethernet interfaces, and switch B is the one where the steps below are performed.

a. Busy and off-line switch A at the OAINPMDIR directory, if this has not already been done.

b. Modify the tuple for switch A in table OANODINV, changing the IPV4ADDR field to the IP address that was datafilled in switch A against switch B in the CMIPADDR field of table OANODINV.

c. At the OAINPMDIR MAP directory, Busy and RTS switch A. Ensure that all session pools to switch A are SysB.

3. At the switch that is to start using XA-Core Ethernet interface cards:

a. Busy and RTS the far-end node and session pools.

4. Check logs and OMs at both both ends, and make test calls.

5. Configure firewalls and routers in the data network to disallow messaging between the CM IP address datafilled in table IPNETWRK and the far-end node, if desired.

Note: Refer to the FN section of this DDOC (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) for a limitation regarding inconsistent IP address datafill detection. This limitation exists only in OSAC remote switches, and only if the OSAC host switch is below SN07/ ISN07, the service node is below OAP release 9, or both.

74: Configuration (CN): A00005190

74.1 Hardware and Software Requirements

Tables IPNETWRK and MSCDINV must be data filled before table SDMINV.

74.2 Initial Configuration

No hardware needs to be present to configure an SDM or CBM connected by DS512 or OC3 on the Core.

74.3 Office/Subnet parameters (OP/SP) (CM & SESM)

No change.

74.4 Upgrade Impact

74.4.1 Dump and Restore

No change

74.4.2 Element Management Upgrade

No change.

74.5 Data schema (DS) (CM, MIBS, RDB)

74.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SDMINV	CHANGED	UNCHANGED

74.5.2 Table/MIB/Remote Database Schema information

74.5.2.1 Name: SDMINV

DS512 connected SDM inventory table

74.5.2.1.1 Functional description

This table contains the PEC codes, location, link information, and IP address information related to a DS512 connected SDM. This activity adds a new PEC for a simplex CBM which is OC3 connected.

74.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

74.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SDMINV	0	1	No change

74.5.2.1.4 Fields/OIDs

The following table lists the changed field for table SDMINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SHELFPEC	Changed	none	NTRX50DA NTRX50EB NTRX51EL NTRX51LS	NTRX51LS is being added for the simplex CBM OC3 connected shelf type.

74.5.2.1.5 Datafill example

```
>table sdminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SDMINV
>lis all
TOP
SDM CONFIG FLOOR ROW POSITION CABTYPE   CABPEC CABNUM SHELFPEC SHELFPOS
         IPADDR LINKRATE          LINKS
-------------------------------------------------------------------------
  0   SIMP     1   A        1    MISC NT0X02AB      1 NTRX51LS        2
 10  40  15   3    SR256        ( 8 0)$

BOTTOM
```

74.5.2.1.6 Table release history update

74.5.2.1.7 Supplementary information

74.5.2.1.8 Translation verification other tools

Not applicable

74.6 Service Orders (SO) (CM & SESM)

Not applicable

74.7 Software optionality control (SOC)

Not applicable

74.8 Element Management

74.8.1 New/modified GUIs

Not applicable.

74.9 Command interface changes

74.9.1 MAP level:mapci;mtc;appl;sdm

Figure 1 SDM MAPCI screen CSP19

```
   CM       MS      IOD      Net       PM      CCS              Trks     Ext      APPL
   .     01MBCD   AMA  B     .         .         .                ...      .       .
                   *C*
SDM             OAMAP           SDM           SWMTC   SDMBIL
 0 Quit           .               .             .       .
 2
 3            SDM 0   OffL        Links_OOS: 4
 4
 5 Trnsl
 6
 7 Bsy
 8 RTS
 9 OffL
10
11
12
13
14 QuerySDM
15 Locate
16
17
18 Platform
  admin
Time  15:57  >
```

Figure 2 SDM MAPCI screen CSP20 (DS512 connected SDM)

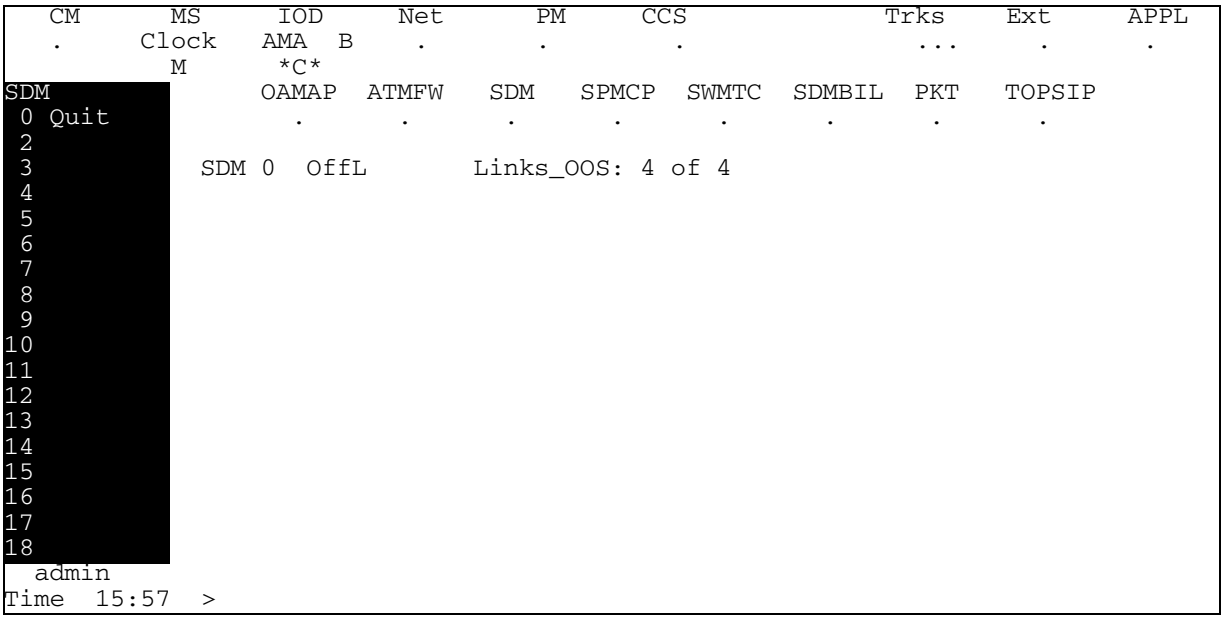
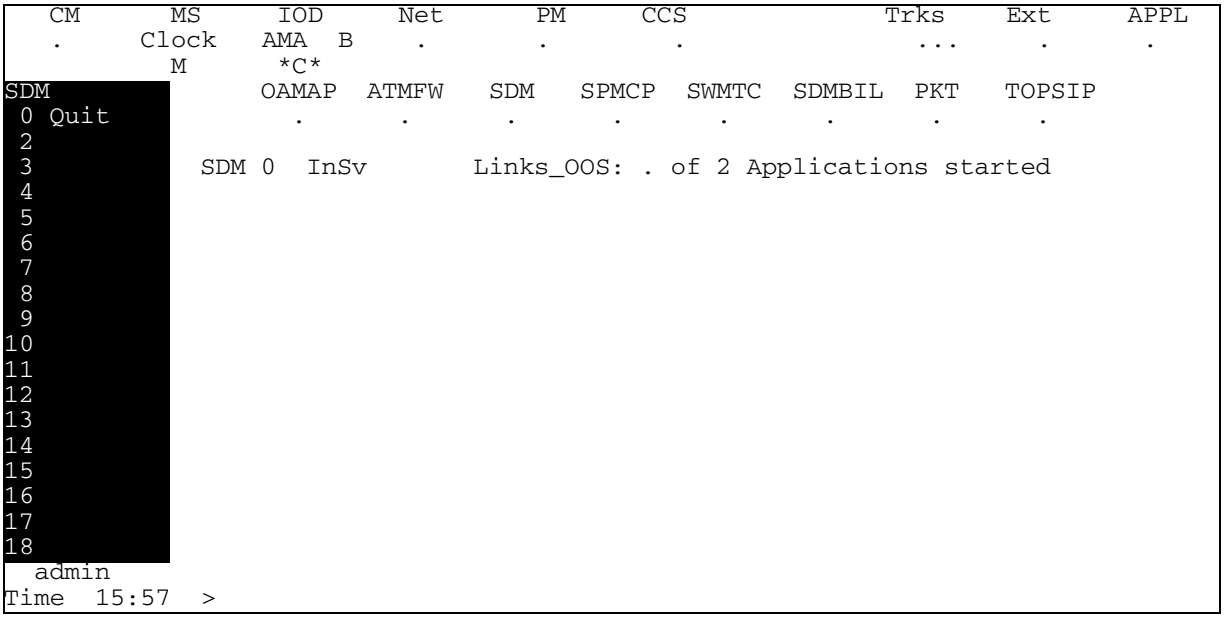


Figure 3 SDM MAPCI screen CSP20 (OC3 connected CBM)



74.9.1.1 MAP level description

This map level displays the state information related to the SDM.

It also provide commands to query additional status as well as control the state of a DS512 connected SDM.

To the existing mapci screen, small modifications are being added to support an OC3 connected CBM.

From the customer's perspective, there is little visual difference between the two supported environments. The differences are as follows:

- Only 2 links are supported to a CBM.
- The platform, locate, querysdm status, querysdm config, and querysdm loads commands are not supported on a CBM.
- The querysdm flt command will only display core side faults for a CBM.
- A new field is visible as long as there is heartbeating with the CBM which presents the overall application status of the CBM. i.e."Applications started" and "Applications stopped".

74.9.1.2 Accessing path: appl:SDM

74.9.1.2.1 Access to directory or MAP level and return to CI

mapci;mtc;appl;sdm

74.9.2 Command: QuerySDM

74.9.2.1 Command type: Listed MENU

74.9.2.2 Command target: All

74.9.2.3 Command availability: RES

74.9.2.4 Command description

This is an existing command to query information concerning the SDM.

The command will be missing parameters when CBM connected and will only return Core side faults on a CBM.

74.9.2.5 Command syntax

Table 4 QuerySDM command parameters and variables

platform	Parameters and variables
sdm	QuerySDM: Query information about the SDM. Parms: [<QuerySDM Option> {FLT, LOADS, STATUS, CONFIG}]
cbm	QuerySDM: Query information about the SDM. Parms: [<QuerySDM Option> {FLT}]

74.9.2.6 Qualifications and warnings

no change

74.9.2.7 Responses

No change in response

74.9.3 Command: Locate

74.9.3.1 Command type: Listed MENU

74.9.3.2 Command target: All

74.9.3.3 Command availability: RES

74.9.3.4 Command description

Displays the card location of all cards on an SDM FX.\

On a CBM, this command is not supported.

74.9.3.5 Command syntax

The locate command has no parameters.

74.9.3.6 Qualifications and warnings

No Change

74.9.3.7 Responses

74.9.3.7.1 <response>

The response for a CBM will be:

```
Locate command is not supported for shelf pec NTRX51LS.
```

74.9.4 Command: rebootsdm

74.9.4.1 Command type: Unlisted MENU

74.9.4.2 Command target: All

74.9.4.3 Command availability: RES

74.9.4.4 Command description

Sends a message to the SDM instructing it to reboot. This command is not supported on a CBM.

74.9.4.5 Command syntax

No parameters

74.9.4.6 Qualifications and warnings

no change

74.9.4.7 Responses

74.9.4.7.1 <response>

The response for a CBM will be:

```
Locate command is not supported for shelf pec NTRX51LS.
```

74.9.5 Command: haltsdm

74.9.5.1 Command type: Unlisted MENU

74.9.5.2 Command target: All

74.9.5.3 Command availability: RES

74.9.5.4 Command description

Sends a message to the SDM instructing it to halt. This command is not supported on a CBM.

74.9.5.5 Command syntax

No parameters

74.9.5.6 Qualifications and warnings

no change

74.9.5.7 Responses

74.9.5.7.1 <response>

The response for a CBM will be:

```
Locate command is not supported for shelf pec NTRX51LS.
```

74.10 Security

Not applicable

74.10.1 Network configuration

74.10.2 Key management

74.10.3 Protocol

74.10.4 Authentication

75: Configuration (CN): A00005193

75.1 Hardware and Software Requirements

N/A

75.2 Initial Configuration

N/A

75.3 Office/Subnet parameters (OP/SP) (CM & SESM)

75.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	RATED_POWER	CHANGED	CM

75.3.2 Parameter information

75.3.2.1 RATED_POWER

75.3.2.1.1 Functional description

This parameter defines the number of PEs engineered in the switch. The Speedometer uses the value of this parameter to calculate the capacity prediction for the switch.

75.3.2.1.2 Provisioning rules

N/A

75.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
1	9	3

75.3.2.1.4 Activation

N/A

75.3.2.1.5 Dependencies

N/A

75.3.2.1.6 Consequences
N/A

75.3.2.1.7 Verification
To verify, users can modify and display the value of RATED_POWER on table OFCENG via table control.

75.3.2.1.8 Memory requirements
No memory impact.

75.3.2.1.9 Parameter release history update
N/A

75.4 Upgrade Impact
N/A

75.5 Data schema (DS) (CM, MIBS, RDB)
N/A

75.6 Service Orders (SO) (CM & SESM)
N/A

75.7 Software optionality control (SOC)
N/A

75.8 Element Management
N/A

75.9 Command interface changes
N/A

75.10 Security
N/A

75.11 Configuration Walkthrough
N/A

76: Configuration (CN): A00005363

76.1 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

76.2 Initial Configuration

Standard configuration applies

76.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

76.4 Data schema (DS) (CM, MIBS, RDB)

76.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CAINRESP	changed	unchanged
CAINREXT	changed	unchanged
CDRTMPLT	changed	unchanged

76.4.2 Table/MIB/Remote Database Schema information

76.4.2.1 Name: CAINRESP

CAIN Simulator Response

76.4.2.1.1 Functional description

This feature adds a new parameter, AMABusinessCustomerId, to the operation types:

- Analyze_Route
- Disconnect
- Send_To_Resource

This feature also adds a new digits id type (300) to the AMADIGS parameter.

76.4.2.1.2 Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

76.4.2.1.3 Size
Unchanged

76.4.2.1.4 Fields/OIDs
The following table lists the changed fields/OIDs for CAINRESP

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CAIN_PARM_VALUE	changed	subfield	AMABUSCUSTID	The range of this subfield is expanded to include the AMABusinessCustomerId parameter.
AMA_DIGS_TYPE	changed	subfield	001, 002, 003, 004, 005, 006 , 011, 012, 300, 301, 302, 303, 304, 305, 999	The range of this subfield is expanded to include the value of 300

76.4.2.1.5 Datafill example
The following example shows sample datafill for table CAINRESP.

```
TABLE: CAINRESP

RESPKEY
                                    DATAAREA
-----------------------------------------------------------------------
RESP123
CR 0 RESP INVL ANALYZE_ROUTE  (CLDNO NATL ISDN 2149201234) (AMABUSCUSTID
01234567890) (AMADIGS 300 9876543210) $ $ $
```

76.4.2.1.6 Table release history update
Not applicable.

76.4.2.1.7 Supplementary information
None.

76.4.2.1.8 Translation verification other tools
None.

76.4.2.2 Name: CAINREXT
CAIN Simulator Response Extension Parameters

76.4.2.2.1 Functional description
This feature adds a new digits id type (300) to the AMADIGS parameter.

76.4.2.2.2 Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

76.4.2.2.3 Size
Unchanged

76.4.2.2.4 Fields/OIDs
The following table lists the changed fields/OIDs for CAINRESP

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AMA_DIGS _TYPE	changed	subfield	001, 002, 003, 004, 005, 006 , 011, 012, 300, 301, 302, 303, 304, 305, 999	The range of this subfield is expanded to include the value of 300

76.4.2.2.5 Datafill example
The following example shows sample datafill for table CAINREXT.

```
TABLE: CAINREXT

REXTKEY
                                    DATAAREA
-----------------------------------------------------------------------
REXT123
 NT (AMA_BUS_CUSTID 01234567890) (AMADIGS 300 9876543210) $ $ $
```

76.4.2.2.6 Table release history update
Not applicable.

76.4.2.2.7 Supplementary information
None.

76.4.2.2.8 Translation verification other tools
None.

76.4.2.3 Name: CDRTMPLT

CDR template table

76.4.2.3.1 Functional description

This feature adds 4 new parameters to the FIELDS and REORIGCP subfileds of table CDRTMPLT.

76.4.2.3.2 Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

76.4.2.3.3 Size

Unchanged

76.4.2.3.4 Fields/OIDs

The following table lists the changed fields/OIDs for CAINRESP

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FIELDS	changed	subfield	BUSCSTID, SLPID1ST, DGI300, DGI301.	The range of this subfield is expanded to include the BUSCSTID, SLPID1ST, DGI300 and DGI301 parameters.
REORIGCP	changed	subfield	BUSCSTID, SLPID1ST, DGI300, DGI301.	The range of this subfield is expanded to include the BUSCSTID, SLPID1ST, DGI300 and DGI301 parameters.

76.4.2.3.5 Datafill example

The following example shows sample datafill for table CDRTMPLT.

```
 TABLE: CDRTMPLT
NAME ACTIVE PRIMARY FIELDS REORIGCP
-------------------------------------------------------------
```

VZN_FLXCDR Y N (SEQNUM) (CIC) (ORIGTIME) (ORIGDATE) (ANSTYPE) (TIMECHNG) (ORIGAMPM) (INCINTL) (DISCTIME) (DISCDATE) (ANISUFF) (DISCAMPM) (INCBILL) (FILL1) (CALLDUR) (PINDIGS) (ANISP) (INFODIG) (BILLNUM) (ACCTCD) (CLGPTYNO) (RLTCDR) (ACCTV) (UNIVACC) (DIALEDNO) (CALLEDNO) (OUTPULNO) (FILL4) (ORIGOPRT) (PREDIG) (CNPREDIG) (OPART) (TPART) (QUEUED) (FILL3) (FILL3) (FILL4) (RTENO) (NETSEC) (OPCHOICE) (COLLTIME) (ADIN) (LNPCHECK) (NUMWBCKT) (WBCKTS) (FINSID) (BILLTYPE) (ORIGGRP) (DISCTYPE) (ORIGMEM) (PASSTHRU) (TERMGRP) (PRESIND) (TERMMEM) (OSRASSOC) (DIGDATA) (FINTKGRP) (TRAP) (COSOVE) (FINTKMEM) (SCPBILL) (FILL3) (FILL3) (FILL3) (FILL2) (FILL3) (FILL2) (TRTMTCD) (COMPCODE) (CRID) (DNIS) (ORIGPVN) (TERMPVN) (ORIGLRN) (PORTEDNO) (CAINCT) (ACG) (DNISNOA) (FILL1) (MLTCOSID) (FILL4) (FILL1) (COSINDEX) (FILL2) (CARRSEL) **(SLPID1ST) (BUSCSTID) (DGI300) (DGI301)** (FILL8) $ $

76.4.2.3.6 Table release history update
Not applicable.

76.4.2.3.7 Supplementary information
None.

76.4.2.3.8 Translation verification other tools
None.

76.5 Service Orders (SO) (CM & SESM)
Not applicable

76.6 Software optionality control (SOC)
The CAIN0202 SOC is added by this feature

Table 5 SOC

SOC option name:	CAIN0202
SOC option title:	CAIN FlexCDR Enhancements
SOC option control type:	state
New SOC option?	Yes
SOC option order code	CAIN0202
Option defined in DRU:	UCS

Table 5 SOC

Affected products:	DMS-250

76.7 Element Management

Not Applicable.

76.8 Command interface changes

Not Applicable.

76.9 Security

Not Applicable.

76.10 Configuration Walkthrough

Not applicable

77: Configuration (CN): A00005734

77.1 Hardware and Software Requirements

All CM processors (PPC, 68K etc) and any SN07 or equivalent CM load

77.2 Initial Configuration

To configure this feature, you must datafill table MULTITM with any relevant timezones, including local time (during non-DST, this is zero offset from the CM clock. During DST, this is the offset from the CM clock to go back to non-DST)

Any lines that required this feature must have the MTZ option added through SERVORD.

77.3 Upgrade Impact

77.3.1 Dump and Restore

No new dump or restore activity required.

77.3.2 Element Management Upgrade

n/a

77.4 Data schema (DS) (CM, MIBS, RDB)

None

77.5 Service Orders (SO) (CM & SESM)

77.5.1 New line option MTZ

77.5.1.1 Description

The option MTZ is used on any line that is physically located in a different time zone to the controlling CM. When the user activates other time related features (Such as Wake Up Call Request), the time will be converted to their local time, rather than the CM time.

77.5.1.2 Example

Figure 1 Example of the MTZ option

```
SO:
>ado
SONUMBER:    NOW   2  2 19 PM
>
DN_OR_LEN
>7205011
OPTkey:
>1
OPTION:
>MTZ
SO_MTZ_NAME:
>loc
OPTKEY:
>$
COMMAND AS ENTERED
ADO NOW 2 2 19 PM 7205011 (1 MTZ LOC)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO eDIT
>Y
```

77.5.1.3 Option prompts

Table 1 System prompts for MTZ option

Prompt	Valid input	Description	Areas affected by prompt
TIMEZONE	Keys in table MULTITM		

77.5.1.4 Assignability

The following functionalities apply to this option:

- set functionality: Yes
- subset functionality: no
- DN functionality: no
- key functionality: no

77.5.1.5 Option prerequisites

Table MULTITM must have data in it.

77.6 Configuration Walkthrough

Datafill table MULTITM with timezone information. Add option MTZ to relevant lines. Feature is activated automatically.

78: Configuration (CN): A00006483

78.1 Hardware and Software Requirements

Multiple Universal Audio Servers (UAS) or Audiocodes Media Servers (AMS) or some other packet-based announcement resource equivalent must be networked to provide the announcement resources. The announcement resource devices must be capable of being configured and networked to meet the announcement port demands.

78.2 Initial Configuration

Table SERVRINV must be datafilled with a gateway controller (GWC) to be used as an Audio Controller GWC that will have subtending announcement resource devices.

78.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

78.4 Upgrade Impact

78.4.1 Dump and Restore

Prior to SN06, the ANNC option did not exist. When the Core is upgraded to SN06, the reformat procedure for table SERVSINV assigns by default the ANNC option. The default value specified for the ANNTERMS field is 300 if no other options (i.e. 3PORT or 6PORT) are datafilled. The default value will not change in SN07. If 3PORT or 6PORT is datafilled, the ANNC ANNTERMS value is adjusted accordingly against the value in NUMTERMS. For upgrades from SN06 to SN07, the ANNC option ANNTERMS value is simply transferred.

78.4.2 Element Management Upgrade

Not applicable.

78.5 Data schema (DS) (CM, MIBS, RDB)

78.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVSINV	CHANGED	UNCHANGED

78.5.2 Table/MIB/Remote Database Schema information

78.5.2.1 Name: SERVSINV

Server Subtending Node Inventory Table

78.5.2.1.1 Functional description

Table SERVSINV contains the names of the server subtending nodes and their associated gateways. The subtending node relevant to this activity is the audio server node(AUD).

78.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

78.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVSINV	0	256	Protected

78.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVSINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVSNAME	Not Changed		see subfields	*Server Subtending Name key*. This field contains subfields XPMTYPE and XPMNO. Specifies the logical subtending node off the GWC
	Not changed	XPMTYPE	PM_TYPE	*XPM Type*. For an audio server node, enter AUD.
	Not changed	XPMNO	0 to 255	*XPM Number*. Enter the XPM number for the peripheral.
SRVRNAME	Not changed		see subfields	*Server Name*. This field contains subfields XPMTYPE and XPMNO. Specifies the associated gateway controller of the subtending node.
	Not changed	XPMTYPE	PM_TYPE	*XPM Type*. Enter GWC.
	Not changed	XPMNO	0 to 255	*XPM Number*. Enter the corresponding GWC node number found in table SERVRINV.
NUMTERMS	Not changed		1024, 2048, or 4095	*Number of Terminals*. FOr AUD node, it is recommended that 4095 be used.
OPTIONS	Not changed		see subfield	*Options*. This field contains subfields for 3PORT, 6PORT, and/or ANNC for conferencing and announcement resources.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTIONS	Not changed		ANNC	*ANNC OPTION*. The subfield ANNC is used for announement terminal allocation and to indicate the number of simultaneous announcements. The field contains the subfield ANNTERMS.
	Changed	ANNTERMS	1 to 1280	Announcement terminals. Enter value up to 1280.

78.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVSINV
:

Table 4 Example of table SERVSINV

```
>table servsinv
TABLE: SERVSINV
>list all
TOP
      SRVSNAME      SRVRNAME NUMTERMS                                  OPTIONS
-------------------------------------------------------------------------------
      AUD   1       GWC   1     4095                                (ANNC 1280)$

      AUD   4       GWC   2     4095     (3PORT 300)(6PORT 120)(ANNC 300)$
```

78.5.2.1.6 Table release history update

The following information was added: The ANNTERMS maximum value for the ANNC option of the OPTIONS field has increased from 300 to 1280.

78.5.2.1.7 Supplementary information

The ANNC option has a maximum ANNTERMS value of 1280 because of a GWC limitation.

78.5.2.1.8 Translation verification other tools

SERVSINV does not use translation verification tools.

78.6 Service Orders (SO) (CM & SESM)

Not applicable

78.7 Software optionality control (SOC)

Not applicable.

78.8 Element Management

Not applicable.

78.9 Command interface changes

Not applicable.

78.10 Security

Not applicable.

78.11 Configuration Walkthrough

79: Configuration (CN): A00006693

79.1 Hardware and Software Requirements

Not applicable.

79.2 Initial Configuration

Not applicable.

79.3 Office/Subnet parameters (OP/SP) (CM & SESM)

79.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	IO_WARNING_ THRESHOLD	NEW	XA-Core

79.3.2 Parameter information

79.3.2.1 IO_WARNING_THRESHOLD

IO_WARNING_THRESHOLD

79.3.2.1.1 Functional description

This parameter defines a utilization warning threshold for all IO service types (CMIC, ETHR, AMDI) in the system. The IOCAP monitoring toolset uses the value of this parameter to peg the IOTHRESH register of the IOCAP OM whenever the IO utilization level of any IO service has exceeded this threshold on the switch.

79.3.2.1.2 Provisioning rules

There is no formula for provisioning this office parameter. However, this office parameter should be set by the customer in such a manner that will allow sufficient advance warning time for their maintenance personnel to upgrade or reconfigure their IO devices in case the condition reoccurs often.

79.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
1	100	100

79.3.2.1.4 Activation

Any change activation for this office parameter is immediate.

79.3.2.1.5 Dependencies

Not applicable.

79.3.2.1.6 Consequences

If this office parameter is set low, the IOTHRESH register might be in pegged more often than necessary. If this office pararmeter is set high, the customer may not have enough advance notice to upgrade their IO configuration.

79.3.2.1.7 Verification

To verify, users can modify and display the value of IO_WARNING_THRESHOLD on table OFCENG via table control.

79.3.2.1.8 Memory requirements

No memory impact.

Units per memory block = <10>

Words per memory block = <510>

If the parameter value = <25>

words required = (((parameter value - 1)/units per block) + 1) *words per block = <>

79.3.2.1.9 Parameter release history update

New office parameter in CSP20.

79.4 Upgrade Impact

79.4.1 Dump and Restore

Not applicable.

79.4.2 Element Management Upgrade

Not applicable.

79.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

79.6 Service Orders (SO) (CM & SESM)

Not applicable.

79.7 Software optionality control (SOC)

Not applicable.

79.8 Element Management

Not applicable.

79.9 Command interface changes

The following new directories will be provided in this feature.

79.9.1 Directory: CAPACITY

This existing CAPACITY MAPCI level will be modified to provide a new IOCAP MAPCI level in XA-Core only. The new IOCAP level will provide IO utilization and IO messaging throughput information for HCMIC and HIOP IO cards.

79.9.1.1 Directory description

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

79.9.1.2 Accessing directory: CAPACITY

79.9.1.2.1 Access to directory or MAP level and return to CI

To access this directory, type:

> MAPCI; MTC; CAPACITY

To return to the CI environment, type:

> QUIT ALL

79.9.2 Command: IOCAP

This is a new command available under the CAPACITY MAPCI level in XA-Core only.

79.9.2.1 Command type: Listed MENU

79.9.2.2 Command target: XA-Core only

79.9.2.3 Command availability: RES

79.9.2.4 Command description

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

79.9.2.5 Command syntax

Table 3 IOCAP command parameters and variables

Command	Parameters and variables
IOCAP	none
Parameters and variables	Description

79.9.2.6 Qualifications and warnings

Not applicable.

79.9.2.7 Responses

79.9.2.7.1 IOCAP response

Table 4 MAP outputs with associated meanings and actions

Command
Service: The type of IO service of the values shown on the same line is captured. **Meaning:** Possible IO service types are CMIC, ETHR and AMDI. **System or user actions:** Not applicable

Table 4 MAP outputs with associated meanings and actions

Command
IOUTIL%: The average utilization of all active links in the system captured in the previous minute. **Meaning:** The value is given as a percent of total system and can take up to 3 digit. **System or user actions:** Not applicable
TxMsg/s: The average number of transmitted messages captured in the last minute for this IO service type. **Meaning:** The unit is number of transmitted messages per second. **System or user actions:** Not applicable
TxSize: The average size (in bytes) of all transmitted messages in the last minute. **Meaning:** The unit is in bytes. **System or user actions:** Not applicable
RxMsg/s: The average number of received messages captured in the last minute for this IO service type. **Meaning:** The value unit is the number of received messages per second. **System or user actions:** Not applicable
RxSize: The average size (in bytes) of all received messages in the last minute. **Meaning:** The unit is in bytes. **System or user actions:** Not applicable

This MAPCI level can be used for monitoring current IO throughput. Under normal condition, there is no response required from maintenance personnel. The descriptions of all fields displayed under this level are given above. These responses are seen in XA-core only.

79.9.2.8 Example

Table 5 Usage examples for IOCAP command

Description of task:	This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.
Command: MAP response:	MAPCI; MTC; CAPACITY; IOCAP See example output below.

An example output of this new MAPCI level is given below.

IOCAP MAPCI Level

```
 XACM      MS     IOD     Net      PM     CCS     Lns     Trks     Ext     APPL
  .        .       .       .       .       .       .       .       .       .

IOCAP
 0 Quit     CATMP/HR UTIL ENGCATMP MAXCATMP ENGLEVEL CCOVRLD CMICOVRLD PESC
 2            120000   75   160000   200000    BELOW     OFF       OFF   NO
 3
 4           Service IOUTIL% TxMsg/s TxSize RxMsg/s RxSize
 5
 6            AMDI     64      15324    107   13234     91
 7            CMIC     17       4102    202    1254    102
 8            ETHR     10       8967    123    3456    123
 9
10           IOCAP:
11
12
13
14
15
16
17
18
 XMAP0
Time  14:12    >
```

79.9.3 Command: QUIT

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

79.9.3.1 Command type: Listed MENU

This QUIT command is listed in IOCAP menu.

79.9.3.2 Command target: XA-Core only

This new IOCAP QUIT command is available in XA-Core only.

79.9.3.3 Command availability: RES

79.9.3.4 Command description

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

79.9.3.5 Command syntax

Table 6 QUIT command parameters and variables

Command	Parameters and variables
QUIT	none

79.9.3.6 Qualifications and warnings

Not applicable.

79.9.3.7 Responses

79.9.3.7.1 QUIT

Table 7 MAP outputs with associated meanings and actions

Command
If QUIT is issued, the user will be returned to one MAPCI level higher than their current MAPCI level. If QUIT ALL is issued, the user will be returned to CI level. **Meaning:** Not applicable. **System or user actions:** Not applicable. **Meaning:** The IOCAP MAPCI level is exitted and user is returned to one MAPCI level higher or to CI level. **System or user actions:** Not applicable.

79.9.3.8 Example

Table 8 Usage examples for QUIT command

Description of task:	
Description of task	Exit the IOCAP MAPCI level and return the user to CI level or one MAPCI level higher..
Command: MAP response:	Example: QUIT ALL Example: >

79.9.4 Directory: IOCAPCI

79.9.4.1 Directory description

This new IOCAPCI is provided to allow customers to display the IO utilization history data.

79.9.4.2 Accessing directory: IOCAPCI

79.9.4.2.1 Access to directory or MAP level and return to CI

To access this directory type:

> IOCAPCI

To return to CI environment, type:

> QUIT

79.9.5 Command: IOMAX

79.9.5.1 Command type: NON-MENU

79.9.5.2 Command target: XA-Core only

79.9.5.3 Command availability: RES

79.9.5.4 Command description

This command displays the hourly high watermark value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

79.9.5.5 Command syntax

The command syntax for this command is as follows.

```
> q iomax
Display IO high watermark report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
                                  ALL}
```

Table 9 IOMAX command parameters and variables

Command	Parameters and variables
IOMAX	service
IOMAX	<Service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly max history data
ETHR	Displays only ETHR hourly max history data

Table 9 IOMAX command parameters and variables

Command	Parameters and variables
AMDI	Displays only AMDI hourly max history data
All	Displays all hourly.max history data for CMIC, ETHR, and AMDI.

79.9.5.6 Qualifications and warnings

Not applicable.

79.9.5.7 Responses

79.9.5.7.1 IOMAX response

The following is the response if IOMAX CMIC is issued.

Table 10 MAP outputs with associated meanings and actions

Command
IOMAX CMIC: history data of CMIC hourly maximum utilization are displayed. **Meaning:** CMIC hourly maximum history data are displayed. **System or user actions:** Not applicable.
IOMAX ETHR: history data of ETHR hourly maximum utilization are displayed. **Meaning:** history data of ETHR hourly maximum utilization are displayed. **System or user actions:** Not applicable.
IOMAX AMDI: history data of AMDI hourly maximum utilization are displayed. Meaning: history data of AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.
IOMAX ALL: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. Meaning: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.

79.9.5.8 Example

Table 11 Usage examples for IOMAX command

Description of task	Display the history data of IO hourly max utilization.

Table 11 Usage examples for IOMAX command

Command:

Example: IOMAX CMIC

MAP response:

Example:

```
Maximum CMIC Utilization
                                                                                                                  Hour
Date    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  21  22  23
-------------------------------------------------------------------------------------------------------------------
2/1     9   7   8   6   5   7   8  11  17  22  28  30  40  55  50  47  61  57  59  62  59  39  31  21
2/2     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/3     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/4     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/5     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/6     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/7     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/8     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/9     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/10    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/11    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/12    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/13    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/14    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/15    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/16    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/17    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/18    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/19    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/20    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/21    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/22    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/23    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/24    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/25    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/26    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/27    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/28    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/29    8   7   8  10   8   9   7
1/30    3   8   7   6   9   8   4  12 16  21  27  29  39  49  47  45  55  53  57  56  51  49  29  14
1/31    8   6   5   7   8   7   6   9  11  19  27  31  39  49  53  43  51  55  53  57  56  51  31  21
```

Command:

Example: IOMAX ETHR

MAP response:

Example:

```
Maximum ETHR Utilization
                                                                                                                  Hour
Date    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  21  22  23
-------------------------------------------------------------------------------------------------------------------
2/1     9   7   8   6   5   7   8  11  17  22  28  30  40  55  50  47  61  57  59  62  59  39  31  21
2/2     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/3     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/4     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/5     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/6     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/7     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/8     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/9     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/10    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/11    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/12    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/13    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/14    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/15    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/16    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/17    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/18    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/19    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/20    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/21    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/22    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/23    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/24    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/25    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/26    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/27    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/28    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/29    8   7   8  10   8   9   7
1/30    3   8   7   6   9   8   4  12 16  21  27  29  39  49  47  45  55  53  57  56  51  49  29  14
1/31    8   6   5   7   8   7   6   9  11  19  27  31  39  49  53  43  51  55  53  57  56  51  31  21
```

Table 11 Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX AMDI Example: Maximum AMDI Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Table 11 Usage examples for IOMAX command

Command: MAP response:

Example: IOMAX ALL
Example:

Maximum CMIC Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Maximum ETHR Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Table 11 Usage examples for IOMAX command

```
Maximum AMDI Utilization
                                                                  Hour
Date    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  21  22  23
-------------------------------------------------------------------------------------------------------
2/1     9   7   8   6   5   7   8  11  17  22  28  30  40  55  50  47  61  57  59  62  59  39  31  21
2/2     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/3     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/4     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/5     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/6     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/7     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/8     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/9     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/10    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/11    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/12    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/13    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/14    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/15    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/16    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/17    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/18    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/19    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/20    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/21    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/22    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/23    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/24    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/25    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/26    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/27    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/28    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/29    8   7   8  10   8   9   7
1/30    3   8   7   6   9   8   4  12  16  21  27  29  39  49  47  45  55  53  57  56  51  49  29  14
1/31    8   6   5   7   8   7   6   9  11  19  27  31  39  49  53  43  51  55  53  57  56  51  31  21
```

79.9.6 Command: IOAVG

79.9.6.1 Command type: NON-MENU

79.9.6.2 Command target: XA-Core only

79.9.6.3 Command availability: RES

79.9.6.4 Command description

This command displays the hourly average value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

79.9.6.5 Command syntax

The command syntax for this command is as follows.

```
> q ioavg
Display IO average report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
```

ALL}

Table 12 IOAVG command parameters and variables

Command	Parameters and variables
IOAVG	service
IOAVG	<Service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly average history data
ETHR	Displays only ETHR hourly average history data
AMDI	Displays only AMDI hourly average history data
All	Displays all hourly.average history data for CMIC, ETHR, and AMDI.

79.9.6.6 Qualifications and warnings

Not applicable.

79.9.6.7 Responses

79.9.6.7.1 IOAVG response

The following is the response if IOAVG CMIC is issued.

Table 13 MAP outputs with associated meanings and actions

Command
IOAVG CMIC: history data of CMIC hourly average utilization are displayed. **Meaning:** CMIC hourly average history data are displayed. **System or user actions:** Not applicable.
IOAVG ETHR: history data of ETHR hourly average utilization are displayed. **Meaning:** history data of ETHR hourly average utilization are displayed. **System or user actions:** Not applicable.
IOAVG AMDI: history data of AMDI hourly average utilization are displayed. Meaning: history data of AMDI hourly average utilization are displayed. System or user actions: Not applicable.

Table 13 MAP outputs with associated meanings and actions

Command
IOAVG ALL: history data of CMIC, ETHR, AMDI hourly average utilization are displayed. Meaning: history data of CMIC, ETHR, AMDI hourly average utilization are displayed. System or user actions: Not applicable.

79.9.6.8 Example

Table 14 Usage examples for IOAVG command

Description of task	Display the history data of IO hourly average utilization.
Command: MAP response:	Example: IOAVG CMIC Example: Average CMIC Utilization Hour Date 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 2/1 9 7 8 6 5 7 8 11 17 22 28 30 40 55 50 47 61 57 59 62 59 39 31 21 2/2 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/3 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/4 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/5 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/6 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/7 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/8 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/9 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/10 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/11 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/12 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/13 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/14 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/15 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/16 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/17 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/18 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/19 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/20 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/21 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/22 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/23 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/24 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/25 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/26 5 7 9 8 7 8 9 8 15 23 21 29 39 53 49 42 59 51 55 57 53 47 31 21 2/27 3 8 7 6 9 8 4 7 11 19 27 31 38 51 47 45 55 53 57 56 51 49 29 14 2/28 9 9 8 7 7 7 8 7 18 28 18 29 37 48 55 48 58 48 59 59 57 48 27 18 2/29 8 7 8 10 8 9 7 1/30 3 8 7 6 9 8 4 12 16 21 27 29 39 49 47 45 55 53 57 56 51 49 29 14 1/31 8 6 5 7 8 7 6 9 11 19 27 31 39 49 53 43 51 55 53 57 56 51 31 21

Table 14 Usage examples for IOAVG command

Command: IOAVG ETHR

MAP response:

Example:

Average ETHR Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8		7		8	10		8		9		7												
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Command: IOAVG AMDI

MAP response:

Example:

Average AMDI Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8		7		8	10		8		9		7												
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Table 14 Usage examples for IOAVG command

Command: MAP response:

Example: IOAVG ALL
Example:

Average CMIC Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Average ETHR Utilization

	Hour																							
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Table 14 Usage examples for IOAVG command

```
Average AMDI Utilization
                                                                  Hour
Date    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  21  22  23
-------------------------------------------------------------------------------------------------------
2/1     9   7   8   6   5   7   8  11  17  22  28  30  40  55  50  47  61  57  59  62  59  39  31  21
2/2     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/3     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/4     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/5     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/6     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/7     3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/8     9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/9     5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/10    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/11    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/12    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/13    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/14    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/15    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/16    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/17    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/18    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/19    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/20    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/21    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/22    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/23    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/24    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/25    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/26    5   7   9   8   7   8   9   8  15  23  21  29  39  53  49  42  59  51  55  57  53  47  31  21
2/27    3   8   7   6   9   8   4   7  11  19  27  31  38  51  47  45  55  53  57  56  51  49  29  14
2/28    9   9   8   7   7   7   8   7  18  28  18  29  37  48  55  48  58  48  59  59  57  48  27  18
2/29    8   7   8  10   8   9   7
1/30    3   8   7   6   9   8   4  12  16  21  27  29  39  49  47  45  55  53  57  56  51  49  29  14
1/31    8   6   5   7   8   7   6   9  11  19  27  31  39  49  53  43  51  55  53  57  56  51  31  21
```

79.9.7 Command: DISP

79.9.7.1 Command type: NON-MENU

79.9.7.2 Command target: XA-Core only

79.9.7.3 Command availability: RES

79.9.7.4 Command description

This DISP command displays the utilization and messaging throughput values of each IO service type of the last 60 minutes with option CURR (for example when a command is issued at 2:35, displayed data is from 1:34 to 2:34) or previous full hour with option PREV (for example when a command is issued at 2:35, displayed data is from 1:00 to 2:00). This information survives all types of restarts (warm, cold and reload).

79.9.7.5 Command syntax

The command syntax for this command is as follows.

```
> q disp
Display table of IO utilization.
Parms: <when> {CURR,
               PREV}
```

```
<service> {CMIC,
           ETHR,
           ATM,
           ALL}
```

Table 15 DISP command parameters and variables

Command	Parameters and variables
DISP	<when> <service>
DISP	<when> (CURR, PREV) <service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
When	Possible values are CURR or PREV
CURR	Displays the last 60 minutes utilization and messaging throughput of the specified IO service type
PREV	Displays the previous full hour utilization and messaging throughput of the specified IO service type
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC utilization and messaging throughput
ETHR	Displays only ETHR utilization and messaging throughput
AMDI	Displays only AMDI utilization and messaging throughput
ALL	Displays utilization and messaging throughput for CMIC, ETHR, and AMDI.

79.9.7.6 Qualifications and warnings

Not applicable.

79.9.7.7 Responses

79.9.7.7.1 DISP response

The following is the response if DISP CURR CMIC is issued.

Table 16 MAP outputs with associated meanings and actions

Command
DISP CURR CMIC: last 60 minutes of CMIC utilization and messaging throughput are displayed. **Meaning:** last 60 minutes data for CMIC utilization and messaging throughput are displayed. **System or user actions:** Not applicable.

Table 16 MAP outputs with associated meanings and actions

Command
DISP CURR ETHR: last 60 minutes of ETHR utilization and messaging throughput are displayed. **Meaning:** last 60 minutes of ETHR utilization and messaging throughput are displayed. **System or user actions:** Not applicable.
DISP CURR AMDI: last 60 minutes of AMDI utilization and messaging throughput are displayed. Meaning: last 60 minutes of AMDI utilization and messaging throughput are displayed. System or user actions: Not applicable.
DISP CURR ALL: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed. Meaning: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed. System or user actions: Not applicable.

79.9.7.8 Example

Table 17 Usage examples for DISP command

Description of task	Display the last 60 minutes of IO utilization and messaging throughput.
Command: MAP response:	Example: DISP CURR CMIC Example: Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 . . . . . . 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34
Command: MAP response:	Example: DISP CURR ETHR Example: Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 . . . . . . 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34
Command: MAP response:	Example: DISP CURR AMDI Example: Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 . . . . . . 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34

Table 17 Usage examples for DISP command

Command: MAP response:	Example: DISP CURR ALL Example: Time CMICUTIL ETHRUTIL AMDIUTIL 16:17 45 21 34 16:18 39 19 31 16:19 38 18 32 16:20 39 21 31 . . . . . . 17:14 41 23 32 17:15 39 21 31 17:16 38 19 33

79.9.8 Command: STATUS

79.9.8.1 Command type: NON-MENU

79.9.8.2 Command target: XA-Core only

79.9.8.3 Command availability: RES

79.9.8.4 Command description

This command displays all status information including current version of IOCAPCI tool, timestamp in terms of hour and minute, the current IO utilization values of all IO services (CMIC, ETHR, AMDI), the current value of the IO_WARNING_THRESHOLD office parm.

79.9.8.5 Command syntax

The command syntax for this command is as follows.

```
> q STATUS
Display current IOCAP status.
```

Table 18 STATUS command parameters and variables

Command	Parameters and variables
STATUS	no parameter

79.9.8.6 Qualifications and warnings

Not applicable.

79.9.8.7 Responses

79.9.8.7.1 STATUS response

The following is the response if STATUS is issued.

Table 19 MAP outputs with associated meanings and actions

Command
STATUS: Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. **Meaning:** Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. **System or user actions:** Not applicable.

79.9.8.8 Example

Table 20 Usage examples for STATUS command

Description of task	Display status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm.

Command: MAP response:	Example: DISP CURR CMIC
	Example:
	`> status`
	`IOCAP Version 1.0`
	`Time CMICUTIL ETHRUTIL AMDIUTIL`
	`17:16 32 29 15`
	`IO_WARNING_THRESHOLD office parm is set to 100.`

79.10 Security

Not applicable.

79.11 Configuration Walkthrough

Not applicable.

Performance Management (PF)

Introduction

This chapter describes impacts to performance management, such as operational measurements and performance measurements, for the features planned for this release. Only those features with performance-management impacts are listed.

Featid	Title
A00002012.AA13	XA-Core CMIC/RTIF HIOP Maintenance Software
A00002340.AA07	Add Extension Registers for Billing OM's
A00002538.AA07	Performance Measurements Tools
A00002766.AA05	Add Extension Registers for Billing OM's
A00003487.AA27	SN07 Trimodal Call Server Features
A00003531	MG9K EM – Frame location enhancements
A00003687.AA06	TOPS Wireless Intelligent Network Integration
A00003767.AA29	IP ABI PPVM Robustness & Msg Loss Alarms
A00003773.AA08	Trunk Group Based Quality of Service (QOS) Operational Measurement (OM) support for MG4K-IP
A00004036.AA42	Off-Board Service Control
A00004271.AA08	SIP App Server SOC
A00004430.AA08	SVC Failure OMs
A00004500.AA15	IN TCAP Messaging on IP

A00005160.AA10	OSSAIN XA-Core Data Messaging Capacity Enhancements
A00006693	XA-Core IO Capacity Monitoring Toolset

1: Performance (PF): A00002012

1.1 Performance management strategy

This feature does not change the performance management strategy of the XA-Core system.

1.2 Performance management tools and utilities

This feature changes the Operational Measurements (OM) structure for the CMIC, RTIF, and AMDI functionality on the XA-Core. This is so that the OMs will reflect port/link separation of the CMIC and RTIF functionality on the new CMIC/RTIF HIOP card. All OMs changed, deleted, or added by this feature belong to the XACORE OM group.

1.3 Operational Measurements (OM), Group XACORE

1.3.1 OM description

1.3.1.1 Current OM structure for CMIC, RTIF, and AMDI

Currently, the CMIC and RTIF functionalities peg the following OMs: XACMIC, XARTIF, XALOCP, and XAREMP. With this OM structure in place for CMIC, RTIF, and AMDI, these OMs do not distinguish between packlet or device (port or link) state changes. Please refer to “Table 1 Current OM structure for CMIC, RTIF and AMDI” on page 3421.

Table 1 Current OM structure for CMIC, RTIF and AMDI

Functionality	OM	Pegged by event
CMIC	XACMIC	- CMIC packlet Insv -> OOS because of fault - CMIC link Insv -> OOS
RTIF	XARTIF	- RTIF packlet InSv -> OOS because of fault
RTIF	XALOCP	- RTIF local port InSv -> OOS because of fault
RTIF	XAREMP	- RTIF remote port InSv -> OOS because of fault

Table 1 Current OM structure for CMIC, RTIF and AMDI

Functionality	OM	Pegged by event
AMDI	XAMDI	- AMDI packlet InSv -> OOS because of fault - AMDI port InSv -> OOS because of fault
AMDI	XAMDILNK	- AMDI link InSv -> OOS because of fault

1.3.1.2 Release history update

The OM group XACORE is being modified in release CSP20.

With the Ethernet Maintenance feature (A59019176) the Ethernet OMs were extended to support port/link separation. This allowed a more accurate count of the various packlet, port, and link faults. Since this feature also implements port/link separation for CMIC and RTIF on HIOP, it will extend the existing CMIC and RTIF OMs to distinguish between packlet and device (port or link) state changes. Consequently, we will have a more refined count of the CMIC and RTIF component state changes.

This feature also changes the OMs related to the AMDI functionality. This is so that we'll have a consistent OM structure for components with port and link devices in the XA-Core system.

1.3.1.3 Please refer to "Table 2 New OM structure for CMIC, RTIF, and AMDI" on page 3423.**Registers**

Table 2 New OM structure for CMIC, RTIF, and AMDI

Functionality	OM	Pegged by event	New/Deleted/ Changed
CMIC	XACMIC	- CMIC packlet InSv -> OOS because of fault - CMIC link InSv -> OOS because of fault	Deleted
CMIC	XCMIC	CMIC packlet InSv -> OOS because of fault	New
CMIC	XCMICPRT	CMIC port InSv -> OOS because of fault	New
CMIC	XCMICLNK	CMIC link InSv -> OOS because of fault	New
RTIF	XARTIF	RTIF packlet InSv -> OOS because of fault	Deleted
RTIF	XALOCP	RTIF local port InSv -> OOS because of fault	Deleted
RTIF	XAREMP	RTIF remote port InSv -> OOS because of fault	Deleted
RTIF	XRTIF	RTIF packlet InSv -> OOS because of fault	New
RTIF	XRTIFPRT	- RTIF local port InSv -> OOS because of fault - RTIF remote port InSv -> OOS because of fault	New
RTIF	XRTIFLNK	- RTIF local link InSv -> OOS because of fault - RTIF remote link InSv -> OOS because of fault	New
AMDI	XAMDI	- AMDI packlet InSv -> OOS because of fault	Changed
AMDI	XAMDIPRT	- AMDI port InSv -> OOS because of fault	New
AMDI	XAMDILNK	- AMDI link InSv -> OOS because of fault	Unchanged

The XACORE group new OM register display on the MAP terminal is as follows:

Figure 1 OM XACORE Group Display

XAPE	XARXPE	XASM	XARXSM
XAIOP	XARXIO	XADISK	XATAPE
XRTIF	XRTIFPRT	XRTIFLNK	XCMIC
XCMICPRT	XCMICLNK	XARXABRT	XARXBASE
XARXFULL	XARXALL	XAMDI	XAMDIPRT
XAMDILNK	XETHR	XETHRPRT	XETHRLNK

1.3.2 Register XACMIC

1.3.2.1 Register description

Existing XA-Core CMIC (XCMIC) peg register counts the number of critical CMIC packlet and link faults detected on the XA-Core.

1.3.2.2 Register release history update

Register is being removed in CSP20. In order to have consistent naming convention for OMs in the XACORE group, from CSP20, the CMIC packlet faults are going to be counted by the new peg register XCMIC. The CMIC link faults are going to be counted by the new peg register XCMICLNK.

1.3.3 Register XCMIC

1.3.3.1 Register description

The XA-Core CMIC (XCMIC) peg register counts the number of critical CMIC packlet faults detected on the XA-Core.

1.3.3.2 Register release history update

Register is being introduced in CSP20.

1.3.3.3 Associated registers

None.

1.3.3.4 Associated logs

The system generates the MScomm log report (XAC303) when a CMIC packlet goes out of service.

The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the packlet.

1.3.4 Register XCMICPRT

1.3.4.1 Register description

The XA-Core CMIC PORT (XCMICPRT) peg register counts the number of critical CMIC port faults detected on the XA-Core.

1.3.4.2 Register release history update

Register is being introduced in CSP20.

1.3.4.3 Associated registers

None.

1.3.4.4 Associated logs

The system generates the MScomm log report (XAC303) when a CMIC port goes out of service.
The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the port.

1.3.5 Register XCMICLNK

1.3.5.1 Register description

The XA-Core CMIC LINK (XCMICLNK) peg register counts the number of critical CMIC link faults detected on the XA-Core.

1.3.5.2 Register release history update

Register is being introduced in CSP20.

1.3.5.3 Associated registers

None.

1.3.5.4 Associated logs

The system generates the MScomm log report (XAC303) when a CMIC link goes out of service.

The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the link.

1.3.6 Register XARTIF

1.3.6.1 Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF packlet faults detected on the XA-Core.

1.3.6.2 Register release history update

Register is being removed in CSP20. In order to have consistent naming convention for OMs in the XACORE group, from CSP20, the RTIF packlet faults are going to be counted by the new peg register XRTIF.

1.3.7 Register XALOCP

1.3.7.1 Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF local port faults detected on the XA-Core.

1.3.7.2 Register release history update

Register is being removed in CSP20. From CSP20, the RTIF local port faults are going to be counted by the new peg register XRTIFPRT.

1.3.8 Register XAREMP

1.3.8.1 Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF remote port faults detected on the XA-Core.

1.3.8.2 Register release history update

Register is being removed in CSP20. From CSP20, the RTIF remote port faults are going to be counted by the new peg register XRTIFPRT.

1.3.9 Register XRTIF

1.3.9.1 Register description

The XA-Core RTIF (XRTIF) peg register counts the number of critical RTIF packlet faults detected on the XA-Core.

1.3.9.2 Register release history update

Register is being introduced in CSP20.

1.3.9.3 Associated registers

None.

1.3.9.4 Associated logs

The system generates the RTIF log report (XAC305) when an RTIF packlet goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the packlet.

1.3.10 Register XRTIFPRT

1.3.10.1 Register description

The XA-Core RTIF PORT (XRTIFPRT) peg register counts the number of critical RTIF port faults detected on the XA-Core.

Note: There are no separate peg registers for local and remote RTIF port faults. Both peg XRTIFPRT.

1.3.10.2 Register release history update

Register is being introduced in CSP20.

1.3.10.3 Associated registers

None.

1.3.10.4 Associated logs

The system generates the RTIF log report (XAC305) when an RTIF port goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the port.

1.3.11 Register XRTIFLNK

1.3.11.1 Register description

The XA-Core RTIF LINK (XRTIFLNK) peg register counts the number of critical RTIF link faults detected on the XA-Core.

Note: There are no separate peg registers for local and remote RTIF link faults. Both peg XRTIFLNK.

1.3.11.2 Register release history update

Register is being introduced in CSP20.

1.3.11.3 Associated registers

None.

1.3.11.4 Associated logs

The system generates the RTIF log report (XAC305) when an RTIF link goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the link.

1.3.12 Register XAMDI

1.3.12.1 Register description

Existing XA-Core AMDI (XAMDI) peg register counts the number of critical AMDI packlet and port faults detected on the XA-Core.

1.3.12.2 Register release history update

Register is being changed in CSP20. From CSP20, the AMDI port faults are going to be counted by the new peg register XAMDIPRT. Register XAMDI will peg the critical faults against the AMDI packlet. No other modification is introduced.

1.3.13 Register XAMDIPRT

1.3.13.1 Register description

The XA-Core AMDI PORT (XAMDIPRT) peg register counts the number of critical AMDI port faults detected on the XA-Core.

1.3.13.2 Register release history update

Register is being introduced in CSP20.

1.3.13.3 Associated logs

The system generates the AMDI log report (XAC309) when an AMDI port goes out of service.

The system generates the AMDI Link Condition Cleared (XAC609) when the AMDI fault clears on the port.

2: Performance (PF): A00002340

2.1 Performance management strategy

This feature provides the new OM groups FCDRTM1E, FCDRTM2E and FCDRALG2.

2.2 Performance management tools and utilities

None

2.3 Performance Measurements (PM), Operational Measurements (OM), and stats

2.3.1 PM, OM, and stats format

N/A

2.3.2 OM Group FCDRTM1E (applies only to DMS)

2.3.2.1 OM description

OM Group FCDRTM1E

The group FCDRTM1E is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRTMP1.

2.3.2.2 Release history update

The OM group is being provided new in the UCS20 release.

2.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

```
FCDRTM1E

CLASS: HOLDING
START:2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;
SLOWSAMPLES:          3 ; FASTSAMPLES:          30 ;

           TMPLT_0     TMPLT_1     TMPLT_2     TMPLT_3
           TMPLT_4     TMPLT_5     TMPLT_6     TMPLT_7
           TMPLT_8     TMPLT_9    TMPLT_10    TMPLT_11
          TMPLT_12    TMPLT_13    TMPLT_14    TMPLT_15
          TMPLT_16    TMPLT_17    TMPLT_18    TMPLT_19
```

```
          TMPLT_20    TMPLT_21    TMPLT_22    TMPLT_23
          TMPLT_24    TMPLT_25    TMPLT_26    TMPLT_27
          TMPLT_28    TMPLT_29    TMPLT_30    TMPLT_31

0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
                0           0           0           0
```

2.3.2.4 Group structure

This OM group provides 32 pre-defined tuples.

2.3.2.5 Associated OM groups

This OM group is used as register overflows for the OM group FCDRTMP1.

2.3.2.6 Associated functional groups

None

2.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code

2.3.2.8 OM group registers logic flow chart

Refer to the comments in the Associated Register section.

2.3.3 Register (applies only to DMS)

TMPLT_0 through TMPLT_31

2.3.3.1 Register description

Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number.

The index number of a CDR template may be viewed from the MAP under the CI CTMPLT. The “TEMPLATE ALL” command will list out the indexes.

The data range for these registers is a decimal value of 0-65535.

This OM group supports indexes 0-31.

Example: CDR template UCS13 is index 9. The related OM register will be TMPLT_9.

```
>ctmplt
>template all
The list of indices and defined templates is as follows:
 0 : CDR2AMA
 1 : CDR2AMA2
 2 : CDR2AMA3
 3 : RESERVED03
 4 : RESERVED04
 5 : AMAREC
 6 : UCS09
 7 : UCS11
 8 : UCS12
 9 : UCS13
```

2.3.3.2 Register release history update

All the registers in this group are new in the UCS20 release.

2.3.3.3 Associated registers

Each register is this OM group is related to a register in group FCDRTMP1. When the register in group FCDRTMP1 reaches 65535, the associated extension register in group FCDRTM1E will be incremented. If the SOC is IDLE, the FCDRTM1E register will not be pegged. In either case, the register in group FCDRTMP1 will wrap to 0 when it overflows.

Example:

Group FCDRTMP1; Register TMPLT_9
Group FCDRTM1E; Register TMPLT_9

A FCDRTM1E register in is pegged once for every FCDRTMP1 register overflow. A value of 1 in the FCDRTM1E overflow register indicates 65535 pegs. A value of 1 in the FCDRTMP1 register indicates one peg.

Once the FCDRTM1E overflow register is pegged, the register in FCDRTMP1 will reset to 0 and resume pegging.

2.3.3.4 Associated logs

None

2.3.4 OM Group FCDRTM2E (applies only to DMS)

2.3.4.1 OM description

OM Group FCDRTM2E

The group FCDRTM2E is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRTMP2.

2.3.4.2 Release history update

The OM group is being provided new in the UCS20 release.

2.3.4.3 Registers

OM group registers display on the MAP terminal as follows:

```
FCDRTM2E

CLASS: ACTIVE
START:2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;
SLOWSAMPLES:          5 ; FASTSAMPLES:          50 ;

          TMPLT_32    TMPLT_33    TMPLT_34    TMPLT_35
          TMPLT_36    TMPLT_37    TMPLT_38    TMPLT_39
          TMPLT_40    TMPLT_41    TMPLT_42    TMPLT_43
          TMPLT_44    TMPLT_45    TMPLT_46    TMPLT_47
          TMPLT_48    TMPLT_49    TMPLT_50    TMPLT_51
          TMPLT_52    TMPLT_53    TMPLT_54    TMPLT_55
          TMPLT_56    TMPLT_57    TMPLT_58    TMPLT_59
          TMPLT_60    TMPLT_61    TMPLT_62    TMPLT_63

    0
                  0           0           0           0
                  0           0           0           0
```

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

2.3.4.4 Group structure

This OM group provides 32 pre-defined tuples.

2.3.4.5 Associated OM groups

This OM group is used as register overflows for the OM group FCDRTMP2.

2.3.4.6 Associated functional groups

None

2.3.4.7 Associated functionality codes

Table 2 Functionality codes associated with OM group

Functionality	Code

2.3.4.8 OM group registers logic flow chart

Refer to the comments in the Associated Register section.

2.3.5 Register (applies only to DMS)

TMPLT-32 through TMPLT_63

2.3.5.1 Register description

Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. The index number of a CDR template may be viewed from the MAP under the CI CTMPLT. The “TEMPLATE ALL” command will list out the indexes.

The data range for these registers is a decimal value of 0-65535.

This OM group supports indexes 32-63.

Example: CDR template UCS13 is index 9. The related OM register will be TMPLT_9.

```
>ctmplt
>template all
The list of indices and defined templates is as follows:
 0 : CDR2AMA
 1 : CDR2AMA2
 2 : CDR2AMA3
 3 : RESERVED03
 4 : RESERVED04
 5 : AMAREC
 6 : UCS09
 7 : UCS11
 8 : UCS12
 9 : UCS13
```

2.3.5.2 Register release history update

All the registers in this group are new in the UCS20 release.

2.3.5.3 Associated registers

Each register is this OM group is related to a register in group FCDRTMP2. When the register in group FCDRTMP2 reaches 65535, the associated extension register in group FCDRTM2E will be incremented. If the SOC is IDLE, the FCDRTM2E register will not be pegged. In either case, the register in group FCDRTMP2 will wrap to 0 when it overflows.

Example:

Group FCDRTMP2; Register TMPLT_21
Group FCDRTM2E; Register TMPLT_21

A FCDRTM2E register in is pegged once for every FCDRTMP2 register overflow. A value of 1 in the FCDRTM2E overflow register indicates 65535 pegs. A value of 1 in the FCDRTMP2 register indicates one peg.

Once the FCDRTM2E overflow register is pegged, the register in FCDRTMP2 will reset to 0 and resume pegging.

2.3.5.4 Associated logs

None

2.3.6 OM Group FCDRALG2 (applies only to DMS)

2.3.6.1 OM description

OM Group FCDRALG2

The group FCDRALG2 is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRALGR.

2.3.6.2 Release history update

The OM group is being provided new in the UCS20 release.

2.3.6.3 Registers

OM group registers display on the MAP terminal as follows:

```
FCDRALG2

CLASS: ACTIVE
START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;
SLOWSAMPLES:          1 ; FASTSAMPLES:           3 ;

          INTERNAL   CALLTYPE    SUBRNUM         TRK
              TCAP      FIXED    BESTFIT    RTEATTR

    0
                 0          0          0          0
                 0          0          0          0
```

2.3.6.4 Group structure

This OM group provides 8 pre-defined tuples.

2.3.6.5 Associated OM groups

This OM group is used as register overflows for the OM group FCDRALGR.

2.3.6.6 Associated functional groups

None

2.3.6.7 Associated functionality codes

Table 3 Functionality codes associated with OM group

Functionality	Code

2.3.6.8 OM group registers logic flow chart

Refer to the comments in the Associated Register section.

2.3.7 Register (applies only to DMS)

INTERNAL
CALLTYPE
SUBRNUM
TRK
TCAP
FIXED
BESTFIT
RTEATTR

2.3.7.1 Register description

These registers have the same description as those in the group FCDRALGR. The only difference is that these are extension registers. This means that one count here is equal to 65535 counts of the same register in FCDRALGR. They keep track of the number of times the register in group FCDRALGR have overflowed.

2.3.7.2 Register release history update

All the registers in this group are new in the UCS20 release.

2.3.7.3 Associated registers

Each register is this OM group is related to a register in group FCDRALGR. When the register in group FCDRALGR reaches 65535, the associated extension register in group FCDRALG2 will be incremented. If the SOC is IDLE, the FCDRALG2 register will not be pegged. In either case, the register in group FCDRALGR will wrap to 0 when it overflows.

Example:

Group FCDRALGR; Register FIXED

Group FCDRALG2; Register FIXED

A FCDRALG2 register in is pegged once for every FCDRALGR register overflow. A value of 1 in the FCDRALG2 overflow register indicates 65535 pegs. A value of 1 in the FCDRALGR register indicates one peg.

Once the FCDRALG2 overflow register is pegged, the register in FCDRALGR will reset to 0 and resume pegging.

2.3.7.4 Associated logs

None

3: Performance (PF): A00002538

3.1 Performance management strategy

3.2 Performance management tools and utilities

3.3 Performance Measurements (PM), Operational Measurements (OM), and stats

XASTAT OM group

3.3.1 PM, OM, and stats format

3.3.2 OM Group template (applies only to DMS)

XASTAT OM group

3.3.2.1 OM description

OM group XASTAT

Capacity operational measurements

3.3.2.2 Release history update

The OM group XASTAT is being modified in CSP20. It will be changed as follows:

Register XASCMPLX will be removed from OM group XASTAT since this measurement is not valid in XA-Core.

3.3.2.3 Registers

It is the same as in previous releases except the register XASCMPLX is removed.

In previous releases, XASTAT OM group registers display on the MAP terminal as follows:

```
XASTAT

CLASS: ACTIVE
START:2003/09/11 12:30:00 THU; STOP: 2003/09/11 12:48:29 THU;
SLOWSAMPLES:        12 ; FASTSAMPLES:        111 ;

          XASUTIL   XASPUTIL   XASCMPLX   XASSCHED
          XASFORE   XASMAINT     XASDNC      XASOM
```

```
          XASGTERM      XASBKG    XASAUXCP     XASNETM
           XASSNIP     XASPESC     XASNXFR     XASOVER
          XASOTHLD

    0
                  0           0           0           0
                  0           0           0           0
                  0           0           0           0
                  0           0           0           0
                  0
```

After removing XASCMPLX in CSP20, it will be displayed as:

```
XASTAT

CLASS: ACTIVE
START:2003/09/11 12:30:00 THU; STOP: 2003/09/11 12:48:29 THU;
SLOWSAMPLES:         12 ; FASTSAMPLES:         111 ;

           XASUTIL    XASPUTIL    XASSCHED     XASFORE
          XASMAINT      XASDNC       XASOM    XASGTERM
            XASBKG    XASAUXCP     XASNETM     XASSNIP
           XASPESC     XASNXFR     XASOVER    XASOTHLD

    0
                  0           0           0           0
                  0           0           0           0
                  0           0           0           0
                  0           0           0           0
```

3.3.2.4 Group structure

No change

3.3.2.5 Associated OM groups

No change

3.3.2.6 Associated functional groups

No change

3.3.2.7 Associated functionality codes

No change

3.3.2.8 OM group registers logic flow chart

No change

3.3.3 Register (applies only to DMS)

No change

3.3.3.1 Register description

3.3.3.2 Register release history update

3.3.3.3 Associated registers

3.3.3.4 Associated logs

4: Performance (PF): A00002766

4.1 Performance management strategy

This feature provides the new OM group ATTAMA2.

4.2 Performance management tools and utilities

None

4.3 Performance Measurements (PM), Operational Measurements (OM), and stats

4.3.1 PM, OM, and stats format

N/A

4.3.2 OM Group ATTAMA2 (applies only to DMS)

4.3.2.1 OM description

OM Group ATTAMA2

The group ATTAMA2 is only pegged when the BAS00023 SOC is ON.

This group is used for register overflows from the OM group ATTAMA.

4.3.2.2 Release history update

The OM group is being provided new in the UCS20 release.

4.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

```
ATTAMA2
CLASS:   ACTIVE
START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;
SLOWSAMPLES:         7 ; FASTSAMPLES:         69 ;
            AMANS2 AMUNANS2

    0           0          0
```

4.3.2.4 Group structure

This OM group provides 2 pre-defined tuples.

4.3.2.5 Associated OM groups

This OM group is used as register overflows for the OM group ATTAMA.

4.3.2.6 Associated functional groups

None

4.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code

4.3.2.8 OM group registers logic flow chart

Refer to the comments in the Associated Register section.

4.3.3 Register (applies only to DMS)

4.3.3.1 Register description

AMANS2 - overflow for AMANS from group ATTAMA

AMUNANS2 - overflow for AMUNANS from group ATTAMA.

4.3.3.2 Register release history update

All the registers in this group are new in the UCS20 release.

4.3.3.3 Associated registers

ATTAMA.AMANS - ATTAMA2.AMANS2
ATTAMA.AMUNANS - ATTAMA2.AMUNAS2

The range of each of these registers is an decimal value of 0 - 32767.

When the ATTAMA register reaches its maximum value of 32767 and overflows, it increments the associated overflow register in group ATTAMA2. The ATTAMA register will then reset to 0 and resume incrementing.

The registers in the group ATTAMA2 indicate the number of times the associated register in group ATTAMA has overflowed. One peg in the ATTAMA2 register indicates 32767 pegs that were handled by the ATTAMA register.

4.3.3.4 Associated logs

None

5: Performance (PF): A00003487

5.1 Performance management strategy

Trimodal Call Server provides support for multiple bearer networks in a single CS2K Call Server. In order to monitor the performance of the call server, additional OMs are needed. These new OMs provide per-bearer network performance metric collection that will enable the customer management system to monitor the performance of the call server as a whole as well as the individual bearer networks.

5.2 Performance management tools and utilities

No change

5.3 Performance Measurements (PM), Operational Measurements (OM), and stats

The following is a list of the new and changed OM groups for the Trimodal Call Server feature:

- DPTNODE (changed)
- DPTOFCP (new)
- IWBM (changed)
- OFZ2NET1 (new)
- OFZ2NET2 (new)
- TRK2NET1 (new)
- TRK2NET2 (new)

5.3.1 PM, OM, and stats format

5.3.2 DPTNODE OM Group

5.3.2.1 OM description

DPTNODE OM group measures the DPT performance for each DPT capable node. The group contains registers that maintain DPT terminal usage and failure counts.

5.3.2.2 Release history update

The DPTNODE OM group is being modified in SN07 to add additional information to the OM tuples. If the DPT Node is a GWC, then the associated DPT protocol (i.e., BICC or SIP-T) is added to the information. If the DPT Node is an SPM (i.e., either MG4K or DTP SPM), then the associated bearer

network, DPT protocol and SPM node type is added to the information. The registers are unchanged and the pegging of the registers are unchanged.

The addition of this new information is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new information is displayed. If the parameter is set to 'N', then the DPTNODE OM group appears as it did prior to SN07.

5.3.2.3 Registers

DPTNODE OM group registers display on the MAP terminal as follows:

Figure 1 DPTNODE OM Group Display

```
>omshow dptnode active

DPTNODE

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PM_INFO)
            DPTGTAT       DPTGTAT2      DPTGTFL       DPTGTFLO
            DPTUSAG       DPTUSAG2      DPTHWT

0
   GWC  3    93 BICC
            0             0             0             0
            0             0             0

1
   GWC   4   94 SIPT
            0             0             0             0
            0             0             0

2
   SPM    1   70 NET 2 NET_AAL1 BICC SMG4
            0             0             0             0
            0             0             0
3
   SPM    2   71 NET 0 ENET_TO_AAL1_DPT   BICC      DPT
            0             0             0             0
            0             0             0
```

5.3.2.4 Group structure

DPTNODE OM group provides 1 tuple(s) for each GWC or SPM node that is capable of hosting a DPT call.

Key field: Unchanged

Info field: DPT_NODE_OM_PM_INFO

For GWC nodes, the info field contains the DPT protocol (BICC or SIP-T) associated with the GWC as data filled in the SERVSINV table.

For MG 4000 and DPT SPM nodes, the info field contains the associated bearer network, the DPT protocol (BICC), and the SPM node type (SMG4 or DPT). The bearer network is comprised of the Network ID and Name as data filled in the BEARNETS table and linked to the SPM-based node through the MNNODE table. The DPT protocol will always be BICC because SPM nodes do not support SIP-T protocol in SN07. The SPM node type is either SMG4 (for MG4Ks) or DPT (for DPT SPMs). This information is derived from the node type found in Table MNNODE.

5.3.2.5 Associated OM groups

Unchanged.

5.3.2.6 Associated functional groups

Unchanged

5.3.2.7 Associated functionality codes

None

5.3.2.8 OM group registers logic flow chart

Unchanged.

5.3.2.9 Register DPTGTAT

5.3.2.9.1 Register description Get Terminal Attempts (DPTGTAT) registers a peg for each attempt to get a DPT terminal on the associated node.

5.3.2.9.2 Register release history update Register is unchanged in SN07.

5.3.2.9.3 Associated registers DPTGTAT2 (an extension register for DPTGTAT)

5.3.2.9.4 Associated logs Unchanged.

5.3.2.10 Register DPTGTFL

5.3.2.10.1 Register description Get Terminal Failures (DPTGTFL) registers a peg for each failed attempt to get an un-optimized DPT terminal on the associated node.

5.3.2.10.2 Register release history update Register is unchanged in SN07.

5.3.2.10.3 Associated registers None.

5.3.2.10.4 Associated logs Unchanged.

5.3.2.11 Register DPTGTFLO

5.3.2.11.1 Register description Get Terminal Failures Optimized (DPTGFLO) registers a peg for each failed attempt to get an optimized DPT terminal on the associated node.

5.3.2.11.2 Register release history update Register is unchanged in SN07.

5.3.2.11.3 Associated registers None.

5.3.2.11.4 Associated logs Unchanged.

5.3.2.12 Register DPTUSAG

5.3.2.12.1 Register description DPT Terminal Usage (DPTUSAG) registers a count of the total usage within a transfer period. Usage is pegged by the number of terminals in Call Processing Busy (CPB) or Call Processing Deload (CPD) state at a sampling that occurs every 100 seconds.

5.3.2.12.2 Register release history update Register is unchanged in SN07.

5.3.2.12.3 Associated registers DPTUSAG2 (extension register for DPTUSAG)

5.3.2.12.4 Associated logs Unchanged.

5.3.2.13 Register DPTHWT

5.3.2.13.1 Register description DPT Terminals usage High Water (DPTHWT) registers a count of the terminal usage high water mark within a transfer period. The high water mark is equivalent to the following:

- (inservice number) - (low water mark)

The low water mark updates for each attempt to get a terminal. The OM compares the current high water mark to the previous high water mark every 100 seconds. An update is made if the current value exceeds the previous value.

5.3.2.13.2 Register release history update Register is unchanged in SN07.

5.3.2.13.3 Associated registers None.

5.3.2.13.4 Associated logs Unchanged.

5.3.3 DPTOFCP OM Group

5.3.3.1 OM description

DPTOFCP OM Group measures the performance of the supported dynamic packet trunk protocols for the office. The two supported protocols are BICC and SIP-T.

5.3.3.2 Release history update

DPTOFCP OM group is new in SN07.

The addition of this new DPTOFCP OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to ‘Y’, then the tuples of the DPTOFCP OM group are displayed. If the parameter is set to ‘N’, then the tuples of the DPTOFCP OM group are not displayed.

5.3.3.3 Registers

DPTOFCP OM group registers display on the MAP terminal as follows:

Figure 2 DPTOFCP OM Group Display

```
>omshow dptofcp active

DPTOFCP

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (DPT_PROTOCOL_INFO)
            DPGTATT       DPGTATT2      DPGETFL       DPGETFL2
            DPUSAGE       DPUSAGE2      DPOTFLO       DPOTFLO2
            DPHWTR        DPHWTR2       DPRTDPL       DPRTDPL2

0
   BICC
            0             0             0             0
            0             0             0             0
            0             0             0             0

1
   SIPT
            0             0             0             0
            0             0             0             0
            0             0             0             0
```

5.3.3.4 Group structure

DPTOFCP OM group provides 1 tuple(s) for each DPT protocol that is active in the office.

Key field: DPT_PROTOCOL_TYPE {BICC, SIP-T}

Info field: DPTOFCP_SIG_INFO

- Identifies the protocol being used in the office.

5.3.3.5 Associated OM groups

DPTOFC OM group gives an overall office-wide DPT performance measurement. DPTOFCP OM group provides a per-DPT capable node performance view.

5.3.3.6 Associated functional groups

The following functional groups are associated with DPTOFCP OM group:

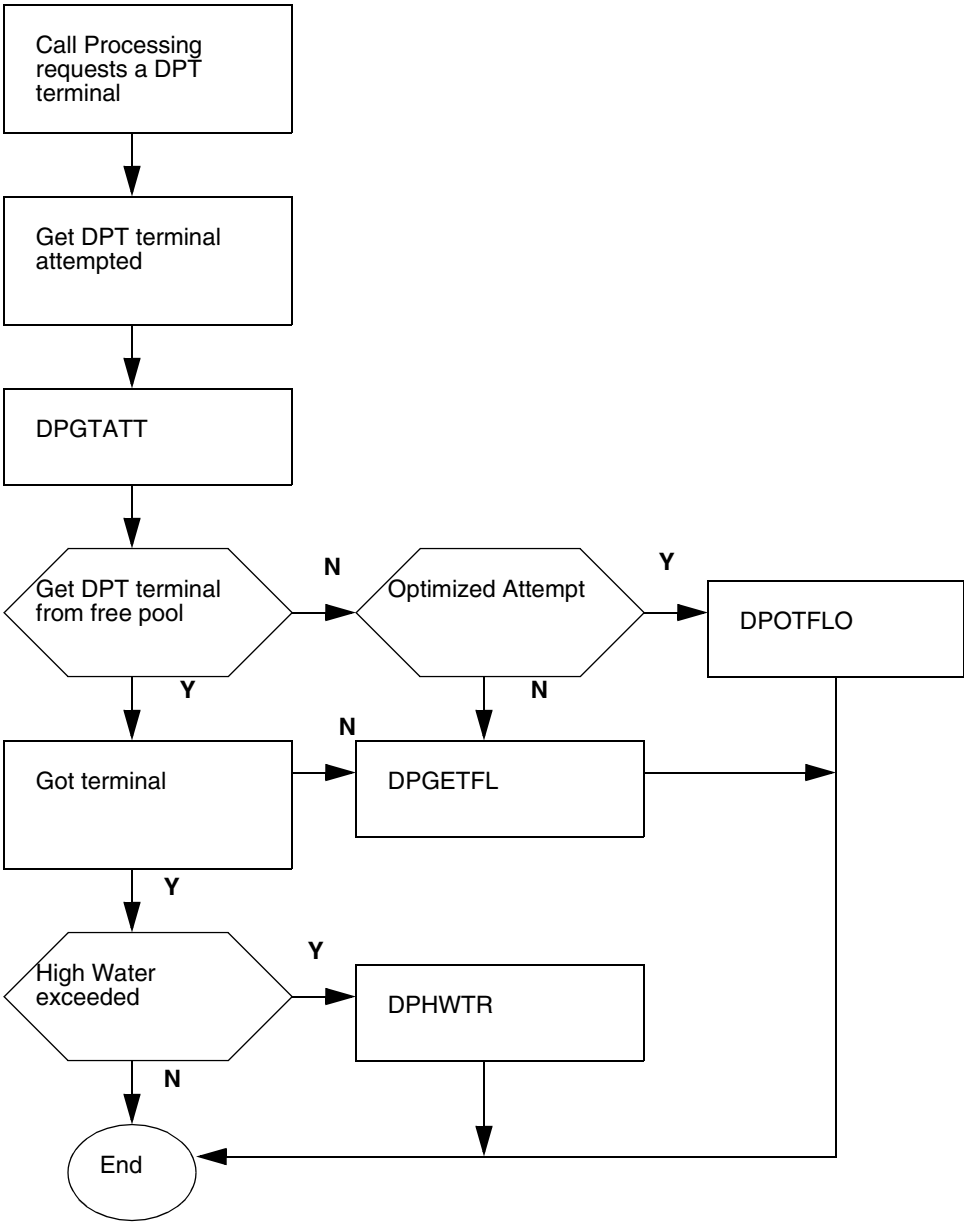
- Dynamic Packet Trunks

5.3.3.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code
Dynamic Packet Trunks	

5.3.3.8 DPTOFCP OM group registers logic flow chart



5.3.3.9 Register DPGTATT

5.3.3.9.1 Register description Get Terminal Attempts (DPGTATT) registers a peg for each attempt to get a DPT terminal on the associated protocol.

5.3.3.9.2 Register release history update Register is new in SN07.

5.3.3.9.3 Associated registers DPGTATT2 (an extension register for DPGTATT)

5.3.3.9.4 Associated logs None.

5.3.3.10 Register DPGETFL

5.3.3.10.1 Register description Get Terminal Failures (DPGETFL) registers a peg for each failed attempt to get an un-optimized DPT terminal on the associated protocol.

5.3.3.10.2 Register release history update Register is new in SN07.

5.3.3.10.3 Associated registers DPGETFL2 (an extension register for DPGETFL).

5.3.3.10.4 Associated logs None.

5.3.3.11 Register DPOTFLO

5.3.3.11.1 Register description Get Terminal Failures Optimized (DPOTFLO) registers a peg for each failed attempt to get an optimized DPT terminal on the associated protocol. Pegs to DPOTFLO are benign and do not require corrective action.

5.3.3.11.2 Register release history update Register is new in SN07.

5.3.3.11.3 Associated registers DPOTFLO2 (an extension register for DPOTFLO).

5.3.3.11.4 Associated logs None.

5.3.3.12 Register DPUSAGE

5.3.3.12.1 Register description DPT Terminal Usage (DPUSAGE) registers a count of the total usage within a transfer period. Usage is pegged by the number of terminals in Call Processing Busy (CPB) or Call Processing Deload (CPD) state at a sampling that occurs every 100 seconds.

5.3.3.12.2 Register release history update Register is new in SN07.

5.3.3.12.3 Associated registers DPUSAGE2 (extension register for DPUSAGE)

5.3.3.12.4 Associated logs None.

5.3.3.13 Register DPHWTR

5.3.3.13.1 Register description DPT Terminals usage High Water (DPHWTR) registers a count of the terminal usage high water mark within a transfer period. The high water mark is equivalent to the following:

- (inservice DPT terminals) - (free DPT terminals)

Free DPT terminals represent inservice terminals in the free queue that are eligible for call processing. The high water mark is calculated every 10 seconds. The register updates if the value from the current calculation is greater than the previous value kept in the register for that transfer period.

5.3.3.13.2 Register release history update Register is new in SN07.

5.3.3.13.3 Associated registers DPHWTR2 (an extension register for DPHWTR).

5.3.3.13.4 Associated logs None.

5.3.3.14 Register DPRTDPL

5.3.3.14.1 Register description DPT Port Depletion (DPRTDPL) registers the number of attempts to get a DPT terminal that failed due to port depletion (i.e., exceeding the DPT_MAX_PORT office parameter value).

5.3.3.14.2 Register release history update Register is new in SN07.

5.3.3.14.3 Associated registers DPRTDPL2 (an extension register for DPRTDPL).

5.3.3.14.4 Associated logs None.

5.3.4 IWBM OM Group

5.3.4.1 OM description

IWBM OM Group is modified to count different events on the specific bridge pools that are defined in the call server.

5.3.4.2 Release history update

IWBM OM group is changed in SN07.

5.3.4.3 Registers

IWBM OM group registers display on the MAP terminal as follows:

Figure 3 IWBM OM Group Display

```
>omshow iwbm active

IWBM

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

INFO (IWBM_POOL_INFO)
              IWGBATT      IWGBATT2     IWGBFAIL     IWGBABRT
              IWFBATT      IWFBATT2     IWFBFAIL     IWFBABRT
              IWONSET1     IWONSET2     IWABATE1     IWABATE2
              IWBTLTST     IWBCNFAN


0
              ENET_TO_ATM
              0            0            0            0
              0            0            0            0
              0            0            0            0
              0            0            0            0

1
              ENET_TO_IP
              0            0            0            0
              0            0            0            0
              0            0            0            0
              0            0            0            0
```

5.3.4.4 Group structure

IWBM OM group provides 1 tuple(s) for each IW SPM bridge pool that is active in the office. .

Key field: IW SPM bridge pools

Info field: BEARER_NETBRIDGE_CLLI

- Associated bridge pool name (i.e., ‘ENET_TO_IP’). This bridge pool name is defined in Table CLLI and Table NETBRDGE. Each IW SPM bridge node is associated with a bridge pool in Table MNNODE.

5.3.4.5 Associated OM groups

None.

5.3.4.6 Associated functional groups

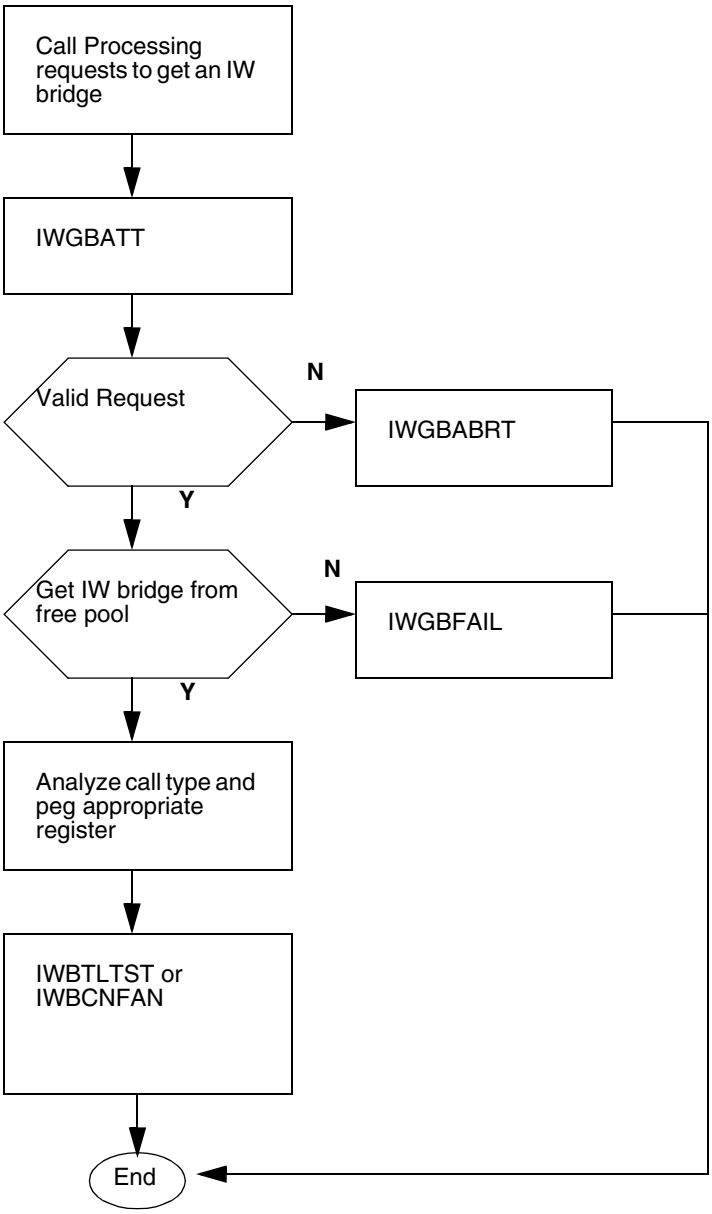
The following functional groups are associated with IWBM OM group:

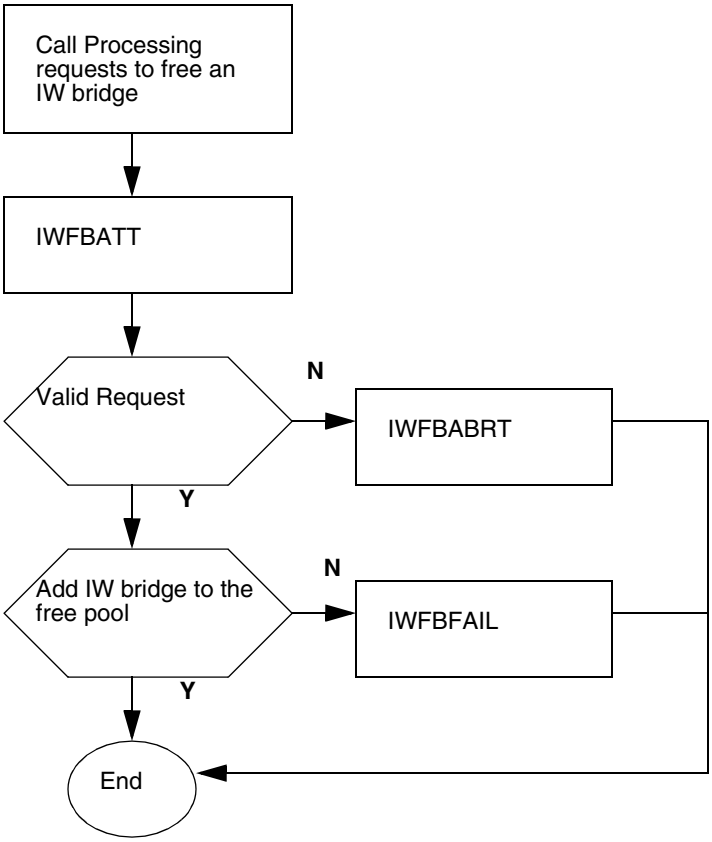
- IW SPM Bridges

5.3.4.7 Associated functionality codes

None

5.3.4.8 IWBM OM group registers logic flow chart





5.3.4.9 Register IWGBATT

5.3.4.9.1 Register description IW Get Bridge Attempts (IWGBATT) registers a peg for each attempt to get an IW SPM bridge port on the associated IW SPM bridge node.

5.3.4.9.2 Register release history update Register is changed in SN07.

5.3.4.9.3 Associated registers IWGBATT2 (an extension register for IWGBATT)

5.3.4.9.4 Associated logs None.

5.3.4.10 Register IWGBFAIL

5.3.4.10.1 Register description IW Get Bridge Failure (IWGBFAIL) registers a peg when a get bridge attempt fails as a result of queue failure. The normal cause of a queue failure is that all bridges are busy on the associated node.

5.3.4.10.2 Register release history update Register is changed in SN07.

5.3.4.10.3 Associated registers None.

5.3.4.10.4 Associated logs None.

5.3.4.11 Register IWGBABRT

5.3.4.11.1 Register description IW Get Bridge Aborted (IWGBABRT) registers a peg when a get bridge attempt aborts the system as a result of incorrect data in the request.

5.3.4.11.2 Register release history update Register is changed in SN07.

5.3.4.11.3 Associated registers None.

5.3.4.11.4 Associated logs None.

5.3.4.12 Register IWFBATT

5.3.4.12.1 Register description IW Free Bridge Attempts (IWFBATT) registers a peg when a attempt is made to free an IW SPM bridge from an associated call. When an interworked call ends, the system makes a free bridge attempt.

5.3.4.12.2 Register release history update Register is changed in SN07.

5.3.4.12.3 Associated registers IWFBATT2 (extension register for IWFBATT)

5.3.4.12.4 Associated logs None.

5.3.4.13 Register IWFBFAIL

5.3.4.13.1 Register description IW Free Bridge Failure (IWFBFAIL) registers a peg when a free bridge attempt fails.

5.3.4.13.2 Register release history update Register is changed in SN07.

5.3.4.13.3 Associated registers None.

5.3.4.13.4 Associated logs None.

5.3.4.14 Register IWFBABRT

5.3.4.14.1 Register description IW Free Bridge Aborted (IWGBABRT) registers a peg when a free bridge attempt aborts the system as a result of incorrect data in the request.

5.3.4.14.2 Register release history update Register is changed in SN07.

5.3.4.14.3 Associated registers None.

5.3.4.14.4 Associated logs None.

5.3.4.15 Register IWBTLTST

5.3.4.15.1 Register description IW Bridge for Trunk and Line Testing (IWBTLTST) registers a peg every time an IW bridge is used for a packet agent's access to trunk and/or line test facilities present on the ENET (i.e., MTM test circuits).

5.3.4.15.2 Register release history update Register is changed in SN07.

5.3.4.15.3 Associated registers None.

5.3.4.15.4 Associated logs None.

5.3.4.16 Register IWONSET1

5.3.4.16.1 Register description IW Bridge Onset 1 (IWONSET1) indicates that the number of in use IW bridges exceeds 70% of the associated bridge pool. The system pegs this register when the number of in use bridges in the pool reaches 70%. The system must peg register IWABATE1 before pegging IWONSET1 again.

5.3.4.16.2 Register release history update Register is changed in SN07.

5.3.4.16.3 Associated registers IWABATE1. The system must peg register IWABATE1 before pegging IWONSET1 again.

5.3.4.16.4 Associated logs None.

5.3.4.17 Register IWONSET2

5.3.4.17.1 Register description IW Bridge Onset 2 (IWONSET2) indicates that the number of in use IW bridges exceeds 90% of the associated bridge pool. The system pegs this register when the number of in use bridges in the pool reaches 90%. The system must peg register IWABATE2 before pegging IWONSET2 again.

5.3.4.17.2 Register release history update Register is changed in SN07.

5.3.4.17.3 Associated registers IWABATE2. The system must peg register IWABATE2 before pegging IWONSET2 again.

5.3.4.17.4 Associated logs None.

5.3.4.18 Register IWABATE1

5.3.4.18.1 Register description IW Bridge Abate 1 (IWABATE1) indicates that the total number of IW bridges in use is less than 65% of the associated bridge pool. The system pegs this register after pegging register IWONSET1 and then crosses the 65% threshold. The system must peg register IWONSET1 again before it pegs this register a second time.

5.3.4.18.2 Register release history update Register is changed in SN07.

5.3.4.18.3 Associated registers IWONSET1. The system pegs this register after pegging register IWONSET1 and then crosses the 65% threshold. The system must peg register IWONSET1 again before it pegs this register a second time.

5.3.4.18.4 Associated logs None.

5.3.4.19 Register IWABATE2

5.3.4.19.1 Register description IW Bridge Abate 2 (IWABATE2) indicates that the total number of IW bridges in use is less than 85% of the associated bridge pool. The system pegs this register after pegging register IWONSET2 and then crosses the 85% threshold. The system must peg register IWONSET2 again before it pegs this register a second time.

5.3.4.19.2 Register release history update Register is changed in SN07.

5.3.4.19.3 Associated registers IWONSET2. The system pegs this register after pegging register IWONSET2 and then crosses the 65% threshold. The system must peg register IWONSET2 again before it pegs this register a second time.

5.3.4.19.4 Associated logs None.

5.3.4.20 Register IWBCNFAN

5.3.4.20.1 Register description IW Bridge for Conference and Announcement Usage (IWBCNFAN) registers a peg every time an IW bridge is used for a packet agent's access to conference or announcement facilities present on the ENET (i.e., MTM service circuits).

5.3.4.20.2 Register release history update Register is new in SN07.

5.3.4.20.3 Associated registers None.

5.3.4.20.4 Associated logs None.

5.3.5 OFZ2NET1 OM Group

5.3.5.1 OM description

OM group Office to Network Group 1 (OFZ2NET1) provides traffic analysis information for each bearer network. Using primary route scoring, the group counts calls for the intended destination rather than for the terminating destination.

OFZ2NET1records the structure of traffic that arrives at an office on a particular bearer network, the first routing, and the routing of outgoing traffic. A call routes to a tone or announcement if:

- the tone or announcement is the intended destination of the call.
- an error condition occurs that includes a tone or announcement as a part of the call treatment.

  Note: The a treatment routes the call to another tone or announcement, OFZ2NET1 counts only the first tone or announcement.

OM groups OFZ and OFZ2 provide traffic analysis information office wide. OFZ2NET1 and OFZ2NET2 provide similar traffic analyses with further refinement on a per-bearer network basis for an office.

New office parameter MULTINET_DISPLAY_ACTIVE must be set to *Y* before the system can display OFZ2NET1.

The following table contains the registers that count incoming calls. The register TRKORIG counts each incoming call on the bearer network. One of the following registers counts each incoming call:

- ICANN
- ICLKT
- NICOG
- ICTRM
- ICTONE
- ICABNC
- ICABNM
- TRKORIG

The count depends on if the source of the call is a line or a trunk.

Table 2 Incoming calls

Register	Intended destination	Routing
NICOG(2)	trunk	trunk
ICTRM(2)	line	line
ICANN	trunk, line, announcement	announcement
ICTONE	trunk, line, tone	tone
ICLKT	trunk, line	lockout
ICABNC	trunk, line	customer abandon
ICABNM	trunk, line	machine abandon
TRKORIG(2)	all	all

The following table contains a list of registers that count originating calls. Register LINEUSG counts each originating call. One register from registers LINEANN, LINELKT, LINEOG, LINETRM, LINETONE and LINEABDN counts each originating call. The system routes a call to an intended destination. The intended destination of the call is either a tone or an announcement. The system routes a call if an error condition is present. The error condition must include a tone or announcement as part of its treatment. If a treatment routes the call to another tone or announcement, the OFZ2NET1 only counts the first tone or announcement.

Table 3 Originating calls

Register	Intended designation	Routing
LINEOG(2)	trunk	trunk
LINETRM(2)	line	line
LINEANN	trunk, line, announcement	announcement
LINETONE	trunk, line, tone	tone
LINELKT	trunk, line	lockout
LINEABDN	trunk, line	abandon
LINEUSG(2)	trunk, line	all

The following table contains registers that count terminating calls on the associated bearer network. Register TRMLNAT counts each terminating call. Registers TRMMCHFL and TRMBLCK count calls on a blocked network. LNMBSYPC counts lines that are made manually busy.

Table 4 Terminating calls

Register	Event
TRMMCHFL	Network Blockage Heavy Traffic (NBLH) or Network Blockage Normal Traffic (NBLN)
TRMBLCK	Network Blockage Normal Traffic (NBLN)
LNMBSYPC	line manual busy
TRMLNAT(2)	all outgoing traffic

5.3.5.2 Release history update

OFZ2NET1 OM group is new in SN07.

Office parameter OFFICETYPE in table OFCSTD controls the generation of the registers for OFZ2NET1. When the system reports an answer indicator to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

5.3.5.3 Registers

OFZ2NET1 OM group registers display on the MAP terminal as follows:

Figure 4 OFZ2NET1 OM Group Display

```
>omshow ofz2net1 active
OFZ2NET1
CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;
   INFO (BEARNETS_INFO)
          ICANN          ICLKT          NICOG          NICOG2
          ICTONE         TRKORIG        TRKORIG2       OGNWAT
          OGNWAT2        OGMFL          OGTRMFL        OGOSF
          OGROSF         ICABNM         ICABNC         LINEANN
          LINELKT        LINEOG         LINEOG2        LINETRM
          LINETRM2       LINETONE       LINEUSG        LINEUSG2
          ICTRM          ICTRM2         TRMLNAT        TRMLNAT2
          TRMMCHFL       TRMBLCK        LNMBSYPC       LINEABDN
0
     NET 0 TDM_ENET
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
1
     NET 1 NET_AAL1
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
2
     NET 2 NET_IP
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
          0              0              0              0
```

The validity of a OFZ2NET2 register in an officetype is given in the following table

Table 5 OFZ2NET1 OM registers

Register	Present In Officetype
ICANN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICLKT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
NICOG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
NICOG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICTONE	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
TRKORIG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
TRKORIG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGNWAT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGNWAT2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGMFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGTRMFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGOSF	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice

Register	Present In Officetype
OGROSF	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICABNM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICABNC	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
LINEANN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINELKT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEOG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEOG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETRM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETRM2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETONE	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEUSG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEUSG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
ICTRM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
ICTRM2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww

Register	Present In Officetype
TRMLNAT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMLNAT2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMMCHFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMBLCK	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LNMBSYPC	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEABDN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww

5.3.5.4 Group structure

OFZ2NET1 OM group provides 1 tuple(s) for each bearer network datafilled in Table BEARNETS. The group structure is dependent upon the office type of the call server.

Key field: Bearer network ID

Info field: BEARNETS_INFO

- Bearer network ID (i.e., ‘NET 0’)
- Bearer network name (i.e., ‘TDM_ENET’)

5.3.5.5 Associated OM groups

OFZ OM group gives an overall office-wide traffic performance measurement.

5.3.5.6 Associated functional groups

The following functional groups are associated with OFZ2NET1 OM group:

- Succession North America
- Succession International

5.3.5.7 Associated functionality codes

None

5.3.5.8 OFZ2NET1 OM group registers logic flow chart

Figure 5 Termination to an outgoing trunk

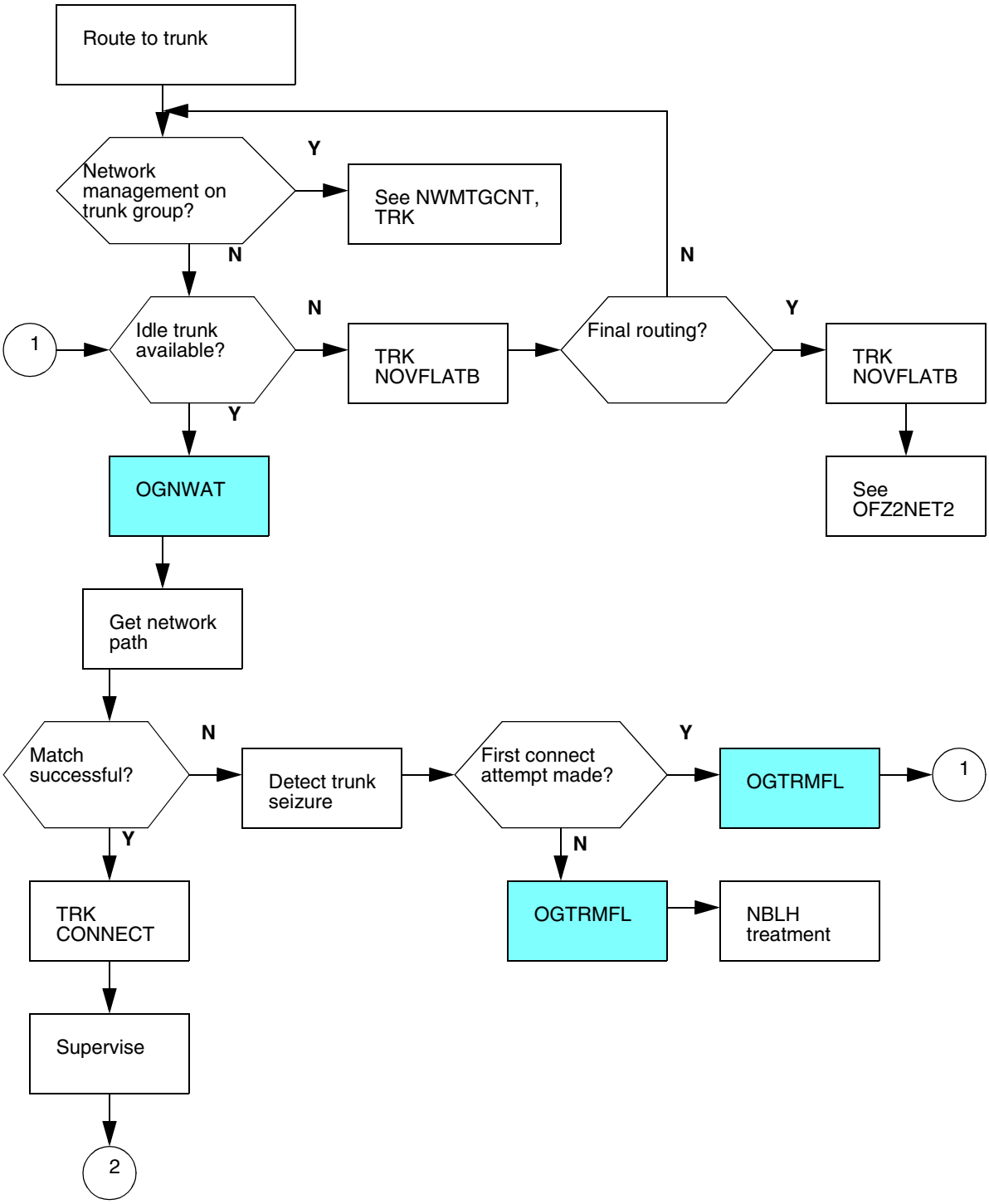


Figure 6 Termination to an outgoing trunk (continued)

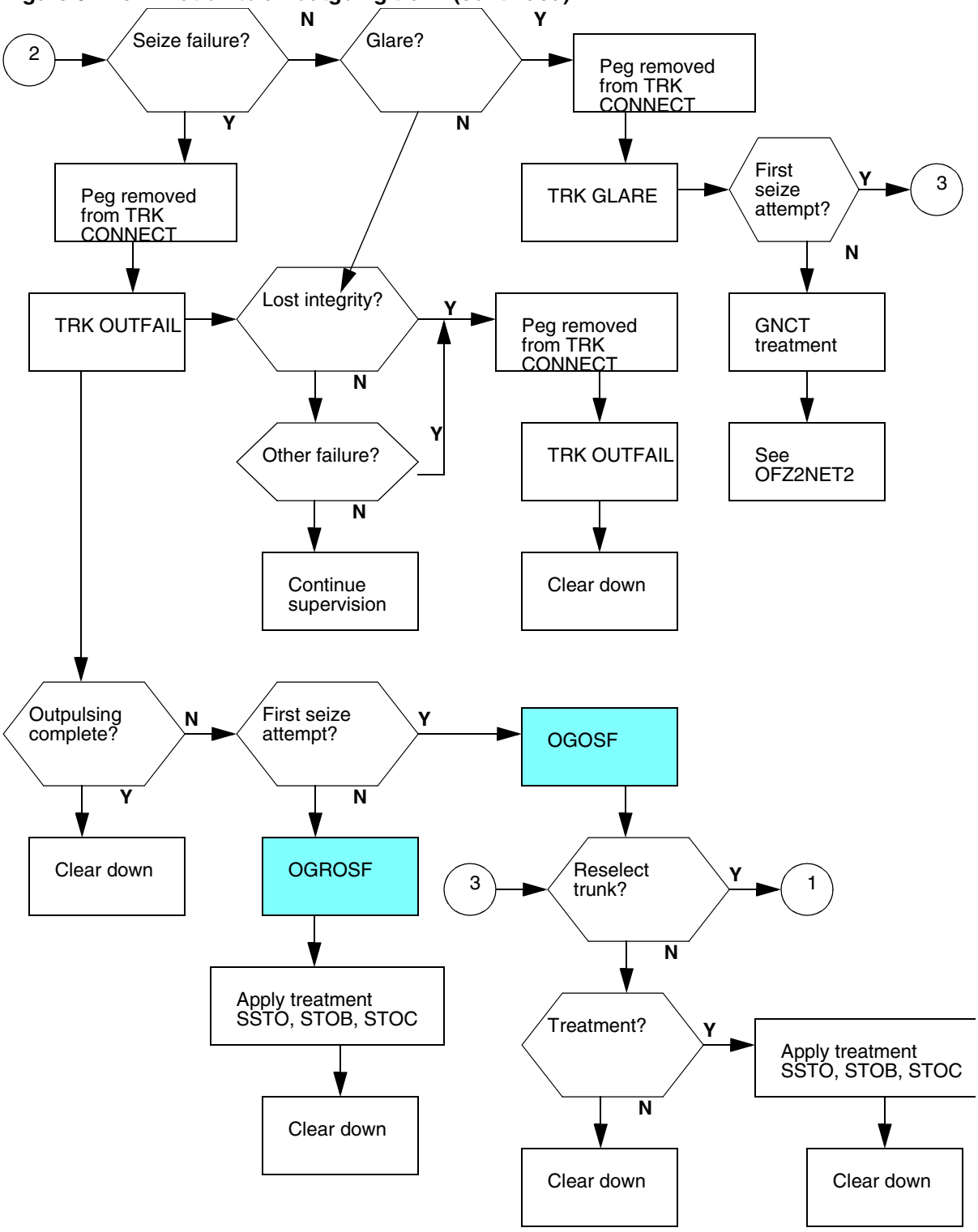


Figure 7 Termination to a line

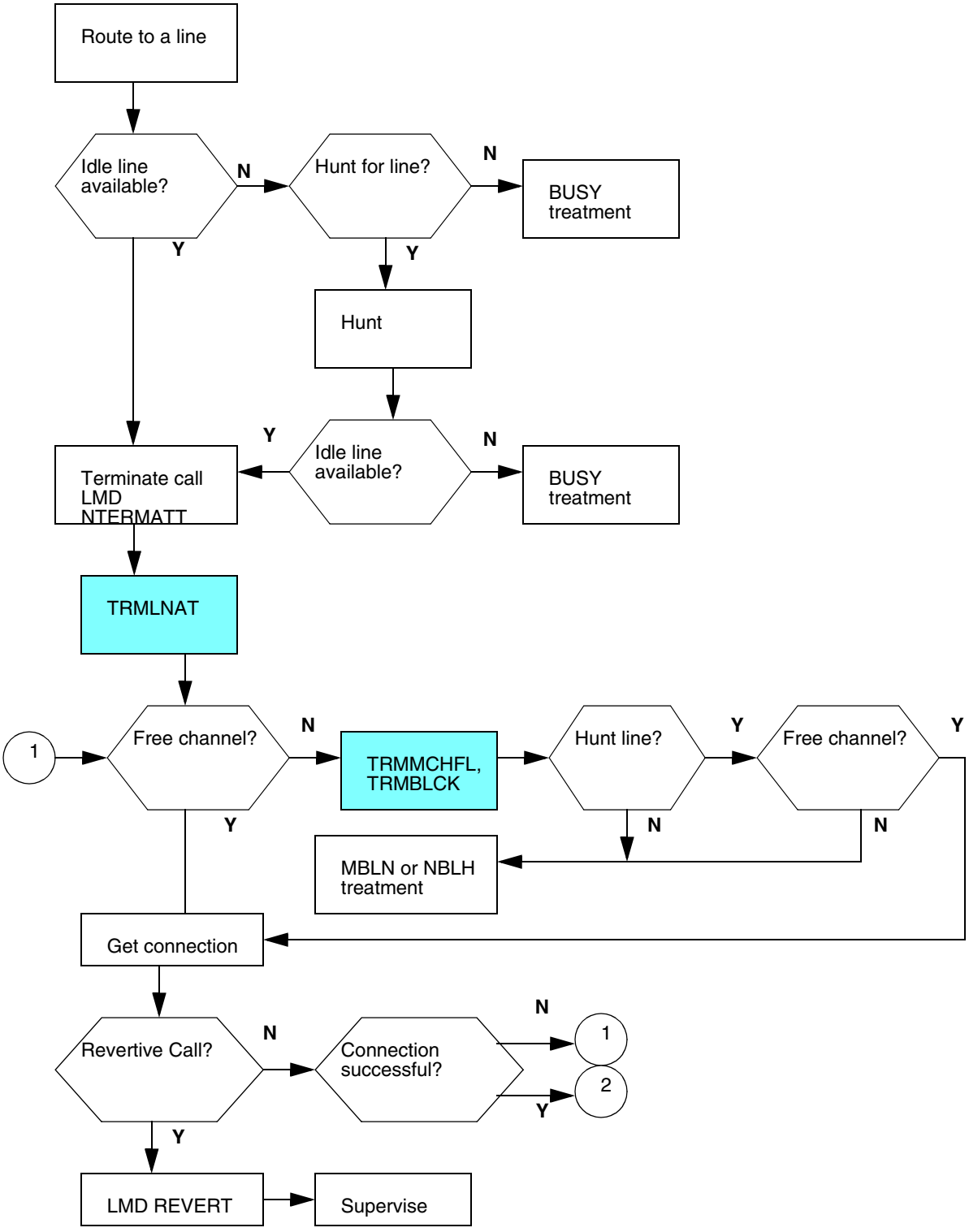


Figure 8 Termination to a line (continued)

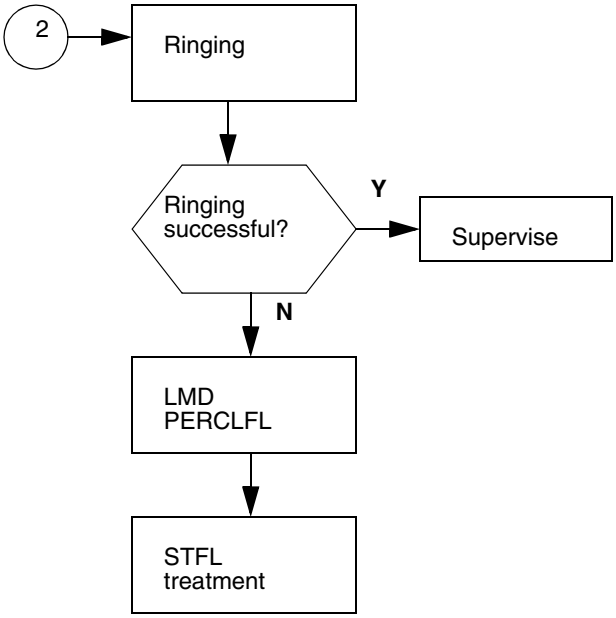


Figure 9 Origination from a trunk

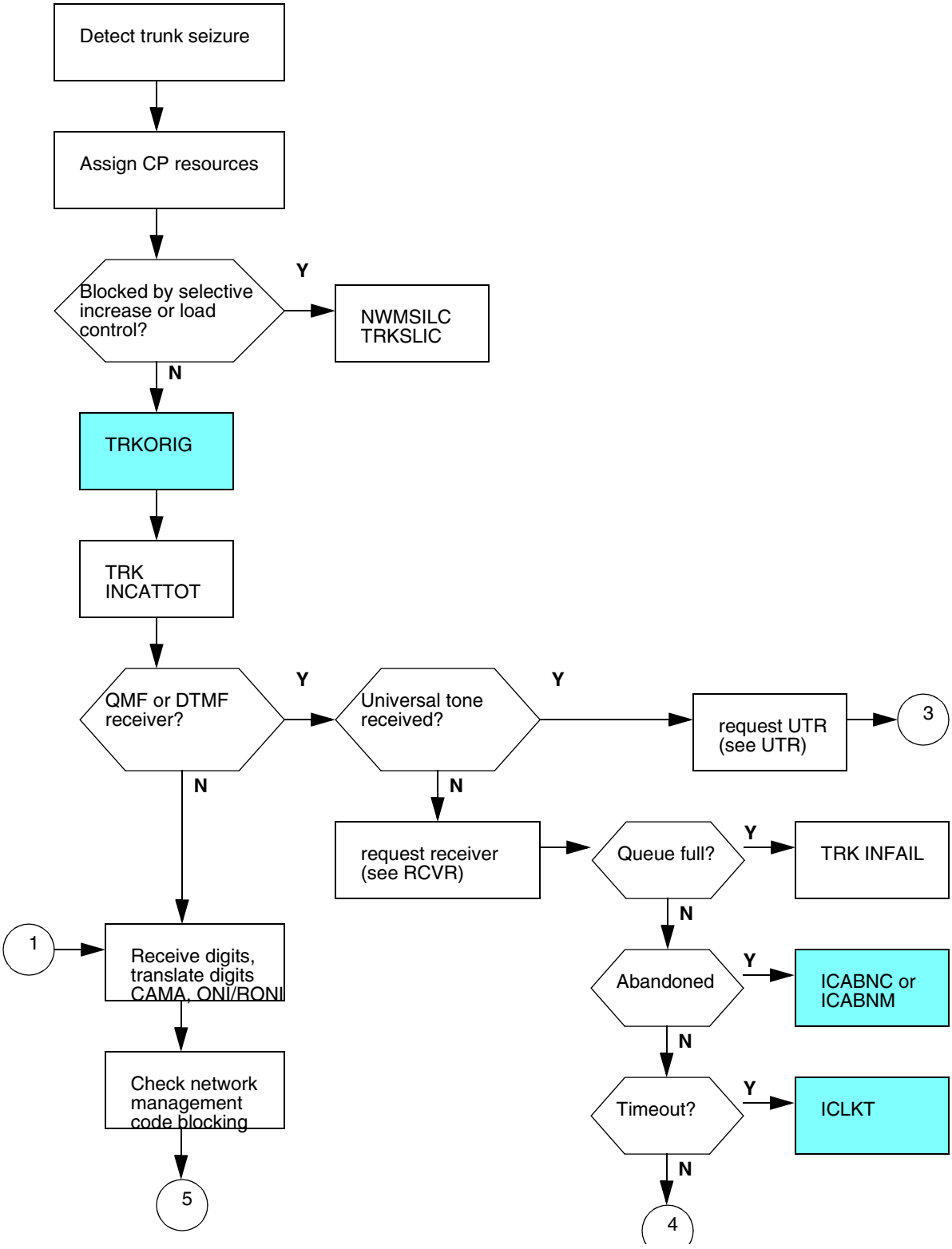


Figure 10 Origination from a trunk (continued)

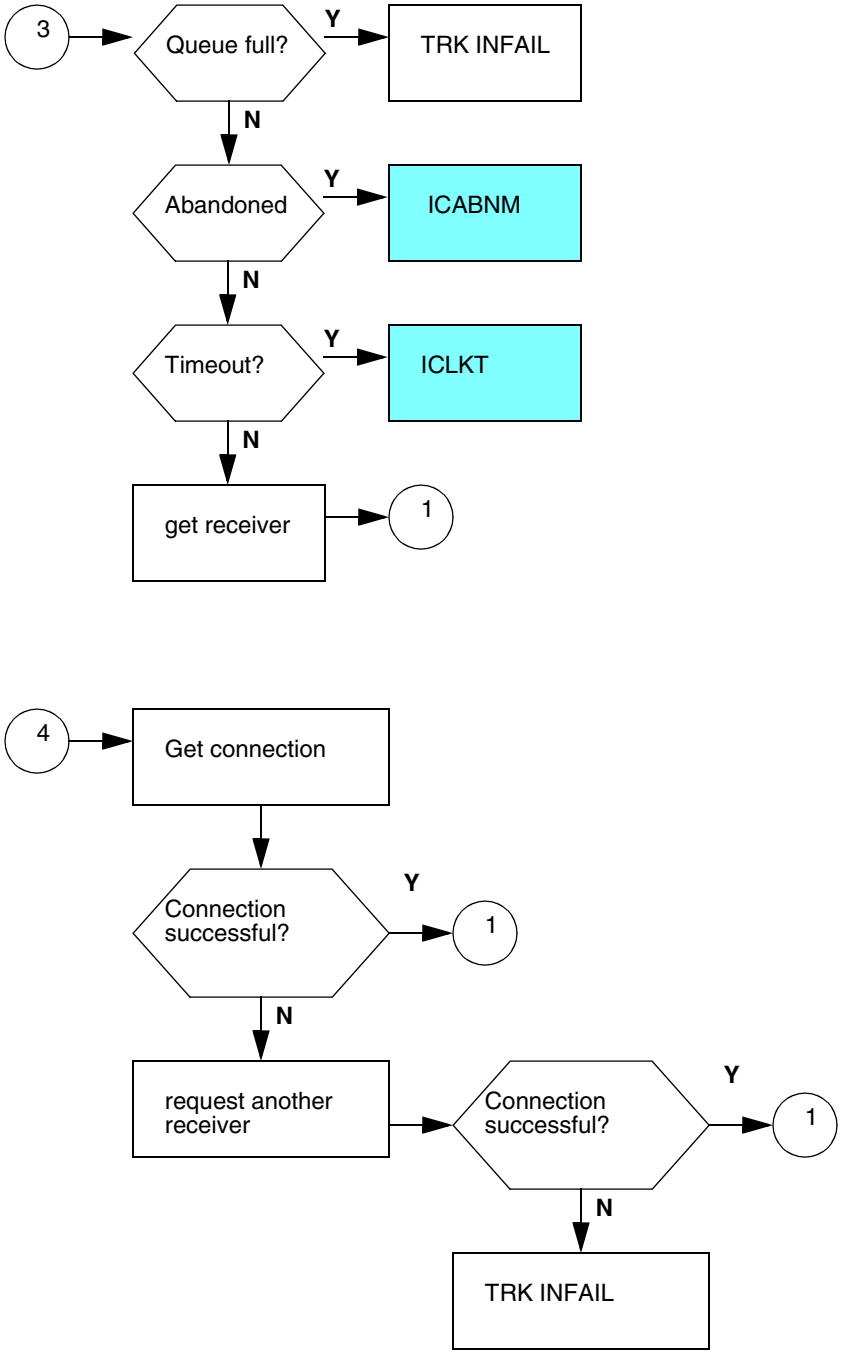


Figure 11 Origination from a trunk (continued)

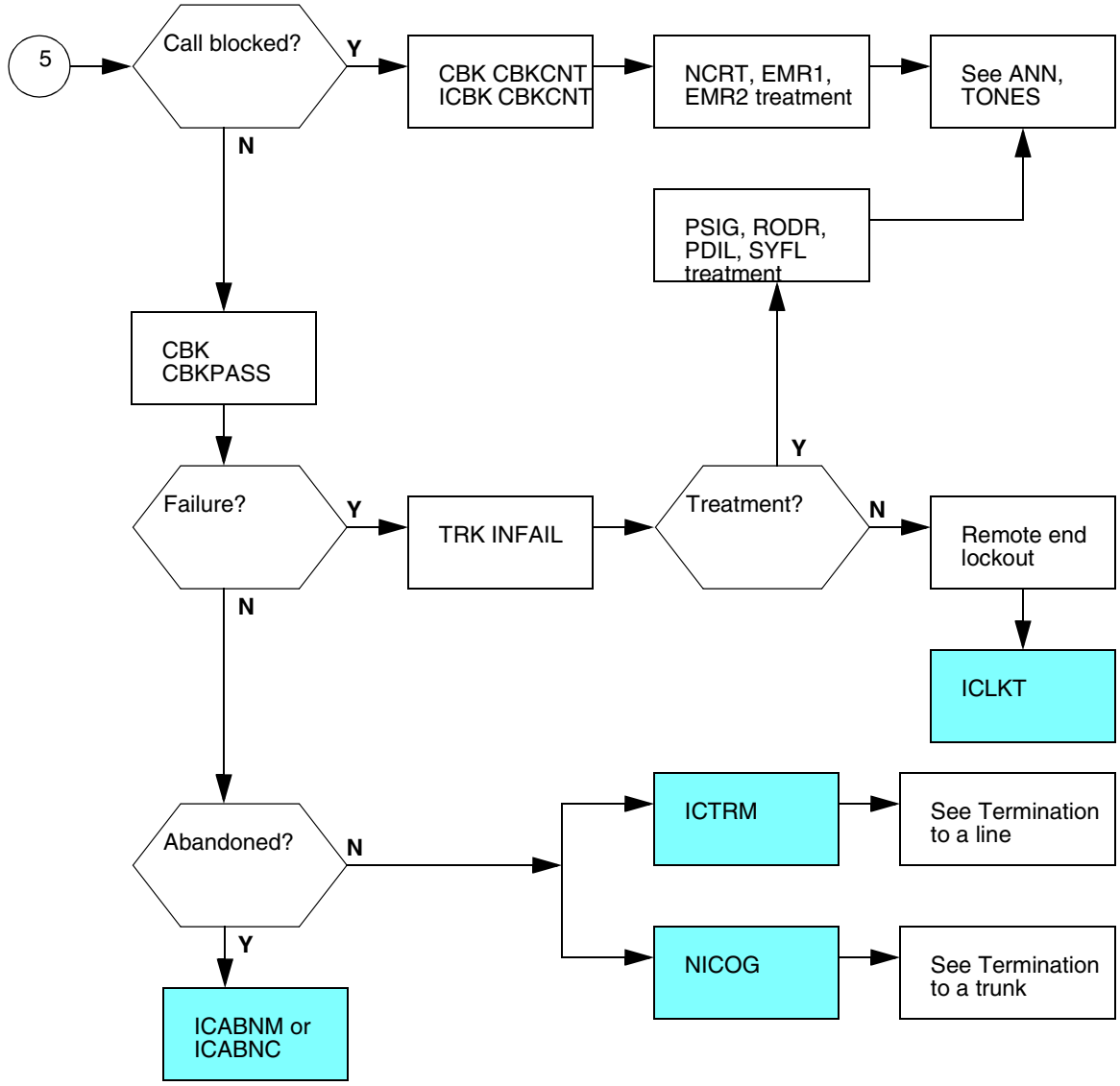


Figure 12 Origination from a line

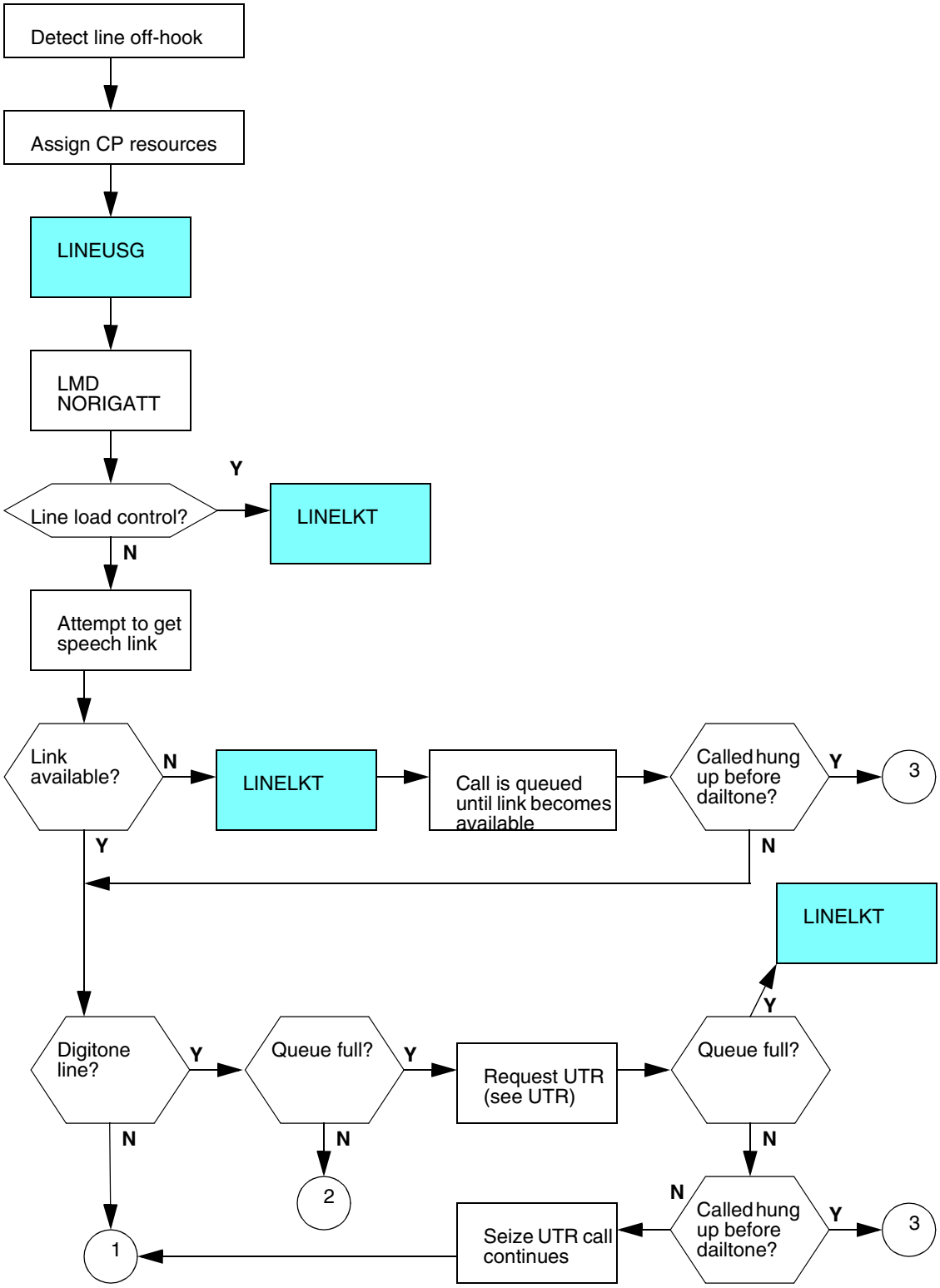


Figure 13 Origination from a line (continued)

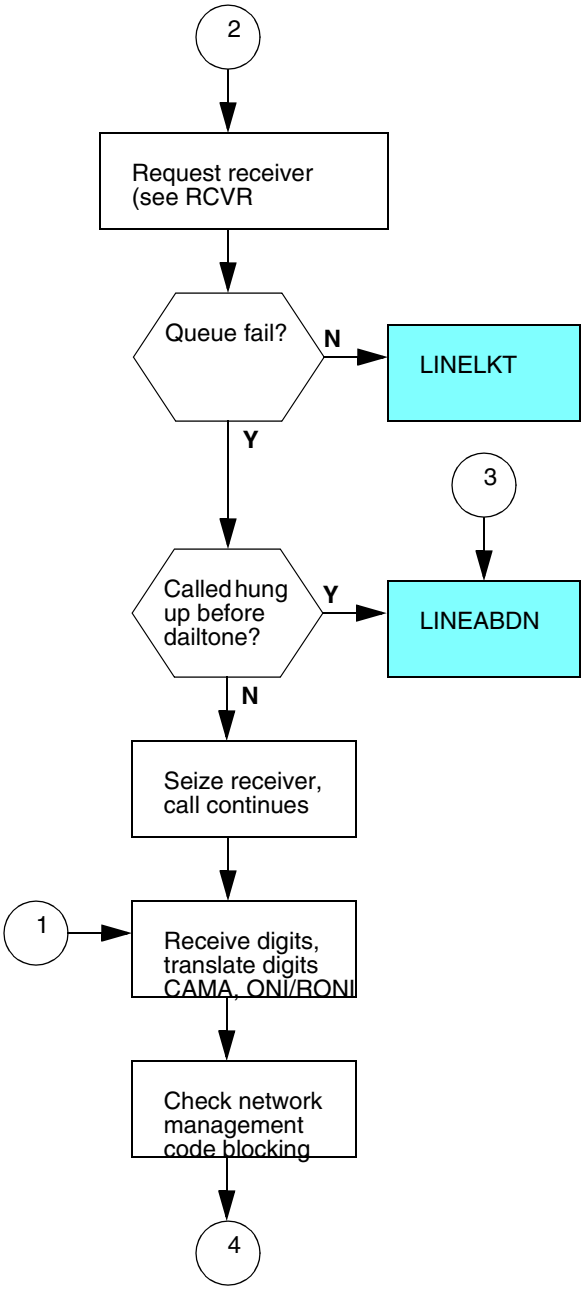
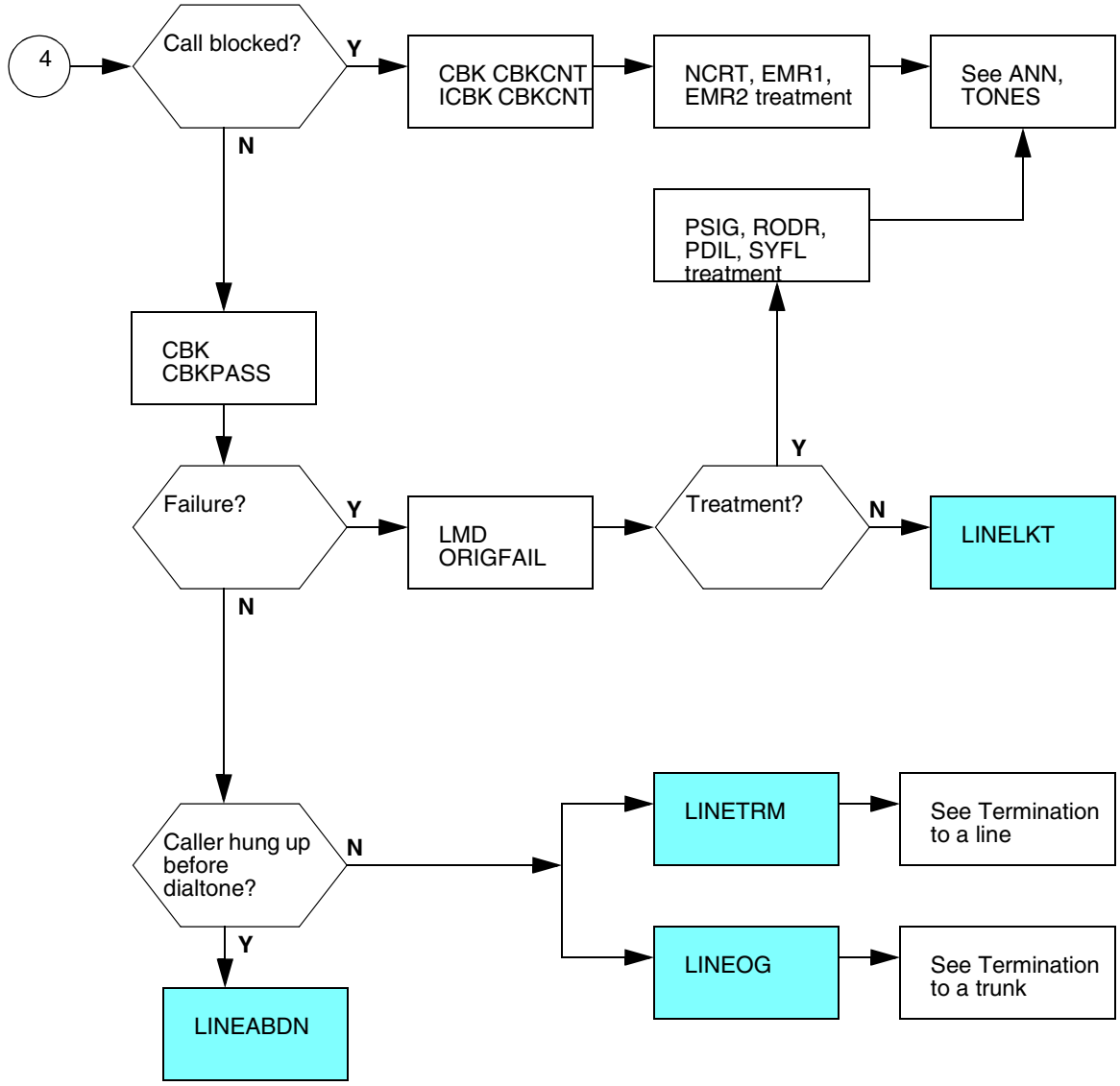


Figure 14 Origination from a line (continued)



5.3.5.9 Register ICABNC

5.3.5.9.1 Register description Incoming Calls Abandoned (ICABNC) counts incoming calls on the associated bearer network that the subscriber abandons before processing. These calls do not require treatment. This register would get pegged against the bearer network of the originator.

5.3.5.9.2 Register release history update Register is new in SN07.

5.3.5.9.3 Associated registers Register ICABNM counts incoming calls on the associated bearer network that the machine abandons.

5.3.5.9.4 Associated logs The system generates TRK114 when the system cannot determine the destination of an incoming call during DP reception.

The system generates TRK116 when the system cannot determine the destination of an incoming call during MF reception.

The system generates TRK162 is the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters trouble. These calls use DTMF signaling.

5.3.5.10 Register ICABNM

5.3.5.10.1 Register description Incoming Calls Abandoned (ICABNM) counts incoming calls on the associated bearer network that the machine abandons before processing. The machine abandons a call when a call times out at the upstream office while waiting for a receiver. The machine also abandons a call when there is an equipment problem. This register would get pegged against the bearer network of the originator.

5.3.5.10.2 Register release history update Register is new in SN07.

5.3.5.10.3 Associated registers Register ICABNC counts incoming calls on the associated bearer network that the subscriber abandons.

5.3.5.10.4 Associated logs The system generates TRK114 when the system cannot determine the destination of an incoming call during DP reception.

The system generates TRK116 when the system cannot determine the destination of an incoming call during MF reception.

The system generates TRK162 is the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters trouble. These calls use DTMF signaling.

5.3.5.11 Register ICANN

5.3.5.11.1 Register description Incoming Call to an Announcement (ICANN) register counts incoming calls on the associated bearer network that the system routes to an announcement.
The announcement is the result of a treatment applied during origination, or the intended result of the call. Register ICANN counts the call before it attempts to get a network connection. Register ICANN counts calls that the system routes to a treatment that routes the call to an announcement. The

register only counts these calls one time. This register would get pegged against the bearer network of the originator.

5.3.5.11.2 Register release history update Register is new in SN07.

5.3.5.11.3 Associated registers Register LINEANN counts originating calls that the system routes to an announcement.

5.3.5.11.4 Associated logs The system generates TRK138 when the system routes a call to a treatment after the call is call processing busy.

5.3.5.12 Register ICLKT

5.3.5.12.1 Register description Incoming Calls to Lockout (ICLKT) counts incoming calls that fail and that the system routes to lockout. The call fails for one of the following reasons:

- The incoming trunk loses its true identity
- The system cannot connect the call to a tone or announcement
- A forced release initiates manually
- A forced release initiates because call processing requests a delay (CP_WAITDENY count the call)

This register would get pegged against the bearer network of the originator.

5.3.5.12.2 Register release history update Register is new in SN07.

5.3.5.12.3 Associated registers None.

5.3.5.12.4 Associated logs The system generates TRK111 if the system encounters a problem or assigns a treatment during a trunk-to-trunk call.

The system generates TRK113 when the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK123 when the node hosting the trunk member sends the wrong message to the core. The system generates TRK123 several times when a problem is present in one of the following elements:

- the originating trunk
- the terminating trunk

5.3.5.13 Register NICOG

5.3.5.13.1 Register description Incoming to Outgoing (NICOG) counts incoming calls on the associated bearer network from the following agents:

- trunks

- preset conferences
- originating test lines

This register would get pegged against the bearer network of the originator.

5.3.5.13.2 Register release history update Register is new in SN07.

5.3.5.13.3 Associated registers NICOG2 register (extension register for NICOG).

5.3.5.13.4 Associated logs None.

5.3.5.14 Register ICTONE

5.3.5.14.1 Register description Incoming Call to Tone (ICTONE) counts oncoming calls on the associated bearer network that the system routes to a tone.
The tone is the result of a treatment applies during origination, or the tone is the intended result of the call. Register ICTONE counts the call before it attempts to find a network connection. Register ICTONE count a call that the system routes to a tone one time. This register would get pegged against the bearer network of the originator.

5.3.5.14.2 Register release history update Register is new in SN07.

5.3.5.14.3 Associated registers Register LINETONE counts originating calls on the associated bearer network that the system routes to a tone.

5.3.5.14.4 Associated logs The system generates TRK138 when the system routes a call to a treatment after the call is call processing busy.

5.3.5.15 Register ICTRM

5.3.5.15.1 Register description Incoming to Terminating (ICTRM) counts incoming calls on the associated bearer network that the system routes to a line. This register would get pegged against the bearer network of the originator.

5.3.5.15.2 Register release history update Register is new in SN07.

5.3.5.15.3 Associated registers Register ICTRM2 (extension register for ICTRM).

5.3.5.15.4 Associated logs None.

5.3.5.16 Register LNMBSYPC

5.3.5.16.1 Register description Line Manual Busy Peg Count (LNMBSYPC) counts lines on the associated bearer network that are manual busy.
Every POTS line is pegged by one when transitioning to a manual busy state. Pegging of each PPhone.PSET/DATA/ISDN line depends upon number of virtual identifiers (VIDs) associated with that line, and may be more than once, when made manual busy either by LTP/BSY or maintenance action. This register would get pegged against the bearer network of the originator.

5.3.5.16.2 Register release history update Register is new in SN07.

5.3.5.16.3 Associated registers None.

5.3.5.16.4 Associated logs None.

5.3.5.17 Register TRKORIG

5.3.5.17.1 Register description Number of Incoming Calls (TRKORIG) counts incoming calls on the associated bearer network that the core recognizes. The intended destination of the call is a line, trunk, announcement or tone. Register TRKORIG counts calls after a call control block and a call process are obtained. The register may count the calls before all incoming digits are received. This register would get pegged against the bearer network of the originator.

5.3.5.17.2 Register release history update Register is new in SN07.

5.3.5.17.3 Associated registers Register TRKORIG counts each incoming call. A peg in this register should have a corresponding peg in one of the following registers as the destination is determined:

- Register ICABNC (counts the call if the subscriber abandons the call)
- Register ICABNM (counts the call if the core abandons the call
- Register ICANN (counts the call if the destination is an announcement)
- Register ICLKT (counts the call if the call locks out)
- Register NICOG (counts the call if the destination is a trunk)
- Register ICTRM (counts the call if the destination is a line)
- Register ICTONE (counts the call if the destination is a tone)

Register TRKORIG2 (extension register for TRKORIG).

5.3.5.17.4 Associated logs None.

5.3.5.18 Register LINEUSG

5.3.5.18.1 Register description Number of Originating Calls (LINEUSG) counts originating call on the associated bearer network that the core recognizes.
After a call condense block and a call process are obtained, LINEUSG counts a call. Register LINEUSG counts the call before dialing is set up. LINEUSG can count a single call at least once. The call is only a single call from the point of view of the caller. The system counts a three-way call when the flashing switch hook recognizes a correct feature origination signal. The feature origination signal is for the flashing line.

5.3.5.18.2 Register release history update Register is new in SN07.

5.3.5.18.3 Associated registers Register LINEUSG counts each originating call. A peg in this register should have a corresponding peg in one of the following registers as the destination is determined:

- Register LINEABDN (counts the call if the call abandons)
- Register LINEANN (counts the call if the destination is an announcement)
- Register LINELKT (counts the call if the call locks out)
- Register LINEOG (counts the call if the destination is a trunk)
- Register LINETRM (counts the call if the destination is a line)
- Register LINETONE (counts the call if the destination is a tone)

Register LINEUSG2 (extension register for LINEUSG).

5.3.5.18.4 Associated logs None.

5.3.5.19 Register LINEABDN

5.3.5.19.1 Register description Originating Calls Abandoned (LINEABDN) counts originating calls on the associated bearer network that the system abandons before the system routes the calls to a trunk, line or treatment.

5.3.5.19.2 Register release history update Register is new in SN07.

5.3.5.19.3 Associated registers None.

5.3.5.19.4 Associated logs The system generates LINE106 if the system cannot determine a call destination during dial pulse reception on a line.

The system generates LINE108 if the digitone reception on a lines encounters a problem.

5.3.5.20 Register LINEANN

5.3.5.20.1 Register description Originating Calls to Announcement (LINEANN) counts originating calls on the associated bearer network that the system routes to an announcement.
The announcement can be the result of a treatment during origination, or the intended result of the call. The system counts the call in LINEANN before an attempt to find a network connection occurs.

5.3.5.20.2 Register release history update Register is new in SN07.

5.3.5.20.3 Associated registers The system counts ICANN incoming calls that the system routes to an announcement.

5.3.5.20.4 Associated logs The system generates LINE138 if the system routes a call to a treatment after it is call processing busy.

5.3.5.21 Register LINELKT

5.3.5.21.1 Register description Originating Calls to Lockout (LINELKT) counts originating calls on the associated bearer network that fail on the intended destination that the system routes to lock out. The register counts these calls when the calls do not connect. Register LINELKT also counts the calls when the system does not routes the call to a treatment. The call fails for one of the following reasons:

- line load control (line is dead)
- a speech link is not available (call is queued until a speech link becomes available and is the caller remains off-hook that call can be successful, but LINELKT only pegs one time)
- A digitone receiver, or one of a network connection to a digitone receiver is not available (if caller remains off-hook, the call clears when the problem is successful, but LINELKT only pegs one time)

5.3.5.21.2 Register release history update Register is new in SN07.

5.3.5.21.3 Associated registers None.

5.3.5.21.4 Associated logs The system generates LINE104, LINE105, LINE109, or LINE204 is call processing encounters a problem.

The system generates NET130 if the system cannot find a network path.

The system generates OM2200 if a threshold condition exceeds the limit.

5.3.5.22 Register LINEOG

5.3.5.22.1 Register description Originating Calls to Outgoing (LINEOG) counts originating calls on the associated bearer network that the system routes to a trunk or a test facility.

5.3.5.22.2 Register release history update Register is new in SN07.

5.3.5.22.3 Associated registers Register LINEOG2 (extension register for LINEOG).

5.3.5.22.4 Associated logs None.

5.3.5.23 Register LINETONE

5.3.5.23.1 Register description Originating Calls to Tone (LINETONE) counts originating calls on the associated bearer network that the system routes to a tone.
Register LINETONE counts the call before it attempts to find a network connection. The tone is either the result of a treatment, or the intended result of the call. Register LINETONE counts calls that the system routes to a treatment that routes the call to a tone. Register LINETONE only counts the call one time.

5.3.5.23.2 Register release history update Register is new in SN07.

5.3.5.23.3 Associated registers Register ICTONE counts incoming calls that the system routes to a tone.

5.3.5.23.4 Associated logs The system generates LINE138 is the system routes a call to a treatment after it is call processing busy.

5.3.5.24 Register LINETRM

5.3.5.24.1 Register description Originating Calls to Terminating (LINETRM) counts originating calls on the associated bearer network that the system routes to a line. Register LINETRM counts the call if a line is available or is not available.

5.3.5.24.2 Register release history update Register is new in SN07.

5.3.5.24.3 Associated registers Register LINETRM2 (extension register for LINETRM).

5.3.5.24.4 Associated logs None.

5.3.5.25 Register OGMFL

5.3.5.25.1 Register description Outgoing Match Failures (OGMFL) counts calls on the associated bearer network that fail to find a network path to a selected outgoing or test trunk on the first attempt. A second attempt occurs to find an idle trunk and a network path.

5.3.5.25.2 Register release history update Register is new in SN07.

5.3.5.25.3 Associated registers None.

5.3.5.25.4 Associated logs The system generates NET130 if the system cannot find a network path.

5.3.5.26 Register OGNWAT

5.3.5.26.1 Register description Outgoing Network Attempts (OGNWAT) counts incoming and outgoing calls on the associated bearer network that are intended for an exact outgoing or test trunk.
A single call can use two or more network paths to different ports for the service circuit. For example, connection by a conference circuit requires more that one network path.

5.3.5.26.2 Register release history update Register is new in SN07.

5.3.5.26.3 Associated registers Register OGNWAT2 (extension register for OGNWAT).

5.3.5.26.4 Associated logs None.

5.3.5.27 Register OGOSF

5.3.5.27.1 Register description Outgoing Original Seize Failures (OGOSF) counts calls on the associated bearer network that fail to seize an outgoing trunk on the first attempt after network paths are acquired. A second attempt occurs to find an idle trunk and a network path, and to seize the trunk. One of the following conditions causes a failure:

- a reversed trunk
- failure to receive a known start-dial
- not planned stop-dial
- time-out before expected stop-dial
- CCS7 errors

5.3.5.27.2 Register release history update Register is new in SN07.

5.3.5.27.3 Associated registers None.

5.3.5.27.4 Associated logs The system generates TRK113 is the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK121 is the system does not receive an acknowledgement wink from the far-end equipment. The wink indicates that it is ready to receive digits. The digits are received during outpulsing on an outgoing trunk.

The system generates TRK162 if the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters a problem. The line-to-trunk calls use DTMF signaling.

The system generates C7UP111 when an outgoing ISUP call attempt fails.

5.3.5.28 Register OGTRMFL

5.3.5.28.1 Register description Outgoing Retrial Match Failures (OGTRMFL) counts calls on the associated bearer network that fail on the seconds attempt to find a network path to a selected outgoing or test trunk.

5.3.5.28.2 Register release history update Register is new in SN07.

5.3.5.28.3 Associated registers Register OGMFL counts the first trial match failures.

5.3.5.28.4 Associated logs The system generates NET130 if the system cannot find a network path.

5.3.5.29 Register OGROSF

5.3.5.29.1 Register description Outgoing Retrial Seize Failures (OGROSF) counts calls on the associated bearer network that fail on the second attempt to seize an outgoing trunk. This attempt occurs after the network paths have been acquired. One of the following conditions causes a failure:

- a reversed trunk
- failure to receive a known start-dial
- not planned stop-dial
- time-out before expected stop-dial
- CCS7 errors

The system disconnects the call after the second failure and the call received start signal time-out (SSTO) treatment. An equal access call received signal timely BOC (STOB) or signal time-out IC.INC (STOC) treatment.
The system pegs OGROSF when a second attempt occurs to ruin a continuity test (COT) for an outgoing ISUP trunk. The second attempt occurs if the first COT attempt fails.

5.3.5.29.2 Register release history update Register is new in SN07.

5.3.5.29.3 Associated registers Register OGOSF counts the first seize failures.

5.3.5.29.4 Associated logs The system generates TRK113 is the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK121 is the system does not receive an acknowledgement wink from the far-end equipment. The wink indicates that it is ready to receive digits. The digits are received during outpulsing on an outgoing trunk.

The system generates TRK162 if the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters a problem. The line-to-trunk calls use DTMF signaling.

The system generates C7UP111 when an outgoing ISUP call attempt fails.

5.3.5.30 Register TRMBLCK

5.3.5.30.1 Register description Terminating Blocks (TRMBLCK) counts attempts to obtain a voice path to a terminating lines on the associated bearer network that fail. This failure occurs when no free channel is present between the host network and the terminating line.

The system counts more that one failed attempt if part of a hunt group directs the call.

The system also counts each attempt in OFZ2NET1 registers TRMMCHFL and TRMLNAT.
If no alternate line is available, the system routes the call to network blockage normal traffic (NBLN) treatment. This register would get pegged against the bearer network of the originator.

5.3.5.30.2 Register release history update Register is new in SN07.

5.3.5.30.3 Associated registers None.

5.3.5.30.4 Associated logs The system generates NET130 if the system cannot find a network path.

The system generates LINE138 or TRK138 when the system routes a call to a treatment after the call is call processing busy.

5.3.5.31 Register TRMMCHFL

5.3.5.31.1 Register description Terminating Match Failures (TRMMCHFL) counts calls on the associated bearer network that fail to find a network path to terminating line.

The system counts more that one failed attempt if the call goes to a part of a hunt group.

Failure in the path search sequence can occur is the host switch network cannot obtain a path. It the network cannot find an alternate path, the system routes the call to a network blockage heavy traffic (NBLH) treatment.

Failure in the path search sequence can occur in the final cause of failure is failure to obtain a free channel on a link between the host switch network and the terminating line. Registers TRKBLK and TERMBLK count the failure to obtain a free channel.
If no alternate line is available, the system routes the call to network blockage normal traffic (MBLN) treatment.

5.3.5.31.2 Register release history update Register is new in SN07.

5.3.5.31.3 Associated registers None.

5.3.5.31.4 Associated logs The system generates NET130 if the system cannot find a network path.

The system generates LINE138 or TRK138 when the system routes a call to a treatment after the call is call processing busy.

5.3.5.32 Register TRMLNAT

5.3.5.32.1 Register description Terminating Network Attempts (TRMLNAT) counts attempts to find a voice path on the associated bearer network to terminating line. The complete path includes the following elements:

- a segment through the network
- a channel on the link between the line module and the network
- a matching channel on the line shelf

Register TRMLNAT counts a call only for each attempt. The calls count each attempt, whether is succeeds or fails.

5.3.5.32.2 Register release history update Register is new in SN07.

5.3.5.32.3 Associated registers Register TRMLNAT2 (extension register for TRMLNAT).

5.3.5.32.4 Associated logs None.

5.3.6 OFZ2NET2 OM Group

5.3.6.1 OM description

OFZ2NET2 OM Group provides information for traffic analysis per bearer network. The OM group is modeled after group OFZ2. The OFZ2NET2 OM group counts calls that the system routes to generalized no circuit treatment (GNCT). The system routes a call to GNCT when a trunk group is the last route in the route list and all trunks are busy.

OFZ2NET2 registers with the prefix *NCKT* count the number of calls by the trunk or call types routed to GNCT for outgoing trunks or for the outgoing side of two-way trunks. Register names correspond to an entry in field No Circuit Class (NCCLS) which is datafilled for each trunk defined in table TRKGRP.

Office parameter OFFICETYPE in table OFCSTD controls the generation of the registers for OFZ2NET2. When the system reports an answer indicator to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

5.3.6.2 Release history update

OFZ2NET2 OM group is new in SN07.

The addition of this new OFZ2NET2 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to ‘Y’, then the new OFZ2NET2 OM group is displayed. If the parameter is set to ‘N’, then the OFZ2NET2 OM group is not displayed.

5.3.6.3 Registers

OFZ2NET2 OM group registers display on the MAP terminal as follows:

Figure 15 OFZ2NET2 OM Group Display

```
>omshow ofz2net2 active
OFZ2NET2

CLASS: ACTIVE
START:2003/09/23 09:05:00  TUE;  STOP:  2003/09/23  09:09:52  Tue;
SLOWSAMPLES:        3  ;   FASTSAMPLES:          29 ;

   INFO (BEARNETS_INFO)
            NCKTIT          NCKTTC          NCKTLT          NCKTBN
            NCKTID          NCKTOSC         NCKTOT          NCKTRT
            NCKTIM          NCKTON          NCKTOF          MDPSIG
            MDPD            DPTRC           DPTRC2

0
NET 0 TDM_ENET
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
1
NET 1 NET_AAL1
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
2
NET 2 NET_IP
            0               0               0               0
            0               0               0               0
            0               0               0               0
            0               0               0
```

5.3.6.4 Group structure

OFZ2NET2 OM group provides 1 tuple(s) for each bearer network datafilled in Table BEARNETS

Key field: None

Even if the key field is none, the Key is bearer network.

Info field: BEARNETS_INFO

- Bearer network ID (i.e., ‘NET 0’)

- Bearer network name (i.e., ‘TDM_ENET’)

5.3.6.5 Associated OM groups

OFZ2 OM group gives an overall office-wide traffic performance measurement.

5.3.6.6 Associated functional groups

The following functional groups are associated with OFZ2NET2 OM group:

- Succession North America
- Succession International

5.3.6.7 Associated functionality codes

None

5.3.6.8 OFZ2NET2 OM group registers logic flow chart

5.3.6.9 Register NCKTBN

5.3.6.9.1 Register description No circuit business network trunks (NCKTBN) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because Meridian Digital Centrex (MDC) trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.9.2 Register release history update Register is new in SN07.

5.3.6.9.3 Associated registers None.

5.3.6.9.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.10 Register NCKTID

5.3.6.10.1 Register description No circuit inward dial trunks (NCKTID) counts calls on the associated bearer network that the system routes

to generalized no circuit treatment (GNCT). The system routes a call to GNCT when a direct inward dial or direct outward dial trunk is not available.

5.3.6.10.2 Register release history update Register is new in SN07.

5.3.6.10.3 Associated registers None.

5.3.6.10.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

This register would get pegged against the bearer network of the originator.

5.3.6.11 Register NCKTIM

5.3.6.11.1 Register description No circuit intermachine trunks (NCKTIM) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a circuit intermachine trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.11.2 Register release history update Register is new in SN07.

5.3.6.11.3 Associated registers None.

5.3.6.11.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.12 Register NCKTIT

5.3.6.12.1 Register description No circuit intertoll trunks (NCKTIT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because an intertoll trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.12.2 Register release history update Register is new in SN07.

5.3.6.12.3 Associated registers None.

5.3.6.12.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.13 Register NCKTLT

5.3.6.13.1 Register description No circuit local tandem trunks (NCKTLT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a local tandem trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.13.2 Register release history update Register is new in SN07.

5.3.6.13.3 Associated registers None.

5.3.6.13.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.14 Register NCKTOF

5.3.6.14.1 Register description No circuit offnet trunks (NCKTOF) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because an offnet or direct dial trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.14.2 Register release history update Register is new in SN07.

5.3.6.14.3 Associated registers None.

5.3.6.14.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.15 Register NCKTON

5.3.6.15.1 Register description No circuit connect trunks (NCKTON) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a dedicated access or mobile telephone exchange trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.15.2 Register release history update Register is new in SN07.

5.3.6.15.3 Associated registers None.

5.3.6.15.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.16 Register NCKTOT

5.3.6.16.1 Register description No circuit other trunk (NCKTOT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because one of the following types of trunk is not available:

- test line
- test desk
- maintenance trunks
- AV101

This register would get pegged against the bearer network of the originator.

5.3.6.16.2 Register release history update Register is new in SN07.

5.3.6.16.3 Associated registers None.

5.3.6.16.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.17 Register NCKTRT

5.3.6.17.1 Register description No circuit trunks (NCKTRT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because one of the following types of trunk is not available:

- 0+/0- tandem to TOPS
- outgoing to AMR2 or CAMA
- outgoing local

- recording completing outgoing
- TOPS outgoing

This register would get pegged against the bearer network of the originator.

5.3.6.17.2 Register release history update Register is new in SN07.

5.3.6.17.3 Associated registers None.

5.3.6.17.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.18 Register NCKTTC

5.3.6.18.1 Register description No circuit toll completing trunks (NCKTTC) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a toll completing trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.18.2 Register release history update Register is new in SN07.

5.3.6.18.3 Associated registers None.

5.3.6.18.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.19 Register NCKTOSC

5.3.6.19.1 Register description No service circuit trunks (NCKTOSC) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the call because automatic number announcement or automatic intercept trunk is not available.

This register would get pegged against the bearer network of the originator.

5.3.6.19.2 Register release history update Register is new in SN07.

5.3.6.19.3 Associated registers None.

5.3.6.19.4 Associated logs The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

5.3.6.20 Register MDPD

5.3.6.20.1 Register description Machine dialed partial dials (MDPD) counts machine-dialed calls on the associated bearer network that the system routes to partial dial treatment.

This register would get pegged against the bearer network of the originator.

5.3.6.20.2 Register release history update Register is new in SN07.

5.3.6.20.3 Associated registers None.

5.3.6.20.4 Associated logs The system generates TRK114 if the system cannot determine call destination during dial pulse (DP) reception for an incoming call.

The system generates TRK116 if the system cannot determine call destination during multi-frequency (MF) reception for an incoming call.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK182 when the system cannot determine call destination of an incoming call because the system had problems during Digitone reception.

5.3.6.21 Register MDPSIG

5.3.6.21.1 Register description Machine dialed permanent signal (MDPSIG) counts machine-dialed calls on the associated bearer network that the system routes to permanent signal treatment.

This register would get pegged against the bearer network of the originator.

5.3.6.21.2 Register release history update Register is new in SN07.

5.3.6.21.3 Associated registers None.

5.3.6.21.4 Associated logs The system generates TRK115 when the system cannot determine call destination. The system was not able to determine call destination because the system had problems during dial pulse (DP) reception for an incoming call.

The system generates TRK117 when the system cannot determine call destination. The system was not able to determine call destination because system had problems during multi-frequency (MF) reception for an incoming call.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK183 when a permanent signal problem occurs. The problem occurs because the system had problems during Digitone reception of an incoming call.

5.3.6.22 Register DPTRC

5.3.6.22.1 Register description DPT Reservation Control (DPTRC) counts the number of DPT terminal requests that are blocked due to DPT bandwidth resevation.

This register would get pegged against the bearer network of the originator.

5.3.6.22.2 Register release history update Register is new in SN07.

5.3.6.22.3 Associated registers Register DPTRC2 is an extension register for DPTRC.

5.3.6.22.4 Associated logs None.

5.3.7 TRK2NET1 OM Group

5.3.7.1 OM description

TRK2NET1 OM Group provides information for per trunk group traffic analysis per bearer network. The OM group is modeled after group TRK. The TRK2NET1 OM group provides information on trunk traffic for each trunk group. The registers in TRK2NET1 count the following:

- routing attempts
- seizure attempts
- seize failures
- total trunk use
- busy state use

OM groups TRK and TRNK2 provide traffic data summaries on a per-trunk group basis for all trunk groups in an office. TRK2NET1 and TRK2NET2 provide similar traffic data summaries with further refinement on a per-bearer network basis for each trunk group for all trunks groups in an office.

Office parameter OFFICETYPE in table OFCSTD controls the generation of the registers for TRK2NET1. When the system reports an answer indicator to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

5.3.7.2 Release history update

TRK2NET1 OM group is new in SN07.

The addition of this new TRK2NET1 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to ‘Y’, then the new TRK2NET1 OM group is displayed. If the parameter is set to ‘N’, then the TRK2NET1 OM group is not displayed.

5.3.7.3 Registers

TRK2NET1 OM group registers display on the MAP terminal as follows:

Figure 16 TRK2NET1 OM Group Display

```
>omshow trk2net1 active 'TRI1ITOGS7 NET 0'

TRK2NET1

CLASS: ACTIVE
START:2004/09/28 16:00:00 TUE; STOP: 2004/09/28 16:28:28 TUE;
SLOWSAMPLES:       18 ; FASTSAMPLES:       171 ;

     INFO (TRK2NET1_INFO)
       INCAATT   PRERTEA1    NINFAIL     NATMPT
       NVFLATB     GLARE1      OUTFL      TRFCU
        SBSYU      MBSYU   TRKNWBLK     CNCTAT
       TNDMATT   ANIOFCFL       NANF    TOTBSYU
       NANSWER   INVATHCD     MAXBSY    NACCCNG
       NOANSWR

   91
       TRI1ITOGS7 NET 0 ENET  379 OG     2     2
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0

>omshow trk2net1 active 'TRI1ITOGS7 NET 1'

TRK2NET1

CLASS: ACTIVE
START:2004/09/28 16:00:00 TUE; STOP: 2004/09/28 16:25:29 TUE;
SLOWSAMPLES:       16 ; FASTSAMPLES:       153 ;

     INFO (TRK2NET1_INFO)
       INCAATT   PRERTEA1    NINFAIL     NATMPT
       NVFLATB     GLARE1      OUTFL      TRFCU
        SBSYU      MBSYU   TRKNWBLK     CNCTAT
       TNDMATT   ANIOFCFL       NANF    TOTBSYU
       NANSWER   INVATHCD     MAXBSY    NACCCNG
       NOANSWR

   92
       TRI1ITOGS7 NET 1 AAL1  379 OG     2     2
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0
```

```
>omshow trk2net1 active 'TRI1ITOGS7 NET 2'

TRK2NET1

CLASS: ACTIVE
START:2004/09/28 16:00:00 TUE; STOP: 2004/09/28 16:26:40 TUE;
SLOWSAMPLES:       16 ; FASTSAMPLES:       160 ;

     INFO (TRK2NET1_INFO)
       INCAATT   PRERTEA1    NINFAIL     NATMPT
       NVFLATB     GLARE1      OUTFL      TRFCU
        SBSYU      MBSYU   TRKNWBLK     CNCTAT
       TNDMATT   ANIOFCFL       NANF    TOTBSYU
       NANSWER   INVATHCD     MAXBSY    NACCCNG
       NOANSWR

   90
       TRI1ITOGS7 NET 2 IP    379 OG     2     2
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
           0        0        0        0
```

5.3.7.4 Group structure

TRK2NET1 OM group provides 1 tuple(s) for each trunk group and each bearer network that the trunk group has members provisioned in.

Key field: None

Info field: OM2TRKINFO

- CLLI
- bearer network ID (i.e., ‘NET 0’)
- bearer network name (i.e., ‘TDM_ENET’)
- trunk group direction. (i.e., ‘IC—incoming trunk, OG—outgoing trunk, 2W—two-way trunk’)
- total number of trunk circuits in the group in the associated bearer network (i.e., ‘20’)
- number of trunk circuits in the associated bearer network available for service at the end of the reporting period. (i.e., ‘19’)

The office parameter OFFICETYPE in table OFCSTD specifies the type of office. The value of OFFICETYPE controls the generation of TRK2NET1 registers. Correct entries for OFFICETYPE appear below:

- OFF100 Local

- OFF1000ESD Australian local
- OFFCOMB Combined local/toll
- OFFCOMBLWW Combined local/toll with wireless
- OFFCOMBTOPS Combined local/toll with traffic operator position system (TOPS)
- OFF200 Toll
- OFF2000ESD Australian toll
- OFF200TOPS Toll with TOPS
- OFF200300 Combned gateway/toll
- OFF250 DMS-250
- OFF250IBN DMS-250/SL-100
- OFF300 Gateway
- OFF500 DMS-500

The office type parameters appear in table OFCSTD. When the system reports an answer indication to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

The validity of a TRK2NET1 register in an officetype is given in the following table

Table 6 TRK2NET1 OM Group Registers

Register	Present In Officetypes
INCAATT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
PRERTEA1	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
NINFAIL	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice

Register	Present In Officetypes
NATMPT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
NVFLATB	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
GLARE1	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
OUTFL	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
TRFCU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd,offcomb300,nooffice
SBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd,offcomb300,nooffice
MBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd,offcomb300,nooffice
TRKNWBLK	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd,offcomb300,nooffice
CNCTAT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp , off100oesd, off200oesd, offcomboesd,offcomb300,nooffice

Register	Present In Officetypes
TNDMATT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd,offcomb300,nooffice
ANIOFCFL	off100, off200, offcomb, offcombitops, off200tops, offcombtops , off200tops, offcombtops, off500, offcomblww, offcomb300, offtollavon,nooffice
NANF	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off200tops, offcombtops, off500, offcomblww, offcomb300, offtollavon,nooffice
TOTBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, offcomb300, offtollavon, off100oesd, off200oesd, offcomboesd, nooffice
NANSWER	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off300, offcomb300, off100oesd, off200oesd, offcomboesd, nooffice
NACCCNG	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, nooffice
NOANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, nooffice
NINANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffice
OUTANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffic
ANSUFIN	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffice
INVATHCD	off250, off250ibn, offmtx100i,off500, offcomblww, offcomb300
MAXBSY	off250, off250ibn, offmtx100i,off500, offcomblww, offcomb300

5.3.7.5 Associated OM groups

The OFZ provides information about calls based on the source of the call. This OM group also provides information about calls based on the intended destination of the call. This information is on an office-wide basis.

The OFZ2NET1 and OFZ2NET2 provide information about calls on a per bearer network based on the source of the call. This OM group also provides

information about calls based on the intended destination of the call. This information is on an office-wide basis per bearer network.

The OTS provides information about calls based on the source of the call. This OM group also provides information about calls based on the intended destination of the call. This information is on an office-wide basis.

5.3.7.6 Associated functional groups

The following functional groups are associated with TRK2NET1 OM group:

- Succession North America
- Succession International

5.3.7.7 Associated functionality codes

None

5.3.7.8 TRK2NET1 OM group registers logic flow chart

Figure 17 Termination to an outgoing trunk

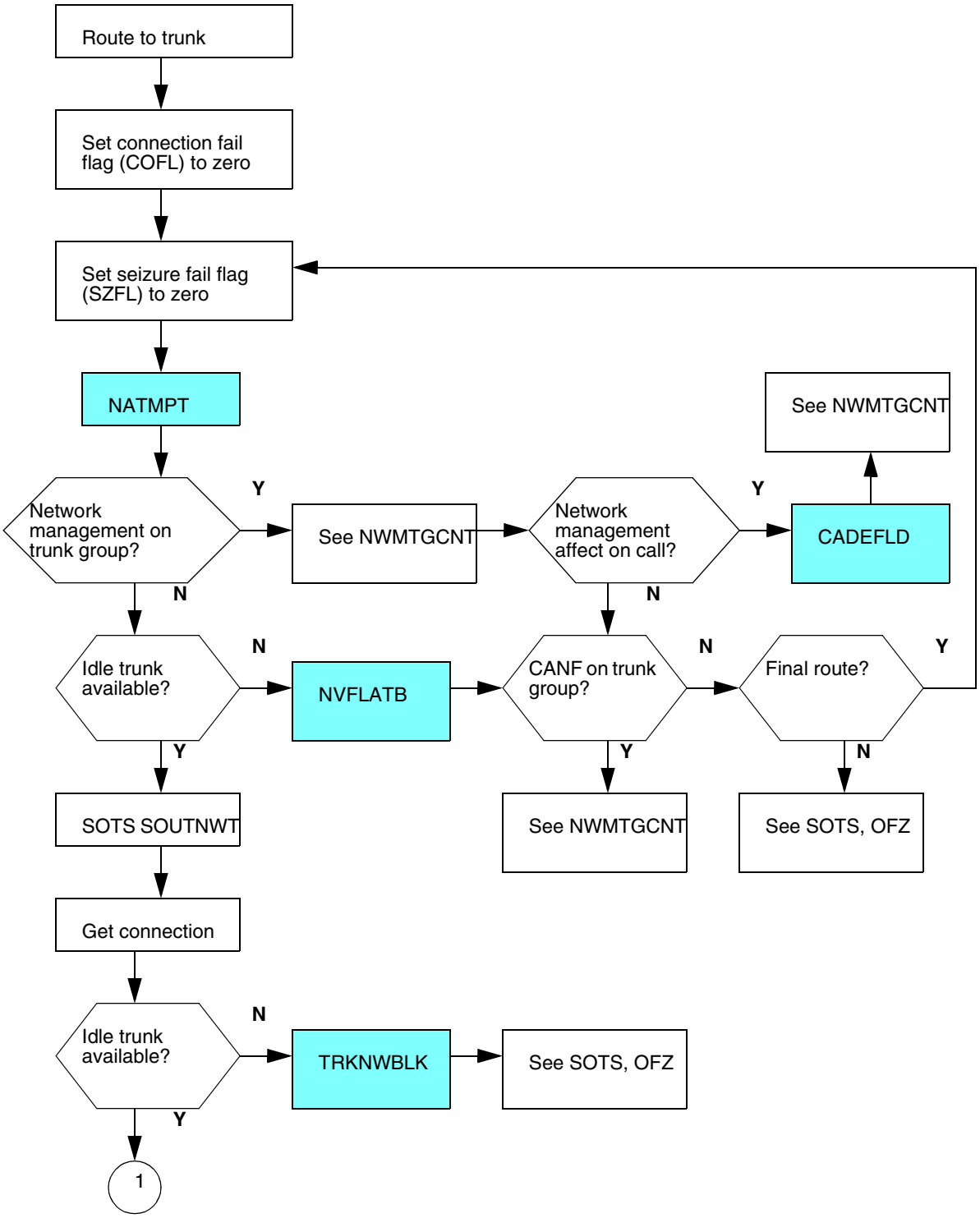


Figure 18 Termination to an outgoing trunk (continued)

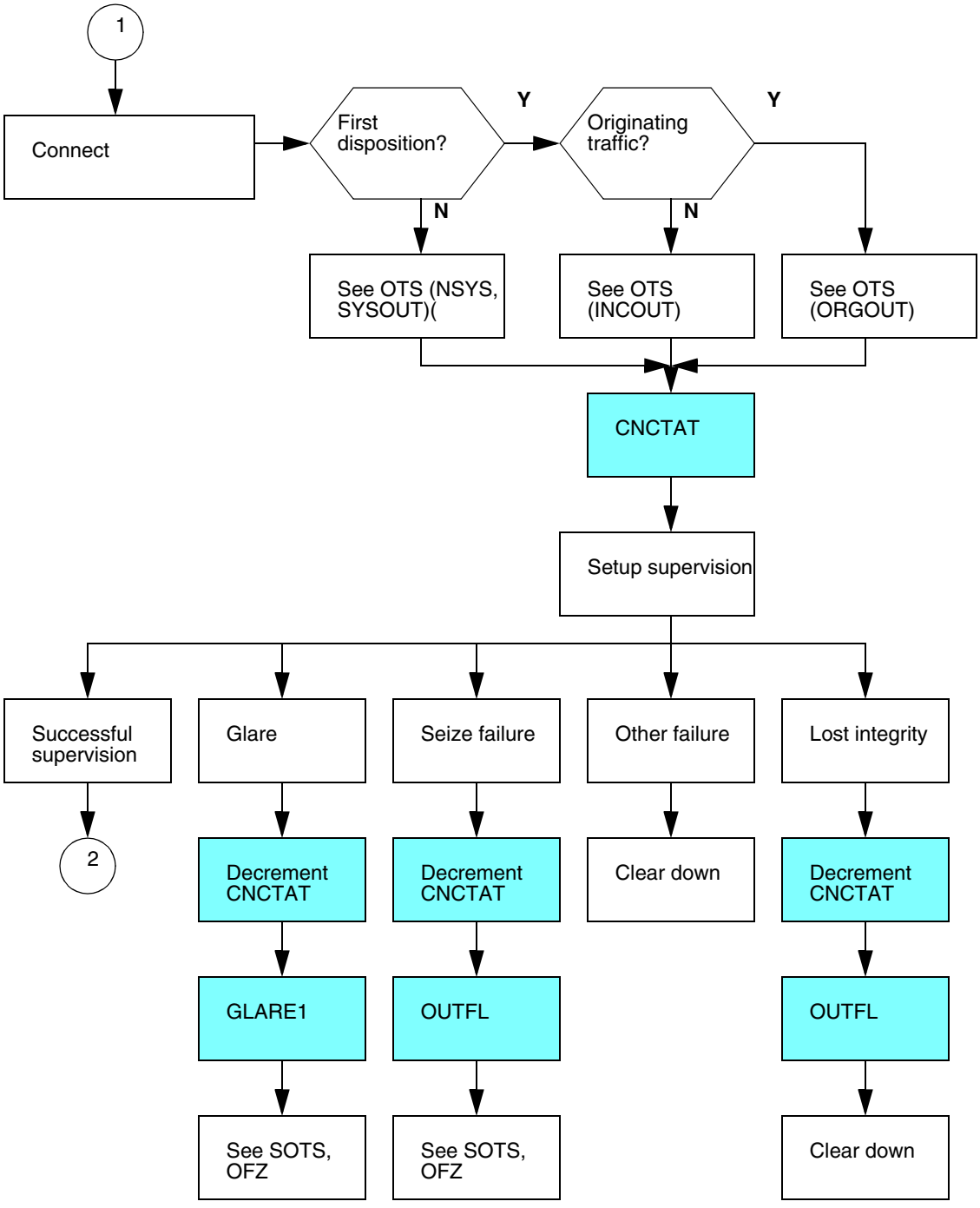


Figure 19 Termination to an outgoing trunk (continued)

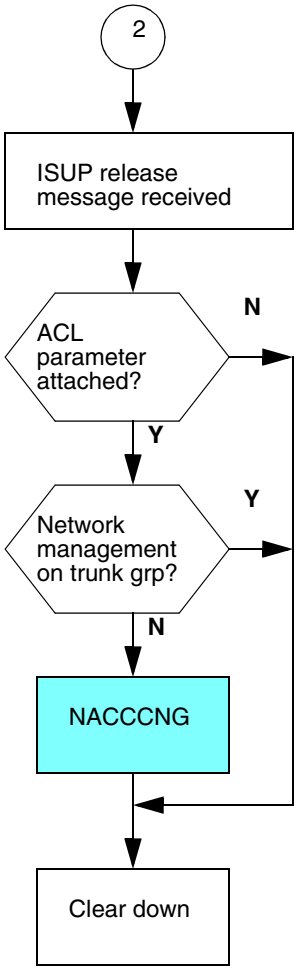


Figure 20 Trunk group busy usage registers

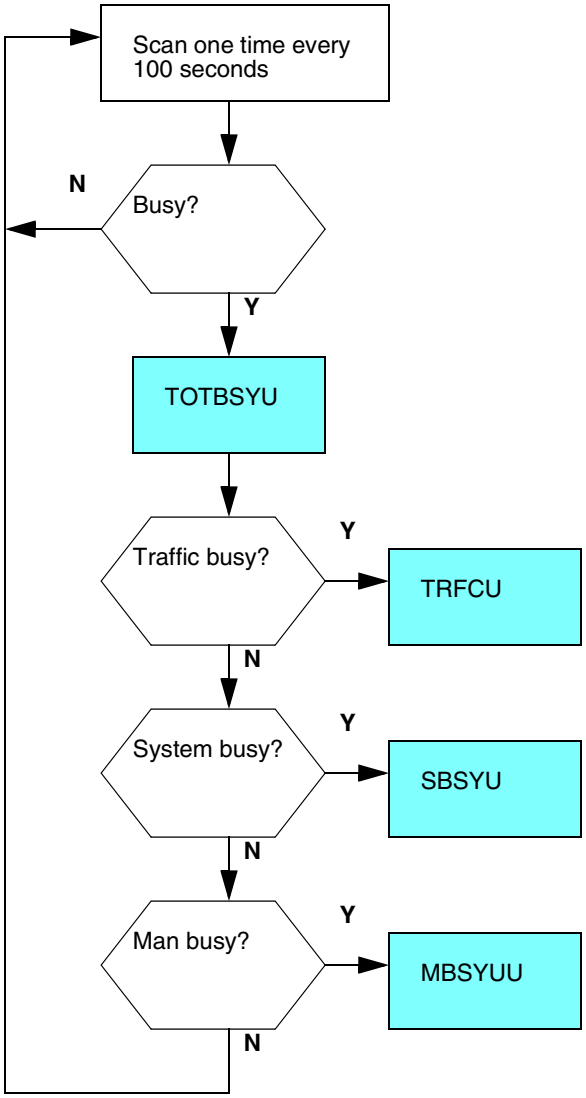


Figure 21 Origination from a trunk

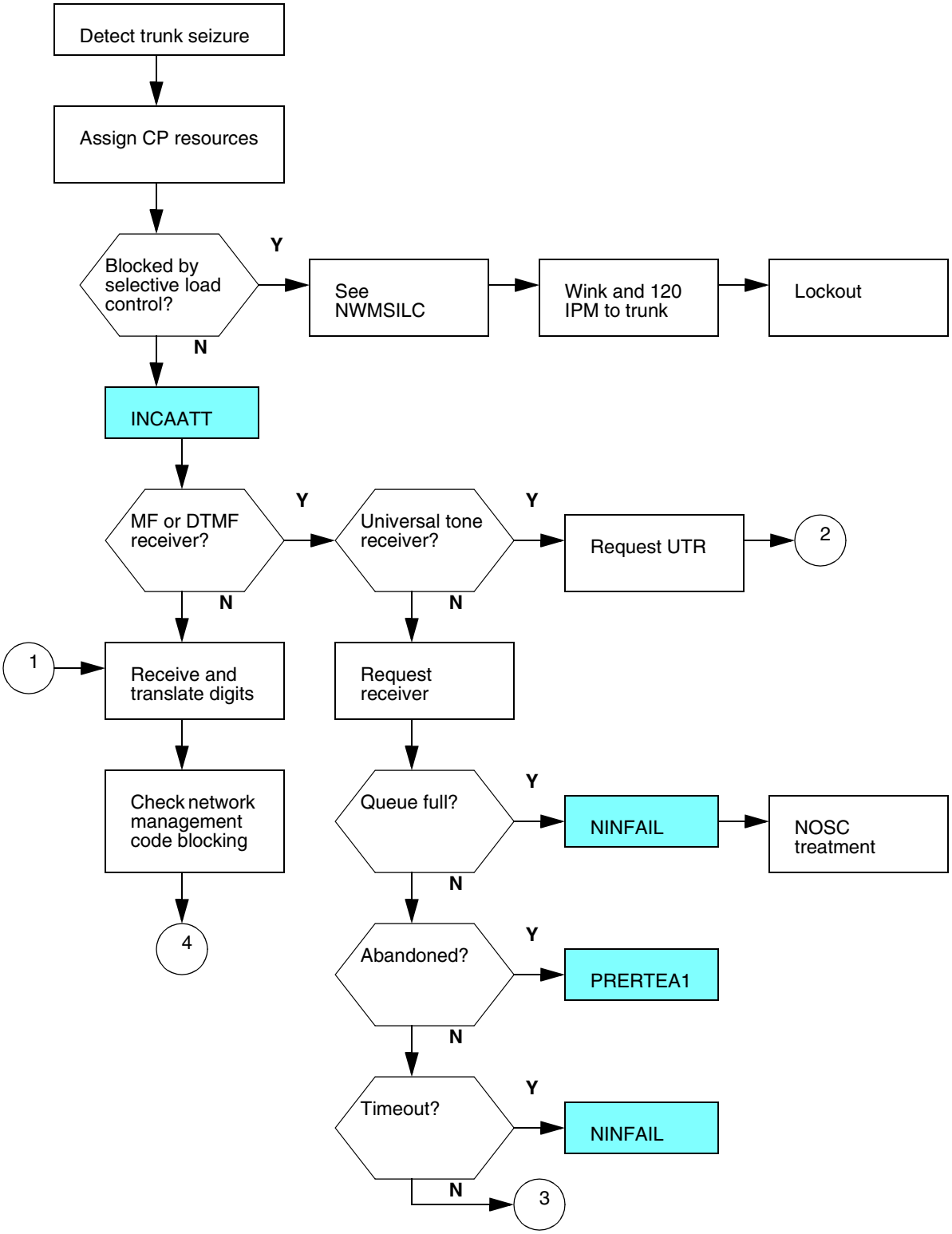


Figure 22 Origination from a trunk (continued)

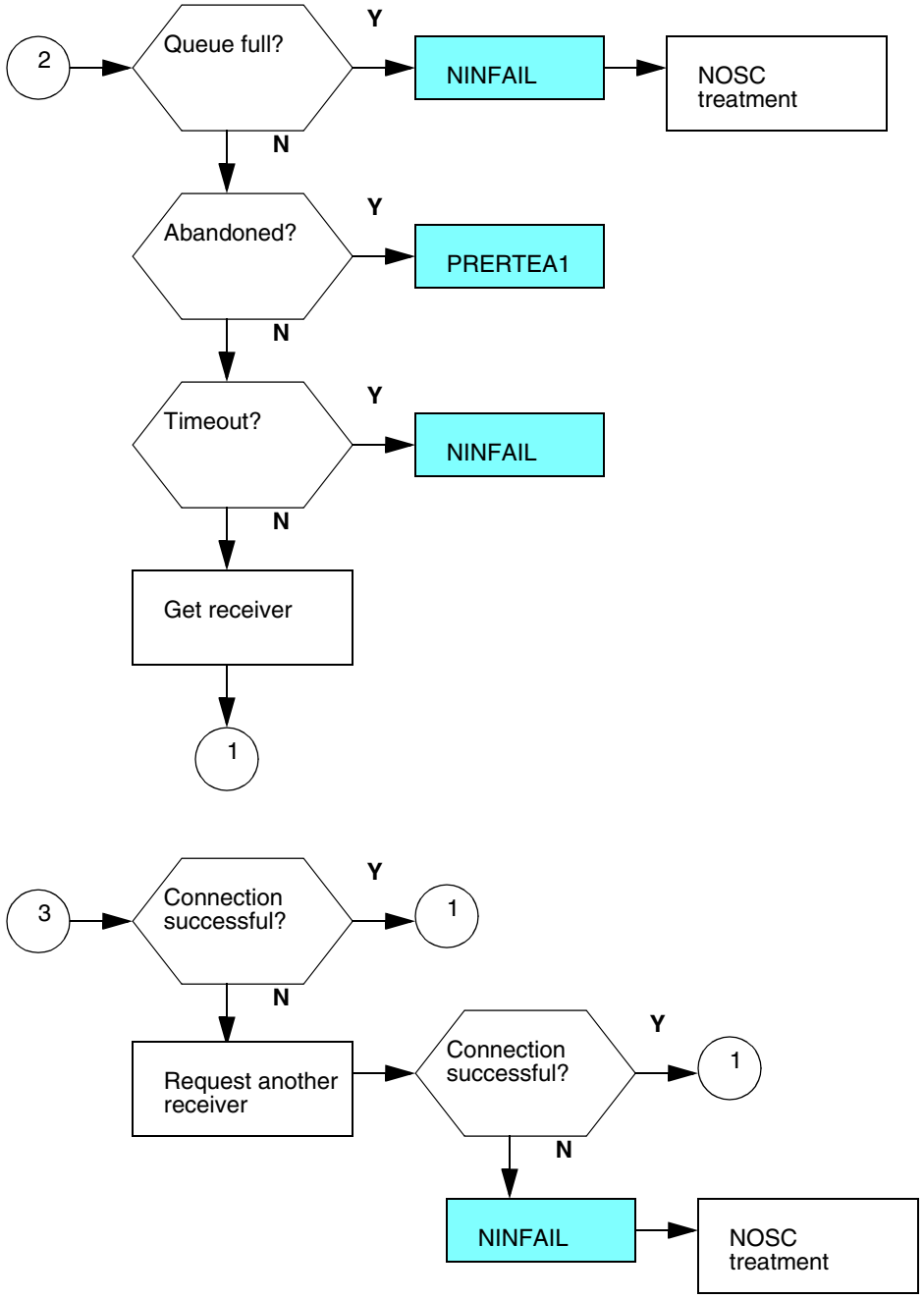


Figure 23 Origination from a trunk (continued)

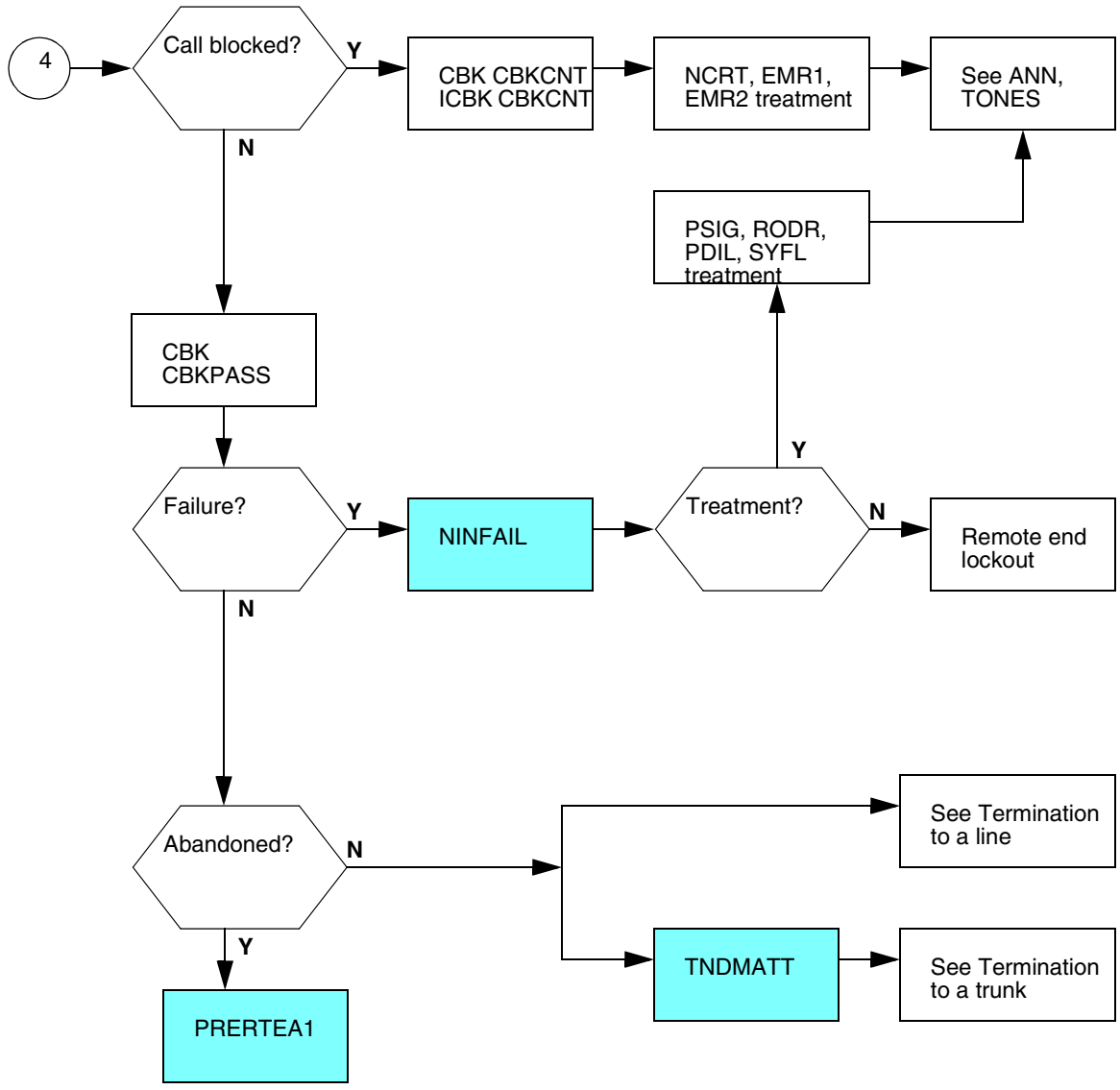
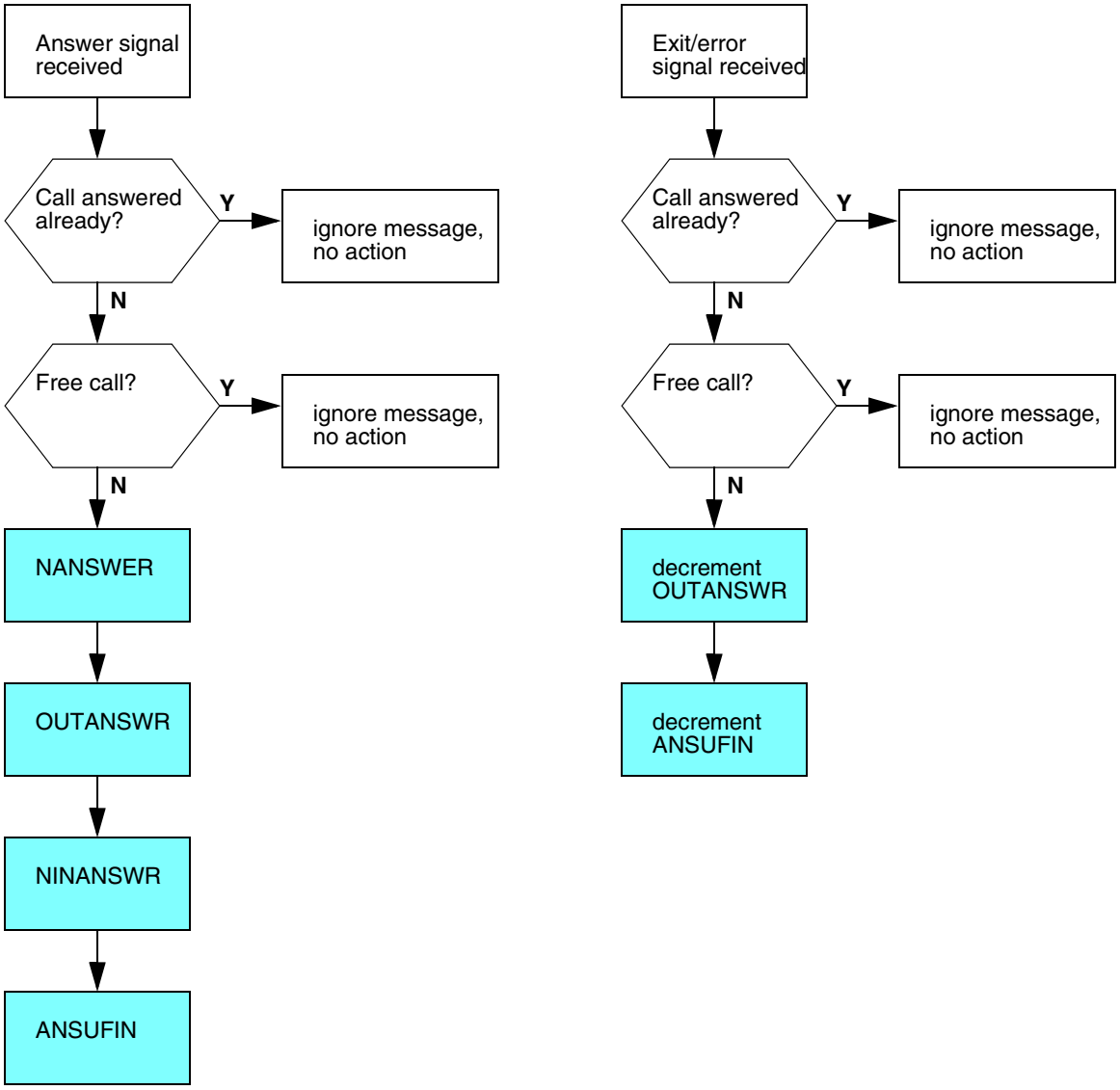


Figure 24 Trunk group answered calls



5.3.7.9 Register NACCCNG

5.3.7.9.1 Register description Automatic congestion control (NACCCNG) counts the number of times that a trunk group enters Automatic Congestion Control (ACC) congestion.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.9.2 Register release history update Register is new in SN07.

5.3.7.9.3 Associated registers None.

5.3.7.9.4 Associated logs None.

5.3.7.10 Register NANF

5.3.7.10.1 Register description Invalid or no automatic number identification (ANI) signals (NANF) counts incoming centralized-automatic message accounting (CAMA) or TOPS calls for which:

- the system receives invalid ANI signaling
- the system did not receive ANI signaling
- the numbering plan area code (N0/1X) or the central office code (NNX) of the calling number for the incoming trunk group is not correct Register ANF increases when the system attaches the necessary receiver to the call.

5.3.7.10.2 Register release history update Register is new in SN07.

5.3.7.10.3 Associated registers None.

5.3.7.10.4 Associated logs The system generates TRK120 when the call server or the intervening operator encounters problems. Problems can occur during operator number identification (ONI) spill for an incoming call over a CAMA trunk. The system cannot determine the call origination address.

5.3.7.11 Register NANSWER

5.3.7.11.1 Register description Answer supervisions (NANSWER) count all line/trunk to trunk answered calls. This register is the answer register for the outgoing trunk.

5.3.7.11.2 Register release history update Register is new in SN07.

5.3.7.11.3 Associated registers None.

5.3.7.11.4 Associated logs None.

5.3.7.12 Register INVATHCD

5.3.7.12.1 Register description
INVATHCD counts authorization codes that are not correct. The register is pegged against the CLLI and bearer network of the originator.

5.3.7.12.2 Register release history update Register is new in SN07.

5.3.7.12.3 Associated registers None

5.3.7.12.4 Associated logs None.

5.3.7.13 Register MAXBSY

5.3.7.13.1 Register description

MAXBSY scans the trunk group and pegs the counter if the number of busy circuits exceeds the maximum number that the system recorded earlier.

Note: MAXBSY will always be set to zero for DPT trunks

5.3.7.13.2 Register release history update Register is new in SN07.

5.3.7.13.3 Associated registers None

5.3.7.13.4 Associated logs None.

5.3.7.14 Register ANIOFCFL

5.3.7.14.1 Register description Automatic number identification (ANI) office failure (ANOOFCFL) counts incoming calls for which the originating office detects an ANI failure. Failure can be detected despite correct key pulse and signaling terminal control signals. The missing information digits, missing category code or the complete lack of digits indicates an ANI failure.

5.3.7.14.2 Register release history update Register is new in SN07.

5.3.7.14.3 Associated registers None.

5.3.7.14.4 Associated logs Register TRK118 generates when the system encounters trouble during ANI spill for an incoming call. In this example, the system cannot determine call originating address.

Register TRK119 generates when an operator keys in the originating station number identification and releases the call. The operator releases the call because the system encounters trouble with DMS ANI.

5.3.7.15 Register CNCTAT

5.3.7.15.1 Register description Successful connections (CNCTAT) counts outgoing seizure attempts on the trunk group that appear to result in successful connection.

Register CNCTAT increases before the system knows if the seizure is successful. The count reduces by 1 (decreases) if an indication of glare or seize failure is received. This register generates for all correct office types.

5.3.7.15.2 Register release history update Register is new in SN07.

5.3.7.15.3 Associated registers Register GLARE1 increases when the system drops an earlier selected trunk. The system drops the trunk because the peripheral module detects an origination before it can seize the trunk.

5.3.7.15.4 Associated logs None.

5.3.7.16 Register GLARE1

5.3.7.16.1 Register description Glare (GLARE1) increases when the system drops a trunk that the system selects at an earlier time. The system drops this trunk because the PM detects an origination before the PM can seize the trunk. The operating company gives information that indicates that outgoing calls give way to simultaneous incoming calls (glare).

The system attempts a new selection. If the system encounters glare again, the system routes the call to generalized no-circuit (GNCT) treatment. Register GLARE1 increases again.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.7.16.2 Register release history update Register is new in SN07.

5.3.7.16.3 Associated registers Register CNCTAT counts outgoing seizure attempts on the trunk group that result in connections.

Register OUTFL counts errors on an outgoing trunk after an attempt to seize the trunk.

5.3.7.16.4 Associated logs The system generates log TRK113 if the system encounters problems during call processing of a trunk-to-trunk call. The system generates TRK121 if the call server does not receive an acknowledgement wink from the far-end equipment. An acknowledgement wink indicates that the far-end equipment is ready to receive digits.

5.3.7.17 Register NINANSWR

5.3.7.17.1 Register description Answer messages sent and received on incoming trunk (NINANSWR) counts the answered calls for incoming traffic for each incoming or two-way trunk.

This register is not pegged in the current load.

5.3.7.17.2 Register release history update Register is new in SN07.

5.3.7.17.3 Associated registers None.

5.3.7.17.4 Associated logs None.

5.3.7.18 Register ANSUFIN

5.3.7.18.1 Register description Answer messages received and sent usage on incoming trunk (ANSUFIN) is a usage register that shows the number of answered calls on incoming trunk calls. This register measures traffic in the answered state for each incoming or two-way trunk. The register measures the occupancy in Erlangs.

The value of register ANSUFIN increases every 100 seconds according to the number of trunks occupied with answered calls.

This register is not pegged in the current load.

5.3.7.18.2 Register release history update Register is new in SN07.

5.3.7.18.3 Associated registers None.

5.3.7.18.4 Associated logs None.

5.3.7.19 Register INCAATT

5.3.7.19.1 Register description Incoming attempts total (INCAATT) counts incoming seizures on a trunk group, including seizures that fail or that the system abandons before routing.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.19.2 Register release history update Register is new in SN07.

5.3.7.19.3 Associated registers None.

5.3.7.19.4 Associated logs None.

5.3.7.20 Register NINFAIL

5.3.7.20.1 Register description Incoming failures (NINFAIL) increases when any one of the following events occurs on a trunk that has originated a call or appears to have originated a call:

- permanent signal
- partial dial time-outs and false starts
- bad digits, including bad signaling terminal (ST) digit
- any originations on one-way outgoing trunks
- lost integrity on the network path while connected to a service circuit or to another trunk before answer

- failure to attach a receiver after two attempts
- receiver queue overflow
- receiver queue wait time-out
- failure to time-out after 30 s while waiting for a multi frequency receiver
- progress message of a type not expected in the current call environment
- force-release before connection

These events can indicate a need for maintenance action. These events can result in call failure if a call was in progress.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.20.2 Register release history update Register is new in SN07.

5.3.7.20.3 Associated registers None.

5.3.7.20.4 Associated logs The system generates TRK111 if a trunk-to-trunk call encounters problems or if the system routes the call to a treatment.

The system generates log TRK114 if the system cannot determine the call destination during dial pulse (DP) reception for an incoming call.

The system generates log TRK115 if the system cannot determine the call destination during DP reception for an incoming call.

The system generates log TRK116 if the system cannot determine call destination during multi frequency (MF) reception for an incoming call.

The system generates log TRK117 if the system cannot determine call destination during MF reception for an incoming call.

The system generates log TRK138 if the system routes a call to a treatment after being call processing busy.

The system generates log TRK182 if the system cannot determine call destination during Digitone (DT) reception for an incoming call.

The system generates log TRK183 if a permanent signal problem occurs when an incoming call encounters problems during DT reception.

The system generates log TRK213 when the system encounters problems on a trunk.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.21 Register MBSYU

5.3.7.21.1 Register description Maintenance busy usage (MBSYU) is a usage register. Every 100 s the system scans the trunk group. This register records if a trunk is in one of the following states:

- manual busy
- seized
- network management busy

5.3.7.21.2 Register release history update Register is new in SN07.

5.3.7.21.3 Associated registers None.

5.3.7.21.4 Associated logs None.

5.3.7.22 Register NATMPT

5.3.7.22.1 Register description Number of attempts (NATMPT) increases when the system routes an outgoing call to a trunk group.

Register NATMPT increases before network management controls increase. This register increases before an idle trunk and a network connection to the trunk are available.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.7.22.2 Register release history update Register is new in SN07.

5.3.7.22.3 Associated registers None.

5.3.7.22.4 Associated logs None.

5.3.7.23 Register NOANSWR

5.3.7.23.1 Register description No Answer on trunk [Timed out] (NOANSWR) is a peg register which counts the number of times a call has been taken down after a specified time-out value has been reached, as part of Black Box Fraud prevention (BBFP). The time-out value is implemented on a trunk-group basis and can be set to either one, two, three, four, or five minute intervals. Upon expiration of the timer, the NOANSWR register is pegged.

NOANSWR functionality is activated and deactivated via the DLYFWDXMT option datafill of table TRKOPTS on a trunk-group basis. Register NOANSWR is pegged when the black box fraud timer or DLYFWDXMT timer expires before an answer supervision signal is received. The time-out value is datafilled in table TRKOPTS.

Register NATMPT gets pegged once per trunk per bearer network attempted.

5.3.7.23.2 Register release history update Register is new in SN07.

5.3.7.23.3 Associated registers None.

5.3.7.23.4 Associated logs Log TRK610 is generated each time the NOANSWR register is pegged.

5.3.7.24 Register NVFLATB

5.3.7.24.1 Register description Number of overflows, all trunks busy (NVFALTB) increases when a call with access to the trunk group overflows the group. The system routes the call because an idle trunk is not available. A call can access the same group more than one time. Overflow can occur only one time. Overflow occurs if the system cannot use the first trunk because of seize fail, glare or network blockage. Register NVFLATB increases when the system cannot find an idle trunk on the first or any of the following access attempts.

Register NATMPT gets pegged once per trunk per bearer network overflowed.

5.3.7.24.2 Register release history update Register is new in SN07.

5.3.7.24.3 Associated registers None.

5.3.7.24.4 Associated logs The system generates ATB100 when the system blocks an attempt to seize a trunk to a specified numbering plan area or central office. The system advances the call to another route.

5.3.7.25 Register OUTANSWR

5.3.7.25.1 Register description Answer message received and sent usage on an outgoing trunk (OUTANSWR) is a usage register that shows the number of answered calls on outgoing trunk calls. This register measures traffic in the answered state for each outgoing or two-way trunk. The register measures the occupancy in Erlangs.

The value of register OUTANSWR increases every 100 seconds according to the number of trunks occupied with answered calls.

This register is not pegged in the current load.

5.3.7.25.2 Register release history update Register is new in SN07.

5.3.7.25.3 Associated registers None.

5.3.7.25.4 Associated logs None.

5.3.7.26 Register OUTFL

5.3.7.26.1 Register description Outgoing failures (OUTFL) counts attempts to seize an outgoing trunk in the trunk group that fail because of following:

- signaling problems
- loss of accuracy
- outgoing failures
- seizure failures

The system releases the trunk. The system performs a maximum of two attempts to seize a trunk. The system counts each failed attempt in OUTFL. If a second attempt to seize a trunk fails, the system routes the call to treatment.

The system can generate a log message. Generation of a log message depends on the cause of the failure.

The system generates register OUTFL for office types that are correct.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.7.26.2 Register release history update Register is new in SN07.

5.3.7.26.3 Associated registers Register CNCTAT counts outgoing seizure attempts on the trunk group that result in connections.

Register GLARE1 increases when the system drops a trunk that the system selects at an earlier time. The system drops the trunk because the PM detected an origination. The PM detects an origination before the PM seizes the trunk.

5.3.7.26.4 Associated logs The system generates TRK113 if the system encounters problems during call processing of a trunk-to-trunk call.

The system generates TRK121 if the DMS does not receive an acknowledgement wink from the far-end equipment. The acknowledgement wink indicates that the equipment is ready to receive digits.

The system generates TRK122 if the central control detects a loss of accuracy on both planes of the trunk equipment.

The system generates TRK162 if the system encounters problems during outpulsing of a trunk-to-trunk or line-to-trunk call. The call uses dual-tone multi frequency (DTMF) signaling.

The system generates TRK213 if the system encounters problems on a trunk.

5.3.7.27 Register TRKNWBLK

5.3.7.27.1 Register description Outgoing matching failure (TRKNWBLK) counts attempts to find a path from an incoming trunk or originating line to a selected trunk that fail. Failure occurs as a result of network blockage.

If the system blocks an outgoing call, the call again attempts to select a trunk. If the system blocks this attempt, TRKNWBLK counts the call again. The system routes the call to NBLH treatment.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.7.27.2 Register release history update Register is new in SN07.

5.3.7.27.3 Associated registers None.

5.3.7.27.4 Associated logs The system generates NET130 if the system cannot find a network path.

5.3.7.28 Register PRERTEA1

5.3.7.28.1 Register description Preroute abandon (PRERTEA1) counts incoming attempts the system abandons before the system can complete routing.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.28.2 Register release history update Register is new in SN07.

5.3.7.28.3 Associated registers None.

5.3.7.28.4 Associated logs The system generates register TRK113 if the system encounters problems during call processing of a trunk-to-trunk call.

The system generates TRK116 if the system cannot determine the call destination during multi frequency reception for an incoming call.

5.3.7.29 Register SBSYU

5.3.7.29.1 Register description System busy usage (SBSYU) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk is in one of the following states:

- remote busy
- peripheral module busy
- system busy
- carrier fail
- deloaded

5.3.7.29.2 Register release history update Register is new in SN07.

5.3.7.29.3 Associated registers None.

5.3.7.29.4 Associated logs The system generates TRK106 if a self-test on trunk equipment fails.

The system generates TRK109 when a self-test on a DS-1 facility fails.

5.3.7.30 Register TNDMATT

5.3.7.30.1 Register description Tandem (TNDMATT) counts incoming calls on a trunk group that first routes to an outgoing trunk group. Register TNDMATT increases before the system determines if the outgoing trunk group is busy, or if a junctor path is available.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.7.30.2 Register release history update Register is new in SN07.

5.3.7.30.3 Associated registers None.

5.3.7.30.4 Associated logs None.

5.3.7.31 Register TOTBSYU

5.3.7.31.1 Register description Total usage (TOTBSYU) is a usage register. Every 100 seconds the system scans the trunk group and register TOTU records if any trunk in the group is busy.

5.3.7.31.2 Register release history update Register is new in SN07.

5.3.7.31.3 Associated registers Register MBU counts manual busy trunks.

Register SBU counts system busy trunks.

Register TRU counts call processing busy trunks.

TOTU = TRU + SBU + MBU.

5.3.7.31.4 Associated logs None.

5.3.7.32 Register TRFCU

5.3.7.32.1 Register description Traffic busy usage (TRFCU) is a usage register. Every 100 s the system scans the trunk group. This register records if a trunk in the group is in one of the following states:

- call processing busy (TK_CP_BUSY)
- call processing busy deload (TK_CP_BUSY_DELOAD)
- lockout (TK_LOCKOUT)

5.3.7.32.2 Register release history update Register is new in SN07.

5.3.7.32.3 Associated registers None.

5.3.7.32.4 Associated logs None.

5.3.8 TRK2NET2 OM Group

5.3.8.1 OM description

TRK2NET2 OM Group provides information for per trunk group traffic analysis per bearer network. It contains extension registers for registers found in OM Group TRK2NET1.

5.3.8.2 Release history update

TRK2NET2 OM group is new in SN07.

The addition of this new TRK2NET2 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to ‘Y’, then the new TRK2NET2 OM group is displayed. If the parameter is set to ‘N’, then the TRK2NET2 OM group is not displayed.

5.3.8.3 Registers

TRK2NET2 OM group registers display on the MAP terminal as follows:

Figure 25 TRK2NET2 OM Group Display

```
>omshow trk2net2 active 'TRI1ITOGS7 NET 0'

TRK2NET2

CLASS: ACTIVE
START:2004/09/28 16:30:00 TUE; STOP: 2004/09/28 16:49:22 TUE;
SLOWSAMPLES:       12 ; FASTSAMPLES:       116 ;

     INFO (TRK2NET1_INFO)
      INCAATT2   NATMPT2    TRFCU2    SBSYU2
      CNCTAT2   TNDMATT2   TOTBSYU2   NANSWER2

  91
      TRI1ITOGS7 NET 0 ENET  379 OG    2    2
          0        0        0        0
          0        0        0        0

>omshow trk2net2 active 'TRI1ITOGS7 NET 1'

TRK2NET2

CLASS: ACTIVE
START:2004/09/28 16:30:00 TUE; STOP: 2004/09/28 16:50:28 TUE;
SLOWSAMPLES:       13 ; FASTSAMPLES:       123 ;

     INFO (TRK2NET1_INFO)
      INCAATT2   NATMPT2    TRFCU2    SBSYU2
      CNCTAT2   TNDMATT2   TOTBSYU2   NANSWER2

  92
      TRI1ITOGS7 NET 1 AAL1  379 OG    2    2
          0        0        0        0
          0        0        0        0

>omshow trk2net2 active 'TRI1ITOGS7 NET 2'

TRK2NET2

CLASS: ACTIVE
START:2004/09/28 16:30:00 TUE; STOP: 2004/09/28 16:50:38 TUE;
SLOWSAMPLES:       13 ; FASTSAMPLES:       124 ;

     INFO (TRK2NET1_INFO)
      INCAATT2   NATMPT2    TRFCU2    SBSYU2
      CNCTAT2   TNDMATT2   TOTBSYU2   NANSWER2

  90
      TRI1ITOGS7 NET 2 IP    379 OG    2    2
          0        0        0        0
          0        0        0        0
```

5.3.8.4 Group structure

TRK2NET2 OM group provides 1 tuple(s) for each trunk group and each bearer network that the trunk group has members provisioned in.

Key field: None

Info field: TRK2NET1_INFO

- CLLI
- bearer network ID (i.e., ‘NET 0’)
- bearer network name (i.e., ‘TDM_ENET’)
- trunk group direction. (i.e., ‘IC—incoming trunk, OG—outgoing trunk, 2W—two-way trunk’)
- total number of trunk circuits in the group in the associated bearer network (i.e., ‘20’)
- number of trunk circuits in the associated bearer network available for service at the end of the reporting period. (i.e., ‘19’)

The office parameter OFFICETYPE in table OFCSTD specifies the type of office. The value of OFFICETYPE controls the generation of TRK2NET2 registers. Correct entries for OFFICETYPE appear below:

- OFF100 Local
- OFF1000ESD Australian local
- OFF100SCP DMS-100 Service Control Point (SCP)
- OFF200 Toll
- OFF200AVON DMS100/200 local/toll with Autovon (U. S. and Canada)
- OFF200ESD Australian toll
- OFF200TOPS Toll with TOPS
- OFF200/300 Combined gateway/toll
- OFF250 DMS-250
- OFF250IBN DMS-250/SL-100
- OFF300 Gateway
- OFF500 DMS-500
- OFFCOMB Combined local/toll
- OFFCOMB300 Combined local/toll and gateway
- OFFCOMB300ITOPS Combined local/toll and gateway with international TOPS (ITOPS)
- OFFCOMBITOPS Combined local/toll with ITOPS

- OFFCOMBLWW Combined local/toll with wireless
- OFFCOMBESD Australian combined local/toll
- OFFCOMBTOPS Combined local/toll with traffic operator position system (TOPS)
- OFFMTX100 DMS-MTX with DMS100

The office type parameters appear in table OFCSTD. When the system reports an answer indication to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

5.3.8.5 Associated OM groups

The TRK2NET1 OM group provides the primary registers. The registers found is TRK2NET2 are pegged only if the registers in TRK2NET1 overflow.

5.3.8.6 Associated functional groups

The following functional groups are associated with TRK2NET2 OM group:

- Succession North America
- Succession International

5.3.8.7 Associated functionality codes

None

5.3.8.8 TRK2NET2 OM group registers logic flow chart

Refer to TRK2NET1 for register flow charts.

5.3.8.9 Register NANSWER2

5.3.8.9.1 Register description Answer supervisions (NANSWER2) count all line/trunk to trunk answered calls. This register is the answer register for the outgoing trunk.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.8.9.2 Register release history update Register is new in SN07.

5.3.8.9.3 Associated registers NANSWER in TRK2NET1 OM group.

5.3.8.9.4 Associated logs None.

5.3.8.10 Register CNCTAT2

5.3.8.10.1 Register description Successful connections (CNCTAT2) counts outgoing seizure attempts on the trunk group that appear to result in successful connection.

Register CNCTAT2 increases before the system knows if the seizure is successful. The count reduces by 1 (decreases) if an indication of glare or seize failure is received. This register generates for all correct office types.

This register will be pegged against the CLLI and bearer network of the terminator.

5.3.8.10.2 Register release history update Register is new in SN07.

5.3.8.10.3 Associated registers CNCTAT in TRK2NET1 OM group.

5.3.8.10.4 Associated logs None.

5.3.8.11 Register INCAATT2

5.3.8.11.1 Register description Incoming attempts total (INCAATT2) counts incoming seizures on a trunk group, including seizures that fail or that the system abandons before routing.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.8.11.2 Register release history update Register is new in SN07.

5.3.8.11.3 Associated registers INCAATT in TRK2NET1 OM group.

5.3.8.11.4 Associated logs None.

5.3.8.12 Register NATMPT2

5.3.8.12.1 Register description Number of attempts (NATMPT2) increases when the system routes an outgoing call to a trunk group.

Register NATMPT2 increases before network management controls increase. This register increases before an idle trunk and a network connection to the trunk are available.

5.3.8.12.2 Register release history update Register is new in SN07.

5.3.8.12.3 Associated registers INATMPT in TRK2NET1 OM group.

5.3.8.12.4 Associated logs None.

5.3.8.13 Register SBSYU2

5.3.8.13.1 Register description System busy usage (SBSYU2) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk is in one of the following states:

- remote busy
- peripheral module busy
- system busy
- carrier fail
- deloaded

5.3.8.13.2 Register release history update Register is new in SN07.

5.3.8.13.3 Associated registers SBSYU in TRK2NET1 OM group.

5.3.8.13.4 Associated logs The system generates TRK106 if a self-test on trunk equipment fails.

The system generates TRK109 when a self-test on a DS-1 facility fails.

5.3.8.14 Register TNDMATT2

5.3.8.14.1 Register description Tandem (TNDMATT2) counts incoming calls on a trunk group that first routes to an outgoing trunk group. Register TNDMATT2 increases before the system determines if the outgoing trunk group is busy, or if a junctor path is available.

This register will be pegged against the CLLI and bearer network of the originator.

5.3.8.14.2 Register release history update Register is new in SN07.

5.3.8.14.3 Associated registers TNDMATT in TRK2NET1 OM group.

5.3.8.14.4 Associated logs None.

5.3.8.15 Register TOTBSYU2

5.3.8.15.1 Register description Total usage (TOTBSYU2) is a usage register. Every 100 seconds the system scans the trunk group and register TOTBSYU2 records if any trunk in the group is busy.

5.3.8.15.2 Register release history update Register is new in SN07.

5.3.8.15.3 Associated registers TOTBSYU in TRK2NET1 OM group.

5.3.8.15.4 Associated logs None.

5.3.8.16 Register TRFCU2

5.3.8.16.1 Register description Traffic busy usage (TRFCU2) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk in the group is in one of the following states:

- call processing busy (TK_CP_BUSY)
- call processing busy deload (TK_CP_BUSY_DELOAD)
- lockout (TK_LOCKOUT)

5.3.8.16.2 Register release history update Register is new in SN07.

5.3.8.16.3 Associated registers TRFCU in TRK2NET1 OM group.

5.3.8.16.4 Associated logs None.

6: Performance (PF): A00003531

6.1 Performance management strategy

OM Collector (OMC) fetches performance data from MG9K through FTP, converts the performance data to CSV format and writes the converted data into a file. In subsequent sections of this document, this file is termed as “OMC CSV file”. OSSs which are present towards north bound interface of OMC, make use of these OMC CSV files.

6.2 Performance management tools and utilities

OMC CSV file contains data in the following format;

<ScalarTableName-1>
<performance parameter name 1>, <performance parameter name 2>...
Value1, Value2...

<NonScalarTableName-2>
<performance parameter name 1>, <performance parameter name 2>...
Source, Value1, Value2...

An example data in a SN06.2 OMC CSV file is as follows;

Miscellaneous
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts
0,0,1769

norCarrSonetMediumIntervalTable
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC
Frame2.Shelf0.Slot10.Port1,99,100
Frame2.Shelf0.Slot11.Port401,100,100

Here, the table ‘Miscellaneous’ is a Scalar table. That means, it’s Performance parameters are Scalar SNMP attributes. So, they are not identified by any ‘source’. Whereas, the table norCarrSonetMediumIntervalTable is a non-scalar table. That means, it’s Performance parameters are non-scalar SNMP attributes. So, they are identified by appropriate source, namely Frame number, Shelf number, Card number and Port number.

In SN06.2, OMC CSV file uses Internal frame number for values of Performance parameters of non-scalar table. In above example, number 2 shown next to ‘Frame’ is Internal frame number of the ‘source’ of the performance parameter.

In SN07, OMC CSV file will use Office frame number for values of Performance parameters of non-scalar table. So, if Frame location information is provisioned for frame-2, example SN06.2 data which is shown above, will be as follows in SN07.

Miscellaneous
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts
0,0,1769

norCarrSonetMediumIntervalTable
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC
Frame080.Shelf0.Slot10.Port1,99,100
Frame080.Shelf0.Slot11.Port401,100,100

In this SN07 example, number '080' shown next to 'Frame' is Office frame number.

If Frame location information is not provisioned partially or completely for frame-2, example SN06.2 data which is shown above, will be as follows in SN07.

Miscellaneous
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts
0,0,1769

norCarrSonetMediumIntervalTable
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC
FrameFFF.Shelf0.Slot10.Port1,99,100
FrameFFF.Shelf0.Slot11.Port401,100,100

6.2.1 Configuring PCF software

Following are the steps to be followed to start/stop collection of OM data.

At the MG 9000 Manager Mid-tier server

1. Issue the following change directory command to enter the appropriate directory:
   # cd /opt/nortel/omcltr_07/bin
2. While configuring OM Collector, specify IP address of the EM server, to which OM Collector is associated.Also specify the IP address of the Oracle server.
   If it is a first time configuration of OM COllector, then Operator will be allowed either to perform configuration or to exit. The script which the user needs to run here is **/opt/nortel/omcltr_07/OMCollector_config.sh**

   If it is a reconfiguration of OM COllector, the Operator will be shown a menu using which she can change the EM server IP Address and/or Oracle Server IP Address. For this the user has to run **/opt/nortel/omcltr_07/bin/OMCollector config**.

   An example result when configuration is done first time:
   # ./OMCollector_config.sh
   Starting OM Configuration ...

```
Please enter the IP Address of MG9K server?
Press the enter key to accept the default ?
Default: [] => 47.142.122.200
Please enter the IP Address of Oracle Server?
Press the enter key to accept the default ?
Default: [] => 47.142.208.207

**********************************************************
**
        EM Server IP Address       : 47.142.122.200
        Oracle IP Address          : 47.142.208.207

                **********************************************
                **********

Is the above information correct?
Press the enter key to accept the default (y/n)?
Default: [n] => y
Configuring system, please wait ...

Configuration complete ...
```

An example result when old configuration exist and Operator reconfigures again:

```
# ./OMCollector_config.sh
Starting OM Configuration ...
Setup has detected configuration settings from a previous installation.


**********************************************************
**
        EM Server IP Address       : 47.142.122.200
        Oracle IP Address          : 47.142.208.207
**********************************************************
**
Is the above information correct?
Press the enter key to accept the default (y/n)?
Default: [n] => n

Please enter the IP Address of MG9K server?
Press the enter key to accept the default ?
Default: [47.142.122.200] => 47.142.92.67

Please enter the IP Address of Oracle Server?
Press the enter key to accept the default ?
Default: [47.142.208.207] => 47.142.217.8
```

```
**********************************************************
**
        EM Server IP Address       : 47.142.92.67
        Oracle IP Address          : 47.142.217.8
**********************************************************
**
Is the above information correct?
Press the enter key to accept the default (y/n)?
Default: [n] => y
Configuring system, please wait ...

Configuration complete ...
```

An example result when old configuration exist and Operator wants to retain the configuration:

```
# ./OMCollector_config.sh
Starting OM Configuration ...
Setup has detected configuration settings from a previous installation.


**********************************************************
**
        EM Server IP Address       : 47.142.92.67
        Oracle IP Address          : 47.142.217.8
**********************************************************
**

Is the above information correct?
Press the enter key to accept the default (y/n)?
Default: [n] => y
Configuring system, please wait ...

Configuration complete ...
```

An example result when the user changes the configuration using the menu options:

```
# ./OMCollector config
Starting OM Configuration ...

Main Configuration Menu

1) Change IP Address of EM Server
2) Change Oracle IP Address
3) Display current settings
4) Exit from Main Menu
```

Please make a selection => 1

EM Server IP Address Configuration Menu

1) Enter new EM Server IP Address
2) Exit to Main Menu
Please make a selection [Current: 47.142.92.67] => 1

Please enter the IP Address of EM Server ?
Default: [47.142.92.67] => 47.142.122.200

Please wait ... trying to contact server.

EM Server IP Address Configuration Menu

1) Enter new EM Server IP Address
2) Exit to Main Menu
Please make a selection [Current: 47.142.122.200] => 2

Main Configuration Menu

1) Change IP Address of EM Server
2) Change Oracle IP Address
3) Display current settings
4) Exit from Main Menu
Please make a selection => 2

Oracle IP Address Configuration Menu

1) Enter new Oracle IP Address
2) Exit to Main Menu
Please make a selection [Current: 47.142.217.8] => 1

Please enter the IP Address of Oracle Server ?
Default: [47.142.217.8] => 47.142.208.207

Please wait ... trying to contact server.

Oracle IP Address Configuration Menu

1) Enter new Oracle IP Address
2) Exit to Main Menu
Please make a selection [Current: 47.142.208.207] => 2

Main Configuration Menu

```
1) Change IP Address of EM Server
2) Change Oracle IP Address
3) Display current settings
4) Exit from Main Menu
Please make a selection => 3

          CURRENT SETTINGS
 Package Name              :NTomclt07
 Version  :NTOMCLTR_7_16_0
EM Server IP Address  : 47.142.122.200
 Oracle Server IP          :47.142.208.207

 Main Configuration Menu

1) Change IP Address of EM Server
2) Change Oracle IP Address
3) Display current settings
4) Exit from Main Menu
Please make a selection => 4
#
```

3. Start EM Server/Midtier and create NE. While creating NE, specify whether OM data needs to be collected by checking the “NE OMCollection” check box. This check box is also modifiable through the GUI "View/Modify NE Properties". Thus, Operator can start, stop, restart OM data collection through MG9K EM.
4. Start "/opt/nortel/omcltr_07/bin/OMCollector start". With this step, OM Collector will start collecting OM data for the NE, for which “NE OMCollection” check box is checked in MG9K EM.

6.3 Performance Measurements (PM), Operational Measurements (OM), and stats

None

7: Performance (PF): A00003687

7.1 Performance management strategy

This feature is an extension of SN06 feature A000000816: “Wireless ADACC with Release.” This feature provides additional functions involving TCAP messaging between mobile switching centers (MSCs), message centers (MCs), and TOPS. The main tools used to monitor the performance of these features are operational measurements (OMs).

OM group IS41TOPS was created by feature A00000816 in SN06. With the functional additions of this SN07 feature, OM group IS41TOPS is no longer sufficient. This feature creates three new OM groups (SMSTOPS, WINTOPS, and TC7WRLSS) and removes group IS41TOPS.

Events which previously pegged registers in group IS41TOPS will now peg registers in OM groups WINTOPS and TC7WRLSS. For more information including a complete mapping of old to new registers, see the Functional Description chapter of this document.

7.2 Performance management tools and utilities

The new OM group is accessed using the OMSHOW command from the Maintenance and Administrative Position (MAP).

7.3 Operational Measurements (OMs)

This feature creates the following OM groups:

- SMSTOPS
- WINTOPS
- TC7WRLSS

This feature removes the following OM group:

- IS41TOPS

All events formerly pegged in group IS41TOPS are now pegged in groups WINTOPS and TC7WRLSS.

Table 1 OM group SMSTOPS

Register	Meaning
SMSSENT, SMSSENT2	SMS sent
SMSSUCC, SMSSUCC2	SMS success

Table 1 OM group SMSTOPS

Register	Meaning
SMSFAIL, SMSFAIL2	SMS failure
SMSTIME, SMSTIME2	SMS time-out
SMSNETWK	SMS failure due to network problems
SMSTERM	SMS failure due to terminal (cell phone) problems
SMSRADIO	SMS failure due to radio interface problems
SMSMISC	Miscellaneous SMS failure

Table 2 OM group WINTOPS

Register	Meaning
WINBEGIN, WINBEGI2	IS-41 AnalyzedInformation or GSM InitialDP received
REQCONN, REQCONN2	IS-41 ConnectResource or GSM EstablishTemporaryConnection sent
DISCONN, DISCONN2	IS-41 AnalyzedInformation with action code of “disconnect call” or GSM DisconnectTemporaryConnection sent. This event is not part of the normal IS-41 call flow, but it is part of the normal GSM call flow. If this is pegged for IS-41, it means ADACC with release was not provided.
CONNECT, CONNECT2	IS-41 AnalyzedInformation or GSM Connect sent
WINEND, WINEND2	GSM Application End received; no equivalent IS-41 message
ERRCONN	MSC could not connect to TOPS using TLDN
ERRDISC	TOPS disconnected unexpectedly while providing operator assistance. IS-41 only; when this occurs in a GSM call, WINEND is pegged but not DISCONN or CONNECT.
ERRSSFT	MSC’s service switching function timer expired. Should not happen if TOPS Reset TImer is datafilled properly in Table ISUPTRK.
ABANDON	Wireless caller disconnected prior to receiving ADACC with release.
RESTIMR, RESTIMR2	ResetTimer sent (IS-41 and GSM)
NOTLDNS	No TLDNs available in Table TOPSTLDN

Table 2 OM group WINTOPS

Register	Meaning
NODATA	TOPS could not find EXT block associated with incoming TLDN call from MSC
RXLAFAIL	TOPS call could not obtain original called digits and defaulted to 411
SANTIMR	MSC did not release trunk to TOPS, or MSC did not send Application End
TLDNTIME	A TLDN was allocated for an MSC call which never arrived. The TLDN is allocated to a new call.

Table 3 OM group TC7WRLSS

Register	Meaning
INVOKES, INVOKES2	TCAP INVOKE sent
INVOKER, INVOKER2	TCAP INVOKE receives
RETRESS, RETRESS2	TCAP RETURN RESULT sent
RETRESR, RETRESR2	TCAP RETURN RESULT received
RETERRS	TCAP RETURN ERROR sent
RETERRR	TCAP RETURN ERROR received
REJECTS	TCAP REJECT sent
REJECTR	TCAP REJECT received
ABORTS	TCAP ABORT sent
ABORTR	TCAP ABORT received
NOTRIDS	No transaction identifiers
MBFULL	Incoming message from MSC ignored due to heavy traffic
RTFNOXLA	SCCP routing failure: No translation of such nature
RTFNOXLS	SCCP routing failure: No translation for this specific address
RTFSUBCG	SCCP routing failure: Subsystem congestion
RTFSUBFL	SCCP routing failure: Subsystem failure
RTFUNEQ	SCCP routing failure: Unequipped user
RTFNETFL	SCCP routing failure: Network failure

Table 3 OM group TC7WRLSS

Register	Meaning
RTFNETCG	SCCP routing failure: Network congestion
RTFMISCE	SCCP routing failure: Failure other than the above seven
GTTFAIL	Global Title Translation failure

7.3.1 OM format

These OMs apply to events occurring on the TOPS switch during the course of a wireless (cellular) phone originated call to TOPS. In large TOPS offices, many such calls can occur during the reporting period, so several of the OMs introduced by this feature include extension registers. The extension registers are noted in the OM register text.

7.4 OM Group SMSTOPS

7.4.1 OM description

SMSTOPS

Short Message Service - TOPS

7.4.2 Release history update

Created in SN07

7.4.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

SMSSENT	SMSSENT2	SMSSUCC	SMSSUCC2
SMSFAIL	SMSFAIL2	SMSTIME	SMSTIME2
SMSNETWK	SMSTERM	SMSRADIO	SMSMISC

7.4.4 Group structure

OM group SMSTOPS provides one tuple for each wireless network type.

Key field: IS41 and GSM. There are two tuples in OM group SMSTOPS: one for IS-41 SMS and one for GSM SMS.

Info field: None

7.4.5 Associated OM groups

Registers in groups SMSTOPS and TC7WRLSS are pegged when TOPS sends an SMS and receives an acknowledgment.

7.4.6 Associated functional groups

None

7.4.7 Associated functionality codes

None

7.4.8 OM group registers logic flow chart

Register SMSSENT is pegged when TOPS sends a short message into the SS7 network.

Register SMSSUCC is pegged when TOPS receives a positive acknowledgment from the message center.

Register SMSFAIL is pegged when TOPS receives a negative acknowledgment from the message center.

Register SMSTIME is pegged when TOPS receives no acknowledgment from the message center within a customer-defined time period.

Patterns

- Every SMS attempt will peg SMSSENT plus one of the other registers. If an acknowledgment arrives after the time period has expired, the success or failure OM is pegged in addition to the time-out OM.
- The value of register SMSSENT should be close to the value of register SMSSUCC, with any slight inequality due to reporting period boundaries. If the value of SMSSUCC is significantly less than the value of SMSSENT, SMS failures are occurring either at TOPS, within the SS7 network, or at the message center.

7.4.9 Register SMSFAIL

7.4.9.1 Register description

Short Message Service Failure

SMSFAIL is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center following an SMS attempt.

7.4.9.2 Register release history update

Created in SN07

7.4.9.3 Associated registers

Extension register SMSFAIL2

7.4.9.4 Associated logs
TOPS131 or TCAP100, depending on type of failure

7.4.10 Register SMSMISC

7.4.10.1 Register description
Short Message Service Miscellaneous failure

SMSMISC is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due to a miscellaneous failure (not network, terminal, or radio interface).

7.4.10.2 Register release history update
Created in SN07

7.4.10.3 Associated registers
None

7.4.10.4 Associated logs
TOPS131

7.4.11 Register SMSNETWK

7.4.11.1 Register description
Short Message Service Network failure

SMSNETWK is a peg register. It is incremented whenever TOPS a negative acknowledgment from the message center saying the message could not be delivered due to a network failure.

7.4.11.2 Register release history update
Created in SN07

7.4.11.3 Associated registers
None

7.4.11.4 Associated logs
TOPS131

7.4.12 Register SMSRADIO

7.4.12.1 Register description
Short Message Service Radio interface failure

SMSRADIO is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due to a radio interface failure.

7.4.12.2 Register release history update
Created in SN07

7.4.12.3 Associated registers
None

7.4.12.4 Associated logs
TOPS131

7.4.13 Register SMSSENT

7.4.13.1 Register description
Short Message Service Sent

SMSSENT is a peg register. It is incremented whenever TOPS sends an SMS to a message center.

7.4.13.2 Register release history update
Created in SN07

7.4.13.3 Associated registers
Extension register SMSSENT2

7.4.13.4 Associated logs
None

7.4.14 Register SMSSUCC

7.4.14.1 Register description
Short Message Service Success

SMSSUCC is a peg register. It is incremented whenever TOPS receives a successful acknowledgment from a message center following an SMS attempt.

7.4.14.2 Register release history update
Created in SN07

7.4.14.3 Associated registers
Extension register SMSSUCC2

7.4.14.4 Associated logs
None

7.4.15 Register SMSTERM

7.4.15.1 Register description

Short Message Service Terminal failure

SMSTERM is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due a terminal (cell phone) failure.

7.4.15.2 Register release history update

Created in SN07

7.4.15.3 Associated registers

None

7.4.15.4 Associated logs

TOPS131

7.4.16 Register SMSTIME

7.4.16.1 Register description

Short Message Service Time-out

SMSTIME is a peg register. It is incremented whenever TOPS receives no acknowledgment from a message center following an SMS attempt in the allotted time-out period. The time-out period is datafilled in Table TOPSPARM (parameter `SMS_TIMEOUT`).

7.4.16.2 Register release history update

Created in SN07

7.4.16.3 Associated registers

Extension register SMSTIME2

7.4.16.4 Associated logs

TOPS131

7.5 OM Group WINTOPS

7.5.1 OM description

WINTOPS

Wireless Intelligent Network - TOPS

7.5.2 Release history update

Created in SN07

7.5.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 2 OM Group Display

WINBEGIN	WINBEGI2	REQCONN	REQCONN2
DISCONN	DISCONN2	CONNECT	CONNECT2
WINEND	WINEND2	RESTIMR	RESTIMR2
ABANDON	ERRCONN	ERRDISC	ERRSSFT
NOTLDNS	NODATA	RXLAFAIL	SANTIMR
TLDNTIME			

7.5.4 Group structure

OM group WINTOPS provides one tuple for each wireless network type.

Key field: IS41 and GSM. There are two tuples in OM group WINTOPS: one for IS-41 WIN and one for GSM CAMEL (Customized Applications for Mobile network Enhanced Logic).

Info field: None

7.5.5 Associated OM groups

Registers in groups WINTOPS and TC7WRLSS are pegged when TOPS provides a Wireless Intelligent Network service such as wireless ADACC with release.

7.5.6 Associated functional groups

None

7.5.7 Associated functionality codes

Table 4 Functionality codes associated with OM group

Functionality	Code
TOPS Wireless RLT	00034426

7.5.8 OM group registers logic flow chart

For a description of when these OMs are pegged, refer to the IS-41 call flow figure at the beginning of the Functional Description chapter.

Patterns

- Every WIN call flow, whether successful or not, will peg WINBEGIN.
- A successful WIN call flow (IS-41 or GSM) pegs registers WINBEGIN, REQCONN, and CONNECT.
- A successful GSM CAMEL call flow also pegs registers DISCONN and WINEND.
- Registers ABANDON and RESTIMR are pegged under normal circumstances and do not indicate problems.
- Register DISCONN on an IS-41 WIN call does not necessarily indicate a problem. In IS-41, it is always pegged in conjunction with another register. The other register indicates if a problem has occurred.
- Problems are indicated by the following registers: ERRCONN, ERRDISC, ERRSSFT, NOTLDNS, NODATA, RXLAFAIL, SANTIMR, and TLDNTIME.

7.5.9 Register ABANDON

7.5.9.1 Register description

Abandon

ABANDON is a peg register. It is incremented on a WIN call when the calling party disconnects before receiving ADACC with release.

This is a common occurrence. The wireless caller can hang up while in queue for operator, or hang up because the operator couldn't find the listing, or hang up without accepting call completion. In all of these cases, ABANDON is pegged.

7.5.9.2 Register release history update

Created in SN07

7.5.9.3 Associated registers

None

7.5.9.4 Associated logs

None

7.5.10 Register CONNECT

7.5.10.1 Register description

Connect

CONNECT is a peg register. It is incremented when TOPS directs the MSC to connect to the requested number. In IS-41, this is when TOPS sends the AnalyzedInformation RETURN RESULT. In GSM, this is when TOPS sends the Connect.

7.5.10.2 Register release history update

Created in SN07

7.5.10.3 Associated registers

Extension register CONNECT2

7.5.10.4 Associated logs

None

7.5.11 Register DISCONN

7.5.11.1 Register description

Disconnect

DISCONN is a peg register. It is incremented when TOPS directs the MSC release the trunk to TOPS. In IS-41, this is when TOPS sends the AnalyzedInformation RETURN RESULT with an Action Code of “disconnect call.”. In GSM, this is when TOPS sends the DisconnectTemporaryConnection.

This register is not normally pegged on an IS-41 call. When it is, it indicates the caller did not receive ADACC with release.

This register is pegged on all successful GSM wireless ADACC with release calls.

7.5.11.2 Register release history update

Created in SN07

7.5.11.3 Associated registers

Extension register DISCONN2

7.5.11.4 Associated logs

None

7.5.12 Register ERRCONN

7.5.12.1 Register description

Error Connect

ERRCONN is a peg register. It is incremented on a WIN call when the MSC cannot connect to TOPS using the TLDN provided by TOPS. This might be due to translation or circuit failures at the MSC or in the network.

7.5.12.2 Register release history update

Created in SN07

7.5.12.3 Associated registers

None

7.5.12.4 Associated logs

TOPS131

7.5.13 Register ERRDISC

7.5.13.1 Register description

Error Disconnect

ERRDISC is a peg register. It is incremented on a WIN call when TOPS unexpectedly releases its trunk to the MSC. This register is only pegged on an IS-41 call. On a GSM call, registers WINBEGIN, REQCONN, and WINEND are pegged, but not DISCONN and CONNECT.

7.5.13.2 Register release history update

Created in SN07

7.5.13.3 Associated registers

None

7.5.13.4 Associated logs

TOPS131

7.5.14 Register ERRSSFT

7.5.14.1 Register description

Error Service Switching Function Timer

ERRSSFT is a peg register. It is incremented on a WIN call when the MSC's SSFT timer expires. This timer ensures TOPS does not take too long to process the WIN call. TOPS can reset this timer using the ResetTimer message. This message is controlled by datafill in Table ISUPTRK.

7.5.14.2 Register release history update
Created in SN07

7.5.14.3 Associated registers
None

7.5.14.4 Associated logs
TOPS131

7.5.15 Register NODATA

7.5.15.1 Register description
No TCAP data

This is a peg register which is incremented whenever TOPS cannot locate a call's IS-41 or GSM TCAP data in the temporary table. See the error scenarios in the Functional Description chapter of this document for more information.

7.5.15.2 Register release history update
Created in SN07.

7.5.15.3 Associated registers
Register RXLAFAIL is always pegged when register NODATA is pegged, since the original called number cannot be determined, and a default of 411 must be used.

7.5.15.4 Associated logs
TOPS131

7.5.16 Register NOTLDNS

7.5.16.1 Register description
No temporary local directory numbers

This is a peg register which is incremented whenever TOPS cannot obtain an idle temporary local directory number (TLDN) from Table TOPSTLDN. See the error scenarios in the Functional Description chapter of this document for more information.

7.5.16.2 Register release history update
Created in SN07.

7.5.16.3 Associated registers
None.

7.5.16.4 Associated logs
TOPS131

7.5.17 Register REQCONN

7.5.17.1 Register description

Request Connection

This is a peg register which is incremented whenever TOPS sends an IS-41 ConnectResource or GSM EstablishTemporaryConnetcion to the MSC.

7.5.17.2 Register release history update

Created in SN07.

7.5.17.3 Associated registers

Extension register REQCONN2

7.5.17.4 Associated logs

None.

7.5.18 Register RESTIMR

7.5.18.1 Register description

ResetTimer

This is a peg register which is incremented whenever TOPS sends an IS-41 or GSM ResetTimer to the MSC.

7.5.18.2 Register release history update

Created in SN07.

7.5.18.3 Associated registers

Extension register RESTIMR2

7.5.18.4 Associated logs

None.

7.5.19 Register RXLAFAIL

7.5.19.1 Register description

Retranslation Failure

This is a peg register which is incremented when a TOPS IS-41 or GSM call arrives, but TOPS cannot find the original called number and must use a default of 411. This register can be pegged in conjunction with NODATA, if the reason the original called number cannot be found is that there is no extension block.

7.5.19.2 Register release history update

Created in SN07.

7.5.19.3 Associated registers

None.

7.5.19.4 Associated logs

A TOPS131 is generated if the reason for using the default 411 is that the TCAP data was not found.

7.5.20 Register SANTIMR

7.5.20.1 Register description

TOPS sanity timer expiration

This is a peg register which is incremented whenever the TOPS IS-41 or GSM call end sanity timer expires. TOPS starts this timer after sending the IS-41 AnalyzedInformation RETURN RESULT or GSM Connect to the MSC. If the MSC does not release the trunk and end the TOPS call before the timer expires, TOPS ends its call and frees resources.

7.5.20.2 Register release history update

Created in SN07.

7.5.20.3 Associated registers

None.

7.5.20.4 Associated logs

TOPS131

7.5.21 Register TLDNTIME

7.5.21.1 Register description

TLDN time-out

This is a peg register which is incremented whenever the TOPS IS-41 or GSM SCP process finds a TLDN which has been allocated for more than 30 seconds. The TLDN is idled, then selected for use by the next TOPS IS-41 or GSM call. This allows the TLDN list to be cleaned up if some MSC calls end before routing to TOPS.

7.5.21.2 Register release history update

Created in SN07.

7.5.21.3 Associated registers

None.

7.5.21.4 Associated logs

None.

7.5.22 Register WINBEGIN

7.5.22.1 Register description

Wireless Intelligent Network Begin

This is a peg register which is incremented whenever TOPS receives an IS-41 AnalyzedInformation or a GSM InitialDP from an MSC. This signifies the beginning of the WIN TOPS call.

7.5.22.2 Register release history update

Created in SN07.

7.5.22.3 Associated registers

Extension register WINBEGI2

7.5.22.4 Associated logs

None.

7.5.23 Register WINEND

7.5.23.1 Register description

Wireless Intelligent Network End

This is a peg register which is incremented whenever TOPS receives a GSM Application End from the MSC. This signifies the end of a successful WIN TOPS call.

This message is not used in the IS-41 call flow, so this OM is not pegged for IS-41 TOPS calls.

Register DARLT in group TOPSISUP can also be used to count instances of successful ADACC with RLT.

7.5.23.2 Register release history update

Created in SN07.

7.5.23.3 Associated registers

Extension register WINEND

7.5.23.4 Associated logs

None

7.6 OM group TC7WRLSS

7.6.1 OM description

TC7WRLSS

TOPS - Common Channel Signalling System #7 - Wireless

7.6.2 Release history update

Created in SN07

7.6.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 3 OM Group Display

INVOKES	INVOKES2	INVOKER	INVOKER2
RETRESS	RETRESS2	RETRESR	RETRESR2
RETERRS	RETERRR	REJECTS	REJECTR
ABORTS	ABORTR	NOTRIDS	MBFULL
RTFNOXLA	RTFNOXLS	RTFSUBCG	RTFSUBFL
RTFUNEQ	RTFNETFL	RTFNETCG	RTFMISCE
GTTFAIL			

7.6.4 Group structure

OM group TC7WRLSS provides one tuple for each combination of wireless network type and TOPS wireless application.

Key field: There are four tuples as follows:

- SMS_IS41
- SMS_GSM
- WIN_IS41
- WIN_GSM

Info field: None

7.6.5 Associated OM groups

Registers in groups SMSTOPS and WINTOPS are also pegged during wireless TOPS calls.

7.6.6 Associated functional groups

None

7.6.7 Associated functionality codes

Table 5 Functionality codes associated with OM group

Functionality	Code
TOPS Wireless RLT	00034426

7.6.8 OM group registers logic flow chart

7.6.8.1 SMS TOPS calls

Register INVOKES is pegged when TOPS sends a short message into the SS7 network.

Register RETRESR is pegged when TOPS receives a positive or negative acknowledgment from the message center (MC). Group SMSTOPS has registers indicating SMS failure has occurred.

The remainder of the registers are pegged in failure scenarios. If registers GTTFAIL or NOTRIDS are being pegged, this means SMS messages are not being sent due to failure at TOPS. If registers beginning with “RTF” (route failure) are being pegged, failures are occurring in the SS7 network before the SMS arrives at the MC.

7.6.8.2 WIN TOPS calls

A successful WIN TOPS call should peg only registers INVOKES, INVOKER, and RETRESS.

The remainder of the registers are pegged in failure scenarios. If registers GTTFAIL or NOTRIDS are being pegged, this means WIN TOPS messages are not being sent due to failures at TOPS. If registers beginning with “RTF” (route failure) are being pegged, failures are occurring in the SS7 network before the TOPS message arrives at the MSC.

7.6.9 Register ABORTR

7.6.9.1 Register description

Abort Received

ABORTR is a peg register. It is incremented whenever TOPS receives a TCAP ABORT.

7.6.9.2 Register release history update

Created in SN07

7.6.9.3 Associated registers

None

7.6.9.4 Associated logs
TCAP100

7.6.10 Register ABORTS

7.6.10.1 Register description
Abort Sent

ABORTS is a peg register. It is incremented whenever TOPS sends a TCAP ABORT.

7.6.10.2 Register release history update
Created in SN07

7.6.10.3 Associated registers
None

7.6.10.4 Associated logs
TCAP100

7.6.11 Register GTTFAIL

7.6.11.1 Register description
Global Title Translation Failure

GTTFAIL is a peg register. It is incremented whenever TOPS cannot look up GTT information for a destination number. The GTT information is datafilled in Tables C7GTTYPE and C7GTT. When TOPS cannot obtain this information, it cannot send the SMS into the network. The operator or automated node receives a failure indication.

A TOPS131 log is generated containing the destination number which caused the failure. Table C7GTT must be updated to include the destination number.

7.6.11.2 Register release history update
Created in SN07

7.6.11.3 Associated registers
None

7.6.11.4 Associated logs
TOPS131

7.6.12 Register INVOKER

7.6.12.1 Register description
INVOKE Received

INVOKER is a peg register. It is incremented whenever TOPS receives a TCAP INVOKE.

7.6.12.2 Register release history update
Created in SN07

7.6.12.3 Associated registers
Extension register INVOKER2

7.6.12.4 Associated logs
None

7.6.13 Register INVOKES

7.6.13.1 Register description
INVOKE Sent

INVOKES is a peg register. It is incremented whenever TOPS sends a TCAP INVOKE.

7.6.13.2 Register release history update
Created in SN07

7.6.13.3 Associated registers
Extension register INVOKES2

7.6.13.4 Associated logs
None

7.6.14 Register MBFULL

7.6.14.1 Register description
Mailbox full

This is a peg register which is incremented whenever a TOPS IS-41 or GSM TCAP message arrives at the TOPS SCP interrupt handler but cannot be sent to the TOPS SCP process due to heavy switch load. This means TOPS is receiving more IS-41 or GSM traffic than it can handle.

On wireless DA calls, the incoming message is ignored, which will result in calls going to treatment in the MSC. It is not anticipated that TOPS IS-41 or GSM messaging will ever be high enough to peg this register. If this register is pegged, contact Nortel Networks to increase the number of internal mailboxes available to the TOPS IS-41 SCP application.

7.6.14.2 Register release history update
Created in SN07.

7.6.14.3 Associated registers
None.

7.6.14.4 Associated logs
None. Generating a log under these circumstances would further degrade switch performance.

7.6.15 Register NOTRIDS

7.6.15.1 Register description
No transaction identifiers

NOTRIDS is a peg register. It is incremented whenever TOPS attempts to send an IS-41 or GSM TCAP message but cannot because no transaction identifiers (TRIDs) are available. Each TCAP operation requires a TRID to process the response.

TRIDs are allocated automatically by the DMS, so if this register is pegged, contact Nortel Networks.

7.6.15.2 Register release history update
Created in SN07

7.6.15.3 Associated registers
None

7.6.15.4 Associated logs
TOPS131

7.6.16 Register REJECTR

7.6.16.1 Register description
REJECT received

REJECTR is a peg register. It is incremented whenever TOPS receives a TCAP REJECT from the MSC or MC. This indicates a problem with the TCAP message sent by TOPS, so Nortel Networks should be contacted.

7.6.16.2 Register release history update
Created in SN07

7.6.16.3 Associated registers
None

7.6.16.4 Associated logs
TCAP100

7.6.17 Register REJECTS

7.6.17.1 Register description
REJECT sent

REJECTS is a peg register. It is incremented whenever TOPS sends a TCAP REJECT to the MSC. This indicates a problem with the TCAP message sent by the MSC, so the MSC's vendor should be contacted.

7.6.17.2 Register release history update
Created in SN07

7.6.17.3 Associated registers
None

7.6.17.4 Associated logs
TCAP100

7.6.18 Register RETERRR

7.6.18.1 Register description
RETURN ERROR received

RETERRR is a peg register. It is incremented whenever TOPS receives a TCAP RETURN ERROR from the MSC. This might indicate a problem on the MSC or TOPS switches, so logs at both switches should be investigated.

7.6.18.2 Register release history update
Created in SN07

7.6.18.3 Associated registers
None

7.6.18.4 Associated logs
TCAP100

7.6.19 Register RETERRS

7.6.19.1 Register description
RETURN ERROR sent

RETERRS is a peg register. It is incremented whenever TOPS sends a TCAP RETURN ERROR to the MSC. This might indicate a problem on the MSC or TOPS switches, so logs at both switches should be investigated.

7.6.19.2 Register release history update
Created in SN07

7.6.19.3 Associated registers
None

7.6.19.4 Associated logs
TCAP100

7.6.20 Register RETRESR

7.6.20.1 Register description
RETURN RESULT received

RETRESR is a peg register. It is incremented whenever TOPS receives a TCAP RETURN RESULT from the MC.

7.6.20.2 Register release history update
Created in SN07

7.6.20.3 Associated registers
Extension register RETRESR2

7.6.20.4 Associated logs
None

7.6.21 Register RETRESS

7.6.21.1 Register description
RETURN RESULT sent

RETRESS is a peg register. It is incremented whenever TOPS sends a TCAP RETURN RESULT to the MSC.

7.6.21.2 Register release history update
Created in SN07

7.6.21.3 Associated registers
Extension register RETRESS2

7.6.21.4 Associated logs
None

7.6.22 Register RTFMISCE

7.6.22.1 Register description
SCCP routing failure: Miscellaneous failure

This is a peg register which is incremented when the TOPS IS-41 SCP process receives a UDTS message containing a diagnostic other than the next seven.

7.6.22.2 Register release history update
Created in TOPS19 (SN06).

7.6.22.3 Associated registers
None.

7.6.22.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

7.6.23 Register RTFNETCG

7.6.23.1 Register description
SCCP routing failure: Network congestion

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating “network congestion”.

7.6.23.2 Register release history update
Created in SN07.

7.6.23.3 Associated registers
None.

7.6.23.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

7.6.24 Register RTFNETFL

7.6.24.1 Register description
SCCP routing failure: Network failure

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating “network failure”.

7.6.24.2 Register release history update
Created in SN07.

7.6.24.3 Associated registers
None.

7.6.24.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

7.6.25 Register RTFNOXLA

7.6.25.1 Register description

SCCP routing failure: No translation of such nature

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating “no translation of such nature”.

7.6.25.2 Register release history update

Created in SN07.

7.6.25.3 Associated registers

None.

7.6.25.4 Associated logs

A TCAP101 log is generated containing the incoming UDTS message.

7.6.26 Register RTFNOXLS

7.6.26.1 Register description

SCCP routing failure: No translation for this specific address

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating “no translation for this specific address”.

7.6.26.2 Register release history update

Created in SN07.

7.6.26.3 Associated registers

None.

7.6.26.4 Associated logs

A TCAP101 log is generated containing the incoming UDTS message.

7.6.27 Register RTFSUBCG

7.6.27.1 Register description

SCCP routing failure: Subsystem congestion

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating “subsystem congestion”.

7.6.27.2 Register release history update

Created in SN07.

7.6.27.3 Associated registers
None.

7.6.27.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

7.6.28 Register RTFSUBFL

7.6.28.1 Register description
SCCP routing failure: Subsystem failure

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating "subsystem failure".

7.6.28.2 Register release history update
Created in SN07.

7.6.28.3 Associated registers
None.

7.6.28.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

7.6.29 Register RTFUNEQ

7.6.29.1 Register description
SCCP routing failure: Unequipped user

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTS message containing a diagnostic indicating "unequipped user".

7.6.29.2 Register release history update
Created in SN07.

7.6.29.3 Associated registers
None.

7.6.29.4 Associated logs
A TCAP101 log is generated containing the incoming UDTS message.

8: Performance (PF): A00003767

8.1 Performance management strategy

The strategy is to collect useful counts for each SCTP association on the ABI cards on the MG9K. The OMs that will be collected will be collected in 15 minute samples and will have a history of the last 96 samples collected. The currently being collected sample will also be visible. The OMs currently being collected will only be viewable from a dshell command on the MG9K ABI card or through a MIB browser. The historical in addition to these methods will also be saved in the MG9K OM journal.

8.2 Performance management tools and utilities

The MG9K will collect the MIB info for the current and historical OMs. The historical OMs will be saved in the OM journal on the MG9K. All the MIBs can also be viewed through a MIB browser and can also be seen using Dshell commands on the ABI card.

8.3 Performance Measurements (PM), Operational Measurements (OM), and stats

NORTEL-UEMG-RELMSGING-MIB

8.3.1 PM, OM, and stats format

Component: MG9K ABI card

History: New MIB in SN07

MIB object type: columnar, there is one MIB instance per SCTP association

MIB syntax:

NnRelMsgSctpAssocOmCurrEntry has the following entries all are 32 bit counters:

nnRelMsgSctpAscCurrClosed: Times the association has been closed

nnRelMsgSctpAscCurrAbort: Times the association has been aborted

nnRelMsgSctpAscCurrOutPacks: Number of packets sent out

nnRelMsgSctpAscCurrInPacks: Number of packets received

nnRelMsgSctpAscCurrDiscPacks: Number of packets discarded

nnRelMsgSctpAscCurrRetranPacks: Number of packets retransmitted

nnRelMsgSctpAscCurrT1expires: Number of times the T1 timer expired

nnRelMsgSctpAscCurrT2expires: Number of times the T2 timer expired

nnRelMsgSctpAscCurrT3expires: Number of times the T3 timer expired

nnRelMsgSctpAscCurrCongCount: Times the association became congested

nnRelMsgSctpAscCurrCongCleared: Times the association cleared congestion

NnRelMsgSctpAssocOmIntervEntry has the following entries all are 32 bit counters:

nnRelMsgSctpAscInterval: Historical intervals 1-96 with 96 the oldest

nnRelMsgSctpAscIntervClosed: Times the association has been closed

nnRelMsgSctpAscIntervAbort: Times the association has been aborted

nnRelMsgSctpAscIntervOutPacks: Number of packets sent out

nnRelMsgSctpAscIntervInPacks: Number of packets received

nnRelMsgSctpAscIntervDiscPacks: Number of packets discarded

nnRelMsgSctpAscIntervRetranPacks: Number of packets retransmitted

nnRelMsgSctpAscIntervT1expires: Number of times the T1 timer expired

nnRelMsgSctpAscIntervT2expires: Number of times the T2 timer expired

nnRelMsgSctpAscIntervT3expires: Number of times the T3 timer expired

nnRelMsgSctpAscIntervCongCount: Times the association became congested

nnRelMsgSctpAscIntervCongCleared: Times the association cleared congestion

8.3.2 OM Group template (applies only to DMS)

NA

8.3.2.1 OM description

NA

8.3.2.2 Release history update

The OM group is being modified in

8.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

<regName> <regName> <regName> <regName>

8.3.2.4 Group structure

OM group provides <tuple> tuple(s) for each <element>.

Key field: <KField><description>

Info field: <IField><description>

8.3.2.5 Associated OM groups

<None>

8.3.2.6 Associated functional groups

The following functional groups are associated with OM group: <None>

8.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code

8.3.2.8 OM group registers logic flow chart

8.3.3 Register (applies only to DMS)

NA

8.3.3.1 Register description

NA

8.3.3.2 Register release history update

NA

8.3.3.3 Associated registers

<None>

Example:
OFZ_ORGFSET

8.3.3.4 Associated logs

The SCTP threshold alarms being added are indirectly based off of several on the OMs being collected in the MIB. The MIB field nnRelMsgSctpAscCurrRetranPacks in nnRelMsgSctpAssocOmCurrTable will show the number of retransmissions being collected in the current sample. Likewise the nnRelMsgSctpAscIntervRetranPacks in NnRelMsgSctpAssocOmIntervEntry will supply the historical counts for the

last 96 15 minute periods that were collected. Both of these can be used to the relMsgLinkDegraded alarm for crossing the retransmission threshold.

The relMsgLinkSevDegraded will also correlate to the crossing of the message loss threshold and will relate to the following MIB fields. nnRelMsgSctpAscCurrDiscPacks in NnRelMsgSctpAssocOmCurrEntry for the currently being collected sample and nnRelMsgSctpAscIntervDiscPacks in NnRelMsgSctpAssocOmIntervEntry for the historical samples.

The nnRelMsgSctpAscCurrClosed and nnRelMsgSctpAscCurrAbort in NnRelMsgSctpAssocOmCurrEntry for the currently being collected sample relate to the relMsgLinkFail alarm for when the SCTP association fails and prevents reliable messaging.This will also be shown by the nnRelMsgSctpAscIntervClosed and nnRelMsgSctpAscIntervClosed in NnRelMsgSctpAssocOmIntervEntry for the historical samples

9: Performance (PF): A00003773

9.1 Performance management strategy

This capability allows QOS monitoring for MG4K-IP based trunks.

9.2 Performance management tools and utilities

The activity A89007725 in SN06, '*Trunk Group based QoS OM'* provided a new trunk group based operational measurement group (TRKQOSOM) on the Succession Call Server. This feature A00003773-'*OM FOR TRKQOS FOR MG4K IP'*, extends trunk group based QoS OM support to MG4K-IP.

QOS threshold values for packet loss, jitter, and delay (latency) shall be datafilled in table OFCVAR tuple PACKET_QOS_OM_THREHSOLDS.

When the capability is enabled via datafilling PACKET_QOS_OM_THREHSOLDS in table OFCVAR, QOS statistics for MG4K-IP based trunk calls will be monitored. If any of the threshold values (jitter, delay, loss) are exceeded for the call, the data for that trunk group in OM group TRKQOSOM will be incremented.

To view the TRKQOSOM data, use the OMSHOW CI command as follows:

```
>OMSHOW TRKQOSOM ACTIVE
```

9.3 Performance Measurements (PM), Operational Measurements (OM), and stats

9.3.1 PM, OM, and stats format

TRKQOSOM:

Components: GWC and MG4K-IP based TDM Trunk Groups

Performance Measurement Name: TRKQOSOM

Performance Measurement Description: Presents QOS threshold crossing counts on a per trunk group basis. Counts presented include JITTER, DELAY, and PACKETLOSS.

History: The TRKQOSOM OM group was created in SN06 for GWC trunk groups. When this feature completes in SN07.1, this OM group will support both GWC and MG4K-IP based TDM trunk groups.

9.3.2 OM Group template

9.3.2.1 OM description

TRKQOSOM -Trunk Quality Of Service Operational Measurement

9.3.2.2 Release history update

The TRKQOSOM OM group was created in SN06. TRKQOSOM OM group support for MG4K-IP based trunk groups is developed in SN07.1.

9.3.2.3 Registers

OM group registers display as follows:

Figure 1 OM Group Display for TRKQOSOM

PKTLOSS	JITTER	DELAY

9.3.2.4 Group structure

OM group provides one tuple for each MG4K-IP based trunk group.

Key field: Common Language Name (*CLLI*): A value corresponding to the entries in table *CLLI* for which MG4K-IP members have been datafilled.

Info field: None.

9.3.2.5 Associated OM groups

None.

9.3.2.6 Associated functional groups

None.

9.3.2.7 Associated functionality codes

None.

9.3.2.8 OM group registers logic flow chart

The registers in this group will be incremented if the QOS statistics collected at the end of a MG4K-IP based trunk call indicate that the statistic has exceeded the threshold value datafilled in table *OFCVAR* tuple *PACKET_QOS_OM_THRESHOLDS*.

9.3.3 Register

9.3.3.1 JITTER Register description

Register *JITTER*.

JITTER is a peg register used to indicate that the jitter QOS statistic for a call has exceeded the datafilled *JITTER* threshold in table *OFCVAR* - *PACKET_QOS_OM_THREHSOLDS*.

Interarrival time jitter is an estimate of the statistical variance of RTP data packet interarrival times. The Jitter value calculated as the smoothed mean absolute value of the difference between the sending interval at a source and the interarrival time at a receiver. It is a running filtered average, basically a low pass filter with a 1/16 contribution each sample.

$jitter_{new} = jitter_{old} + [(\text{instantaneous jitter} - jitter_{old}) / 16]$

Where, instantaneous jitter = $| [rec_i - rec_{i-1})] - [sent_i - sent_{i-1}] |$
rec_i / $sent_i$ = Time when i^{th} data packet is received/sent.

9.3.3.2 DELAY Register description

Register *DELAY.*

DELAY is a peg register used to indicate that the delay/latency QOS statistic for a call has exceeded the datafilled *DELAY* threshold in table *OFCVAR - PACKET_QOS_OM_THREHSOLDS*.

The round-trip delay is calculated when a RTCP reception report is received. The Delay (latency) is smoothed as,
$delay_{new} = delay_{old} + [(\text{instantaneous delay} - delay_{old}) / 16]$

Where instantaneous delay = | A - LSR - DLSR |
A = time a source received this reception report
LSR = last Send Report timestamp received field
DLSR = delay since last Send Report field

9.3.3.3 PKTLOSS Register description

Register *PKTLOSS*.

PKTLOSS is a peg register used to indicate that the packet loss QOS statistic for a call has exceeded the datafilled *LOSS* threshold in table *OFCVAR - PACKET_QOS_OM_THREHSOLDS*.

Packet loss rate is calculated in percentage as
[RtpCumulativeLostPackets *100] / [RtpPacketsReceived + RtpCumulativeLostPackets]

Where, RtpPacketsReceived - The number of the RTP packets received from the IP network.
RtpCumulativeLostPackets - The number of lost RTP packets in the receiving direction. The count represents the Cumulative Number of Packets Lost field that is inserted in to the RTCP reception blocks.

9.3.3.4 Register release history update

Registers are existing for GWC trunk groups from SN06. From SN07.1 these registers supports both GWC based TDM trunk groups and MG4K-IP based trunk groups.

9.3.3.5 Associated registers

None

9.3.3.6 Associated logs

A new log - *MG4K-IP OM Failure log,* shall be introduced by feature *A00003650 - 'MG4K-IP ECAN, SCTP and OM Failure logs'*. The QOS measurements shall be pegged on the GEM card per CLLI basis. The pegs are stored in 16 bit integers. If these overflow, then the MG4K-IP OM Failure log shall be generated with a reason. The reason code description for the log are Jitter peg overflow, Delay Peg Overflow, Packet Loss Peg Overflow. The pegs in the GEM shall be reset to 0 when this log is generated.

10: Performance (PF): A00004036

10.1 Performance management strategy

Not applicable.

10.2 Performance management tools and utilities

Not applicable.

10.3 Operational Measurements (OM)

This activity will not be enabling any new OMs, however, similar to operations performed due to service access code driven commands, existing OM groups/ registers will be pegged to reflect the relevant incremental update attempts for the same service. For example, an attempt to activate SCF via some off-board interface will be pegged as though the subscriber had gone off-hook and dialed the activation access code for SCF.

For clarity, the following sections will outline in detail what OMs, if any, will be pegged when a request for an off-board service update or change is being processed.

10.3.1 Group1 Services OM Group

The following sub-sections defined the OM groups associated with the Group1 services.

The service CSMI and LDS pegs perticular OM group. However, these OM groups are for CallP specific pegging. Therefore, for service control perspective they are not affected nor pegged.

Other Group1 services does not have any OM groups.

10.3.1.1 ACRJ OM Group

Operational Measures associated with the Anonymous Call Rejection service.

10.3.1.1.1 Release history update

Not Applicable

10.3.1.1.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.1.1.3 ACRJ OM Group Display

Figure 1 ACRJ OM Group Display

```
>omshow acrj active

ACRJ

CLASS: ACTIVE
START:2003/09/10 08:30:00 WED; STOP: 2003/09/10 09:55:39 WED;
SLOWSAMPLES:        5 ; FASTSAMPLES:       48 ;

      ACRJACT  ACRJDACT   ACRJANN  ACRJAUNV
     ACRJDUNV  ACRJDENY

  0
          0       0       0       0
          0       0
```

10.3.1.1.4 ACRJACT

Register ACRJACT (Anonymous Call Rejection Activation) will be pegged if the ACRJ Update message successfully activate the ACRJ service.

10.3.1.1.5 ACRJDACT

Register ACRJDACT (Anonymous Call Rejection Deactivation) will be pegged if the ACRJ Update message successfully deactivate the ACRJ service.

10.3.1.1.6 ACRJAUNV

Register ACRJAUNV (Anonymous Call Rejection Universal Activation) will be pegged if the ACRJ Update message successfully activate the usage based ACRJ service.

10.3.1.1.7 ACRJDUNV

Register ACRJDUNV (Anonymous Call Rejection Universal Deactivation) will be pegged if the ACRJ Update message successfully deactivate the usage based ACRJ service.

10.3.1.1.8 Register release history update

Not Applicable.

10.3.1.1.9 Associated registers

Not applicable.

10.3.1.1.10 Associated logs

<None>

10.3.1.2 AR OM Group

Operational Measures associated with the Automatic Recall service.

10.3.1.2.1 Release history update

Not Applicable

10.3.1.2.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.1.2.3 AR OM Group Display

Figure 2 AR OM Group Display

```
>omshow ar active

AR

CLASS: ACTIVE
START:2003/09/10 10:00:00 WED; STOP: 2003/09/10 10:13:33 WED;
SLOWSAMPLES:        1 ; FASTSAMPLES:        1 ;

        ARATT    ARFDEN    AROVFL    ARLTDA
       ARSTDA    ARSTDT    ARIMED    ARDLAY
       ARTIME    ARRSCN     ARSCR    ARDATT
       ARPRCD    AROPTO    ARBDIN     ARABT
       ARRACT     ARSTR    ARTSCN    AROSCN
        ARARN   ARNIMED    ARUNIV    ARDENY
     ARPVTBLK   ARPVTALW   ARDSBLID

  0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0
```

10.3.1.2.4 ARDATT

Register ARDATT (Automatic Recall Deactivation ATTempt) will be pegged if the AR Update message to deactivate AR service is received.

10.3.1.2.5 ARUNIV

Register ARUNIV (Automatic Recall Universal) will be pegged if the AR Update message to deactivate the Universal AR service is received.

10.3.1.2.6 Register release history update

Not Applicable.

10.3.1.2.7 Associated registers

Every time Universal AR deactivate request is received, both ARUNIV and ARDATT will be pegged.

10.3.1.2.8 Associated logs

<None>

10.3.1.3 ACB OM Group

Operational Measures associated with the Automatic Call Back service.

10.3.1.3.1 Release history update

Not Applicable

10.3.1.3.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.1.3.3 ACB OM Group Display

Figure 3 ACB OM Group Display

```
>omshow acb active

ACB

CLASS: ACTIVE
START:2003/09/10 08:30:00 WED; STOP: 2003/09/10 10:01:40 WED;
SLOWSAMPLES:        6 ; FASTSAMPLES:       52 ;

        ACBATT   ACBFDEN   ACBOVFL   ACBLTDA
       ACBSTDA   ACBSTDT   ACBIMED   ACBDLAY
       ACBTIME   ACBRSCN   ACBSCR    ACBDATT
        ACBABT   ACBRACT   ACBSTR    ACBTSCN
       ACBOSCN   ACBACBN   ACBNIMED  ACBUNIV
       ACBDENY

  0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0
```

10.3.1.3.4 ACBDATT

Register ACBDATT (Automatic Call Back Deactivation ATTempt) will be pegged if the ACB Update message to deactivate ACB service is received.

10.3.1.3.5 ACBUNIV

Register ACBUNIV (Automatic Call Back Universal) will be pegged if the ACB Update message to deactivate the Universal ACB service is received.

10.3.1.3.6 Register release history update

Not Applicable.

10.3.1.3.7 Associated registers

Every time Universal ACB deactivate request is received, both ACBUNIV and ACBDATT will be pegged.

10.3.1.3.8 Associated logs

<None>

10.3.2 Group2 Services OM Group

No OM generated for Group2. Therefore, no OM changes identified.

10.3.3 Group3 Services OM Group

Operational Measures associated with the Selective Call Rejection, Distinctive Ring/Call Waiting and Simultaneous Ringing services.

10.3.3.1 Release history update

Not Applicable

10.3.3.2 Registers used for SCRJ Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 4 SCRJ OM Group Display

```
>omshow scrj active

SCRJ

CLASS: ACTIVE
START:2003/10/31 11:30:00 FRI; STOP: 2003/10/31 11:58:19 FRI;
SLOWSAMPLES:       17 ; FASTSAMPLES:       170 ;

      SCRJEATT  SCRJEDEN  SCRJEOVF   SCRJACT
      SCRJDACT  SCRJEUSG  SCRJSAT   SCRJSAT2
      SCRJSDEN  SCRJSBLK  SCRJSRJT  SCRJUNIV
      SCRJDENY  SCRJAUNV  SCRJDUNV

  0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0

>
```

10.3.3.2.1 SCRJEATT

Register SCRJEATT (Selective Call ReJection Editing ATTempt) is pegged each time a subscriber updates his/her SCRJ programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SCRJEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCRJ list

- deletion of a DN from a subscriber's SCRJ list
- request to delete all DNs in a subscriber's SCRJ list
- request to delete all anonymous or private entries in a subscriber's SCRJ list

10.3.3.2.2 SCRJEDEN

Register SCRJEDEN (Selective Call ReJection Editing DENial) is pegged each time a subscriber's attempt to update his/her SCRJ programmed data via some edit session is denied. The SCRJEDEN register will be pegged when/if the following is true for a given SCRJ off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCRJ not ENABLED in table RESOFC

10.3.3.2.3 SCRJACT

Register SCRJACT (Selective Call ReJection ACTivation) is pegged each time a subscriber activates his/her SCRJ service. Similar to the operations performed via service access code controlled activation, the SCRJACT register will be pegged for each occurrance of the an off-board service update activation request.

10.3.3.2.4 SCRJDACT

Register SCRJDACT (Selective Call ReJection DeACTivation) is pegged each time a subscriber deactivates his/her SCRJ service. Similar to the operations performed via service access code controlled activation, the SCRJDACT register will be pegged for each occurrance of the an off-board service update deactivation request.

10.3.3.2.5 SCRJDENY

Register SCRJDENY (Selective Call ReJection DENY) is pegged each time a subscriber's attempt to update his/her SCRJ programmed data via some edit session is denied due to the presence of the DENY option. The SCRJDENY register will be pegged for each of the following off-board service update request attempts.

- DOR option present on the given SCRJ subscriber's line
- SCRJ enabled office wide and DENY SCRJ option present on the given subscriber's line

10.3.3.3 Registers used for DRCW Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 5 DRCW OM Group Display

```
>omshow drcw active

DRCW

CLASS: ACTIVE
START:2003/10/31 12:00:00 FRI; STOP: 2003/10/31 12:03:59 FRI;
SLOWSAMPLES:        3 ; FASTSAMPLES:        24 ;

     DRCWEATT  DRCWEDEN  DRCWEOVF   DRCWACT
     DRCWDACT  DRCWEUSG   DRCWSAT   DRCWSAT2
     DRCWSDEN  DRCWSBLK   DRCWRING   DRCWTATT
     DRCWTOVF  DRCWUNIV  DRCWDENY   DRCWAUNV
     DRCWDUNV

  0
          0      0      0      0
          0      0      0      0
          0      0      0      0
          0      0      0      0
          0

>
```

10.3.3.3.1 DRCWEATT

Register DRCWEATT (Distinctive Ringing Call Wait Editing ATTempt) is pegged each time a subscriber updates his/her DRCW programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the DRCWEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's DRCW list
- deletion of a DN from a subscriber's DRCW list
- request to delete all DNs in a subscriber's DRCW list
- request to delete all anonymous or private entries in a subscriber's DRCW list

10.3.3.3.2 DRCWEDEN

Register DRCWEDEN (Distinctive Ringing Call Wait Editing DENial) is pegged each time a subscriber's attempt to update his/her DRCW programmed data via some edit session is denied. The DRCWEDEN register will be pegged when/if the following is true for a given DRCW off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

10.3.3.3.3 DRCWACT

Register DRCWACT (Distinctive Ringing Call Wait ACTivation) is pegged each time a subscriber activates his/her DRCW service. Similar to the operations performed via service access code controlled activation, the DRCWACT register will be pegged for each occurrance of the an off-board service update activation request.

10.3.3.3.4 DRCWDACT

Register DRCWDACT (Distinctive Ringing Call Wait DeACTivation) is pegged each time a subscriber deactivates his/her DRCW service. Similar to the operations performed via service access code controlled activation, the DRCWDACT register will be pegged for each occurrance of the an off-board service update deactivation request.

10.3.3.3.5 DRCWDENY

Register DRCWDENY (Distinctive Ringing Call Wait DENY) is pegged each time a subscriber's attempt to update his/her DRCW programmed data via some edit session is denied due to the presence of the DENY option. The DRCWDENY register will be pegged when/if the following is true for a given DRCW off-board service update request.

- DOR option present on the given DRCW subscriber's line
- DRCW enabled office wide and DENY SCA option present on the given subscriber's line

10.3.3.4 Registers used for SimRing Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 6 SimRing OM Group Display

```
>omshow simring active

SIMRING

CLASS: ACTIVE
START:2003/10/31 12:00:00 FRI; STOP: 2003/10/31 12:08:27 FRI;
SLOWSAMPLES:        6 ; FASTSAMPLES:        51 ;

      SIMRACT   SIMRDACT   SIMREATT   SIMREDEN
      SIMREOVF    SIMRINV   SIMRFAIL

   0
           0       0       0       0
           0       0       0

>
```

10.3.3.4.1 SIMRACT

Register SIMRACT (SIMultaneous Ringing ACTivation) is pegged each time a subscriber activates his/her SIMRing service. Similar to the operations performed via service access code controlled activation, the SIMRACT register will be pegged for each occurrance of the an off-board service update activation request.

10.3.3.4.2 SIMRDACT

Register SIMRDACT (SIMultaneous Ringing DeACTivation) is pegged each time a subscriber deactivates his/her SIMRing service. Similar to the operations performed via service access code controlled activation, the SIMRDACT register will be pegged for each occurrance of the an off-board service update deactivation request.

10.3.3.4.3 SIMREATT

Register SIMREATT (SIMultaneous Ringing Editing ATTempt) is pegged each time a subscriber updates his/her SIMRing programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SIMREATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SIMRing list
- deletion of a DN from a subscriber's SIMRing list

10.3.3.4.4 SIMREDEN

Register SIMREDEN (SIMultaneous Ringing Editing DENial) is pegged each time a subscriber's attempt to update his/her SIMRing programmed data via

some edit session is denied. The SIMREDEN register will be pegged when/if the following is true for a given SIMRing off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

10.3.3.5 Register release history update

Not Applicable.

10.3.3.6 Associated registers

Not applicable.

10.3.3.7 Associated logs

<None>

10.3.4 Group4 Services OM Group

Operational Measures associated with the Call Forwarding service. Activation and deactivation OMs exist only for POTS CFW. There are no current OMs for RES/IBN CFW activation and deactivation. There are no current OMs for any type of Call Forward Busy or Don't Answer (POTS or RES/IBN).

This service does not operate in a call processing environment. Therefore no call processing related OM will be pegged. Examples of those are OTS (Office Traffic Summary) and traffic separation pegs.

10.3.4.1 Release history update

Not Applicable

10.3.4.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 7 CFWPOTS OM Group Display

```
>omshow cfwpots active
CFWPOTS
CLASS: ACTIVE
START:2003/10/03 09:00:00 FRI; STOP: 2003/10/03 09:06:39 FRI;
SLOWSAMPLES:        4 ; FASTSAMPLES:        40 ;
      CFWPAATT   CFWPSUC1   CFWPSUC2   CFPAOVFL
      CFPADENY   CFWPFATT   CFPFOVFL   CFPFDENY
       CFWSOV    CFBPATT   CFBPDENY   CFBPOVFL
       CFBPSOV   CFDPATT1   CFDPATT2   CFDPDENY
      CFDPOVFL   CFDPCNC1   CFDPCNC2    CFDPSOV
      CFDPFAIL
  0
            1        1        0        0
            0        0        0        0
            0        0        0        0
            0        0        0        0
            0        0        0        0
            0
```

10.3.4.3 CFWPAATT

Register CFWPAATT will be pegged for each activation attempt for POTS CFW.

10.3.4.4 CFWPSUC1

Register CFWPSUC1 will be pegged each time activation of POTS CFW is successful. Register CFWPSUC2 which is pegged when the courtesy call is successful during POTS CFW programming and activation will not be pegged by this service because courtesy calls are not supported.

10.3.4.5 CFPADENY

Register CFPADENY is pegged while attempting to set a forward to DN and the forward to DN fails validation for any reason.

10.3.4.6 CFPAOVFL

Register CFPAOVFL is pegged if there is some software or data storage problem with storing the forward to DN after it has been validated successfully.

10.3.4.7 Register release history update

Not Applicable.

10.3.4.8 Associated registers

Not applicable.

10.3.4.9 Associated logs

<None>

10.3.5 Group5 Services OM Group

Operational Measures associated with the Selective Call Forwarding and Selective Call Acceptance services.

10.3.5.1 Release history update

Not Applicable

10.3.5.2 Registers used for SCF Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 8 SCF OM Group Display

```
>omshow scf active

SCF

CLASS: ACTIVE
START:2003/08/27 09:30:00 WED; STOP: 2003/08/27 09:31:39 WED;
SLOWSAMPLES:        1 ; FASTSAMPLES:        10 ;

      SCFEATT   SCFEOVF SCFEDEN   SCFEUSG
        SCFACT   SCFDACT    SCFFWD   SCFFWD2
       SCFSAT   SCFSAT2   SCFFAIL   SCFOVFL
     SCFSOVFL   SCFSDEN   SCFSBLK   SCFUNIV
      SCFDENY   SCFAUNV   SCFDUNV

  0
        0      0      0      0
        0      0      0      0
        0      0      0      0
        0      0      0      0
        0      0      0
>
```

10.3.5.2.1 SCFEATT

Register SCFEATT (Selective Call Forwarding Editing ATTempt) is pegged each time a subscriber updates his/her SCF programmed data via some edit session. Similar to the operations performed via service access code controlled

edit session, the SCFEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCF list
- deletion of a DN from a subscriber's SCF list
- request to delete all DNs in a subscriber's SCF list
- request to delete all anonymous or private entries in a subscriber's SCF list
- set the forwarding DN
- clear the forwarding DN

10.3.5.2.2 SCFEDEN

Register SCFEDEN (Selective Call Forwarding Editing DENial) is pegged each time a subscriber's attempt to update his/her SCF programmed data via some edit session is denied. The SCFEDEN register will be pegged when/if the following is true for a given SCF off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

10.3.5.2.3 SCFACT

Register SCFACT (Selective Call Forwarding ACTivation) is pegged each time a subscriber activates his/her SCF service. Similar to the operations performed via service access code controlled activation, the SCFACT register will be pegged for each occurrance of the an off-board service update activation request.

10.3.5.2.4 SCFDACT

Register SCFDACT (Selective Call Forwarding DeACTivation) is pegged each time a subscriber deactivates his/her SCF service. Similar to the operations performed via service access code controlled activation, the SCFDACT register will be pegged for each occurrance of the an off-board service update deactivation request.

10.3.5.2.5 SCFDENY

Register SCFDENY (Selective Call Forwarding DENY) is pegged each time a subscriber's attempt to update his/her SCF programmed data via some edit session is denied due to the presence of the DENY option. The SCFDENY register will be pegged for each of the following off-board service update request attempts.

- DOR option present on the given SCF subscriber's line

- SCF enabled office wide and DENY SCF option present on the given subscriber's line

10.3.5.3 Registers used for SCA Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

Figure 9 SCA OM Group Display

```
>omshow sca active

SCA

CLASS: ACTIVE
START:2003/10/30 16:00:00 THU; STOP: 2003/10/30 16:17:59 THU;
SLOWSAMPLES:       11 ; FASTSAMPLES:       108 ;

      SCAEATT   SCAEDEN   SCAEOVF    SCAACT
      SCADACT   SCAEUSG   SCASAT   SCASAT2
      SCASDEN   SCASBLK   SCASRJT  SCASRJT2
      SCASTRM   SCAUNIV   SCADENY   SCAAUNV
      SCADUNV

  0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0
```

10.3.5.3.1 SCAEATT

Register SCAEATT (Selective Call Acceptance Editing ATTempt) is pegged each time a subscriber updates his/her SCA programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SCAEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCA list
- deletion of a DN from a subscriber's SCA list
- request to delete all DNs in a subscriber's SCA list
- request to delete all anonymous or private entries in a subscriber's SCA list

10.3.5.3.2 SCAEDEN

Register SCAEDEN (Selective Call Acceptance Editing DENial) is pegged each time a subscriber's attempt to update his/her SCA programmed data via

some edit session is denied. The SCAEDEN register will be pegged when/if the following is true for a given SCA off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

10.3.5.3.3 SCAACT

Register SCAACT (Selective Call Acceptance ACTivation) is pegged each time a subscriber activates his/her SCA service. Similar to the operations performed via service access code controlled activation, the SCAACT register will be pegged for each occurrance of the an off-board service update activation request.

10.3.5.3.4 SCADACT

Register SCADACT (Selective Call Acceptance DeACTivation) is pegged each time a subscriber deactivates his/her SCA service. Similar to the operations performed via service access code controlled activation, the SCADACT register will be pegged for each occurrance of the an off-board service update deactivation request.

10.3.5.3.5 SCADENY

Register SCADENY (Selective Call Acceptance DENY) is pegged each time a subscriber's attempt to update his/her SCA programmed data via some edit session is denied due to the presence of the DENY option. The SCADENY register will be pegged when/if the following is true for a given SCA off-board service update request.

- DOR option present on the given SCA subscriber's line
- SCA enabled office wide and DENY SCA option present on the given subscriber's line

10.3.5.4 Register release history update

Not Applicable.

10.3.5.5 Associated registers

Not applicable.

10.3.5.6 Associated logs

<None>

10.3.6 Group6 Services OM Group

Operational Measures associated with the Call Forwarding Don't Answer Timer service.

10.3.6.1 Release history update

Not Applicable

10.3.6.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.6.3 SPRING OM Group Display

Figure 10 SPRING OM Group Display

```
> >omshow spring active

SPRING

CLASS: ACTIVE
START:2003/10/30 11:00:00 THU; STOP: 2003/10/30 11:05:57 THU;
SLOWSAMPLES:        4 ; FASTSAMPLES:        36 ;

      RCTRLLA   RCTRLRA   RCTRLSLA   RCTRLSRA
      RCTRLFA

  0
          0       0       0       0
          0
```

10.3.6.4 RCTRLLA

Register RCTRLLA(Ring ConTRoL Local Activation ATTempt) will be pegged if a CFDVT update request is received.

10.3.6.5 RCTRLSLA

Register RCTRLSLA (Ring ConTRoL Successful Local Activation) will be pegged each time the user is given access to update the CFDVT data whether or not the data is successfully altered or not.

10.3.6.6 RCTRLFA

Register RCTRLFA (Ring ConTRoL Local FAilure) will be pegged each time there is a failure due to unavailable resources.

10.3.6.6.1 Register release history update

Not Applicable.

10.3.6.6.2 Associated registers

Not applicable.

10.3.6.6.3 Associated logs

<None>

10.3.7 Group7 Services OM Group

No OM generated for Group7. Therefore, no OM changes identified.

10.3.8 Group8 Services OM Group

10.3.8.1 Customer Originated Trace (COT) OM Group

Operational Measures associated with the Customer Originated Trace (COT) service.

10.3.8.1.1 Release history update

Not Applicable

10.3.8.1.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.8.1.3 COT OM Group Display

Figure 11 COT OM Group Display

```
>omshow cot active

COT

CLASS: ACTIVE
START:2003/09/10 10:00:00 WED; STOP: 2003/09/10 10:21:58 WED;
SLOWSAMPLES:        1 ; FASTSAMPLES:        8 ;

      COTATT   COTFDEN   COTOVFL   COTCMPL
     COTINCM   COTPRCD   COTOPTO   COTBDIN
     COTPFLR   COTUNIV   COTDENY

  0
        0       0       0       0
        0       0       0       0
        0       0       0
```

10.3.8.1.4 COTATT

Register COTATT (Customer Originated Trace Activation Attempt) will be pegged if the COT Update message for the COT service is received.

10.3.8.1.5 COTUNIV

Register COTUNIV (Customer Originated Trace Universal) will be pegged if the COT Update message is received for the universal COT service.

10.3.8.1.6 Register release history update

Not Applicable.

10.3.8.1.7 Associated registers

Not applicable.

10.3.8.1.8 Associated logs

<None>

10.3.9 Group9 Services OM Group

10.3.9.1 Speed Call OM Group

Operational Measures associated with the Speed Calling service.

10.3.9.1.1 Release history update

Not Applicable

10.3.9.1.2 Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

10.3.9.1.3 POTS Speed Call, SC1 or SC2

Figure 12 SCPOTS OM Group Display

```
>omshow scpots active

SCPOTS

CLASS: ACTIVE
START:2003/10/24 10:00:00 FRI; STOP: 2003/10/24 10:22:51 FRI;
SLOWSAMPLES:       14 ; FASTSAMPLES:       137 ;

     KEY (SC_OM_TUPLES)
       SCPAATT  SCPAOVFL  SCPADENY   SCPFATT
       SCPFDENY

  0 SC1_TUPLE
          0       0       0       0
          0
  1 SC2_TUPLE
          0       0       0       0
          0
```

10.3.9.1.4 SCPAATT

Register SCPAATT (Speed Calling Program Activation ATTempt) will be pegged if the Speed Call Update message successfully added or changed a Speed Call DN.

10.3.9.1.5 SCAOVFL

Register SCAOVFL (Speed Calling Activation OVerFLow) is pegged if the Speed Call Update message failed to program the Speed Call Cell because of a lack of software resources; for example, a lack of HEAP memory in reserve for Speed Calling.

10.3.9.1.6 SCADENY

Register SCADENY (Speed Calling Activation DENY) is pegged if the Speed Call Update message failed to program or erase a Speed Call Cell because of an invalid Speed Call Cell number.

10.3.9.1.7 Register release history update

Not Applicable.

10.3.9.1.8 Associated registers

Not applicable.

10.3.9.1.9 Associated logs

<None>

10.3.9.2 Office Traffic Summary (OTS)

Figure 13 OTS OM Group Display

```
>omshow ots active

OTS

CLASS: ACTIVE
START:2003/10/24 10:00:00 FRI; STOP: 2003/10/24 10:22:51 FRI;
SLOWSAMPLES:       14 ; FASTSAMPLES:       137 ;

    KEY ( )
      NORG NORG2 ORGTRM ORGTRM2
      ORGOUT ORGOUT2 ORGTRMT ORGABDN
      ORGLKT ORGFSET ORGFSET2 NINC
      NINC2 INCTRM INCTRM2 INCOUT
      INCOUT2 INCTRMT INCABNM INCABNC
      INCLKT INCFSET NSYS NSYS2
      SYSTRM SYSOUT SYSTRMT SYSABDN
      SYSLKT SYSFSET

      0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0       0       0
        0       0
```

10.3.9.2.1 ORGFSET

Register ORGFSET (Originating Feature SET) is pegged when a Speed Call feature is successfully programmed by a user via the Speed Call Update message.

10.3.9.2.2 ORGTRMT

Register ORGTRMT (Originating Treatment) is pegged if the Speed Call Update message failed to program the Speed Call feature because of an error condition.

10.3.9.2.3 Register release history update

Not Applicable.

10.3.9.2.4 Associated registers

Not applicable.

10.3.9.2.5 Associated logs

<None>

11: Performance (PF): A00004271

11.1 Performance management strategy

The system needs to monitor and provide output as to whether the limit settings for SOCs CS2B0008 and CS2B0009 are being exceeded, as well as what the high water usage mark is for each. A new DMS OM group is the method chosen to capture this information.

11.2 Performance management tools and utilities

The DMS OM system.

11.3 Performance Measurements (PM), Operational Measurements (OM), and stats

11.3.1 PM, OM, and stats format

N/A

11.3.2 OM Group NGSSOM

11.3.2.1 OM description

The NGSSOM group provides information on the maximum number of simultaneous calls that utilize the NGSS platform as well as indication of the number of times the limit settings of the CS2B0008 and CS2B0009 usage SOCs have been exceeded.

11.3.2.2 Release history update

The OM group is created in SN07.

11.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

CS2CSHW	CS2CSHW2	CS2ASHW	CS2ASHW2
CS2CSOV	CS2CSOV2	CS2ASOV	CS2ASOV2

11.3.2.4 Group structure

OM group provides 1 tuple for the entire CS2K.

Key field: N/A

Info field: N/A

11.3.2.5 Associated OM groups

None

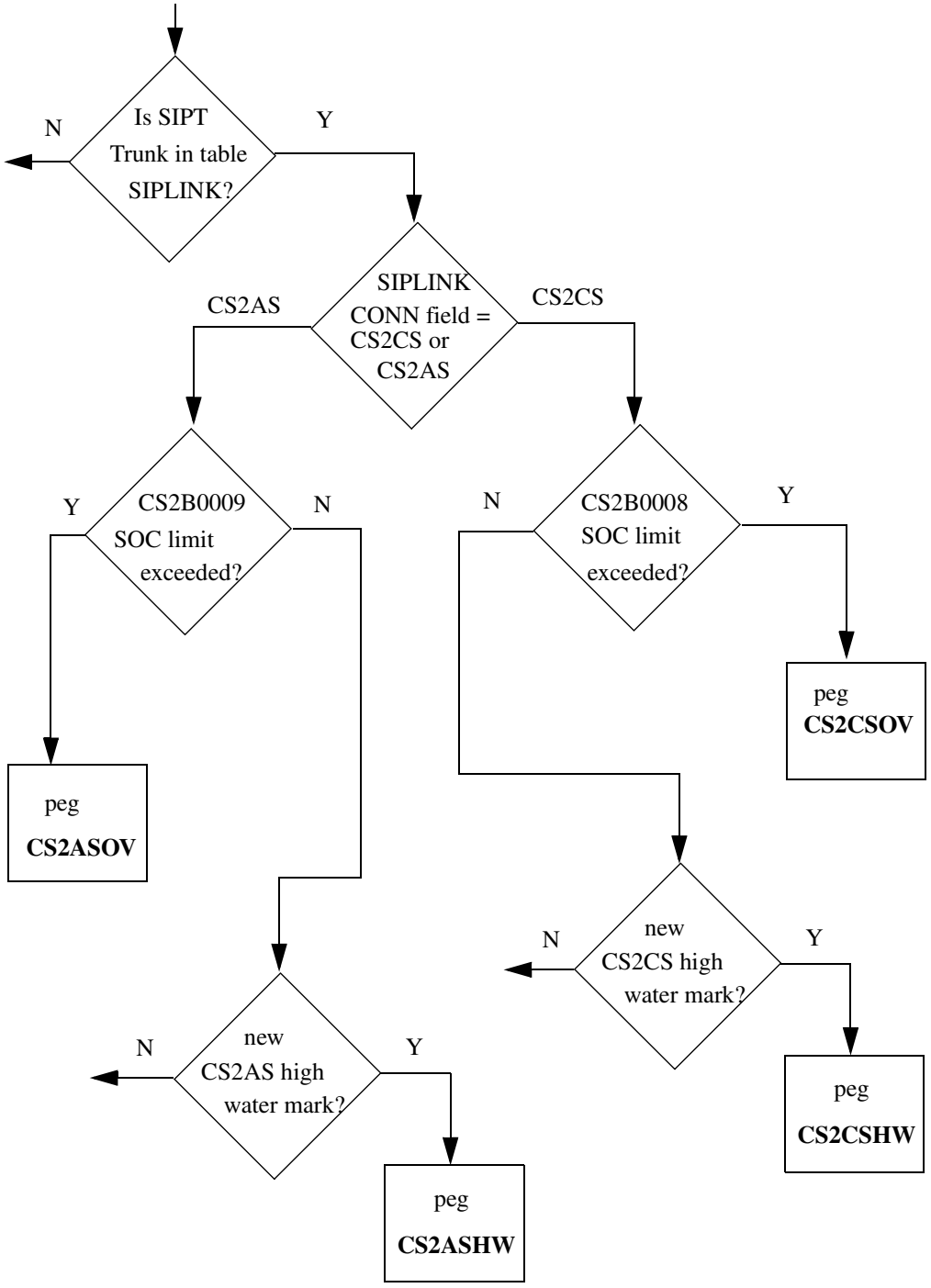
11.3.2.6 Associated functional groups

None

11.3.2.7 Associated functionality codes

None

11.3.2.8 NGSSOM registers logic flow chart



11.3.3 Register CS2CSHW

11.3.3.1 Register description

Holds the value of the highest number of simultaneous SIPT calls that utilize the NGSS platform to handle a call to or from another CS2K.

11.3.3.2 Register release history update

Register is created in SN07

11.3.3.3 Associated registers

Overflow register is CS2CSHW2

11.3.3.4 Associated logs

None

11.3.4 Register CS2CSOV

11.3.4.1 Register description

Holds the number of times a SIPT call did one of the following:

— attempted to utilize the NGSS platform to reach a far-end CS2K and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0008.

— was received from a far-end CS2K via the NGSS platform and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0008.

11.3.4.2 Register release history update

Register is created in SN07

11.3.4.3 Associated registers

Overflow register is CS2CSOV2

11.3.4.4 Associated logs

None

11.3.5 Register CS2ASHW

11.3.5.1 Register description

Holds the value of the highest number of simultaneous SIPT calls that utilize the NGSS platform to reach a far-end SIP application server.

11.3.5.2 Register release history update

Register is created in SN07.

11.3.5.3 Associated registers

Overflow register is CS2ASHW2

11.3.5.4 Associated logs

None

11.3.6 Register CS2ASOV

11.3.6.1 Register description

Holds the number of times a SIPT call did one of the following:

— attempted to utilize the NGSS platform to reach a far-end SIP application server and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0009.

— was received from a far-end SIP application server via the NGSS platform and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0009.

11.3.6.2 Register release history update

Register is created in SN07.

11.3.6.3 Associated registers

Overflow register is CS2ASOV2.

11.3.6.4 Associated logs

None

12: Performance (PF): A00004430

12.1 Performance management strategy

OM group AL1SVCOM is introduced in SN07. This OM group maintains OM peg counts for ATM SVC origination and ATM SVC failures on a nodal basis for SMG4, IW SPM, DPT SPM, MG9K, and MG9K ABI gateways.

Origination registers are pegged upon external network setup attempts by the Core. Failure registers are pegged when the Core receives ATM SVC failure messages from SMG4, IW SPM, DPT SPM, MG9K, and MG9K ABI gateways.

12.2 Performance management tools and utilities

12.3 Performance Measurements (PM), Operational Measurements (OM), and stats

12.3.1 PM, OM, and stats format

Component: Core OM group
Performance Measurement name: AL1SVCOM
Performance measurement description: AAL1 external network origination and failure pegs per node.
History: Created in SN07

12.3.2 OM Group - AL1SVCOM

Table 1 Registers for OM group AL1SVCOM

Register	Description
NOSVCAT	Number of SVC call attempts.
NOSVCAT2	Extension register for nosvcatt.
NOSVCFL	Number of SVC call failures.
ISSVCAT	Number of intraswitched (local) SVC call attempts
ISSVCAT2	Extension register for issvcsat.
ISSVCFL	Number of intraswitch (local) SVC call failures.
DPTSVCA	Number of interswitch (DPT) SVC call attempts.

Table 1 Registers for OM group AL1SVCOM

Register	Description
DPTSVCA2	Extension register for dptsvca.
DPTSVCF	Number of interswitch (DPT) SVC call failures.
NRTEDEST	ATM cause code 3 - no route to destination - SVC call failures.
NOUSRRES	ATM cause code 18 - no user responding - SVC call failures.
VPCINAVL	ATM cause code 35 - requested VPI/VCI not available - SVC call failures.
BWTHNAVL	ATM cause code 37 - user cell rate not available - SVC call failures.
TEMPFAIL	ATM cause code 41 - temp failure - SVC call failure reference.
RESUNAVL	ATM cause code 47 - Resource unavailable SVC call failure reference
OTH_CC	All other ATM cause codes SVC call failures.

12.3.2.1 OM group AL1SVCOM description

AL1SVCOM provides origination and failure register pegs, on a nodal basis, for SMG4, IW SPM, DPT SPM, MG9K, and MG9K ABI AAL1 external bearer path connections.

12.3.2.2 Release history update

SN07 - Introduced by activity A00004430.

12.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 AL1SVCOM - OM Group Display

```
AL1SVCOM

CLASS: ACTIVE
START:2004/02/14 11:10:00 SAT; STOP: 2004/02/14 11:11:21 SAT;
SLOWSAMPLES:        1 ; FASTSAMPLES:        8 ;

     KEY (SVC_OM_PM_INFO1)
     INFO (SVC_OM_TUPLE_DATA1)
       NOSVCAT   NOSVCAT2   NOSVCFL   ISSVCAT
      ISSVCAT2   ISSVCFL   DPTSVCA   DPTSVCA2
       DPTSVCF   NRTEDEST   NOUSRRES   VPCINAVL
       BWTHNAVL   TEMPFAIL   RESUNAVL    OTH_CC

   66
     SMG4 SPM    0
          0       0       0       0
          0       0       0       0
          0       0       0       0
          0       0       0       0
```

12.3.2.4 Group structure

OM group provides one tuple(s) for each node.

Key field: <SVC_OM_PM_INFO1><Refinement of OMINFOAREA, contains one field -> SVC_OM_TUPLE_DATA1.
>

Info field: <SVC_OM_TUPLE_DATA1>{<Node_name (eight characters)>, <device_name (fifteen characters)>}.

12.3.2.5 Associated OM groups

<None>

12.3.2.6 Associated functional groups

The following functional groups are associated with OM group: <None>

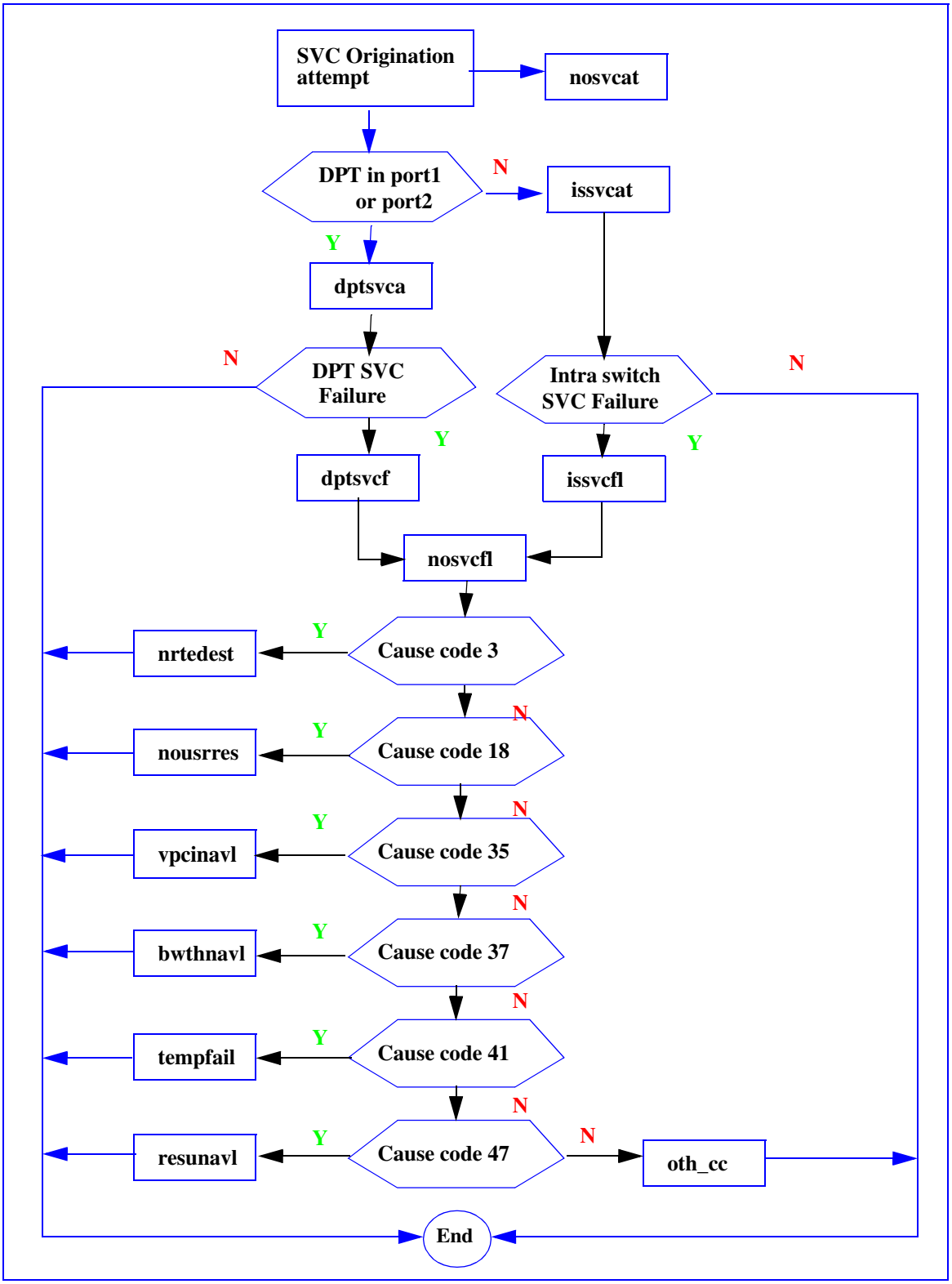
12.3.2.7 Associated functionality codes

Table 2 Functionality codes associated with OM group

Functionality	Code

12.3.2.8 OM group registers logic flow chart

Figure 2 AL1SVCFL OM Group Register Flow



12.3.3 Register BWTHNAVL

12.3.3.1 Register description

Bandwidth not available.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 37 (user cell rate not available).

12.3.3.2 Register release history update

Introduced in SN07.

12.3.3.3 Associated registers

ISSVCFL, DPTSVCF, NOSVCFL

12.3.3.4 Associated logs

XPKT301 or XPKT302.

12.3.4 Register DPTSVCA

12.3.4.1 Register description

Number of interswitch (DPT) SVC call attempts.

This register is pegged against an originating or terminating agent's node for SVC origination attempts, when the originating or terminating agent call processing selector is a DPT trunk.

12.3.4.2 Register release history update

Introduced in SN07.

12.3.4.3 Associated registers

NOSVCAT, ISSVCAT

DPTSVCA + ISSVCAT = NOSVCAT

12.3.4.4 Associated logs

<None>

12.3.5 Register DPTSVCF

12.3.5.1 Register description

Number of interswitch (DPT) SVC call failures.

This register is pegged against an originating or terminating agent's node when the originating or terminating agent call processing selector is a DPT trunk, and the SVC connection either fails during call setup, or is taken down for an established call.

12.3.5.2 Register release history update

Introduced in SN07.

12.3.5.3 Associated registers

NOSVCFL, ISSVCFL

DPTSVCF + ISSVCFL = NOSVCFL

12.3.5.4 Associated logs

XPKT301 or XPKT302.

12.3.6 Register ISSVCAT

12.3.6.1 Register description

Number of intraswitch SVC call attempts.

This register is pegged for each intraswitched external network bearer path SVC origination.

12.3.6.2 Register release history update

Introduced in SN07.

12.3.6.3 Associated registers

DPTSVCA, NOSVCAT

DPTSVCA + ISSVCAT = NOSVCAT

12.3.6.4 Associated logs

<None>

12.3.7 Register ISSVCFL

12.3.7.1 Register description

Number of intraswitch SVC connection failures.

This register is pegged for each intraswitch SVC connection failure that occurs during call setup, or for established connections.

12.3.7.2 Register release history update

Introduced in SN07.

12.3.7.3 Associated registers

DPTSVCF, NOSVCFL

DPTSVCF + ISSVCFL = NOSVCFL

12.3.7.4 Associated logs

XPKT301 or XPKT302.

12.3.8 Register NOSVCAT

12.3.8.1 Register description

Number of SVC attempts.

This register is pegged for each external network bearer path SVC origination, for each node.

12.3.8.2 Register release history update

Introduced in SN07.

12.3.8.3 Associated registers

ISSVCAT and DPTSVCA

ISSVCAT + DPTSVCA = NOSVCAT

12.3.8.4 Associated logs

<None>

12.3.9 Register NOSVCFL

12.3.9.1 Register description

Number of SVC connection failures.

This register is pegged for all SVC setup and established call connection failures against the node.

12.3.9.2 Register release history update
Introduced in SN07.

12.3.9.3 Associated registers
ISSVCFL and DPTSVCF

ISSVCFL + DPTSVCF = NOSVCFL

12.3.9.4 Associated logs
XPKT 301 and XPKT302.

12.3.10 Register NOUSRRES

12.3.10.1 Register description

No user responding SVC connection failure.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 18 (no user responding).

12.3.10.2 Register release history update
Introduced in SN07.

12.3.10.3 Associated registers
ISSVCFL, DPTSVCF, NOSVCFL

12.3.10.4 Associated logs
XPKT301 and XPKT302.

12.3.11 Register NRTEDEST

12.3.11.1 Register description

No route to destination SVC call failure.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 3 (no route to destination).

12.3.11.2 Register release history update
Introduced in SN07.

12.3.11.3 Associated registers
ISSVCFL, DPTSVCF, NOSVCFL

12.3.11.4 Associated logs
XPKT301 and XPKT302

12.3.12 Register OTH_CC

12.3.12.1 Register description

All other ATM cause codes.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) is not one of (3, 18, 35, 37, 41, or 47).

12.3.12.2 Register release history update
Introduced in SN07.

12.3.12.3 Associated registers
ISSVCFL, DPTSVCF, NOSVCFL

12.3.12.4 Associated logs
XPKT301 and XPKT302

12.3.13 Register RESUNAVL

12.3.13.1 Register description

Resource unavailable SVC connection failure.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 47(resource unavailable).

12.3.13.2 Register release history update
Introduced in SN07.

12.3.13.3 Associated registers
ISSVCFL, DPTSVCF, NOSVCFL

12.3.13.4 Associated logs
XPKT301 and XPKT302

12.3.14 Register TEMPFAIL

12.3.14.1 Register description

Temp failure SVC connection failure.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 41 (temp failure).

12.3.14.2 Register release history update

Introduced in SN07.

12.3.14.3 Associated registers

ISSVCFL, DPTSVCF, NOSVCFL

12.3.14.4 Associated logs

XPKT301 and XPKT302

12.3.15 Register VPCINAVL

12.3.15.1 Register description

Request VPI/VCI not available.

This register is pegged for external network bearer path ATM SVC failures when the ATM cause code sent back from either an SPM node (SMG4, IW SPM, DPT SPM) or GWC is cause code 35 (requested VPI/VCI not available).

12.3.15.2 Register release history update

Introduced in SN07.

12.3.15.3 Associated registers

ISSVCFL, DPTSVCF, NOSVCFL

12.3.15.4 Associated logs

XPKT301 and XPKT302

13: Performance (PF): A00004500

13.1 Performance management strategy

Not Applicable

13.2 Performance management tools and utilities

Not Applicable

13.3 Performance Measurements (PM), Operational Measurements (OM), and stats

This activity adds new OMs in a ne OM group. The new OM group is INSCTP OM for AIN transports. The following sections will outline in detail what OMs will be pegged.

13.3.1 New OMs

MSGOUT - Pegs Outgoing IN messages using SCTP

MSGIN - Pegs Incoming IN messages using SCTP

SENDFAIL - Pegs IN messages using SCTP for which send failed

DATAERR - Pegs IN messages which encountered errors at application data

DATARCVD - Pegs for Incoming IN message decoding

MSG2BIG- Pegs IN Messages which failed due to message length

BMSFAIL - Pegs instances when buffer errors encountered while sending IN messages over SCTP

NOTREADY - Pegs when SCTP layer indicates that it is not ready to process the message.Please note that this register even though displayed part of the OM group INSCTP, is NOT used by this activity.

Figure 1 INSCTP Group Display

```
>omshow INSCTP active

INSCTP

CLASS: ACTIVE
START:2004/01/12 08:30:00 MON; STOP: 2004/01/12 09:55:39 MON;
SLOWSAMPLES:        5 ; FASTSAMPLES:       48 ;


MSGOUT MSGIN SENDFAIL DATAERR
MSG2BIG BMSFAIL DATARCVD NOTREADY

  0
        0       0       0       0
        0       0       0       0
```

13.3.1.1 MSGOUT

Register MSGOUT (IN SCTP MSG Out) will be pegged for every outgoing AIN message using the SCTP transport.

13.3.1.2 MSGIN

Register MSGIN (IN SCTP MSG In) will be pegged for every incoming AIN message using the SCTP transport.

13.3.1.3 SENDFAIL

Register SENDFAIL (IN SCTP SeND FAilure) will be pegged for every outgoing AIN message using the SCTP transport that failed.

13.3.1.4 DATAERR

Register DATAERR (IN SCTP Data ERRor) will be pegged for every Data Error that occurs which causes a messaging failure.

13.3.1.5 MSG2BIG

Register MSG2BIG (IN SCTP message too BIG) will be pegged for every outgoing message that failed to be send because of the message size being too BIG. (i.e beyond the maximum size) Please refer to the EI section for maximum message size allowed.

13.3.1.6 BMSFAIL

Register INSCTBMS (IN SCTP BMS buffer failure) will be pegged if any buffer failure results in send or recieve failure.

13.3.1.7 DATARCVD

Register DATARCVD will be pegged when the IN msg is received from SCTP stack and we are ready to decode the IN message.

13.3.1.8 NOTREADY

Register NOTREADY is used to indicate that the SCTP layer is not ready to send or receive a message. This Register is presently not used with the current functionality(but will be displayed on OMSHOW as one of the registers in the group).

13.3.1.9 Associated OM groups

Not Applicable

13.3.1.10 Associated logs

TBD

13.3.2 OM Group template (applies only to DMS)

Not Applicable

13.3.3 Register (applies only to DMS)

Not Applicable

14: Performance (PF): A00005160

14.1 Performance management strategy

Performance management for the OSSAIN product is described in 297-8403-901, *Operator Services System Advanced Intelligent Network (OSSAIN) User's Guide*.

This feature (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) adds registers to one existing OM group in the DMS core, and adds one new OM group in the DMS Core. The new OM group can be used in analyzing messaging throughput of TOPS applications that send and receive UDP datagrams.

14.2 Performance management tools and utilities

Standard DMS tools for managing OMs.

14.3 Operational Measurements (OM)

14.3.1 OM Group template

14.3.1.1 OM description

OM group OAPNMTC

Open Automated Protocol (OAP) Node Maintenance Operations and Responses

OAPNMTC contains a register for each node maintenance operation and response message defined in the OAP protocol. The purpose of the registers in this OM group is to track usage of the operations and responses. These OM registers are pegged on a per node basis.

14.3.1.2 Release history update

Six new registers, three basic and three extension, are added in SN07. The new registers are associated with the Node Connectivity Test operation.

As of SN07, tuples are displayed for nodes datafilled as OSN as well as for nodes datafilled as OSNM.

14.3.1.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group OAPNMTC Display

```
NODEAUD     NODEAUD2    NDEAUDS   NDEAUDS2
NDEAUDE     NDEAUDE2    NODEBSY   NODEBSY2
NDEBSYS     NDEBSYS2    NDEBSYE   NDEBSYE2
NODETST     NODETST2    NDETSTS   NDETSTS2
NDETSTE     NDETSTE2    NODERTS   NODERTS2
NDERTSS     NDERTSS2    NDERTSE   NDERTSE2
  NDLOG       NDALARM   NODECON   NODECON2
NDECONS     NDECONS2    NDECONE   NDECONE2
```

14.3.1.4 Group structure

Unchanged.

14.3.1.5 Associated OM groups

Unchanged.

14.3.1.6 Associated functional groups

Unchanged.

14.3.1.7 Associated functionality codes

OSAN0101, OSSAIN Base.

14.3.1.8 OM group registers logic flow chart

A flow chart is not helpful in understanding this particular OM group.

14.3.1.9 Register description

Note: Registers that existed prior to SN07 are unchanged, and are not re-documented here. This section documents only the new registers.

14.3.1.9.1 Register NODECON

Node Connectivity Test

Register NODECON is pegged each time a Node Connectivity Test request or response is sent from or received by the switch.

Register release history: Register NODECON is introduced in SN07.

Associated registers: NDECONS, NDECONE.

Associated logs: None.

Extension register: NODECON2

14.3.1.9.2 Register NDECONS

Node Connectivity Test Success Response

Register NDECONS is pegged each time a Node Connectivity Test Success Response is sent from or received by the switch.

Register release history: Register NDECONS is introduced in SN07.

Associated registers: NODECON, NDECONE.

Associated logs: None.

Extension register: NDECONS2

14.3.1.9.3 Register NDECONE

Node Connectivity Test Error Response

Register NDECONE is pegged each time a Node Connectivity Test Error Response is sent from or received by the switch.

Register release history: Register NDECONE is introduced in SN07.

Associated registers: NODECON, NDECONS.

Associated logs: None.

Extension register: NDECONE2

14.3.2 OM Group template

14.3.2.1 OM description

OM group TDGTHRU

TOPS Datagram Throughput

14.3.2.2 Release history update

The OM group is being created in TOPS20/SN07/ISN07.

14.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 2 OM Group TDGTHRU Display

SND48	SND48X	SND96	SND96X
SND160	SND160X	SND224	SND224X
SND296	SND296X	SND368	SND368X
SND512	SND512X	SNDLG	SNDLGX
RCV48	RCV48X	RCV96	RCV96X
RCV160	RCV160X	RCV224	RCV224X
RCV296	RCV296X	RCV368	RCV368X
RCVLG	RCVLGX		

Each register counts the number of messages in a particular size range that a TOPS application sent or received during the reporting period. The numbers in the register names indicate the size ranges or "buckets," as explained in Table 2, "TDGTHRU Registers," on page 3622.

14.3.2.4 Group structure

OM group TDGTHRU provides 1 tuple for each of the four fixed key values shown below.

Key field: TOPS_DGRAM_IDX specifies the TOPS application and data path to which the peg counts in the tuple apply. The fixed key values are listed below along with their meanings:

Figure 3 Key values for OM group TDGTHRU

Key Value	Meaning
OA_EIU	OSSAIN application using Ethernet Interface Unit
OA_XAETHR	OSSAIN application using XA-Core Ethernet interface
POS_IPXPM	TOPS position application using IP-XPM
OC_IPXPM	Operator Centralization application using IP-XPM

Info field: None

14.3.2.5 Associated OM groups

None.

14.3.2.6 Associated functional groups

None.

14.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code
Base TOPS	OSB0101

14.3.2.8 OM group registers logic flow charts

This section includes 8 flow charts: one for pegging SNDxxx registers and one for pegging RCVxxx registers, for each of the four tuples.

For more information about the specific registers, please refer to Table 2, "TDGTHRU Registers," on page 3622.

Figure 4 Flow chart for pegging send (SND) registers in OA_EIU tuple

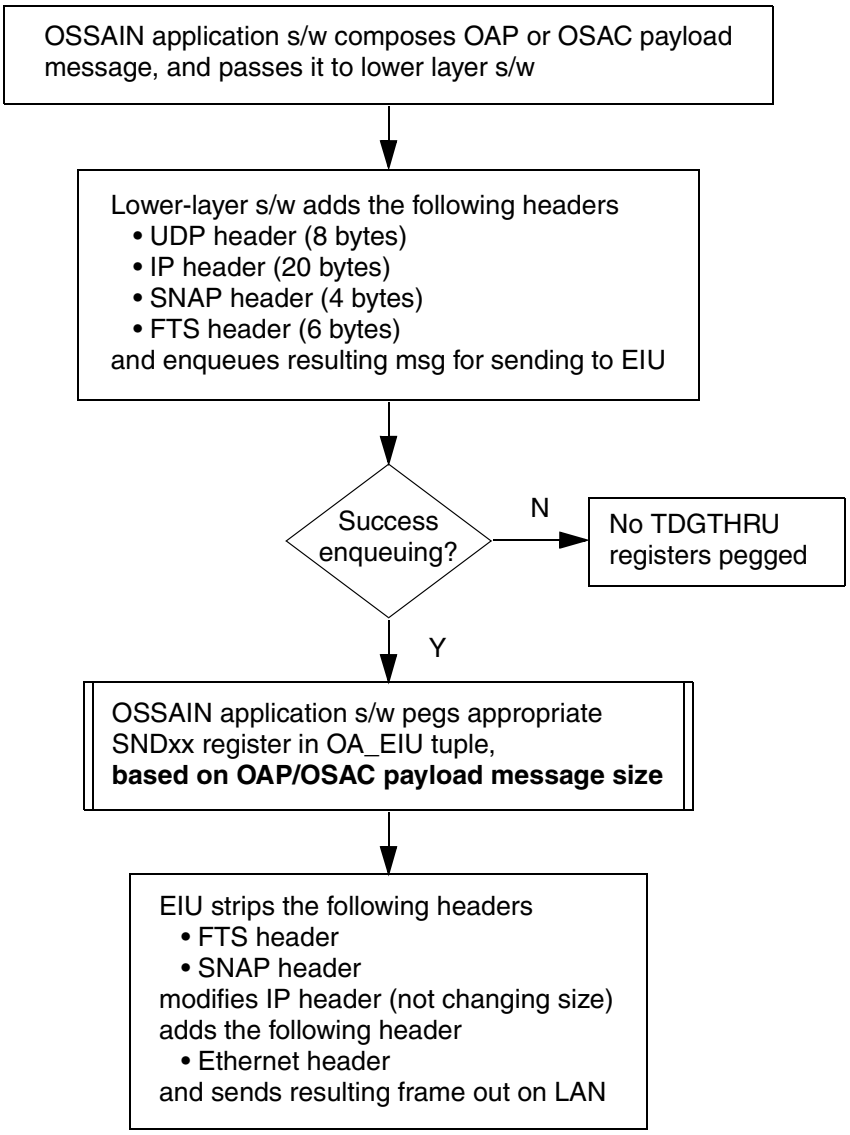


Figure 5 Flow chart for pegging send (SND) registers in OA_XAETHR tuple

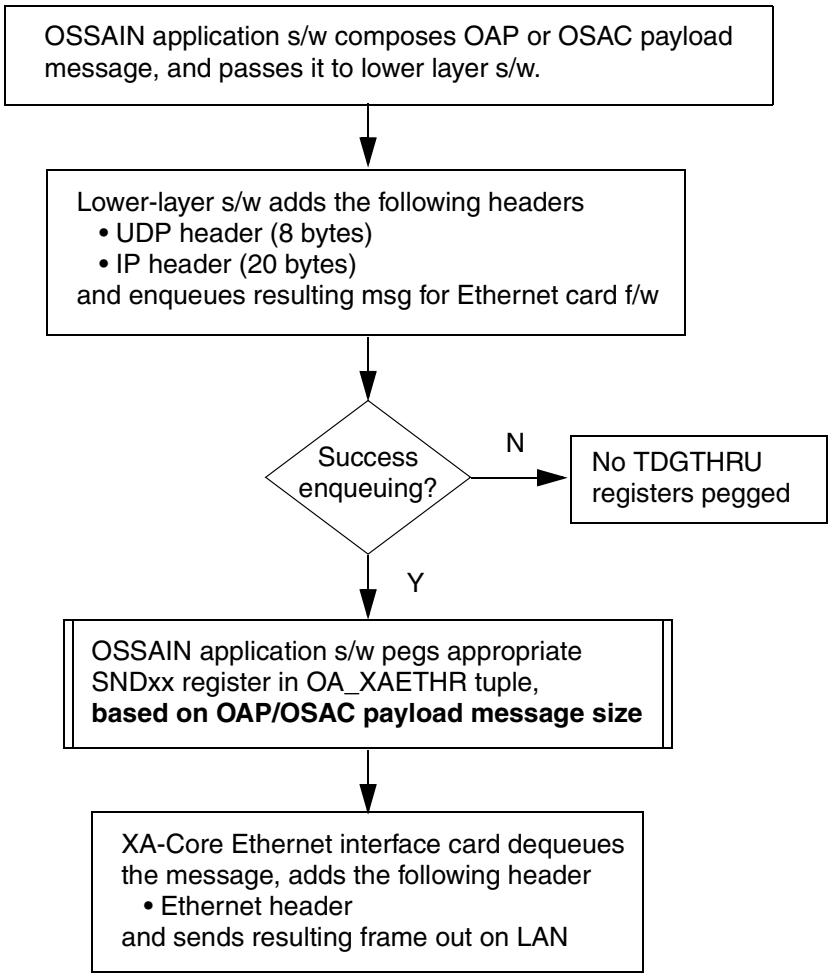


Figure 6 Flow chart for pegging send (SND) registers in POS_IPXPM tuple

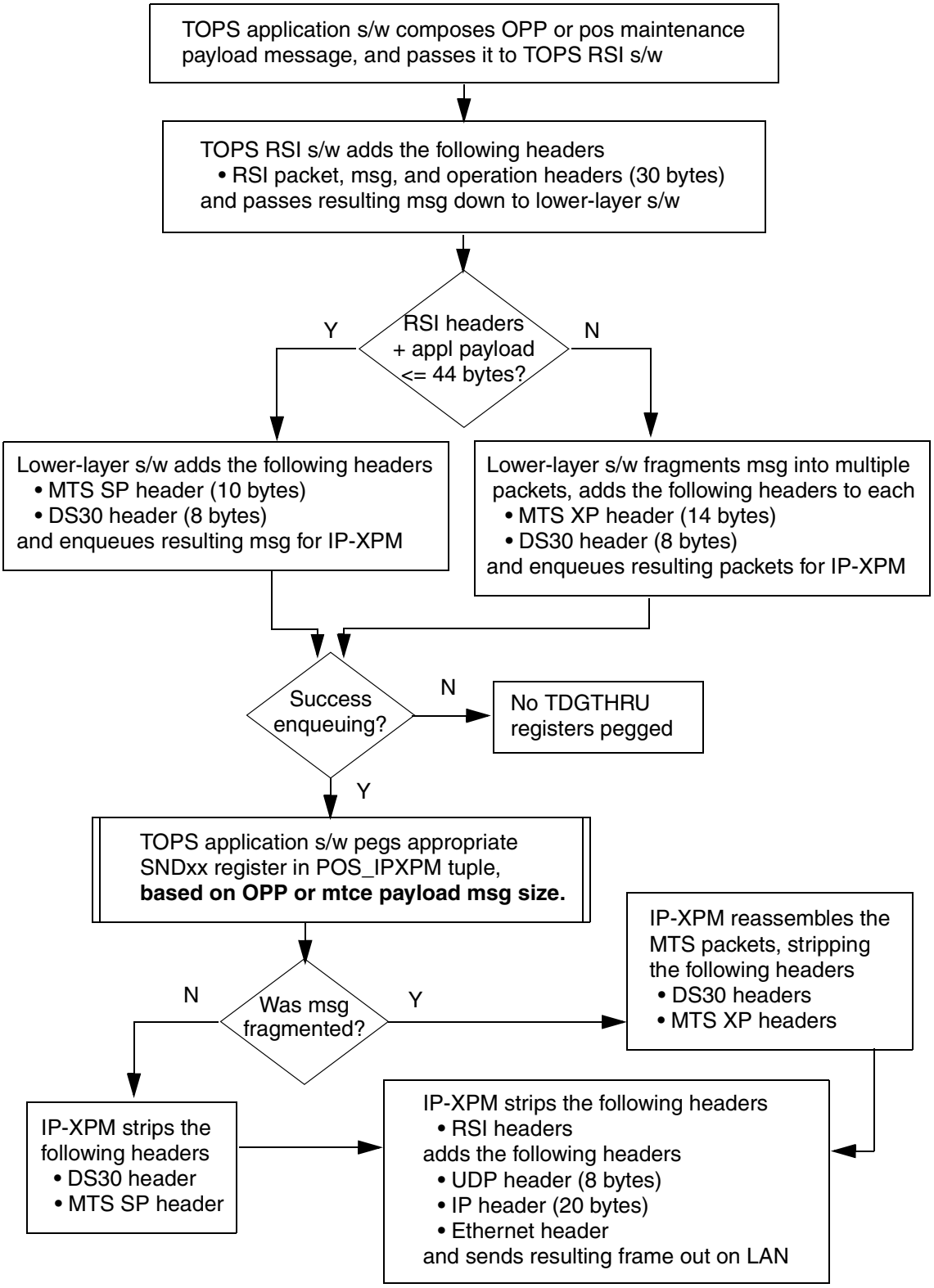


Figure 7 Flow chart for pegging send (SND) registers in OC_IPXPM tuple

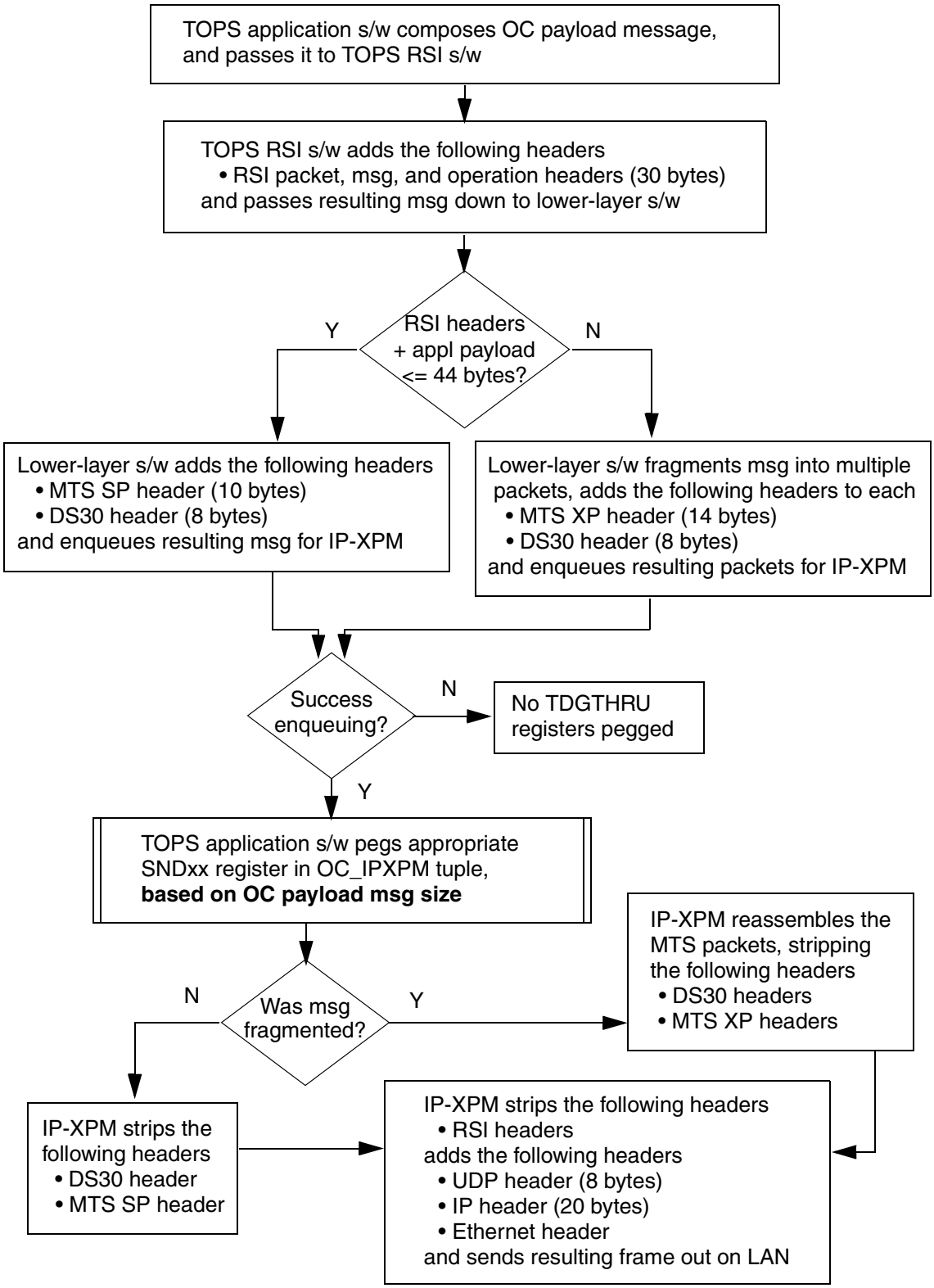


Figure 8 Flow chart for pegging receive (RCV) registers in OA_EIU tuple

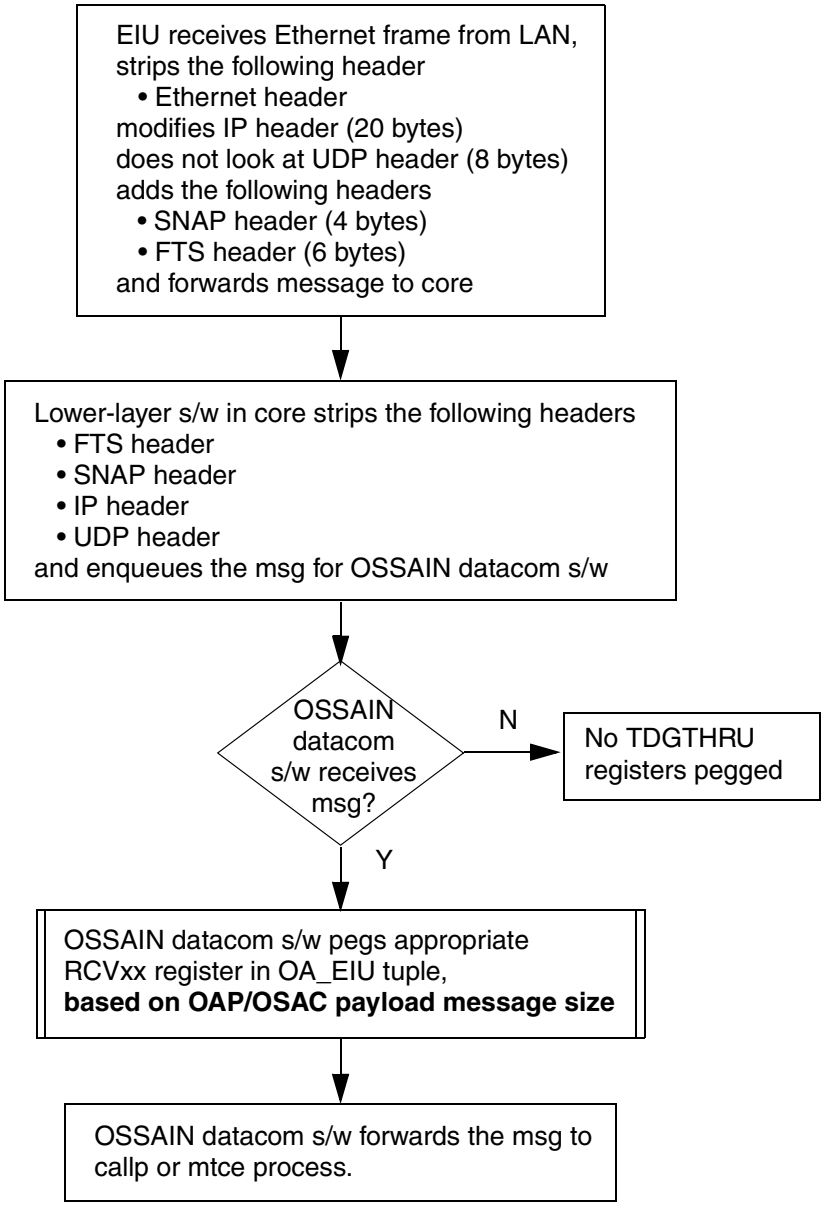


Figure 9 Flow chart for pegging receive (RCV) registers in OA_XAETHR tuple

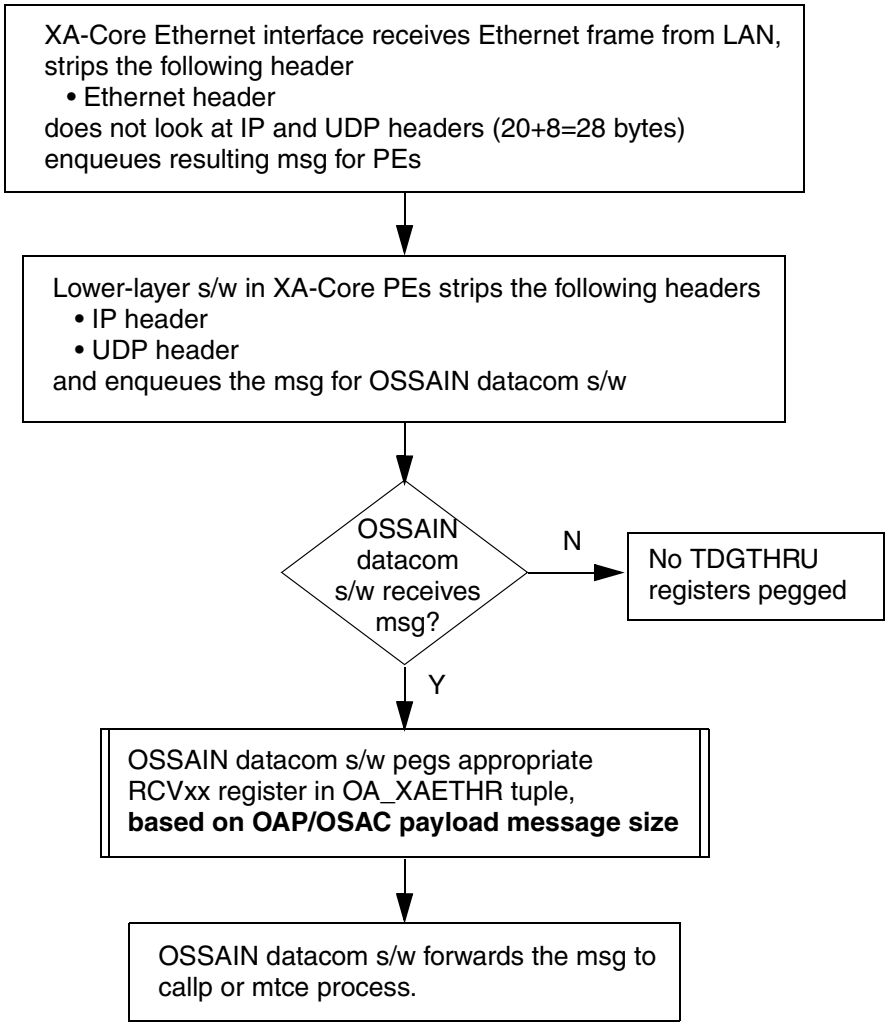
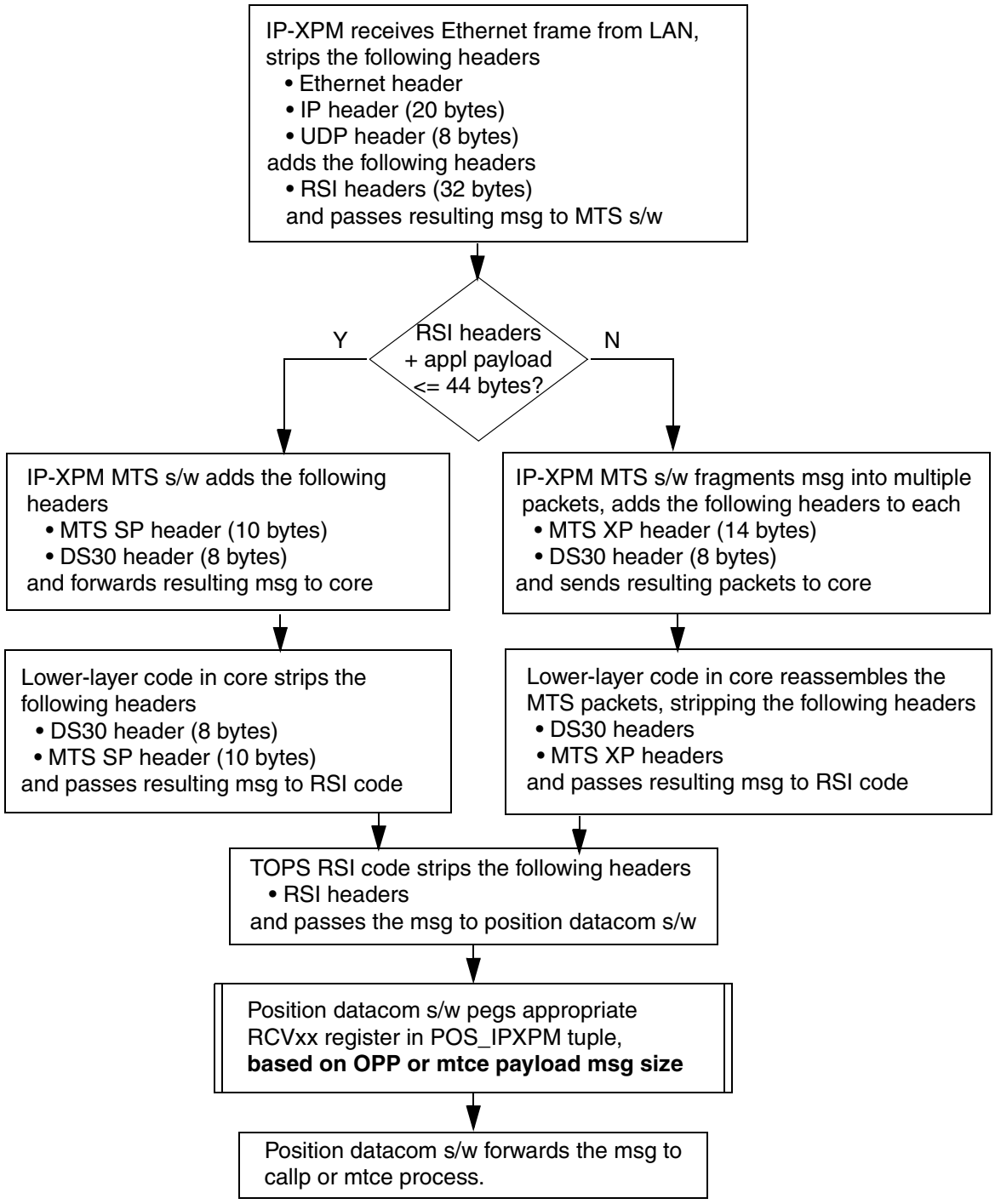
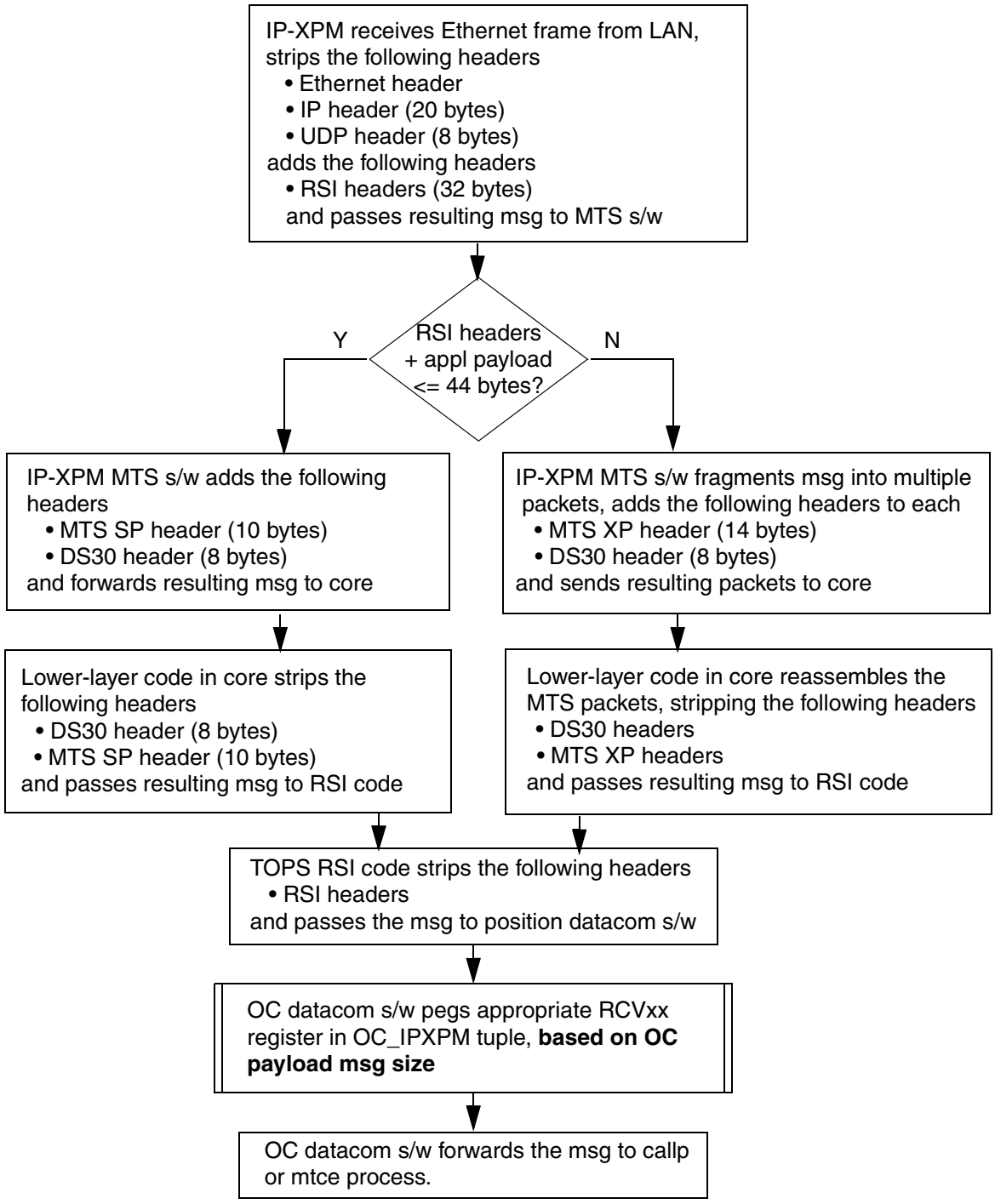


Figure 10 Flow chart for pegging receive (RCV) registers in POS_IPXPM tuple



Note: Failure at any point before the message gets to position datacom s/w results in no registers being pegged in group TDGTHRU.

Figure 11 Flow chart for pegging receive (RCV) registers in OC_IPXPM tuple



Note: Failure at any point before the message gets to OC datacom s/w results in no registers being pegged in group TDGTHRU.

0.0.0.1 Register release history update

All registers in this group were created in TOPS20/SN07/ISN07.

0.0.0.2 Associated registers

None.

0.0.0.3 Associated logs

None

Table 2 TDGTHRU Registers

Short Register Name	Long Name	Explanation
SND368 and SND368X	Send 368 Bytes	Peg register. Counts the number of messages sent from the core, of size > 296 bytes and <= 368 bytes. SND368X is an extension register.
SND512 and SND512X	Send 512 Bytes	Peg register. Counts the number of messages sent from the core, of size > 368 bytes and <= 512 bytes. SND368X is an extension register.
SNDLG and SNDLGX	Send Large	Peg register. Counts the number of messages sent from the core, of size > 512 bytes. SNDLGX is an extension register.
RCV48 and RCV48X	Receive 48 Bytes	Peg register. Counts the number of messages received by the core, of size <= 48 bytes. RCV48X is an extension register.
RCV96 and RCV96X	Receive 96 Bytes	Peg register. Counts the number of messages received by the core, of size > 48 bytes and <= 96 bytes. RCV96X is an extension register.
RCV160 and RCV160X	Receive 160 Bytes	Peg register. Counts the number of messages received by the core, of size > 96 bytes and <= 160 bytes. RCV160X is an extension register.
RCV224 and RCV224X	Receive 224 Bytes	Peg register. Counts the number of messages received by the core, of size > 160 bytes and <= 224 bytes. RCV224X is an extension register.
RCV296 and RCV296X	Receive 296 Bytes	Peg register. Counts the number of messages received by the core, of size > 224 bytes and <= 296 bytes. RCV296X is an extension register.

Table 2 TDGTHRU Registers

Short Register Name	Long Name	Explanation
RCV368 and RCV368X	Receive 368 Bytes	Peg register. Counts the number of messages received by the core, of size > 296 bytes and <= 368 bytes. RCV368X is an extension register.
RCVLG and RCVLGX	Receive Large	Peg register. Counts the number of messages received by the core, of size > 368 bytes. RCVLGX is an extension register.

14.3.3.2 Register release history update

All registers in this group were created in TOPS20/SN07/ISN07.

14.3.3.3 Associated registers

None.

14.3.3.4 Associated logs

None

14.3.3.5 elease history update

All registers in this group were created in TOPS20/SN07/ISN07.

14.3.3.6 Associated registers

None.

14.3.3.7 Associated logs

None

15: Performance (PF): A00005160

15.1 Performance management strategy

15.2 Performance management tools and utilities

The new OM group can be displayed and collected via OMSHOW interface regularly by Telcos to monitor system IO throughput.

15.3 Performance Measurements (PM), Operational Measurements (OM), and stats

This feature will provide a new OM group IOCAP.

15.3.1 PM, OM, and stats format

15.3.2 OM Group template (applies only to DMS)

New OM group IOCAP provides information on IO capacity such as utilization and utilization high watermark and IO throughput information on a per IO service type (CMIC, ETHR and AMDI).

15.3.2.1 OM description

OM group IOCAP provides one tuple per IO service type available in the office. Possible IO service types are CMIC, ETHR and AMDI.

Key field: IO_SERVICE.

Info field: none.

15.3.2.2 Release history update

The OM group is being created in CSP21 and will be patched backed to CSP20.

15.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

IO_SERVICE IOUTIL IOHWM TXMSGPS TXSIZE RXMSGPS RXSIZE IOTHRESH

15.3.2.4 Group structure

OM group provides one tuple for each IO service type. There are 3 possible IO service types (CMIC, ETHR, AMDI).

Key field: IO_SERVICE indicates the IO service type the information is captured. Possible IO service types are CMIC, ETHR, and AMDI. The service type is displayed as 4 character string (CMIC, ETHR, AMDI).

Info field: None.

15.3.2.5 Associated OM groups

Not applicable.

15.3.2.6 Associated functional groups

The following functional groups are associated with OM group: none

15.3.2.7 OM group registers logic flow chart

Not applicable.

15.3.3 Register (applies only to DMS)

IOHWM

15.3.3.1 Register description

IOHWM is a high watermark register holding the highest utilization value of the specified IO service type over the OM transfer period.

15.3.3.2 Register release history update

Register is being created in CSP21 and patched back to CSP20.

15.3.3.3 Associated registers

None.

15.3.3.4 Associated logs

None.

15.3.4 Register (applies only to DMS)

IOTHRESH

15.3.4.1 Register description

IOTHRESH is a peg register holding the number of one minute interval in the transfer period the IO utilization has exceeded the value of the IO_WARNING_THRESHOLD office parm.

15.3.4.2 Register release history update

Register is being created in CSP21 and patched back to CSP20.

15.3.4.3 Associated registers

None.

15.3.4.4 Associated logs

None.

15.3.5 Register (applies only to DMS)

IOUTIL

15.3.5.1 Register description

IOUTIL is a usage register holding the average utilization value of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period.

15.3.5.2 Register release history update

Register is being created in CSP21 and patched back to CSP20.

15.3.5.3 Associated registers

None.

15.3.5.4 Associated logs

None.

15.3.6 Register (applies only to DMS)

RXMSGPS

15.3.6.1 Register description

RXMSGPS is a usage register holding the average total system number of received messages of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The unit is number of messages per second.

15.3.6.2 Register release history update

Register is being created in CSP21 and patched back to CSP20.

15.3.6.3 Associated registers

None.

15.3.6.4 Associated logs

None.

15.3.7 Register (applies only to DMS)

RXSIZE

15.3.7.1 Register description

RXSIZE is a usage register holding the average incoming message size of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The message size unit is in bytes.

15.3.7.2 Register release history update

Register is being created in CSP21 and patched back to CSP20.

15.3.7.3 Associated registers
None.

15.3.7.4 Associated logs
None.

15.3.8 Register (applies only to DMS)
TXMSGPS

15.3.8.1 Register description
TXMSGPS is a usage register holding the average total number of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every OM transfer period. The unit is in number of messages per second.

15.3.8.2 Register release history update
Register is being created in CSP21 and patched back to CSP20.

15.3.8.3 Associated registers
None.

15.3.8.4 Associated logs
None.

15.3.9 Register (applies only to DMS)
TXSIZE

15.3.9.1 Register description
TXSIZE is a usage register holding the value of average size of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every transfer period. The value unit is in bytes.

15.3.9.2 Register release history update
Register is being created in CSP21 and patched back to CSP20.

15.3.9.3 Associated registers
None.

15.3.9.4 Associated logs
None.

Accounting (ACC)

Introduction

This chapter describes new and changed features that are planned for this release.

Featid	Title
A00003007.AA34	AMA Enhancements for DTAG International Gateway
A00004036.AA42	Off-Board Service Control
A00004137.AA12	ANI Billing
A00005363.AA16	CAIN FlexCDR Enhancements

1: Accounting (ACC): A00004036

1.1 Accounting strategy

The generally accounting strategy for this activity is to continue to perform whatever billing for successful updates that is done today for service activation/deactivation, list editing, etc. In addition to performing the standard billing, a Service Logic Identification Module (module code 039) will be appended to the current record is an AMAslpid is included in the corresponding update request.

1.2 CM billing due to Update Requests

The AMA records generated as per the service requirements and the GR1298 requirements (Update and Query messages) for all the service groups whose provisioning and activation is being controlled and queried by the Update and query messages are as follows :

1.2.1 Group1 Services AMA

Only three services Automatic Call Back (ACB), Automatic Recall (AR) and Make Set Busy (MSB) generates the AMA record. All other services does not have any AMA record associated with them.

1.2.1.1 Update Message for ACB (Universal) and AR (Universal)

Consistent with the billing performed as a result of Automatic Call Back (universal - usage based), and Automatic Recall (universal - usage based) being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful deactivation of ACB (universal) , and AR (universal). All other service in this group do not generate an AMA record.

1.2.1.2 Update Message for MSB

Consistent with the billing performed as a result of MSB being modified via access code, a callcode 006 record (structure code 510) will also be provided to record successful activation and deactivation of MSB.

1.2.1.3 Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Figure 1 Example: ACB deactivation - Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:069C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508160C ELAPSED TIME:000000059C CLASS FUNCTION:000C FEATURE STATUS:000C SCRN LIST SCF:000C SCRN LIST SCR:000C SCRN LIST DRCW:000C
MODULE CODE:039C SLP ID:123456789C MODULE CODE:000C

Figure 2 Example: AR deactivation - Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:068C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508160C ELAPSED TIME:000000059C CLASS FUNCTION:000C FEATURE STATUS:000C SCRN LIST SCF:000C SCRN LIST SCR:000C SCRN LIST DRCW:000C
MODULE CODE:039C SLP ID:123456789C MODULE CODE:000C

Figure 3 Example: MSB activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:40510C CALL CODE:006C SENSOR TYPE:036C SENSOR ID:0000000C REC OFFICE TYPE:036C REC OFFICE ID:0000000C DATE:80218C TIMING IND: 00000C STUDY IND:0000000C CLD PTY OFF-HK:0C SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C SIG DIGITS NEXT FIELD:009C ORIG OPEN DIGITS 1:00036340101C ORIG OPEN DIGITS 2:FFFFFFFFFF ORIGINATING CHARGE INFO:FFFF DOMESTIC/INTL INDICATOR:1C SIG DIGITS NEXT FIELD:007C TERM OPEN DIGITS 1:00006340102C TERM OPEN DIGITS 2:FFFFFFFFF CONNECT TIME:1451038C ELAPSED TIME:000000138C MODULE CODE:611C GENERIC CONTEXT ID:8002415C GENERIC DIGITS STRING ONE:94A28200000090C
MODULE CODE:039C SLP ID:123456789C MODULE CODE:000C

1.2.2 Group2 Services AMA

No AMA records are generated for Group2 services.

1.2.3 Group3 Services AMA

1.2.3.1 Update Message for DRCW, SCRJ and SIMRING

Consistent with the billing performed as a result of Distinctive Ringing / Call Waiting , Selective Call Rejection being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful DRCW or SCRJ activation, deactivation, list edit operations, etc. SIMRING does not generate a AMA record.

1.2.3.2 Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Figure 4 Example: DRCW activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:073C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508160C ELAPSED TIME:000000059C CLASS FUNCTION:002C FEATURE STATUS:000C SCRN LIST SCF:FFFF SCRN LIST SCR:FFFF SCRN LIST DRCW:001C ***MODULE CODE:039C SLP ID:111111111C*** MODULE CODE:000C

Figure 5 Example: SCRJ activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:072C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508302C ELAPSED TIME:000000081C CLASS FUNCTION:002C FEATURE STATUS:000C SCRN LIST SCF:FFFF SCRN LIST SCR:001C SCRN LIST DRCW:FFFF ***MODULE CODE:039C SLP ID:111111111C*** MODULE CODE:000C

1.2.4 Group4 Services AMA

1.2.4.1 Updates to Call Forwarding

Consistent with the billing performed as a result of Call Forwarding being modified via access code, a callcode 31 record (structure code 614) will be provided for successful CFW activation (POTS or IBN/RES) and a callcode 31 record (structure code 96) will be provided for successful CFW deactivation (POTS or IBN/RES).

There are no billing records provided for Call Forward Busy or Don't Answer activation or deactivation for either POTS or IBN/RES.

1.2.4.2 Module code 039

Impact to be determined.

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Figure 6 Example: Call Forward activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:00614C CALL CODE:031C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30926C TIMING IND:00100C STUDY IND:0000000C SERVICE FEATURE:012C ACTIVATING NPA:613C ACTIVATING NUMBER:6213502C FWD OVERSEAS IND:1C FWD NPA:00613C FWD NUMBER:6212500C ACTIVATION TIME:1426285C
MODULE CODE:039C SLP ID:111111111C MODULE CODE:000C

Figure 7 Example: Call Fwd deactivation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:00096C CALL CODE:031C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30926C TIMING IND:00300C STUDY IND:0000000C SERVICE FEATURE:012C ACTIVATING NPA:613C ACTIVATING NUMBER:6213502C FWD OVERSEAS IND:1C FWD NPA:00613C FWD NUMBER:6212500C ACTIVATION TIME:1426285C ELAPSED TIME:000000265C PRESENT DATE:30926C PRESENT TIME:1426568C
MODULE CODE:039C SLP ID:111111111C MODULE CODE:000C

1.2.5 Group5 Services AMA

1.2.5.1 Updates to Selective Call Forwarding

Consistent with the billing performed as a result of Selective Call Forwarding being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful SCF activation, deactivation, list edit operations, etc.

1.2.5.2 Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure illustrates the above as it relates to the extension of a Selective Call Forwarding CLASS AMA record . The Module Code 039 portion of the record is represented as ***bold italics***.

Figure 8 Example: Update message for SCF

*HEX ID:AA STRUCTURE CODE:41030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30731C CLASS FEATURE:052C ORIG NPA:000C ORIG NUMBER:0000000C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:0857083C ELAPSED TIME:000000000C CLASS FUNCTION:001C FEATURE STATUS:000C SCRN LIST SCF:001C SCRN LIST SCR:FFFF SCRN LIST DRCW:FFFF ***MODULE CODE:039C SLP ID:111111111C*** MODULE CODE:000C

1.2.6 Group6 Services AMA

No AMA records are generated for Group6 Services.

1.2.7 Group7 Services AMA

1.2.7.1 Update Messages for CallingNunberDeliveryBlocking

Consistent with the billing performed as a result of CNDB being activated via an access code, a callcode 330 record (structure code 1030) will be provided to record successful CNDB activation. Service CNAB does not generate an AMA record.

1.2.7.2 Module Code 039

When an *AMAsplidid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslipid* will be appended to any base record associated with the upate.

Figure 9 Example CNDB Activation

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:31030C CLASS FEATURE:075C ORIG NPA:613C ORIG NUMBER:6213513C OVERSEAS IND:1C TERM NPA:00613C TERM NUMBER:7234535C CONNECT TIME:0949248C ELAPSED TIME:000000000C CLASS FUNCTION:000C FEATURE STATUS:000C SCRN LIST SCF:000C SCRN LIST SCR:000C SCRN LIST DRCW:000C *MODULE CODE:039C SLIP ID:111111111C MODULE CODE:000C*

1.2.8 Group8 Services AMA

1.2.8.1 Update Message for COT and CCW

Consistent with the billing performed as a result of Customer Originated Trace and CancelCall Waiting being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful COT or CCW invocation.

1.2.8.2 Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Figure 10 Example COT activation and LINE 150 Log

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:070C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:0C TERM NPA:00613C TERM NUMBER:6215121C CONNECT TIME:1510368C ELAPSED TIME:000000000C CLASS FUNCTION:000C FEATURE STATUS:000C SCRN LIST SCF:000C SCRN LIST SCR:000C SCRN LIST DRCW:000C ***MODULE CODE:039C SLIP ID:111111111C MODULE CODE:000C***

>open line 150
Done.
RTPT07BD LINE150 SEP29 15:10:36 2600 INFO FULL COT TRACE
SUBSCRIBER LEN: HOST 05 0 08 21 SUBSCRIBER DN: 613 6215821
TRACE DUMP
TIME CALL RCVD: SEP29 15:10:07 DN: 613 6215121
INTRAOFFICE: Y ORIG ADDR TYPE: 003 (UNIQUE)
OUT OF AREA: N CWT: N PRIVATE: N GIC: N
NETWORK: PUBLIC
JIP: 000000
JIP REASON: HOMELRN USED

1.2.9 Group9 Services AMA

No AMA records are generated for Group9 Services.

1.3 Other changes

Not applicable.

2: Accounting (ACC): A00004137

2.1 Accounting strategy

Module Code 838[1] is appended to SC0220 AMA records when the Calling Party Number (CPN) or Billing Number (BN) are delivered to the terminating party over a PRI connection.

2.2 Accounting tools and utilities

Not applicable.

2.3 Accounting task flows

Not applicable.

2.4 CM billing changes

2.4.1 Structure codes

No changes are made to the SC0220; however, a new module, MC838, will be appended for PRI terminating calls that deliver CPN/BN when this feature is active.

2.4.2 Structure code 220

SC220 is generated for calls that perform a CAIN query and return an AMASlpID in the response. When this feature is active (SOC UTRS0014 is set to ON), an MC838 will be appended to the SC0220 AMA record for calls that terminate on PRI trunks that signal the CPN or BN in the SETUP message.

Only one MC828 will ever be appended to a SC220 record.

Table 1 Structure code

Information	Field number
Structure code	220

2.4.3 Module code

Module Code 838 - Egress Data Module

2.4.4 Module code 838

Module description. The following table provides information for module code 838.

[1]Module Code 838 is not a Bellcore defined module in GR-1100-CORE.

.

Table 2 Module code

Information	Field number	Number of characters
Module Code	88	4
Communications ISDN (ACI)/ISDN Features	344	4

2.4.5 Tables (fields)

This feature has the following field:

- Communications ISDN (ACI)/ISDN Features

2.4.6 Field 344

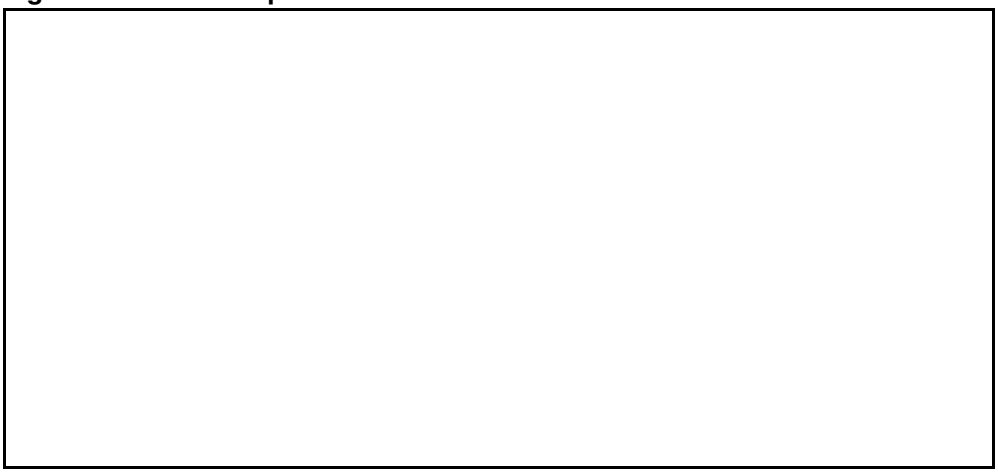
Field description. The following table provides information for field 344.

Table 3 Table (Field) 344 characters - values and meaning

Character	Value	Meaning
1-2	00	Constant
3	1	CPN/BN has been delivered to the terminating end.
	2-9	unassigned
4	C	SIGN character (HEX C)

The following MAP example figure is in non-printing text.

Figure 1 MAP example



2.5 Other changes

Not applicable.

3: Accounting (ACC): A00005363

3.1 Accounting strategy

This activity creates 4 new fields: BUSCSTID, SLPID1ST, DGI300, and DGI301. The new fields are not part of and cannot be added to any predefined templates. The new fields are available for the use in creation of telco defined flexible CDR templates. The billing format of the new fields is NT format and therefore do not contain structure codes or module codes.

3.2 Accounting tools and utilities

The following tools are used to create data for or display the new fields: CDRTST, CDRDUMP, FCDRSRCH and CTMPLT

3.3 Accounting task flows

NA

3.4 CM billing changes

3.4.1 Structure codes

NA

3.4.2 Structure code nnn

NA

Table 1 Structure code

Information	Field number
Structure code	nn
	nn

3.4.3 Module code

NA

3.4.4 Module code nnn

.NA

Table 2 Module code

Information	Field number	Number of characters
Module code	nn	nn
	nn	nn

3.4.5 Tables (fields)

NA

3.4.6 Field nnn

NA

3.4.7 Record codes

NA

3.4.8 Tables (fields)

This feature has the following new fields:

- SLPID1ST
- BUSCSTID
- DGI300
- DGI301

3.4.9 Field SLPID1ST

Field description. The following table provides information for field SLPID1ST..

Table 3 Field information

Character(s)	Valuer	Meaning
1-9	000000000-999999999	The first received SLPID which is received by the CAIN software.

3.4.10 Field BUSCSTID

Field description. The following table provides information for field BUSCSTID..

Table 4 Field information

Character(s)	Valuer	Meaning
1-11	00000000000- 99999999999	The business customeri d which is captured by the CAIN software.

3.4.11 Field DGI300

Field description. The following table provides information for field DGI300..

Table 5 Field information

Character(s)	Valuer	Meaning
1-3	300	Dgit id 300
4-27	000000000000000000000000- 999999999999999999999999	The dialed digits which are captured when the digit id is 300.

3.4.12 Field DGI301

Field description. The following table provides information for field DGI301..

Table 6 Field information

Character(s)	Valuer	Meaning
1-3	301	Digit id 301
4-27	000000000000000000000000- 999999999999999999999999	The dialed digits which are captured when the digit id is 301.

3.5 Sample Log

```
RECCD     F0                          TEMPLID   016
ACTIDX    6                           TOOLGEN   Y
USEEDIT   N                           VARLNGTH  N
SEQNUM    00001                       CIC       5676
ORIGTIME  34992                       ORIGDATE  035
ANSTYPE   03                          TIMECHNG  N
ORIGAMPM  1                           INCINTL   N
DISCTIME  35052                       DISCDATE  035
ANISUFF   1                           DISCAMPM  1
INCBILL   1                           CALLDUR   00013107
PINDIGS   6987                        ANISP     5124599628
INFODIG   1                           BILLNUM   50854321499779000001234
ACCTCD    802000012345                CLGPTYNO  214684552900000
RLTCDR    Y                           ACCTV     3
UNIVACC   8007654321                  DIALEDNO  508345214997799
CALLEDNO  508543214997790             OUTPULNO  508345129479970
ORIGOPRT  501                         PREDIG    1
CNPREDIG  1                           OPART     511
TPART     31                          QUEUED    Y
OPCHOICE  232                         COLLTIME  060
ADIN      12                          LNPCHECK  7
NUMWBCKT  16                          WBCKTS    10000000 10000000 00000000
FINSID    111                         BILLTYPE  35
ORIGGRP   0353                        DISCTYPE  1
ORIGMEM   0101                        PASSTHRU  2
TERMGRP   0355                        PRESIND   1
TERMMEM   0101                        OSRASSOC  N
DIGDATA   Y                           FINTKGRP  09999
TRAP      N                           COSOVE    Y
FINTKMEM  62843                       SCPBILL   FE17700B
TRTMTCD   010                         COMPCODE  3
CRID      684149400                   DNIS      214684149400000
ORIGPVN   214684149400000             TERMPVN   214684466200000
ORIGLRN   2146841494                  PORTEDNO  2146844662
CAINCT    1                           ACG       Y
DNISNOA   103                         MLTCOSID  0001
COSINDEX  0001                        CARRSEL   02
SLPID1ST  032401234                   BUSCSTID  02532401234
DGI300    300997799912345678901234567DGI301    301997799912345678901234567
```

3.6 Other changes

None

SN07 Feature Subset Cross Reference Tables: International Features 5
Functional Descriptions List 13
Functional Description (FN): A00001914 17
Functional Description (FN): A00001918 24
Functional Description (FN): A00001919 35
Functional Description (FN): A00001920 74
Functional Description (FN): A00001921 91
Functional Description (FN): A00001923 100
Functional Description (FN): A00001929 111
Functional Description (FN): A00001930 130
Functional Description (FN): A00001935 159
Functional Description (FN): A00001965 161
Functional Description (FN): A00002053 184
Functional Description (FN): A00002100 201
Functional Description (FN): A00002101 220
Functional Description (FN): A0002173 257
Functional description (FN): A00002252 562
Functional Description (FN): A00002291 565
Functional Description (FN): A00002293 588
Functional Description (FN): A00002319 593
Functional Description (FN): A00002358 598
Functional Description (FN): A00002364 601
Functional Description (FN): A00002365. 610
Functional Description (FN): A00002367 621
Functional Description (FN): A00002377 645
Functional Description (FN): A00002470 654
Functional Description (FN): A00002512 659
Functional Description (FN): A00002638 709
Functional Description (FN): A00002639 726
Functional Description (FN): A00002640 746
Functional Description (FN): A00002641. 753
Functional description (FN): A00002642 758
Functional Description (FN): A00002644 762
Functional Description (FN): A00002654 789
Functional description (FN): A00002655 813
Functional Description (FN): A00002678 819
Functional Description (FN): A00002680. 841
Functional Description (FN): A00002702. 851
Functional Description (FN): A00002713. 858
Functional Description (FN): A00002751 884
Functional Description (FN): A00002754. 900
Functional Description (FN): A00002755 913
Functional Description (FN): A00002756 963

Functional Description (FN): A00002844 1037
Functional Description (FN): A00002884. 1051
Functional Description (FN): A00002900 1072
Functional Description (FN): A00002904 1083
Functional Description (FN): A00002916 1107
Functional Description (FN): A00003147. 1121
Functional Description (FN): A00003051. 1126
Functional Description (FN): A00003227 1132
Functional Description (FN): A00003405. 1137
Functional Description (FN): A00003410. 1138
Functional Description (FN): A00003411. 1149
Functional Description (FN): A00003465. 1164
Functional Description (FN): A00003466 1172
Functional Description (FN): A00003467 1174
Functional Description (FN): A00003624 1223
Functional Description (FN): A00003495 1226
Functional Description (FN): A00003624. 1228
Functional Description (FN): A00003627 1232
Functional Description (FN): A00003686. 1260
Functional Description (FN): A00003695. 1268
Functional Description (FN): A00003696. 1270
Functional Description (FN): A00003951 1301
Functional Description (FN): A00004205 1325
Functional Description (FN): A00004503. 1332
Functional Description (FN): A00004563. 1345
Functional Description (FN): A00004565 1372
Functional Description (FN): A00004743 1406
Functional Description (FN): A00004750 1412
Functional Description (FN): A00004931 1418
Functional Description (FN): A00004933 1443
Functional Description (FN): A00004981. 1464
Functional Description (FN): A00005164 1481
Functional Description (FN): A00005802. 1484
Functional Description (FN): A00006001. 1487
Functional Description (FN): A0006032. 1527

Fault Management List1531
Fault Management (FM): A00001919. 1533
Fault Management (FM): A00001920. 1539
Fault Management (FM): A00002252. 1541
Fault Management (FM): A00002364 1543
Fault Management (FM): A00002702 1546
Fault Management (FM): A00002844 1550

Fault Management (FM): A00003147 1553
Fault Management (FM): A00003696 1554
Fault Management (FM): A00004565 1558

Configuration Management List 1567
Configuration (CN): A00001914 1571
Configuration (CN): A00001918 1582
Configuration (CN): A00001919 1588
Configuration (CN): A00001920 1606
Configuration (CN): A00001921 1612
Configuration (CN): A00001923 1620
Configuration (CN): A00001930 1642
Configuration (CN): A00001935 1666
Configuration (CN): A00002053 1673
Configuration (CN): A00002101 1675
Configuration (CN): A00002173 1681
Configuration (CN): A00002252. 1691
Configuration (CN): A00002291 1696
Configuration (CN): A00002293 1700
Configuration (CN): A00002319. 1713
Configuration (CN): A00002364. 1726
Configuration (CN): A00002365. 1729
Configuration (CN): A00002377. 1735
Configuration (CN): A00002639 1741
Configuration (CN): A00002641. 1747
Configuration (CN): A00002642. 1751
Configuration (CN): A00002654 1754
Configuration (CN): A00002678 1769
Configuration (CN): A00002680. 1781
Configuration (CN): A00002702 1782
Configuration (CN): A00002713 1788
Configuration (CN): A00002751. 1791
Configuration (CN): A00002754. 1798
Configuration (CN): A00002755 1802
Configuration (CN): A00002844 1812
Configuration (CN): A00002900. 1814
Configuration (CN): A00002904. 1818
Configuration (CN): A00002907 1823
Configuration (CN): A00002916 1828
Configuration (CN): A00003051 1837
Configuration (CN): A00003147 1841
Configuration (CN): A00003227 1844
Configuration (CN): A00003410 1849

Configuration (CN): A00003411 1852
Configuration (CN): A00003467 1856
Configuration (CN): A00003686 1862
Configuration (CN): A00003696 1864
Configuration (CN): A00004205 1874
Configuration (CN): A00004503 1877
Configuration (CN): A00004563 1890
Configuration (CN): A00004565 1893
Configuration (CN): A00004743 1905
Configuration (CN): A00004750. 1909
Configuration (CN): A00005164 1912
Configuration (CN): A00005802 1915

Performance Management (PF) 1925
Performance (PF): A00001914 1927
Performance (PF): A00001930 1934
Performance (PF): A00002904 1940

Accounting (ACC) 1945
Accounting (ACC): A00002053 1947
Accounting (ACC): A00002364 1954

SN07 Feature Subset Cross Reference Tables: International Features

Feature to Functional Group Cross Reference

Table 1 shows feature IDs, feature titles, and the corresponding functional group (under Stream and release).

For details on specific features, please refer to the FN sections starting on

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00001914.AA11	CEPT International Line Restriction Enhancements	WT20
A00001918.AA13	CEPT Feature Warning with Announcement for Bangladesh	WT20, Core20
A00001919.AA09	CEPT Services Password Enhancement	WT20, Core20
A00001920.AA09	Metering OOS Enhancements	WT20
A00001921.AA14	CIS Toll Call Ringing	WT20, Core20
A00001923.AA16	CIS Subscriber Categories	WT20, Core20
A00001930.AA14	Last and Total Call Meter Inquiry Services	WT20
A00001935	Provisioning Support for Centrex-IP Nodes and Lines	PNM07
A00002053.AA14	AMA Records for Metered Features	WT20, Core20
A00002101.AA17	Allow ITX only SSUTR2	WT20, XPM20
A0002173.AB06	System of Operative-Searching Measures (SOSM) for Digital Multiplex System (DMS) MMP	WT20, Core20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
A00002252.AA04	MG9K Lines Preprovisioning	Core20
A00002291.AA20	Trunk Offering Expansion	WT20, Core20, XPM20
A00002293.AA12	Registered Call Line Option	WT20, Core20
A00002319.AA09	MWI control via ISUP	WT20
A00002364.AA08	CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20	WT20
A00002365.AA08	CWR Support over Trunks for Brazil Market	WT20, Core20
A00002367.AA12	BRI Preset Conference Base	WT20, Core20
A00002377.AA12	10 AFC Keys for BRI Directory Number	WT20, Core20, XPM20
A00002512	GWC-EM Internet Transparency VCAC Provisioning	PNM07
A00002638.AA14	PCA SW Metering Support for Billing	WT20, Core20
A00002639.AA14	CEPT PSTN: Analogue Call Waiting Indication	WT20, Core20
A00002640	CEPT PSTN: Call Forward Delayed Programming	WT20
A00002641.AA20	CEPT PSTN: Analogue Outgoing Call Barring	WT20
A00002642.AA14	CEPT PSTN: Analogue Query and 3Party	WT20, Core20
A00002644	Common Topology Identifier Provisioning	PNM07
A00002654.AA24	CEPT AR (Class Callback)	WT20, Core20
A00002655.AA13	CEPT ACRJ (Rejection of Unidentified Calls)	WT20, Core20
A00002678.AA15	Telefonica IN Enhancements	WT20, Core20
A00002680.AB09	CEPT / Telefonica Spain Changed Number Indication	Core20
A00002702.AA15	No Line Origination Without Charging	WT20
A00002713.AA17	Spanish ISUP enhancements for Telefonica	WT20, CICM07
A00002751.AA08	China BRI Supplementary Services using Keypad protocol	WT20, Core20
A00002754.AA12	China INAP Compliance Enhancement Part 1	WT20

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
A00002755.AA13	China PSTN Line Service Compliance	WT20, Core20
A00002756.AA21	Japan Trunk Services	WT20, Core20, GWC10
A00002844.AA09	Excessive Metering Detection (EMD) Support for Metered Trunks	WT20
A00002884.AA16	ETSI BRI Preset Conference Service Interactions	WT20, Core20
A00002900.AA09	China INAP Compliance Enhancement Part 2	WT20, XPM20, GWC10
A00002904.AA12	CTI Toggle	Core20
A00002916.AA33	CS2K connectivity to XPM remote	Core20, GWC07, XPM07
A00003051.AA07	Call Forward Do Not Answer for BRI Hunt	WT20, Core20
A00003147.AA09	DP Digit Reception Control	WT20, Core20, XPM07
A00003227	SN07, IN support for User to User Service (UUS)	WT20
A00003405.AA03	ECAN Support for International Trunks	Core20
A00003410.AA12	Honduras ETSI ISUP variant	WT20, Core20, XPM07
A00003411.AA10	New TONESET for Honduras	WT20
A00003465.AA14	ETSI BRI Channel reservation override	WT20, XPM20
A00003466.AA06	MLPP Default Precedence Level on Terminations	WT20
A00003467.AA13	Reverse Translations Enhancements via CUSTMOD Option	WT20, Core20
A00003495	APG Integration with MP for NAT Traversal	GWC10
A00003624	H.323 Out-of-band Interworking with APG	GWC10
A00003627.AA24	T.38 FAX Support for International H.323	GWC10

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
A00003686.AA11	Re-Routing Based on Release Cause Value	WT20
A00003695.AA08	ANSI ISUP FGD on CS2K	GWC10
A00003696.AA15	G-ISUP Routing Enhancements	WT20, Core20, GWC10
A00003951	Support for the i2001 Internet Telephone	
A00004205.AA12	Japan PRI Backward Voice Path Solution	WT20, Core20
A00004503.AA11	Calling Party Number Serving Country Code(SCC)	WT20
A00004563.AA12	Moroccan ISUP v2 on DMS100	WT20, XPM20
A00004565.AA15	Line to Moroccan ISUP V2 interworking	WT20, Core20, XPM20
A00004743.AA07	Line originations CLI modification through CALLCNTL in ISN07	WT20
A00004750.AA13	Even Bit Inversion(EBI) Support on DTCO2	Core20
A00004931.AA07	Indian ISUP	WT20, Core20, GWC10
A00004933.AA04	Indian ISUP Charging	WT20, GWC10
A00004981	GWC-EM Internet Transparency VCAC provisioning support for CentrexIP gateways	PNM07
A00005164.AA06	Russia ISUP V2+ on CS2K	WT20, Core20, GWC10
A00005802.AA07	SPM Companding Law Provisioning	Core20
A00006001.AA16	Russian ISUP and Tones for International SPM	Core20, SPM20
A00006032	LROA, LRS and NOCOLL SN07 Support for C&W Cayman	GWC10

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.						
Core20	A00002252.AA04	Y	Y	Y		
Core20	A00002680.AB09	Y		Y		
Core20	A00002904.AA12	Y		Y		Y
Core20, GWC07, XPM07	A00002916.AA33	Y		Y		
Core20	A00003405.AA03	Y				
Core20	A00004750.AA13	Y		Y		
Core20	A00005802.AA07	Y		Y		
Core20, SPM20	A00006001.AA16	Y				
GWC10	A00003495	Y				
GWC10	A00003624	Y				
GWC10	A00003627.AA24	Y				
GWC10	A00003696.AA15	Y				
GWC10	A00006032	Y				
PNM07	A00001935	Y		Y		
PNM07	A00002512	Y				
PNM07	A00002644	Y				
PNM07	A00004981	Y				

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
WT20	A00001914.AA11	Y		Y		Y
WT20, Core20	A00001918.AA13	Y		Y		
WT20, Core20	A00001919.AA09	Y	Y	Y		
WT20	A00001920.AA09	Y	Y	Y		
WT20, Core20	A00001921.AA14	Y		Y		
WT20, Core20	A00001923.AA16	Y		Y		
WT20	A00001930.AA14	Y		Y		Y
WT20, Core20	A00002053.AA14	Y		Y	Y	
WT20, XPM20	A00002101.AA17	Y		Y		
WT20, Core20	A0002173.AB06	Y		Y		
WT20, Core20, XPM20	A00002291.AA20	Y		Y		
WT20, Core2	A00002293.AA12	Y		Y		
WT20	A00002319.AA09	Y		Y		
WT20	A00002364.AA08	Y	Y	Y	Y	
WT20, Core20	A00002365.AA08	Y		Y		
WT20, Core20	A00002367.AA12	Y				
WT20, Core20, XPM20	A00002377.AA12	Y		Y		
WT20, Core20	A00002639.AA14	Y		Y		
WT20	A00002640	Y				

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
WT20	A00002641.AA20	Y		Y		
WT20, Core20	A00002642.AA14	Y		Y		
WT20, Core20	A00002654.AA24	Y		Y		
WT20, Core20	A00002655.AA13	Y				
WT20, Core20	A00002678.AA15	Y		Y		
WT20	A00002702.AA15	Y	Y	Y		
WT20, CICM07	A00002713.AA17	Y		Y		
WT20, Core20	A00002751.AA08	Y		Y		
WT20	A00002754.AA12	Y		Y		
WT20, Core20	A00002755.AA13	Y		Y		
WT20, Core20, GWC10	A00002756.AA21	Y				
WT20	A00002844.AA09	Y	Y	Y		
WT20, Core20	A00002884.AA16	Y				
WT20, XPM20, GWC10	A00002900.AA09	Y		Y		
WT20, Core20	A00003051.AA07	Y		Y		
WT20, Core20, XPM07	A00003147.AA09	Y	Y	Y		
WT20	A00003227	Y		Y		
WT20, Core20, XPM07	A00003410.AA12	Y		Y		
WT20	A00003411.AA10	Y		Y		

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
WT20, XPM20	A00003465.AA14	Y				
WT20	A00003466.AA06	Y				
WT20, Core20	A00003467.AA13	Y		Y		
WT20	A00003686.AA11	Y		Y		
WT20, Core20, GWC10	A00003696.AA15	Y	Y	Y		
WT20, Core20	A00004205.AA12	Y		Y		
WT20	A00004503.AA11	Y		Y		
WT20, XPM20	A00004563.AA12	Y		Y		
WT20, Core20, XPM20	A00004565.AA15	Y	Y	Y		
WT20	A00004743.AA07	Y		Y		
WT20, Core20, GWC10	A00004931.AA07	Y				
WT20, GWC10	A00004933.AA04	Y				
WT20, Core20, GWC10	A00005164.AA06	Y		Y		

Functional Descriptions (FN)

Introduction

This chapter describes new and changed Internatonal features that are planned for this release.

Featid	Title
A00001914.AA11	CEPT International Line Restriction Enhancements
A00001918.AA13	CEPT Feature Warning with Announcement for Bangladesh
A00001919.AA09	CEPT Services Password Enhancement
A00001920.AA09	Metering OOS Enhancements
A00001921.AA14	CIS Toll Call Ringing
A00001923.AA16	CIS Subscriber Categories
A00001929.AA15	RUSSIAN ISUP-ISDN Interworking
A00001930.AA14	Last and Total Call Meter Inquiry Services
A00001935	Provisioning Support for Centrex-IP Nodes and Lines
A00002053.AA14	AMA Records for Metered Features
A00002100.AA12	ISUP_R_2000 (Russia ISUP V2+) Operator Call on Busy Subscriber (Toll Break In)
A00002101.AA17	Allow ITX only SSUTR2
A0002173.AB06	System of Operative-Searching Measures (SOSM) for Digital Multiplex System (DMS) MMP
A00002252.AA04	MG9K Lines Preprovisioning
A00002291.AA20	Trunk Offering Expansion

A00002293.AA12	Registered Call Line Option
A00002319.AA09	MWI control via ISUP
A00002358.AB01	H.323 tunneling over QSIG
A00002364.AA08	CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20
A00002365.AA08	CWR Support over Trunks for Brazil Market
A00002367.AA12	BRI Preset Conference Base
A00002377.AA12	10 AFC Keys for BRI Directory Number
A00002470.AA09	Fixed Price Service for Turkey
A00002512	GWC-EM Internet Transparency VCAC Provisioning
A00002638.AA14	PCA SW Metering Support for Billing
A00002639.AA14	CEPT PSTN: Analogue Call Waiting Indication
A00002640	CEPT PSTN: Call Forward Delayed Programming
A00002641.AA20	CEPT PSTN: Analogue Outgoing Call Barring
A00002642.AA14	CEPT PSTN: Analogue Query and 3Party
A00002644	Common Topology Identifier Provisioning
A00002654.AA24	CEPT AR (Class Callback)
A00002655.AA13	CEPT ACRJ (Rejection of Unidentified Calls)
A00002678.AA15	Telefonica IN Enhancements
A00002680.AB09	CEPT / Telefonica Spain Changed Number Indication
A00002702.AA15	No Line Origination Without Charging
A00002713.AA17	Spanish ISUP enhancements for Telefonica
A00002751.AA08	China BRI Supplementary Services using Keypad protocol
A00002754.AA12	China INAP Compliance Enhancement Part 1
A00002755.AA13	China PSTN Line Service Compliance
A00002756.AA21	Japan Trunk Services

A00002844.AA09	Excessive Metering Detection (EMD) Support for Metered Trunks
A00002884.AA16	ETSI BRI Preset Conference Service Interactions
A00002900.AA09	China INAP Compliance Enhancement Part 2
A00002904.AA12	CTI Toggle
A00002916.AA33	CS2K connectivity to XPM remote
A00003051.AA07	CFGD (Call Forward Group Don't Answer) for BRI Hunt Groups
A00003147.AA09	DP Digit Reception Control
A00003227	SN07, IN support for User to User Service (UUS)
A00003405.AA03	ECAN Support for International Trunks
A00003410.AA12	Honduras ETSI ISUP variant
A00003411.AA10	New TONESET for Honduras
A00003465.AA14	ETSI BRI Channel reservation override
A00003466.AA06	MLPP Default Precedence Level on Terminations
A00003467.AA13	Reverse Translations Enhancements via CUSTMOD Option
A00003495	APG Integration with MP for NAT Traversal
A00003624	H.323 Out-of-band Interworking with APG
A00003627.AA24	T.38 FAX Support for International H.323
A00003686.AA11	Re-Routing Based on Release Cause Value
A00003695.AA08	ANSI ISUP FGD on CS2K
A00003696.AA15	G-ISUP Routing Enhancements
A00003951	Support for the i2001 Internet Telephone
A00004205.AA12	Japan PRI Backward Voice Path Solution
A00004503.AA11	Calling Party Number Serving Country Code(SCC)
A00004563.AA12	Moroccan ISUP v2 on DMS100

A00004565.AA15	Line to Moroccan ISUP V2 interworking
A00004743.AA07	Line originations CLI modification through CALLCNTL in ISN07
A00004750.AA13	Even Bit Inversion(EBI) Support on DTCO2
A00004931.AA07	Indian ISUP
A00004933.AA04	Indian ISUP Charging
A00004981	GWC-EM Internet Transparency VCAC provisioning support for CentrexIP gateways
A00005164.AA06	Russia ISUP V2+ on CS2K
A00005802.AA07	SPM Companding Law Provisioning
A00006001.AA16	Russian ISUP and Tones for International SPM
A00006032	LROA, LRS and NOCOLL SN07 Support for C&W Cayman

1: Functional Description (FN): A00001914

1.1 Feature name

CEPT International Line Restriction Enhancements.

1.2 Description

1.2.1 Introduction

International Line Restriction feature gives the administrator the capability to restrict outgoing calls for the subscriber according to the predefined restriction classes. The administrator can assign, de-assign, activate or deactivate this feature on a line via Service Order or assign and de-assign the feature by using the default option functionality. Subscribers are able to activate, deactivate or interrogate ILR feature by dialing access codes.

The following enhancements are provided by this activity over existing CEPT International Line Restriction Feature:

- Two new restriction classes are defined.
- Temporary opening of barred lines are provided.
- Special tone is given to subscriber who has ILR feature active.

These enhancements are developed according to the requirements of the Bangladesh Market.

The existing International Line Restrictions feature became more flexible by a new activity A00002641 CEPT PSTN: Analogue Outgoing Call Barring. A new table ILRCLASS is defined for datafilling barring classes. For detailed information about this new table, please refer to that feature's FN document.

The ILRCLASS table stores the definition of the barring programs for the ILR service. The International Line Restriction line option references this table.

Table ILRCLASS can hold up to maximum of 100 tuples and the same should be the number of R-Codes, that is R-code range varies from 00 to 99. The R-Codes values are unique in table ILRCLASS, except 'NN'.

During ONP the ILRCLASS table is populated with the previously hard coded barring programs and the R-codes of the ILRCLS tuple in table ISERVOPT. The R-codes are not stored in the ILRCLS tuple in ISERVOPT any more.

During ONPs to this activity, the default tuples are restored.

The existing behavior about activating, deactivating or interrogating ILR feature sequence has not been changed.

The details of the enhancements developed according to the requirements of the Bangladesh Market are below:

1.2.2 New Restriction Classes

Two new restriction classes are defined. These are Deny only National calls (DNATL) and Deny only LoCaL calls (DLCL).

- **DNATL (Deny only NATionaL):** In this restriction class, deny only national class calls but allow other calls.
- **DLCL (Deny only LoCaL):** In this restriction class, deny only local class calls but allow other calls.

These restriction classes are added to the default restriction classes. They will be restored at ONPs similar to existing ones.

Figure 1 Example of table ISERVOPT datafill

```
>table iservopt
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>y
SDT:
>y
CR_PSWD:
>n
TUPLE TO BE ADDED:
ILRCLS
                                        ILRCLS Y Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Figure 2 Example of table ILRCLASS datafil

```
>table ilrclass
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ILRCLASS
>pos dnatl
        DNATL    NN
                                                ( NATL)$
                                                  $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RCODE: NN
>02
IXLAOPT: NATL
>
IXLAOPT:
>$
DNOPT:
>$
TUPLE TO BE CHANGED:
        DNATL    02
                                                ( NATL)$
                                                  $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

1.2.3 Temporary Opening Of Barred Lines

A new functionality is defined for ILR feature. This functionality provides the subscriber to deactivate the feature per call basis. The line will be barred again automatically after subscriber going on hook.

This functionality can be used either for a single party call or at the second leg of a complex call such as enquiry, I3WC or I6WC.

If a subscriber wants to make a call through a direction which has been restricted by his ILR feature already, can use this temporary opening functionality to make the call instead of deactivating the feature totally.

For the single party call, temporary deactivation is done by the subscriber in this way:

(idle) LH SDT # SC * PW # (Special Dial Tone) DIGITS

For complex calls, temporary deactivation is done after flashing:

(flash) SDT # SC * PW # (Special Dial Tone) DIGITS

The Service Code for temporary deactivation is datafilled at table ACCODE. Example datafill at table ACCODE is as follows:

Figure 3 Example datafill of table ACCODE.

```
>table accode
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ACCODE
>pos STARCEPT 34 34
STARCEPT 34 34 FEAT (FTR ILR) (PF 2) (MM 2 15) (FUNC TEMPDEACT) $
```

1.2.4 Special Dial Tone Given To Subscriber when ILR is Active

The subscriber will be warned with a special tone by the system on off hook if he has ILR option active. If the ILR feature is inactive, then the subscriber will hear the ordinary dial tone.

Giving special tone will be optional and determined according to a datafill at table ISERVOPT. A new field is added to the existing ILRCLS tuple named SDT. It can be datafilled as either YES indicating that the special tone will be given or NO for giving ordinary dial tone. The default value for SDT field is N. Example datafill can be seen at Figure 1 for SDT field in ISERVOPT table for ILRCLS tuple.

At MMP19 to MMP20 ONP this field will have the default value N.

1.2.5 Feature Metering

In table MTRFEAT, the feature metering counts are provisioned for ILR operations.

ILR index is used on MTRFEAT table to get the corresponding charge unit counts for assignment, de-assignment, administrator activation, administrator deactivation, subscriber activation, subscriber deactivation and subscriber interrogation.

ILR usage metering option will be used for Temporary Deactivation functionality.

For other details about metering please refer to the A59019295-CEPT International Line Restriction FN document.

1.2.6 OM (Operational Measurements)

The ILR OMs are adopted to support the flexible definition of the barring programs in table ILRCLASS. The ILR OM provides per OM group the number of activations, deactivations, usages and unsuccessful deactivations.

There are two OM groups for ILR. ILR OM group includes ILRCERR, ILRUINT, ILRINTG and newly defined TEMPDAC and TEMPUDAC OM registers.

TEMPDAC, TEMPUDAC OMs are defined for successful temporary deactivation and unsuccessful temporary deactivation counts.

ILRCLASS OM group includes activation, deactivation, usage and unsuccessful deactivation OM registers for barring classes defined at table ILRCLASS.

Refer to PF Section for the details about these registers.

1.3 Hardware Requirements or Dependencies

No hardware dependency.

1.4 Software Requirements or Dependencies

None.

1.5 Limitations and restrictions

Please refer to the activity A59019295-CEPT International Line Restriction FN document for limitations and restrictions about the basic ILR functionalities.

In order to use ILR temporary deactivation functionality when subscriber also has WML feature active, the parameter WML_OCT_IS_LINE_OPT_PARM at table OFCENG should be set to Y and FTCODE field for the WML line option should be Y.

NACK treatment will be applied to the subscriber if he tries to use temporary deactivation when ILR is inactive.

If subscriber interrogates the ILR feature after successful temporary deactivation, CONF tone will be applied as the feature is not fully deactivated but only temporary deactivation has occurred.

After establishing a conference call, it is not able to use temporary deactivation functionality.

Table ILRCLASS does not apply to BRI line option.

The barring programs apply to the whole office. Different barring programs for different customer groups are not possible.

1.6 Interactions

Please refer to the interactions part of the activity A59019295-CEPT International Line Restriction about ILR functionalities.

1.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema ___X___
- User Interface _____
- Element Management _____
- Security _____
- Service Order ___X___
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) ___X___

1.8 Glossary

Term	Description
ILR	International Line Restriction Feature
SC	Service Code
PW	Password
SDT	Special Dial Tone
LH	Lift Handset

2: Functional Description (FN): A00001918

2.1 Feature name

CEPT Feature Warning with Announcement for Bangladesh.

2.2 Description

This feature provides special announcements as warning message for the existing CEPT features, the system will give an announcement (which tells the feature is active) to the subscriber when he goes off hook and then will give dial tone to the subscriber.

This feature provides optional special announcements for the following features ;

- CEPT Do Not Disturb (CDND)
- CEPT Call Diversion Flavours ;
  a. Call Forward Universal (CFU)
  b. Call Forward Fixed (CFF)
  c. Call Forward Busy (CFB - Programmable and Fixed)
  d. Call Forward Don't Answer (CFD - Programmable and Fixed)
  e. Call Diversion To Announcement (CDTA - Absentee service)
  f. Call Diversion To Operator (CDTO)
- CEPT Wakeup Call (IWUC)

Please refer to FN document A59019083 in PLS FMDOC for more detailed information about CDND and CEPT Call Forwarding and also FN document A59019097 for IWUC feature.

This feature also enhances the special dial tone for the line which has active call forward feature. If announcement doesn't take place, providing special dial tone when the user goes off hook will be optional. The telco will have the optionality to give special dial tone or only dial tone to the subscribers.

2.2.1 General Considerations

This activity is being developed for lines which satisfy the following conditions.

- Line must have IBN as Line Class Code.

- Customer group must have CEPT customer group option.
- Line must have CEPT line option.
- Line must have at least one of the CDND, CFU, CFF, CFB, CFD, CDTA, CDTO, IWUC options and its state must be active;

2.2.2 Provisioning the Special Dial Tone

Special dial tone will be optional. If any warning announcement doesn't take place, and any call forward feature is active the system will give special dial tone or only dial tone to the subscriber when he goes off hook according to the new implemented field **SPECIAL_DIAL_TONE** of the existing tuple **CEPT_CFX** in **ISERVOPT** table. Existing **CFD_CFB_INDICATION** field will appear for datafilling only if **SPECIAL_DIAL_TONE** field is datafilled as Y.

Figure 1 Providing the Special Dial Tone in ISERVOPT table

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_cfx
OPTION:
>cept_cfx
OPTIONAL_HASH:
>y
FROM_RANGE:
>1
TO_RANGE:
>18
PRG_OVERRIDE:
>y
ACTIVATE_WITHOUT_PRG:
>y
ISUP_RESTRICTION:
>n
CDND_BSY_TRTMT_SUPP:
>n
MULTIPLE_CFX_ACTIVE:
>n
CFRA_ANNC:
>n
SPECIAL_DIAL_TONE:
>y
CFD_CFB_INDICATION:
>y
TUPLE TO BE ADDED:
CEPT_CFX CEPT_CFX Y 1 18 Y Y N N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

2.2.3 Provisioning the Announcements

This feature makes the warning announcements optional. The Telco operator have the optionality to choose the announcements as warning message.

For taking control of the new announcements, new **CEPT_ANN** tuple is implemented in the existing **ISERVOPT** table.

New **CEPT_ANN** tuple has two main fields as following;

- ANN_STATE
- CEPTANNS
  - — CFU
  - — CFB
  - — CFD
  - — CDND
  - — CDTA
  - — CDTO
  - — IWUC

ANN_STATE field can be datafilled with one of the **DIAL_TONE**, **SPECIAL_DIAL_TONE** or **IMMEDIATELY** options.

Due to more than one subscriber can connect to the same announcement CLLI at the same time, some special conditions may happen as following; if a subscriber goes off hook while another subscriber is already listening to the announcement, then the following subscriber hears DIAL_TONE, SPECIAL_DIAL_TONE or the announcement IMMEDIATELY according to the ANN_STATE field until the announcement returns to the beginning.

If **ANN_STATE** field is set to;

- **DIAL_TONE** : the following subscriber hears dial tone until the announcement returns to the beginning, then he listens to the warning announcement and then hears the dial tone.
- **SPECIAL_DIAL_TONE** : the following subscriber hears special dial tone until the announcement returns to the beginning, then he listens to the warning announcement and then hears the dial tone.
- **IMMEDIATELY** : the following subscriber hears the announcement immediately regardless of which part of the announcement is currently being played, after this part ends, it returns to the beginning and the subscriber listens to the warning announcement from beginning to the end and then hears the dial tone.

The **ANN_STATE** field covers all the announcement types and is valid for all of them.

CEPTANNS field can be datafilled with the feature options which have warning announcements. At least one option must be datafilled for this field and also more than one feature options can be datafilled as well.

If no option was provided for **CEPT_ANN** tuple then an error is given as following and addition or changing the tuple is rejected.

Figure 2 Error message for no option

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_ann
OPTION:
>cept_ann
ANN_STATE:
>IMMEDIATELY
CEPTANNS:
>$
AT LEAST ONE ANNOUNCEMENT OPTION MUST BE DATAFILLED FOR CEPT_ANN TUPLE
TUPLE TO BE ADDED:
CEPT_ANN CEPT_ANN IMMEDIATELY $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

If any of the feature options are provided more than once then an error is given as following and addition or changing the tuple is rejected.

Figure 3 Error message for multiple options

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_ann
OPTION:
>cept_ann
ANN_STATE:
>IMMEDIATELY
CEPTANNS:
>cfu
CEPTANNS:
>cfb
CEPTANNS:
>cfb
CEPTANNS:
>$
MULTIPLE ANNOUNCEMENT OPTIONS ARE NOT ALLLOWED FOR CEPT_ANN TUPLE
TUPLE TO BE ADDED:
CEPT_ANN CEPT_ANN IMMEDIATELY (CFU) (CFB) (CFB) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

If the related feature option is datafilled for the **CEPTANNS** field then, when the subscriber goes off hook he hears warning announcement for this feature. If the related feature option is not datafilled for the **CEPTANNS** field or **CEPT_ANN** tuple does not exist in **ISERVOPT** table, then the subscriber hears the special dial tone or only dial tone as existing states of the features (table 4 describes them).

CFF Functionality is included in CFU, because they have same functionality excluding subscriber programming. If one of CFU or CFF feature is active and **CFU** option is datafilled for the **CEPTANNS** field then subscriber hears announcement as warning message.

In case of one or more features are active together on the same line, each feature will have priority over the other ones. CFU has highest priority in this case. According to these priorities , it is decided which announcement will be given. The following table lists the possible conditions of the announcements in case more than one feature active together (CFU, CFB and CFD can be active together only in case of MULTIPLE_CFX_ACTIVE field of CEPT_CFX tuple in ISERVOPT table is set to Y).

Table 1 Announcement to be given in case of more than one options are active together

Features which are active together	Announcement to be given
CFU or CFF, CFB, CFD, IWUC	CFU
CFU of CFF, CFB, IWUC	CFU
CFU or CFF, CFD, IWUC	CFU
CFB, CFD, IWUC	CFB
CFB, IWUC	CFB
CFD, IWUC	CFD
CDND, IWUC	CDND
CDTA, IWUC	CDTA
CDTO, IWUC	CDTO
Only IWUC	IWUC

If a wakeup request is active for the line and the same line has other announcement options then IWUC announcement has the lowest priority than the other feature announcements.

If the user dials a digit before the announcement hasn't finished then announcement is stopped and it's reverted to normal call processing.

The following table gives brief information about what the subscriber hears when he goes of hook if the announcements take place and the features' oldstates without the announcements.

Table 2 What the subscriber hears when he goes off hook

Features	Old States : SPECIAL_DIAL_TONE : N	Old States : SPECIAL_DIAL_TONE : Y	New states with the announcements
CFU or CFF	Dial Tone	Special Dial Tone	"Your Call Forward Universal feature is active"
CFB	Dial Tone	Special Dial Tone	"Your Call Forward Busy feature is active"
CFD	Dial Tone	Special Dial Tone	"Your Call Forward Don't Answer feature is active"
CDND	Dial Tone	Special Dial Tone	"Your Do Not Disturb feature is active"
CDTA	Dial Tone	Special Dial Tone	"YourCall Diversion To Announcement feature is active"
CDTO	Dial Tone	Special Dial Tone	"Your Call Diversion To Operator feature is active"
IWUC	Dial Tone	Dial Tone	"Your Wakeup Call feature is active"

Example **CEPT_ANN** tuple provisioning is as following;

Figure 4 Provisioning of CEPT_ANN tuple

```
>table iservopt
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_ann
OPTION:
>cept_ann
ANN_STATE:
>IMMEDIATELY
CEPTANNS:
>CFU
CEPTANNS:
>CFB
CEPTANNS:
>CFD
CEPTANNS:
>CDND
CEPTANNS:
>CDTA
CEPTANNS:
>CDTO
CEPTANNS:
>IWUC
TUPLE TO BE ADDED:
CEPT_ANN CEPT_ANN IMMEDIATELY (CFU) (CFB) (CFD) (CDND) (CDTA) (CDTO) (IWUC) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Figure 5 Listing of CEPT_ANN tuple

```
>lis
SOPTSKEY SOPTSVAR
-----------------
CEPT_ANN CEPT_ANN IMMEDIATELY (CFU) (CFB) (CFD) (CDND) (CDTA) (CDTO) (IWUC) $
```

Example announcement datafills are as following;

Figure 6 Table CLLI

```
CLLI ADNUM TRKGRSIZ ADMININF
----------------------------
CEPTCFU 92 30 CEPT_ANNOUNCEMENT
CEPTCFB 93 30 CEPT_ANNOUNCEMENT
CEPTCFD 94 30 CEPT_ANNOUNCEMENT
CEPTCDND 90 30 CEPT_ANNOUNCEMENT
CEPTCDTA 96 30 CEPT_ANNOUNCEMENT
CEPTCDTO 91 30 CEPT_ANNOUNCEMENT
CEPTIWUC 95 30 CEPT_ANNOUNCEMENT
```

Figure 7 Table ANNS

```
CLLI ANNARCH TRAFSNO CYTIME MAXCYC DATA
---------------------------------------
CEPTCFU ALL 1 3 1 STND N 255 1
CEPTCFB ALL 1 3 1 STND N 255 1
CEPTCFD ALL 1 3 1 STND N 255 1
CEPTCDND ALL 1 3 1 STND N 255 1
CEPTCDTA ALL 1 3 1 STND N 255 1
CEPTCDTO ALL 1 3 1 STND N 255 1
CEPTIWUC ALL 1 3 1 STND N 255 1
```

Figure 8 Table ANNMEMS

```
ANNMEM HDWTYPE CARD MEMINFO
---------------------------
CEPTCFU 0 DRAM DRA (0 DTM 0 5) $
CEPTCFB 0 DRAM DRA (0 DTM 0 6) $
CEPTCFD 0 DRAM DRA (0 DTM 0 7) $
CEPTCDND 0 DRAM DRA (0 DTM 0 8) $
CEPTCDTA 0 DRAM DRA (0 DTM 0 9) $
CEPTCDTO 0 DRAM DRA (0 DTM 0 10) $
CEPTIWUC 0 DRAM DRA (0 DTM 0 11) $
```

Figure 9 TABLE ANNPHLST

```
ANNPHKEY PHSLIST
----------------
CEPTCFU 0 (CEPTCFU) $
CEPTCFB 0 (CEPTCFB) $
CEPTCFD 0 (CEPTCFD) $
CEPTCDND 0 (CEPTCDND) $
CEPTCDTA 0 (CEPTCDTA) $
CEPTCDTO 0 (CEPTCDTO) $
CEPTIWUC 0 (CEPTIWUC) $
```

Figure 10 Phrase recording using dramrec level in CI prompt

```
>dramrec
DRAM:
>connect 0 hset 2
CONNECTION MADE
>position CEPTCFU 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTCFB 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTCFD 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTCDND 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTCDTA 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTCDTO 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTIWUC 3 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>disconnect
TRUNK DISCONNECTED
```

The CLLI names of the CEPT announcements are hardcoded and will be added to the CLLI table by the code itself when the CEPT_ANN tuple is added to ISERVOPT table.

Table ANNPHLST can be datafilled after the phrases are recorded in **dramrec** level. The announcement CLLIs use the phrases according to the datafills in table ANNPHLST. In order to be in service, each announcement CLLI must be taken in service by **"bsy;rts"** using the **"mapci;mtc;trks;ttp"** level.

Since the standart announcement type is used for implementing this feature, many subscribers may connect to the same announcement CLLI at the same time, and this max connections number is datafilled at the MAXCONN field of the announcement tuple in table ANNS. This field can be set up to 255.

2.3 Hardware Requirements or Dependencies

n/a

2.4 Software Requirements or Dependencies

n/a

2.5 Limitations and restrictions

- If all the datafills for CEPT announcements are done and if an announce can not be started due to a failure of the announce trunk then special dial tone or only dial tone is provided according to **SPECIAL_DIAL_TONE** of the **CEPT_CFX** tuple. For IWUC feature, only dial tone will be provided.
- In table ANNS, CYTIME field of the announcement tuples should be datafilled the same as the recorded announcement phrase time. If the recorded phrase lengths are bigger than the datafilled CYTIME field of the ANNS table, then from the beginning of the recorded phrase, only the datafilled CYTIME period is played. If the recorded phrase lengths are smaller than the datafilled CYTIME, then after the phrase is finished it will return to the beginning and be played until the datafilled CYTIME period is ended, and dial tone is provided after this time period.
- If a PLGC warm swact takes place during the announcement, digit collection can not be performed, user must go on hook and off hook again.
- Flexible digit analysis can not be used due to the nature of warning announcement feature. Because during the announcement the first digit must be reported to CM to end the announcement and the feature. The feature will revert to normal CallP, so XPM will report the digits seperately.
- When the first subscriber goes off hook and connected to the empty annc trunk member, and if ANN_STATE field is set to DIAL_TONE or SPECIAL_DIAL_TONE, then a short time such as 0.5 sec. dial tone may be connected and then the whole annc is applied due to the XPM applies annc over dial tone in this case.

2.6 Interactions

- Interactions with CFIND and MWT;
  CEPT announcements have lowest priority than CFIND and MWT announcements. If one of them has applied the announcement then CEPT announcements will not be applied.
- WML (Warm Line);
  Warm line timer will start after the announcement is completed.
- If the pilot of DLH/MLH hunt group has one or more of the active announcement features, its members will not get warning announcement due to the members don’t have these feature options. Only the pilot has warning announcement.

2.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema __X__
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

2.8 Glossary

Term	Description
CEPT	Conference of European Posts and Telecommunications
CFU	Call Forward Unconditional
CFF	Call Forward Fixed
CFD	Call Forward Don't Answer
CFB	Call Forward Busy
CDTA	Call Diversion To Announcement
CDTO	Call Diversion To Operator
CDND	CEPT Do Not Disturb
IWUC	CEPT Wakeup Call
SDT	Special Dial Tone
CFIND	Call Forward Indication
MWT	Message Waiting
WML	Warm Line

3: Functional Description (FN): A00001919

3.1 Feature name

CEPT SERVICES PASSWORD ENHANCEMENT

3.2 Description

3.2.1 Introduction

This feature provides password enhancement for CEPT features and remote access to CEPT feature. These two main functionalities are:

3.2.1.1 CEPT Features' Password (CEPTPW)

This feature introduces a new line option to provide unique password for the subscriber. This password is valid for the features which are ILR (International Line Restriction) for IBN lines, OCB (Outgoing Call Barring) for BRI lines.

Currently, ILR and OCB have password utility and have their own passwords. Subscriber can set a new password which is valid for that feature when activating ILR on IBN lines or OCB on BRI lines. Therefore, subscriber can program different passwords for each activation of ILR or OCB.

Instead of this, new password feature provides a unique password for the subscriber, and subscriber will have ability to change this password by activation/programming this feature.

This unique password is used for existing password controlled features ILR, OCB and new feature CEPT Features Remote Access which is described in next section.

3.2.1.2 Cept Features Remote Access (CEPTRA)

This feature introduces new framework (CEPTRA - CEPT Features Remote Access) to control some CEPT feature functionalities of IBN lines from remote agents.

Currently, only CFRA is supported to control CEPT Call Forwarding flavors remotely. This feature replaces this CFRA functionality and CEPTRA controls following CEPT Features

- ILR (International Line Restriction)
- IWUC (International Wake-Up)
- Call Forwarding flavours (CFU, CFB and CFDA)
- CEPTPW (Cept Features' Password which is going to be implemented by first part of this activity).

CEPTRA allows activation/programming, deactivation or interrogation of CEPT features on end user's phone from a remote location. Two ways of using CEPTRA are:

- from a telephone resident on the same switch as the end user's set.
- from a set outside the end user's switch using a Direct Inward System Access (DISA) number

Note: Throughout this document, "base station" refers to end user's telephone set, and base station can only be IBN line.

3.2.2 Notation

ACK Positive acknowledgement

BT Busy Tone

CT Confirmation Tone

DT Dial Tone

FC Feature Code

IND Indication Tone

LH Lift Handset

NACK Negative Acknowledgement

RR Register Call (Flash)

RH Replace Handset

SC Service Code

SCT Special Confirmation tone

SDT Special Dial Tone

SIT Special Information Tone

TN Telephony Number

3.2.3 General Considerations

CEPTPW feature is provided for both IBN and BRI lines. There are some prerequisites to allow CEPTPW which are

- Line should have CEPT line option in order to use CEPTPW option if line class code is IBN.

- CEPTPW is supported only on ETSI version of BRI lines.
- CEPTPW is applicable only Point To Multipoint connection type of BRI lines.
- A new tuple CEPTPW should be provisioned to assign this feature to the subscriber.

CEPTRA is provided for only base agents whose Line Class Code is IBN.

- Line should have CEPTPW option.
- CEPTPW feature should be in “ACTIVE” state.

3.2.4 Feature Description of CEPTPW

This feature (CEPTPW) is assigned to the subscriber in following two ways:

- Assign directly to the subscriber by SERVORD
- Assign as a default CEPT feature via customer group

Feature has one line option field “STATUS” indicating status of the feature, it has three different states which are:

- DEACTIVE : states that password is equal to DEFAULT PIN which is provisioned in ISERVOPT table. Subscriber should activate password by using password changing sequence on his telephone, after that he will be able to use password controlled features such as ILR or CEPTRA. If he tries to perform one of the actions of password controlled features, he will get announcement “PLEASE CHANGE YOUR PASSWORD FIRSTLY”, after that he should goes on hook and should change the password by dialing activating/programming digit sequence of CEPTPW.
- ACTIVE: states that password is changed by the subscriber on his telephone, and has ability to use password controlled features.
- LOCKED: states that maximum wrong password entry is reached while performing password controlled features. Subscriber could not use password controlled features if the status of feature is LOCKED, he will get announcement “YOUR PASSWORD IS LOCKED, PLEASE CONTACT WITH NEAREST TELECOM MANAGEMENT TO YOU” while he tries to perform one of the actions of password controlled features.

Administrator can assign, deassign, activate and deactivate this feature via SERVORD. Administrator can only activate this feature via SERVORD if and only if CEPTPW is in “LOCKED” state in order to give permission to subscriber to control password related features. In this case, password is not changed, remains same as before and subscriber continues to use old password, this process is used if subscriber remembers the old password. Otherwise, if subscriber does not remember the PIN while CEPTPW is in “LOCKED” or “ACTIVE” state, administrator deactivates the feature via

SERVORD in order to reset the password as DEFAULT_PIN and set feature status as “DEACTIVE” which means subscriber should change the PIN to activate the feature by dialing activation digit sequence.

Subscriber can perform two actions to control this feature which are:

- **Activation/Programming**: (idle) LH DT * SC * OLD_PW * NEW_PW * NEW_PW# SCT RH
- **Interrogation**: (idle) LH DT *# SC * PW # SCT RH

The prerequisites to execute the CEPTPW are the followings:

- provisioning parameters in a new CEPTPW tuple in ISERVOPT table
- provisioning announcements
- assigning CEPTPW by SERVORD or as a default CEPT feature for IBN lines.

There are some parameters which are provisioned in existing ISERVOPT table in order to execute this feature, this is done by adding new tuple named as CEPTPW in this table and explained in detail at next section.

3.2.4.1 Provisioning ISERVOPT parameters

There is a new tuple defined for this feature in table ISERVOPT, and the parameters of this tuple is required for CEPTPW and CEPTRA performing. This new tuple includes the following parameters:

- **MAX_PIN_RETRY** {0 TO 9}: indicates that how many times that subscriber can enter wrong PIN while doing password related issues. ‘0’ means infinite PIN retry is allowed.
- **DEFAULT_PIN** {TABLE [0 TO 3] OF DIGIT}: indicates that the initial PIN when administrator assigns this feature to the subscriber. Subscriber should change the default PIN to activate the password feature.
- **PIN_VALIDATION** {BOOLEAN}: indicates that changing of unique password of which all digits are same as each other such as ‘2222 or 3333’ is disallowed or allowed. If it is set as ‘Y’, PIN validity is on and such PIN programming is not allowed and subscriber will get NACK tone or announcement “PASSWORD NUMBERS CAN NOT BE SAME AS EACH OTHER. PLEASE PROGRAM A DIFFERENT PASSWORD” according to announcement availability.
- **ANNOUNCE** {BOOLEAN}: indicates that announcements are used instead of SDT while user programming. Announcements will be applied to the subscriber if it is set as ’Y’; otherwise when it is set as ’N’, SDT or NACK/CONFIRMATION tone will be applied instead of announcements.
- **ANNOUNCE_STATE** {SILENCE, AUD_ RNG}: indicates that the subscriber hears only silence or audible ringing until the announcement

returns to the beginning, then he listens related announcement. This field is visible only if ANNOUNCE field is set as ‘Y’; otherwise it is invisible because there is no need to define announcement state since tones are used instead of them.

- **CEPT_ANNCS** {CEPT_ANNC_VECTOR}: indicates the used announcements in CEPTRA and CEPTPW features and the corresponding announcement trunk which is connected for the entered announcement name. This optionality provides flexibility to use any announcement CLLIs. Please refer to the Configuration section of this feature for more details.

The ISERVOPT table can be datafilled as follows:

Figure 1 Example of datafilling CEPTPW tuple when ANNOUNCE is ‘Y’

```
>table iservopt
>add
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT PIN:
>1111
PIN_VALIDATION:
>y
ANNOUNCE
>y
ANNC_STATE:
>SILENCE
CEPT_ANNCS:
>dnpin ceptra_dnpin
CEPT_ANNCS:
>chgpin ceptpw_chgpin
CEPT_ANNCS:
>vldpin ceptpw_vldpin
CEPT_ANNCS:
>$
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1234 Y Y AUD_RNG (DNPIN CEPTRA_DNPIN)
(CHGPIN CEPTPW_CHGPIN) (VLDPIN CEPTPW_VLDPIN) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

The tuple can be seen from the listing of ISERVOPT table as follows:

Figure 2 The View of CEPTPW Tuple in ISERVOPT Table (ANNOUNCE is 'Y')

```
>table iservopt

SOPTSKEY                                                SOPTSVAR
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
CEPTPW CEPTPW 3 1111 Y Y SILENCE (DNPIN CEPTRA_DNPIN) (CHGPIN CEPTPW_CHGPIN)
(VLDPIN CEPTPW_VLDPIN)$
```

Figure 3 Example of datafilling CEPTPW while ANNOUNCE field is 'N'

```
>table iservopt
>add
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT PIN:
>1111
PIN_VALIDATION:
 >y
ANNOUNCE
 >n
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1111 Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

In this case, the tuple can be seen from the listing of ISERVOPT table as follows:

Figure 4 The View of CEPTPW Tuple in ISERVOPT Table (ANNOUNCE is 'N')

```
>table iservopt

SOPTSKEY                                                SOPTSVAR
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
CEPTPW  CEPTPW                                          3 1111 Y N$
```

Deletion of this tuple is allowed even if there is already a line with CEPTPW option or CEPTPW is provisioned as a default CEPT feature. However, a message is displayed in order to warn administrator that CEPTPW will not provide its functionality at all. This warning message is :

'WARNING: CEPTPW can be on any agent or default CEPT feature. WARNING: CEPTPW does not work without this tuple.'

Additionally, if this tuple is not datafilled in ISERVOPT table, assigning of this feature by SERVORD or default CEPT feature is not allowed. A message is generated as warning **'CEPTPW tuple is not datafilled in ISERVOPT table'**

3.2.4.2 Provisioning Announcements

Announcements can optionally be provided instead of supported tones. The new tuple CEPTPW has ANNOUNCE fields, taking the values {N, Y}.

- if the CEPTPW tuple is not present, or the field ANNOUNCE is set to 'N', tones are given
- If ANNOUNCE is set to 'Y' announcements are provided instead of tones.

The announcement type to be used in table ANNS is STD.

The announcements are:

- **CEPTPW_CHGPIN** : '*Please change your password firstly by activating CEPTPW feature*'

This announcement is applied to the subscriber when he tries to use one of the password controlled features in case of CEPTPW is in DEACTIVE state (means unique password is reset as DEFAULT PIN provisioned in ISERVOPT table). This announcement is datafilled as CEPTPW_CHGPIN 0 in the Figure 5.

- **CEPTPW_LOCKED** : '*Your password is LOCKED. Please contact with nearest TELECOM management to you*'

This announcement is applied to the subscriber when he tries to use one of the password controlled features in case of CEPTPW is in LOCKED state (meant subscriber had entered number of MAX_PIN_RETRY times wrong password sequentially). This announcement is datafilled as CEPTPW_LOCKED 0 in the Figure 5.

- **CEPTPW_VLDPIN** : '*Password numbers can not be same as each other. Please program a different password*'

This announcement is applied to the subscriber when he tries to change/ program a unique password of which digits are the same as each other such as '1111' or '3333'. This restriction is valid only if the PIN_VALIDATION field of CEPTPW tuple in ISERVOPT table is set as 'Y'; otherwise such PIN entries

are allowed.This announcement is datafilled as CEPTPW_VLDPIN 0 in the Figure 5.

Additionally, this announcement is applied to the subscriber when he tries to change the unique password to the default password provisioned in CEPTPW tuple. In this case,

if **PIN_VALIDATION** is **N**, this announcement is:

'*Password can not be equal to default password. Please program a different password*'

If **PIN_VALIDATION** is **Y**, this announcement is:

'*Password can not be changed as default password or password digits can not be same as each other. Please program a different password*'

- **CEPTRA_DNPIN** : 'Please enter your telephone number followed by the star key and your unique password'

This is an interruptible announcement and applied to the subscriber when he dials DISA DN in order to use CEPTRA. It is datafilled as CEPTRA_DNPIN 0 in the datafill example in the Figure 5.

- **CEPTRA_SCODE** : '*Please enter a code to activate deactivate or query the status of desired CEPT feature*'

This is an interruptible announcement and is applied to the subscriber when he entered telephone number and password successfully in time of using CEPTRA. It is datafilled as CEPTRA_SCODE 0 in the datafill example in the Figure 5.

In case of failure of applying any of this announcements (for example, desired announcement is not provisioned in CEPTPW tuple) the corresponding tone will be applied to the subscriber. Mapping between tones and announcements is as shown Table 1 below.

Table 1 Announcement to Tone mapping

Announcement	Tone
CEPTRA_DNPIN	**Special Dial Tone (SDT)** or **Dial Tone** (it is applied in case of R1 loopback trunk connection required)
CEPTRA_SCODE	

Announcement	Tone
CEPTPW_CHGPIN	NACK tone
CEPTPW_LOCKED	
CEPTPW_VLDPIN	

Figure 5 Announcement Provisioning

```
TABLE CLLI
CLLI          ADNUM TRKGRSIZ        ADMININF
-------------------------------------------------------------------------------------------
CEPTPW_CHGPIN 991          5    CEPTPW_ANNOUNCEMENT
CEPTPW_LOCKED 992          5    CEPTPW_ANNOUNCEMENT
CEPTPW_VLDPIN 993          5    CEPTPW_ANNOUNCEMENT
CEPTRA_DNPIN    994        5    CEPTRA_ANNOUNCEMENT
CEPTRA_SCODE   995         5    CEPTRA_ANNOUNCEMENT

TABLE: ANNS
CLLI          ANNTYP          TRAFSNO MAXCONN CYTIME MAXCYC
-------------------------------------------------------------------------------------------
CEPTPW_CHGPIN     ALL 1 3 1 STND N 255 1
CEPTPW_LOCKED     ALL 1 3 1 STND N 255 1
CEPTPW_VLDPIN     ALL 1 3 1 STND N 255 1
CEPTRA_DNPIN      ALL 1 3 1 STND N 255 1
CEPTRA_SCODE      ALL 1 3 1 STND N 255 1


TABLE: ANNMEMS
ANNMEM HDWTYPE           CARD    MEMINFO
-------------------------------------------------------------------
CEPTPW_CHGPIN 0 DRAM DRA (0 DTM 0 5)$
CEPTPW_LOCKED 0 DRAM DRA (0 DTM 0 6)$
CEPTPW_VLDPIN 0 DRAM DRA (0 DTM 0 7)$
CEPTRA_DNPIN   0 DRAM DRA (0 DTM 0 8)$
CEPTRA_SCODE   0 DRAM DRA (0 DTM 0 9)$

TABLE: ANNPHLST
ANNPHKEY    PHSLIST
-----------------------------------
CEPTPW_CHGPIN 0 (CEPTPW_CHGPIN) $
CEPTPW_LOCKED 0 (CEPTPW_LOCKED) $
CEPTPW_VLDPIN 0 (CEPTPW_VLDPIN) $
CEPTRA_DNPIN 0 (CEPTRA_DNPIN) $
CEPTRA_SCODE 0 (CEPTRA_SCODE) $
```

NOTE: This announcement applied to the subscriber if ANNOUNCE field in CEPTPW tuple which is provisioned in ISERVOPT table is datafilled as ‘Y’, otherwise tones (SDT, NACK) are used instead of announcements if this field is datafilled as ‘N’.

Figure 6 Phrase recording using dramrec level in CI prompt

```
>dramrec
DRAM:
>connect 1 hset 0
CONNECTION MADE
>position CEPTPW_CHGPIN 5 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTPW_LOCKED 5 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTPW_VLDPIN 5 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTRA_DNPIN 5 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>position CEPTRA_SCODE 5 pad 1
RECORDING ON DRAM 0
USE TRUNK HSET MEMBER 2
>disconnect
TRUNK DISCONNECTED
```

Table ANNPHLST can be datafilled after the phrases are recorded in **dramrec** level. The announcement CLLIs use the phrases according to the datafills in table ANNPHLST. In order to be in service, each announcement CLLI must be takes in service by **"bsy;rts"** using the **"mapci;mtc;trks;ttp"** level.

Since the standard announcement type is used for implementing this feature, many subscribers may connect to that same announcement CLLI at the same time, and this max connections number is datafilled at the MAXCONN field of the announcement tuple in ANNS. This field can be set up to 255.

3.2.4.3 Provisioning CEPTPW as Default Feature for IBN lines

In the existing functionality, CEPT customer line option is assigned to customer group with DEFAULT_FEATURE_ON (Y/N) parameter, and if the default feature is set to Y, there will be optional sub fields indicate default features. It is expressed as following:

CUST783 CEPT CEPT Y (ICWT)(WML) (IWUC) (CDND) (CFU) (CFB) (CFD) (CFRA) (ILR)(SCL) (ICT)(LNR) (I3WC)(I6WC) (CCBS) $

This feature defines a new default feature CEPTPW as sub field of CEPT tuple in CUSTSTN. Since CEPTPW option is incompatible with CFRA option, operator could not add CEPTPW and CFRA together to the same customer group, that means they can not be assigned same customer group. In this case, an error message will be printed

"**WARNING: CEPTPW AND CFRA ARE INCOMPATIBLE OPTIONS. WARNING: PLEASE REMOVE ONE OF THEM**".

Subscriber can activate CEPTPW even if it isn't on line while CEPTPW is a default feature. In this case, subscriber can try activation infinite times.

The datafilled tuple will be as following:

CUST783 CEPT CEPT Y (ICWT)(WML) (IWUC) (CDND) (CFU) (CFB) (CFD) (ILR)(SCL) (ICT)(LNR) (I3WC)(I6WC) (CCBS) (**CEPTPW**)$

3.2.4.4 Servord Provisioning

Servord Provisioning is provided only CEPTPW feature, and it can be controlled by the following operations:

- Administrator assignment
- Administrator deassignment
- Administrator activation
- Administrator deactivation
- Subscriber activation/programming
- Subscriber interrogation

3.2.4.4.1 Administrator Assignment

This feature is assigned by the administrator via Service Order when requested by the subscriber.

For IBN lines:

The CEPT line option is prerequisite for CEPTPW line option, so CEPT line option must be assigned first or at the same time to assign CEPTPW line option to a subscriber.

If CEPTPW option is assigned to a subscriber not having CEPT option, an error message "**Can not add CEPTPW option if line does not have CEPT option, firstly add CEPT line option**" is printed on screen.

The administrator has to enter one field STATUS within the CEPTPW option.

- STATUS should be entered "DEACTIVE". The administrator is unauthorized to enter "ACTIVE" or "LOCKED" as STATUS in order to comply with the requirement that is subscriber should activate password feature on his telephone after assignment.

Figure 7 Example of CEPTPW Assignment via Service Order for IBN lines

```
>servord
SO:
>ado
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
---------------------------------------------------------------------------------------
>qdn 7835487
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DN:       7835487
NAME: UNASSIGNED
TYPE: SINGLE PARTY
LINESNPA: 111   SIG: DT    LNATTIDX:    1
LINE EQUIPMENT NUMBER:     HOST  00 0 00 04
LINE CLASS CODE:      STD
LINE TREATMENT GROUP:     0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    45
PM TERMINAL NUMBER :    5
OPTIONS
DGT  CEPT  CEPTPW  DEACTIVE
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 8 Example of CEPTPW Assignment via Service Order for BRI lines

```
>servord
SO:
>ado
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
>1
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
>qdn 7831012
--------------------------------------------------------------------------------
DN:    7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1      2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC
CEPTPW DEACTIVE

--------------------------------------------------------------------------------
```

3.2.4.4.2 Administrator Deassignment

The administrator may deassign CEPTPW option by using the DEO (Delete Option) command via Service Order.

For IBN lines:

Removing of CEPT line option from a line is not allowed to the administrator, when CEPT and CEPTPW options are both on the line. An error message '**Deletion of CEPT line option is not allowed when CEPTPW option is on**

the line' is printed when the administrator tries to delete CEPT option from a line.

Figure 9 Example of Deassignment via Service Order for IBN lines

```
>servord
SO:
>deo
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 0 2 15 AM  7835487 (CEPTPW) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY?  (Y OR N)
>y
```

Figure 10 Example of Deassignment via Service Order for BRI lines

```
>servord
SO:
>deo
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY
>1
OPTION:
>ceptpw
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 0 2 15 AM  7835487 (CEPTPW) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY?  (Y OR N)
>y
```

3.2.4.4.3 Administrator Activation

The administrator can activate CEPTPW feature if and only if CEPTPW is already in “LOCKED” state which means subscriber exceeds the maximum wrong PIN entry while performing password related feature actions.

This action is performed when subscriber remembers the old PIN and wants to continue to use this PIN as CEPT password.

Figure 11 Example of CEPTPW Activation via Service Order for IBN lines

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>ACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW ACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
---------------------------------------------------------------------------------------
>qdn 7835487
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DN:       7835487
NAME: UNASSIGNED
TYPE: SINGLE PARTY
LINESNPA: 111   SIG: DT    LNATTIDX:    1
LINE EQUIPMENT NUMBER:     HOST  00 0 00 04
LINE CLASS CODE:      STD
LINE TREATMENT GROUP:     0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    45
PM TERMINAL NUMBER :    5
OPTIONS
DGT  CEPT  CEPTPW  ACTIVE
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 12 Example of CEPTPW Activation via Service Order for BRI lines

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
> 1
OPTION:
>ceptpw
STATUS:
>ACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW ACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
>qdn 7831012
--------------------------------------------------------------------------------
DN:    7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1      2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC
CEPTPW ACTIVE

--------------------------------------------------------------------------------
```

3.2.4.4.4 Administrator Deactivation

The administrator may deactivate the CEPTPW on a subscriber line by using the CHF (Change Feature) command, this action can be performed if CEPTPW is already in “ACTIVE or “LOCKED” states.

This action is performed when subscriber do not remember the old PIN and wants to use default password as CEPT password. However, subscriber should have activate the CEPTPW after this function because it is now in DEACTIVE state.

Figure 13 Example of CEPTPW Deactivation via Service Order for IBN lines

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
---------------------------------------------------------------------------------------
>qdn 7835487
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DN:       7835487
NAME: UNASSIGNED
TYPE: SINGLE PARTY
LINESNPA: 111   SIG: DT    LNATTIDX:    1
LINE EQUIPMENT NUMBER:     HOST  00 0 00 04
LINE CLASS CODE:      STD
LINE TREATMENT GROUP:     0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    45
PM TERMINAL NUMBER :    5
OPTIONS
DGT  CEPT  CEPTPW  DEACTIVE
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 14 Example of CEPTPW Deactivation via Service Order for BRI lines

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
> 1
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
>qdn 7831012
--------------------------------------------------------------------------------
DN:    7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1      2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC
CEPTPW DEACTIVE

--------------------------------------------------------------------------------
```

3.2.4.4.5 Subscriber Activation/Programming

CEPTPW option is in DEACTIVE state after assignment or deactivation by administrator, after these two actions subscriber should activate CEPTPW by using following dialing sequence:

(idle) LH DT * SC * OLD_PW * NEW_PW * NEW_PW# SCT RH

OLD_PW and NEW PW is a four digits pass code and OLD PW is equal to DEFAULT_PW provisioned in table ISERVOPT. NEW_PW should be different that OLD_PW and should not be equal to DEFAULT_PIN.

There is no difference in dialing digit sequence for activation or programming, the difference is if the OLD_PIN is equal to DEFAULT_PIN, this action is called as “activation” and state of the CEPTPW feature is set as “ACTIVE”, NEW_PW is set as a unique CEPT password; otherwise, action is called as ‘programming” and only action is setting NEW_PW as unique CEPT password.

For only IBN lines, during the talking mode the subscriber may activate the CEPTPW by dialing the following digit sequence:

(talking) RR SDT * SC * OLD_PW * NEW_PW * NEW_PW# SCT RH

The dialling accode for activation is provisioned in ACCODE table for IBN lines. The datafilling of ACCODE table is as follows:

For IBN lines:

```
>table accode

XLANAME     FROMD     TOD     XLADATA
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
STARCEPT  66  66  FEAT (FTR  CEPTPW) (PF 2) (MM 2 20) (FUNC  ACT) $
```

The dialling code for activation is provisioned in IBNXLA table for BRI lines. The datafilling of IBNXLA table is as follows:

For BRI lines:

```
>table ibnxla
TOP
KEY RESULT
----------
PTTACT 66 FEAT N N CEPTPWA
```

When journal file is active, subscriber activation data is updated on journal file. If journal file is inactive, CSFJF log is generated.

3.2.4.4.6 Subscriber Interrogation

The subscriber may interrogate if the subscriber remembers the right CEPT unique password. In the following sequence, the subscriber receives a SCT, when dialed password is equal to CEPT unique password.

(idle) LH DT *# SC * PW # SCT RH

For IBN lines, during the talking mode the subscriber may interrogate the password by dialing the following sequence:

(talking) RR SDT *# SC * PW # SCT (talking) RH

If the dialed password is same as the CEPT unique password the subscriber receives a SCT, otherwise the dialed password is not right receives a SIT.

The dialling accode for interrogation is provisioned in ACCODE table for IBN lines. The datafilling of ACCODE table is as follows:

For IBN lines:

```
>table accode

XLANAME     FROMD     TOD     XLADATA
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
STARCEPT  C66  C66  FEAT (FTR  CEPTPW) (PF 3) (MM 2 10) (FUNC  INT) $
```

The dialling code for interrogation is provisioned in IBNXLA table for BRI lines. The datafilling of IBNXLA table is as follows:

For BRI lines:

```
>table ibnxla
TOP
KEY RESULT
----------
PTTACT C66 FEAT N N CEPTPWI
```

3.2.4.5 CEPTPW Interactions with ILR & OCB

CEPTPW feature provides a generic CEPT password for all password related CEPT features which are ILR on IBN lines and OCB on BRI lines. Normally, subscriber have ability to set different passwords while activating these features, therefore if the line has CEPTPW, subscriber should use this unique password for all functions which needs password such as activation or deactivation. However, there are some scenarios in assignment of CEPTPW, and these are explained in Table 2.

Table 2 Password status after feature assignments

Password Status according to options on agent after action is performed						
Before Action			**After Action**			**PASSWORD STATUS**
ILR	OCB	CEPTPW	ILR	OCB	CEPTPW	
X			X		X	Subscriber should use unique CEPT password* while activating ILR.
X		X	X			Subscriber can choose different passwords while activating ILR.
	X			X	X	Subscriber should use unique CEPT password* while activating OCB.
	X	X		X		Subscriber can choose different passwords while activating OCB.
		X	X		X	Subscriber should use unique CEPT password* while activating ILR.
		X		X	X	Subscriber should use unique CEPT password* while activating OCB.

X abbreviates this option exists on this agent.

* Subscriber should activate CEPT generic password after assignment of CEPTPW (by SERVORD or as DEFAULT feature) in order to use password related features (ILR, OCB or CEPTRA). Otherwise, announcement "**Please change your password firstly by activating CEPTPW feature**" is applied to the subscriber and not allowed to control the requested feature.

Administrator assignment of ILR and OCB is different than normal cases when CEPTPW has already on line as line option or default CEPT feature. It is explained as following:

3.2.4.5.1 Administrator Assignment of ILR when CEPTPW is on line

Administrator may assign ILR via SERVORD currently as shown in Figure 11, however when CEPTPW is already on line while assigning ILR, the ILRPW field is not prompted for provisioning since CEPTPW is providing a unique password for this line.

Figure 15 Current Administrator Assignment of ILR (reminder)

```
SO:
>ado
SONUMBER:     NOW   3  4 16 PM
>
DN_OR_LEN:
>7835471
OPTION:
>ilr
ILRCLASS:
>dabe
ILRPW:
>1234
ILRACTIVE:
>y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 16 PM 7835471 ( ILR DABE 1234 Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y

>qdn 7835471
------------------------------------------------------------------------------
DN:     7835471
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  02 0 00 01
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:       CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    44
PM TERMINAL NUMBER :    2
OPTIONS:
CEPT DGT ILR DABE NNNN Y

------------------------------------------------------------------------------
```

Figure 16 Administrator Assignment of ILR while CEPTPW is on line.

```
SO:
>ado
SONUMBER:     NOW   3  4 16 PM
>
DN_OR_LEN:
>7835471
OPTION:
>ilr
ILRCLASS:
>dabe
ILRACTIVE:
>y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 16 PM 7835471 ( ILR DABE Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y

>qdn 7835471
-------------------------------------------------------------------------------
DN:     7835471
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  02 0 00 01
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:       CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    44
PM TERMINAL NUMBER :    2
OPTIONS:
CEPT DGT ILR DABE Y CEPTPW DEACTIVE

-------------------------------------------------------------------------------
>
```

3.2.4.5.2 Administrator Assignment of OCB when CEPTPW is on line

Administrator may assign OCB via SERVORD currently as shown below

Figure 17 Current Administrator Assignment of OCB (reminder)

```
SO:
>
>ado
SONUMBER:     NOW   3  4 17 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
>1
OPTION:
>ocb
BPROG:
>dabe
OCBPW:
>1234
OCBACTIVE:
>y
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 17 AM 7831012 ( 1 OCB DABE 1234 Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>qdn 7831012
------------------------------------------------------------------------------
DN:     7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1       2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:        CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC SMDR
OCB DABE NNNN Y
------------------------------------------------------------------------
```

Assignment of OCB has small difference while CEPTPW is already on line (via SERVORD or as default CEPT feature), the OCBPW field is not prompted for provisioning since CEPTPW is providing unique password for this line. It is expressed as following,

Figure 18 Administrator Assignment of CEPTPW while CEPTPW is on line.

```
SO:
>
>ado
SONUMBER:     NOW   3  4 17 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
>1
OPTION:
>ocb
BPROG:
>dabe
OCBACTIVE:
>y
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 17 AM 7831012 ( 1 OCB DABE Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>qdn 7831012
------------------------------------------------------------------------------
DN:     7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1       2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:        CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC SMDR
OCB DABE Y CEPTPW ACTIVE
------------------------------------------------------------------------
```

3.2.5 Feature Description of CEPTRA

This feature introduces a new framework (CEPTRA - CEPT Features Remote Access) to control some CEPT feature functionalities of IBN lines from remote agents.

3.2.5.1 Provisioning CEPTRA feature

CEPTRA (Cept Features Remote Access) feature provides remote programming of the some CEPT features which are:

- ILR (International Line Restriction)
- IWUC (International Wake-Up)
- Call Forwarding flavours (CFU, CFB and CFD)
- CEPTPW (Cept Features' Password which is going to be implemented by first part of this activity).

In order to use this feature, a DISA DN should be defined with 'CEPTRA' option. This option should be the only option on this DISA DN and is not compatible with other DISA options. This definition can be done in two ways:

- by provisioning DNROUTE table
- by using NEWDN servord command

3.2.5.1.1 Definition DISA DN by provisioning DNROUTE table

DISA DN could be defined by provisioning DNROUTE table as following:

Figure 19 Provision of DNROUTE table

```
TABLE: DNROUTE
>
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AREACODE:
>102
OFCCODE:
>783
STNCODE:
>9999
DN_SEL:
>feat
FEATURE:
>disa
CUSTGRP:
>cust783
SUBGRP:
>0
AUTHREQ:
>n
SMDRTO:
>n
SMDRFROM:
>n
INTRAGRP:
>n
DISAOPT:
>cptra
DISAOPT:
>$
TUPLE TO BE ADDED:
    102    783      9999      FEAT DISA CUST783 0 N N N N (CEPTRA ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
>lis all
TOP
AREACODE OFCCODE   STNCODE                                    DNRESULT
------------------------------------------------------------------------
    102    783      9999      FEAT DISA CUST783 0 N N N N (CEPTRA ) $
BOTTOM
>
```

3.2.5.1.2 Definition DISA DN by NEWDN servord command

DISA DN can be defined with CEPTRA option by using NEWDN command as following:

Figure 20 Processing NEWDN command to define DISA DN with CEPTRA opt.

```
SO:
>newdn
SONUMBER:    NOW  3  4  9 PM
>
BLOCK_OF_DNS:
>no
DN:
>7835499
VDNTYPE:
>disa
CUSTGRP:
>cust783
SUBGRP:
>0
AUTHREQ:
>n
SMDRTO:
>n
SMDRFROM:
>n
INTRAGRP:
>n
DISAOPT:
>cptra
DISAOPT:
>$
OPTION:
>$
COMMAND AS ENTERED:
NEWDN NOW 3 4 9 PM NO 7835499 DISA CUST783 0 N N N N ( CEPTRA ) $ $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>
>qdn 7835499
-------------------------------------------------------------------------------
DN:    7835499
TYPE:                              DISA CUST783 0 NNN
DISAOPT:    CEPTRA
OPTIONS: NONE
-------------------------------------------------------------------------------
```

3.2.5.2 Remote Programming of CEPT Features

The common abbrevations used programming of the CEPT features remotely are explained as following.

A service code (SC), PIN is the Personal Identification Number, TN1 is the DISA DN, TN2 is the base station DN, TN3 is the destination number to which incoming calls of T2 shall be diverted.

3.2.5.2.1 ILR -International Line Restriction

Control Procedure

- Activation and programming: (idle) LH DT TN1 Announcement "CEPTRA_DNPIN" (SDT) TN2 * PIN # Announcement "CEPTRA_SCODE" (SDT) * SC * PIN * CR# SCT RH
- Deactivation: (idle) LH DT TN1 Announcement "CEPTRA_DNPIN" (SDT) TN2 * PIN # Announcement "CEPTRA_SCODE" (SDT) # SC * PIN # SCT RH
- Interrogation: (idle) LH DT TN1 Announcement "CEPTRA_DNPIN" (SDT) TN2 * PIN # Announcement "CEPTRA_SCODE" (SDT) *# SC # SCT RH

A service code (SC) is 33, PIN is the personal Identification Number, CR Call Restriction Programming Digits (provisioned in ILRCLS tuple ISERVOPT table)

During activation and programming;

The subscriber will receive a SIT instead of SCT if the activation fails,

If a restriction needs to be applied on the line, the previous restriction must be cancelled by the subscriber. This ensures that no one can change the restriction class except for those who knows the password.

During deletion;

The subscriber receives a SIT, if an invalid password (PIN) is dialled.

During interrogation;

If ILR is active in the line, subscriber receives SCT otherwise receives SIT.

Please refer to 'CEPT International Line Restriction AT.59019295' for more details.

3.2.5.2.2 IWUC -International Wake-Up Call

- **Control Procedure**
- Activation and programming: (idle) LH DT TN1 Announcement "CEPTRA_DNPIN" (SDT) TN2 * PIN # Announcement "CEPTRA_SCODE" (SDT) * SC * Time # SCT RH
- Deactivation: LH DT TN1 Announcement "CEPTRA_DNPIN" (SDT) TN2 * PIN # Announcement "CEPTRA_SCODE" (SDT) # SC * Time #

SCT RH **or** LH DT TN1 Announcement CEPTRA_DNPIN (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) # SC # SCT RH

- Interrogation: LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *# SC * Time# SCT RH **or** LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *# SC * Time# SCT RH

A service code (SC) of 55 is recommended for the feature.

During activation and programming;

On a successful subscriber activation with programming, ACK treatment will be given.

The subscriber will receive special dial tone when going off hook while feature is active.

During deletion;

On a successful subscriber deletion sequence, ACK treatment will be given and the diversion is cancelled.

For unsuccessful deletion NACK is given and no change in the state of the diversion.

During interrogation;

On a successful subscriber interrogation results in ACK treatment.

On a un successful subscriber interrogation results in NACK treatment.

Please refer to ‘International Wake-Up Call AT.59019097’ for more details.

3.2.5.2.3 CFU – Call Forward Unconditional

Control Procedure

- Activation and programming: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) * SC * TN3 # SCT RH

- Deactivation: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) # SC# SCT RH
- Interrogation: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *# SC # SCT RH

A service code (SC) of 21 is recommended for the feature.

During activation and programming;

On a successful subscriber activation with programming, ACK treatment will be given.

The subscriber will receive special dial tone when going off hook while feature is active.

During deletion;

On a successful subscriber deletion sequence, ACK treatment will be given and the diversion is cancelled.

For unsuccessful deletion NACK is given and no change in the state of the diversion.

During interrogation;

On a successful subscriber interrogation results in ACK treatment.

On a un successful subscriber interrogation results in NACK treatment.

Please refer to ‘CEPT Call Diversion and CEPT Do Not Disturb AT.59019083’ for more details.

3.2.5.2.4 CFB P – Call Forward Busy Programmable

Control Procedure

Activation and programming: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *SC*TN3 ACK RH

Deletion:(idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) #SC#ACK RH

Interrogation: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *#SC#IND RH

A service code (SC) of 60 is recommended for the feature.

During activation and programming;

On a successful subscriber activation with programming, ACK treatment will be given.

The subscriber will receive special dial tone when going off hook while feature is active.

During deletion;

On a successful subscriber deletion sequence, ACK treatment will be given and the diversion is cancelled.

For unsuccessful deletion NACK is given and no change in the state of the diversion.

During interrogation;

On a successful subscriber interrogation results in ACK treatment.

On an unsuccessful subscriber interrogation results in NACK treatment.

Please refer to ‘CEPT Call Diversion and CEPT Do Not Disturb AT.59019083’ for more details.

3.2.5.2.5 CFD P - Call Forward Do not Answer Programmable

Control Procedure

Activation and programming: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *SC*TN3 ACK RH

Deletion: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) #SC#ACK RH

Interrogation: (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) # SC TN3#IND RH

or (idle) LH DT TN1 Announcement “CEPTRA_DNPIN” (SDT) TN2 * PIN # Announcement “CEPTRA_SCODE” (SDT) *#SC#IND RH

A service code (SC) for CFD is datafillable in table ACCODE by the administrator.

During activation and programming;

On a successful subscriber activation with programming, ACK treatment will be given.

The subscriber will receive special dial tone when going off hook while feature is active.

During deletion;

On a successful subscriber deletion sequence, ACK treatment will be given and the diversion is cancelled.

For unsuccessful deletion NACK is given and no change in the state of the diversion.

During interrogation;

On a successful subscriber interrogation results in ACK treatment.

On a unsuccessful subscriber interrogation results in NACK treatment.

Please refer to ‘CEPT Call Diversion and CEPT Do Not Disturb AT.59019083’ for more details.

3.2.6 Info Log for CEPTRA usages

A new log family (CEPT) is introduced by this feature, and it has two members CEPT100 and CEPT101 logs. These are explained as:

3.2.6.1 CEPT100 Log

A new log (CEPT100) is introduced by this feature due to the security reasons and provides to trace back. This log records the some informations which are:

- Base DN
- Originating DN
- Originating Trunk

CEPT100 log is generated if and only if subscriber password feature (CEPTPW) is locked via remote accessing to CEPT features by using CEPTRA.

3.2.6.1.1 CEPT101 Log

This log is generated when subscriber attempts to use supported CEPT features (ILR, IWUC, CEPTPW, CFU, CFD, and CFB) from remote agents via CEPTRA. This log has five fields which are:

- Base DN
- Originating DN
- Originating Trunk
- Feature
- Action

If subscriber can not pass the authorization state (PIN verifying for base agent) or the subscriber has dialed invalid digits of which translation does not result on any CEPT feature request, this log is not generated since there is no feature request.

Please refer to FM section of this book for more details.

3.2.7 Feature Metering

Feature metering is a system used to charge for subscriber feature meterable activities either by the administrator or the subscriber itself. Since this system is not supported on BRI agents, there will be no feature charging for this type of agents while CEPTPW actions are performed.

3.2.7.1 Feature Metering for CEPTPW

In table MTRFEAT, the feature metering counts are provisioned for CEPTPW operations and subscriber is metered for the following operations:

Administrator assignment : A datafillable number of charge units may be charged for each time when the administrator assigns the feature to a line.

Administrator deassignment : A datafillable number of charge units may be charged for each time when the administrator deassigns the feature from a line.

If CEPTPW is a default feature (for only IBN lines), when cancelling default feature optionality of CEPTPW (via removing CEPTPW from CEPT tuple in CUSTSTN table), CEPTPW is automatically deassigned from lines of this customer group, and lines having CEPTPW option is charged as deassign feature metering.

Administrator activation : A datafillable number of charge units may be charged each time when the administrator successfully activates CEPTPW feature in case it is in “LOCKED” state.

Administrator deactivation : A datafillable number of charge units may be charged each time when the administrator successfully deactivates (resets password) CEPTPW feature in case it is in “LOCKED” state.

Subscriber activation : A datafillable number of charge units may be charged for each subscriber successful activation that results with a SCT.

Subscriber Interrogation : A datafillable number of charge units may be charged for each subscriber interrogation.

CEPTPW index is used on MTRFEAT table to get the corresponding charge unit counts for assignment,deassignment, administrator activation, administrator deactivation, subscriber activation and subscriber interrogation.

The subscriber is metered when the administrator enters MOG option and MOG_ID like (mog_0, mog_1, mog_2, . . . etc.) to subscriber’s line via Service Order.

In Figure 21, from the map the provisioning is as follows:

Figure 21 CEPTPW Metering

```
>table mtrfeat
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MTRFEAT

CEPTPW MOG_0  44  (ASSIGN 12)  (DEASSIGN 10) (ADMACT 9)
                  (ADMDEACT 7) (SUBACT 6) (INTERROG 2)  $
```

3.2.7.2 Feature Metering for CEPTRA

There is not new additional feature metering definition for CEPTRA feature and existing procedures are valid. Subscriber is charged for meterable activities when he/she performs remote access programming of related feature, there will be no any additional feature metering for using CEPTRA.

3.2.8 OM (Operational Measurements)

The new OM group CEPTPW is introduced to measure CEPTPW operations. This OM group has 9 registers and named as:

PWACT, PWUACT, PWCHG, PWUCHG, PWINTG, PWUINTG, PWLCK, PWUSG, PWCERR

Additionally, the new OM group CEPTRA is introduced to measure CEPTRA operations. This OM group has 5 registers and named as:

CPTRAATT, CPTRAHOV, CPTRASOV, CPTRAFAL, CPTRASUC

Refer to PF Section for the meaning of these registers and details.

3.3 Hardware Requirements or Dependencies

Not Applicable

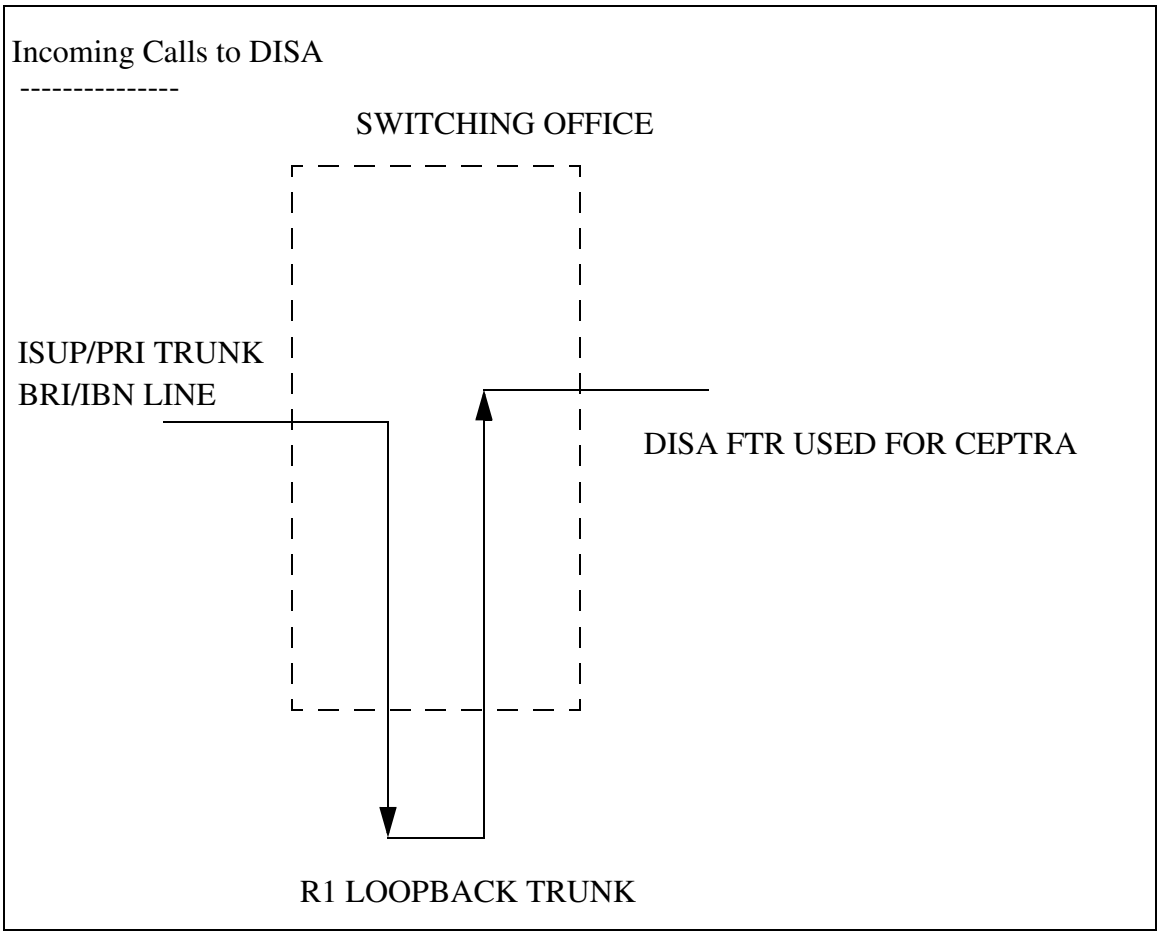
3.4 Software Requirements or Dependencies

Not Applicable

3.5 Limitations and restrictions

- The R1 loopback trunks are required for the CEPTRA feature activation calls made over ISUP/PRI trunks and the BRI lines. Although R1 loopback trunks are not needed for the calls made over IBN line, they are used to have consistency for the metering point of view, therefore, the calls through DISA DN can be metered. Loopback trunks are inserted between all incoming calls and the DISA at the terminating office. In this case, if tones are used instead of announcements, DIAL TONE is applied to the subscriber instead of SDT.

Figure 22 Loopback Trunk Configuration



- CEPTRA should be the only option provisioned in DISA DN. There must be no additional option such as CFRA, SIMRING on DISA DN.
- CEPTPW is incompatible with CFRA option. Administrator could not provision these two option on same agent by SERVORD. In addition, same customer group could not have both options as default CEPT feature, these actions are restricted.
- Digits dialed by subscriber are not considered till related announcement starts. (in CEPTRA)
- Supported trunks are represented in below table. (in CEPTRA)

Table 3 Supported Trunks

ETSI ISUP
R1 (NTLS01, 02,09) , R2 (Base)
ETSI PRI

- For the markets that support the UTR (Universal Tone Receiver) card configuration on the XPM, the digit collection is supported on incoming ISUP/TUP/FDCP R2 trunk directly, no R1 loopback trunks are required. Please refer to activity A00002755 for more details.

3.6 Interactions

- CEPT FEATURES REMOTE ACCESS (CEPTRA) : If the remote station has 3WC, then the remote station will not be allowed to flash & initiate a 3WC once the remote access has started. If the remote station is involved in a call which allows three way calling, the remote station will be allowed to flash and make a remote access call. Once the remote access call is made the remote station will not be allowed to flash again to conference in the original call. The caller must wait for the remote access to complete before attempting to return to the original call. The above restriction is applied only if the remote access call is intra nodal.
- CEPTPW and AUL are incompatible with each other.
- CEPTPW and CFRA are incompatible with each other.

3.7 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	_____
Configuration	
Data Schema	___X__
User Interface	_____
Element Management	_____
Security	_____
Service Order	__X___
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	__X___

3.8 Glossary

Term	Description
CEPT	Counsel for European Postal and Telecommunications
CFBP	Call Forward Busy Programmable
CFDP	Call Forward Don't Answer Programmable
CFU	Call Forward Universal Programmable
CR	Call Restriction Programming Digits
IBN	International Business Network
IWUC	International Wake-Up Call
MOG	Metered Originator Group
OCB	Outgoing Call Barring

3.9 References

REF #	Description of Reference
A59039255 (FMDOC)	Default CEPT feature assignment to all subscribers
A59019083 (FMDOC)	CEPT Call Diversions
A59019295 (FMDOC)	International Line Restriction
A59032661 (FMDOC)	Outgoing Call Barring
A59019097 (FMDOC)	International Wake-Up Call

4: Functional Description (FN): A00001920

4.1 Feature name

Metering OOS Enhancements.

4.2 Description

This feature enhances existing metering structure in terms of deassigned meters of lines. In current metering system, a subscriber becomes meterable via a MOG option. Depending on assigned MOG id, software meters (which may be up to 4) are assigned to subscriber.

When MOG option is removed from subscriber, all assigned meters on subscriber are sent to OOS. If MOG option is reprovisioned on the same DN, meter counts of assigned meters starts with zero, since it is initialized.

The purpose of this feature is to store meter counts of agents when any MOG deletion process is performed and to restore meter counts back when MOG addition is performed on same agent.

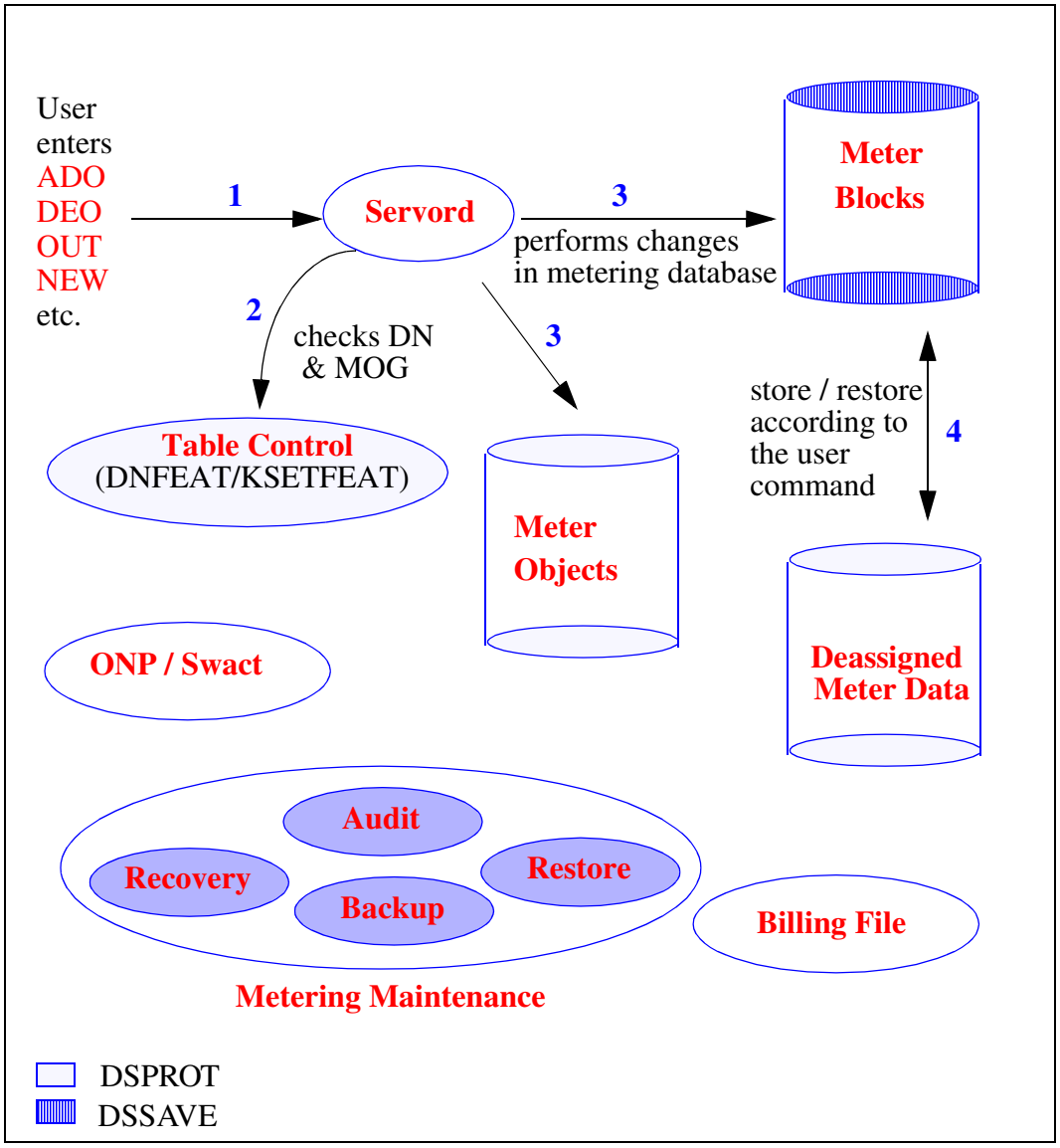
While storing line meter counts, it is important to supply consistency after restarts, image reloads or restore operations. To manage metering consistency for deassigned meters, line metering maintenance processes (Backup & Restore, Audit, Recovery, ONP) are enhanced.

In addition to this, in current metering system, billing records for metered lines are generated by referring to billing file. Billing file includes both OOS meters and INUSE meters which means that deassigned meters are also included in this file.

This feature is optional with a SOC option. When state of SOC is ON, feature becomes active, otherwise system behaves as it was before this functionality.

The feature is implemented in ISN07.

Figure 1 Functional Behavior of Feature



Main changes that have been introduced with this feature can be listed as follows;

- Activation of Feature
- New Table MTRDEASS
- Adding / Deleting MOG Option
- Metering Maintenance Support
- Billing File Interaction
- New Log MTR150

- New NONRES Command DEASCLR

In following sections, changes introduced with this feature are mentioned in details.

4.2.1 Activation of Feature

This feature is functional in Bangladesh and TRNC market. For the other markets this feature is not functional. So activation of feature is controlled by SOC.

METR_Deassigned_Support is a state SOC and it has two states, ON and IDLE. Default state of *METR_Deassigned_Support* is IDLE. When its state is ON, this feature becomes functional.

Table 1 SOC for Activation of Feature

SOC group:	METR
SOC option name:	METR0016
SOC option title:	METR_Deassigned_Support
SOC option control type:	state
New SOC option?	Yes
Option defined in DRU:	WT20
Affected products:	DMS100-MMP

Activation of SOC is done by a password control. The passwords are unique for each office. When deactivation is being performed, a restriction is handled in order not to change state of SOC easily. NCW_MOG parameter in MTRSYSPM table is checked. If value of this parameter is “DISALLOWED”, changing SOC state to IDLE is forbidden. SOC can be set to IDLE, when this parameter is “ALLOWED”. Also if there is at least one tuple in MTRDEASS table, setting state of METR0016 SOC is forbidden.

Note: Changing value of NCW_MOG parameter requires a reload restart.

There is another SOC option within this feature. It is used to decide sending deassigned meters to OOS or not, where Bangladesh behaves differently from other markets.

Table 2 SOC for Preventing to Sent Deassigned Meters to OOS

SOC group:	METR
SOC option name:	METR0017

SOC option title:	METR_Prevent_Sent_OOS
SOC option control type:	state
New SOC option?	Yes
Option defined in DRU:	WT20
Affected products:	DMS100 - MMP

METR_Prevent_Sent_OOS is also a state SOC which has two possible states; ON and IDLE. Default state of SOC is IDLE.

Activation/Deactivation of these two SOC options depends to one another as follows:

- State of *METR_Deassigned_Support* can be set to IDLE only when state of *METR_Prevent_Sent_OOS* is IDLE.
- State of *METR_Prevent_Sent_OOS* can be set to ON only when state of *METR_Deassigned_Support* is ON.

Activation of feature for Bangladesh market is as following:

- State of *METR_Deassigned_Support* is set to ON
- Then, state of *METR_Prevent_Sent_OOS* is set to ON.

Activation of feature for TRNC market is as following:

- State of *METR_Deassigned_Support* is set to ON.
- State of *METR_Prevent_Sent_OOS* is always IDLE.

Activation/Deactivation of *METR_Deassigned_Support* and *METR_Prevent_Sent_OOS* is forbidden while a maintenance process (meter audit/recovery) or billing process is running.

4.2.2 New Table MTRDEASS

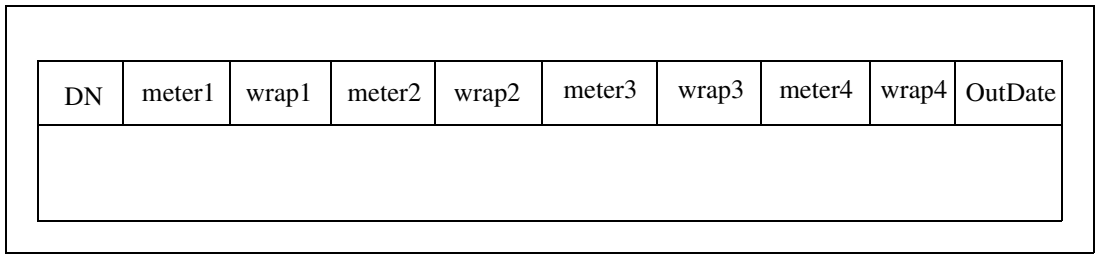
When a metered line (IBN/ETSI BRI) is deleted or when MOG option is removed from a line, assigned meters (which may be up to 4) of DN are stored as deassigned meters in a new table in DSPROT.

To provide a user interface of new storage of deassigned meters, MTRDEASS table is created. This table is read only that is, any of the tuples can not be changed or deleted. But user can see meter counts of deassigned meters of agents whenever requests.

It is important to mention that, while listing meter counts of each meter of agent, meter counts are retrieved from meter blocks in DSSAVE.

The content of each tuple in MTRDEASS table is as follows;

Figure 2 Structure of MTRDEASS Table



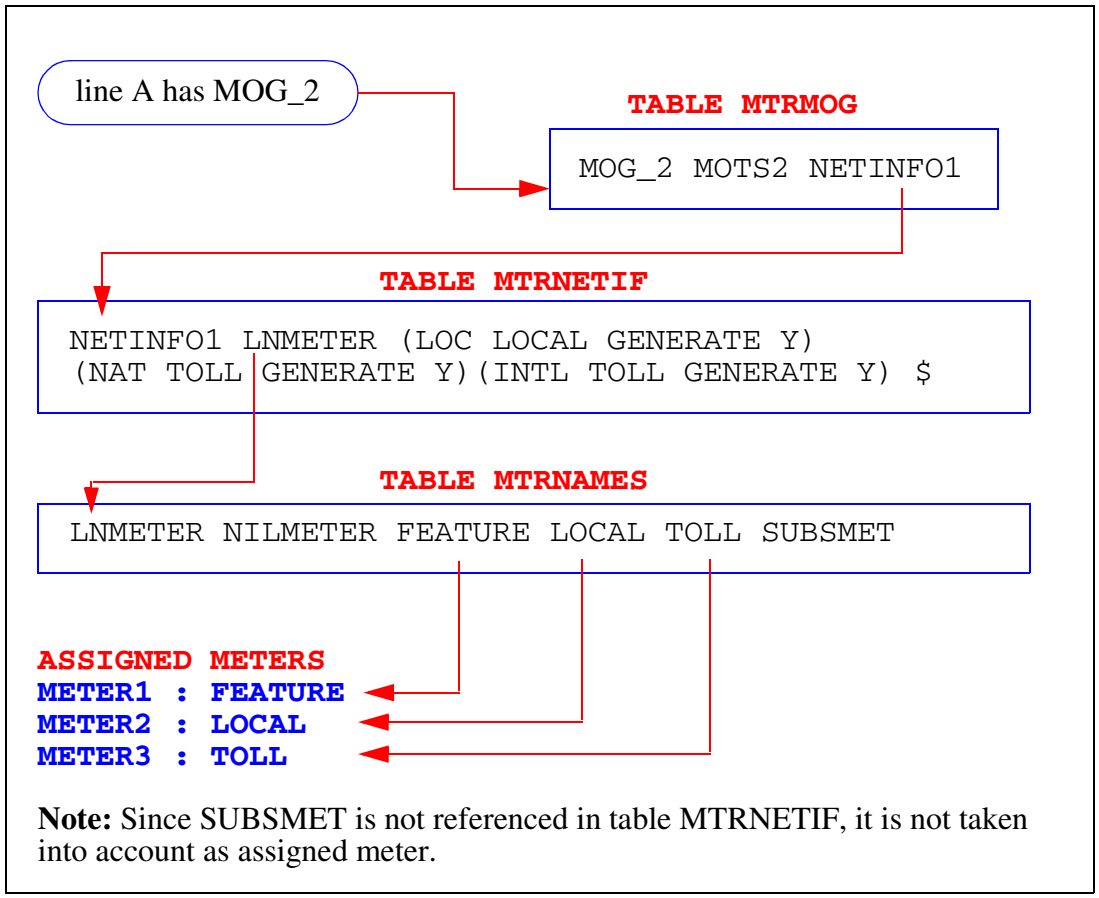
DN: Directory number of agent (which may be up to 18)

Wrap: Y/N, indicating date meter counts has exceeded 99999999 and wrapped.

Date: Date of deleting MOG option. Its format is as follows; yyyy/mm/dd hh:mm:ss. Date is modified every time a change has been made on tuple in MTRDEASS table.

Meter1, meter2, meter3, meter4: Assigned meters which depends on MOG id. These meters are determined as follows:

Figure 3 Retrieving Assigned Meters



Note: Since SUBSMET is not referenced in table MTRNETIF, it is not taken into account as assigned meter.

The table lists last counts of agent when MOG deletion is performed. For every assigned meters (which may be up to 4) of agent, meter count and wrap information are listed with date of adding tuple to MTRDEASS table.

Maximum number of tuples in MTRDEASS table is limited to 65520.

4.2.3 Adding / Deleting MOG Option

When user performs any operation that results with MOG deletion, assigned meters of agent are stored in MTRDEASS table. All servord commands that causes MOG deletion/addition is considered. Some examples of commands are below.

4.2.3.1 Delete MOG Option

DEO command is used to remove an option from a specified DN. While removing MOG option from an agent, its assigned meters are stored in the system as deassigned meters.

If there is no space available in MTRDEASS table to add deassigned meters, a warning message is displayed to inform user about this.

```
Format of warning message is as follows;

NO SPACE AVAILABLE IN MTRDEASS
TABLE.DEASSIGNED METER COUNTS WILL BE LOST!
```

In addition to this, a new MTR log is generated to log last count of each deassigned meter.

Here is the an example of MOG deletion process.

```
>qdn 7835401
-----------------------------------------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:         CUST783      SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA   GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    42
PM TERMINAL NUMBER :    4
OPTIONS:
DGT MOG MOG_2
-----------------------------------------------------
>deo $ 7835401 mog $ y y
COMMAND AS ENTERED:
DEO NOW 3 3 31 AM 7835401 ( MOG ) $
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
```

When MOG option is deleted, corresponding meters in meter block are marked as DEASSIGNED and an entry is added into MTRDEASS table to store deassigned meters.

```
TABLE MTRDEASS
TOP

DEAKEY    METER1   WRAP1 METER2  WRAP2  METER3 WRAP3 METER4 WRAP4  OUT_DATE
-------------------------------------------------------------------------------
1027835401 00000012 N   00000015  N   00000020  N   -------- -   2003/03/31 12:34:00

BOTTOM
```

4.2.3.2 Add MOG Option

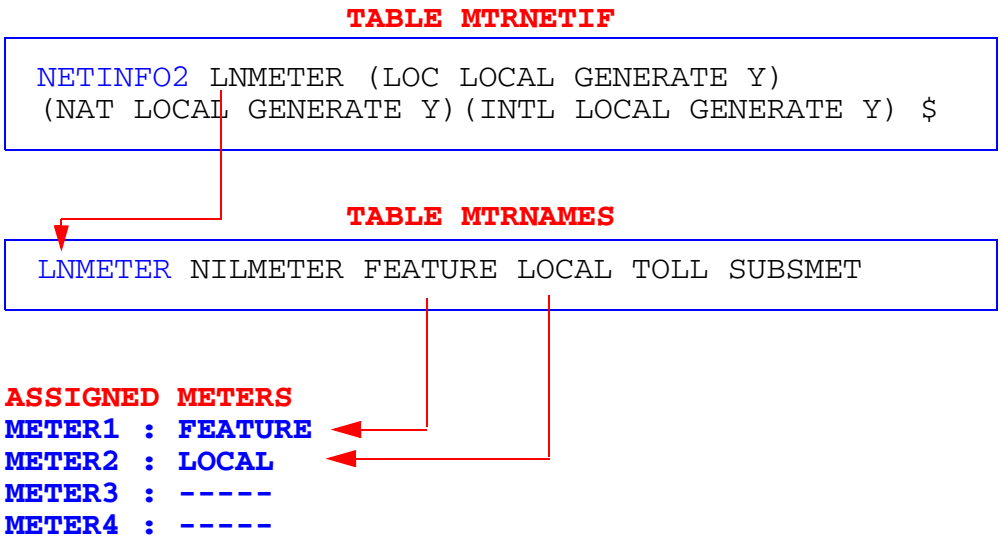
ADO command is used to assign an option to a specified DN. While adding MOG option to a DN, deassigned meter table is checked before assigning new meters to DN. If there is any deassigned meter for the DN, a cross check between new meters and previously deassigned meters is performed. If there is any matching meters, meter counts of these meters are restored. If not, newly assigned meters are initialized to zero.

- If same MOG option is assigned to DN, all deassigned meters are reassigned with last meter counts.

```
>ado $ 7835401 mog mog_2 $ y y
COMMAND AS ENTERED:
ADO NOW 3 3 31 AM 7835401 ( MOG MOG_2) $
1. METER NAME: FEATURE     2.METER NAME: LOCAL
3. METER NAME: TOLL         4.METER NAME: -------
MOGID MOG_2  HAS ABOVE METERS ASSIGNED.

>mtrcount line 7835401
**************************************************
DN      : 1027835401
DATE    : 03/04/01
MTR NAME: FEATURE     MTR COUNT: 00000012 WRAP: N
MTR NAME: LOCAL       MTR COUNT: 00000015 WRAP: N
MTR NAME: TOLL        MTR COUNT: 00000020 WRAP: N
**************************************************
```

- If a different MOG id is assigned to DN,

```
>ado $ 7835401 mog mog_3 $ y y
COMMAND AS ENTERED:
ADO NOW 3 3 31 AM 7835401 ( MOG MOG_3) $
1. METER NAME: FEATURE        2. METER NAME: LOCAL
3. METER NAME: -------        4. METER NAME: ------
MOGID MOG_3 HAS ABOVE METERS ASSIGNED.

Assigned meters of MOG_3 is as follows:
```



Entry in MTRDEASS table is checked whether there is any matching meters with previously deassigned meters. For any matching meter, assigned bits are set to TRUE and mismatched meters are stored in MTRDEASS table.

```
TABLE MTRDEASS
TOP

DEAKEY     METER1    WRAP1 METER2    WRAP2   METER3   WRAP3 METER4    WRAP4 OUT_DATE
-------------------------------------------------------------------------------------
1027835401 -------- -   -------- -    00000020   N   -------- -  2003/03/31 12:34:00

BOTTOM
```

```
>mtrcount line 783540
************************************************
DN      : 1027835401
DATE    : 03/04/01
MTR NAME: FEATURE     MTR COUNT: 00000012 WRAP: N
MTR NAME: LOCAL       MTR COUNT: 00000015 WRAP: N
```

4.2.3.3 Remove a DN From System

OUT command is used to remove an agent from system. If there is MOG option on outed DN, its assigned meters are stored in MTRDEASS table to be able to restore when this DN is given into service with MOG option again.

4.2.3.4 Add a DN to System

NEW command is used to define a new DN in system. With this command, specified option can be assigned to DN. If MOG option is being assigned with NEW command, MTRDEASS table is checked whether there is an entry for DN. If there is, and if any deassigned meters match with newly assigned meters, meter counts of matching meters are restored back.

> ***Note:*** This feature supports restoring deassigned meters of huntgroups (DLH, DNH, MLH) too.

4.2.4 Line Metering Maintenance

Metering database composed of more than one component. Some of them resides in DSSAVE and some of them in DSPROT. These two places are affected by different process such as; DSPROT is affected by image reloads or survives all restarts whereas DSSAVE survives during image reboots and affected by RESTORE process.

Because of different effects of restarts, image reloads or restore operations there may occur inconsistencies between data in DSSAVE and data in DSPROT.

To detect and recover these inconsistencies, Audit and Recovery processes are run.

- **Meter recovery process**

Meter recovery process runs after each reload restarts and meter restore processes. After reload restarts or restore processes there may be inconsistencies in metering system. Recovery process handles this within three main passes.

In first pass, link between meter object (DSPROT) and meter blocks (DSSAVE) are broken to be associated again in further steps.

In second pass, meter blocks in inservice meter table in DSSAVE are traversed. For every in use meter block, its meter object pointer and mog id is retrieved from DNFEAT/KSETFEAT table.

- If there is no entry for this DN in DNFEAT/KSETFEAT table, or
- If there is no meter object pointer, or
- If there is no MOG option on this agent,

then this agent is decided to be recycled with its all assigned meters.

If agent has a valid meter object pointer and MOG option, assigned meters in agent data and in meter block are compared, if there is a difference, mismatched meter is recycled.

In third pass of recovery process, all meter objects are traversed to find if there is any meter object which has MOG option but has no associated meter block. If there is any, a new meter block is allocated in DSSAVE.

- **Line Meter Audit Process**

Line audit runs periodically, manually and after all restarts to verify the integrity between DSPROT (meter objects) and DSSAVE (meter blocks). It is composed of two main passes.

In first pass, all meter objects are traversed and a cross checking is done between the agent data and the information in meter block. During this cross check operation,

- agent that doesn't have a meter block although there is MOG in meter object
- agent whose owner doesn't match with the owner in the meter block
- agent whose assigned meters doesn't match with the ones in meter block

are controlled and necessary logs are generated to inform the user about inconsistency.

If there an inconsistency between assigned meters of an agent, mismatched meters are set as recycled and if at least one meter of meter block is recycled this meter block is added into recovery table. During third run of audit process after line meter recovery, these recycled meters are cleared and sent to OOS.

In second pass of audit process, all in service meter blocks are traversed (examining audited meter blocks) to report such inconsistencies as non-existent owners and to rebuild the free queue as it goes along. During second pass,

- if owner of meter block is not valid, then agent is recycled.
- If meter block is in use, its meter object is tried to be reached. If there is no associated meter object with this meter block, then this agent is recycled.
- Or, if agent has a meter object but it doesn't have mog option, then agent is recycled.

4.2.4.1 Enhancement of Metering Recovery Process

Behavior of metering recovery process is changed as follows:

In terms of deassigned meters in meter block, recovery process tries to provide a consistency between data in meter block and data in MTRDEASS table.

In second pass, if DN doesn't exist in KSETFEAT/DNFEAT tables, MTRDEASS table is checked.

- If it is there, agent is not recycled and if there is any deassigned meter in meter block, date information of related tuple in MTRDEASS is updated. If there is not any deassigned meter in meter block, tuple in MTRDEASS table is cleared.
- But if doesn't exist in MTRDEASS table too, deassigned meters in meter block are checked. If there is at least one deassigned meter in meter block, a new entry is added into MTRDEASS table to be in sync with meter block.
- While adding a tuple into MTRDEAS table during recovery, MTR153 log is not generated.

In third pass of recovery process, after allocating a new meter block for DN, MTRDEASS table is checked whether there is an entry in MTRDEASS for this DN. If there is, tuple is deleted since there is not any deassigned meter in newly allocated meter block.

4.2.4.2 Enhancement of Metering Audit Process

Behavior of metering audit process is changed as follows;

Audit process tries to recycle agent whose DNs doesn't exist in KSETFEAT/DNFEAT tables. But within this feature, a further check is made in MTRDEASS table, since DN can be found there. If it is there, recycling agent is avoided.

During third run of audit process after recovery, meters that are decided to be recycled are saved in MTRDEASS table as deassigned meters.

To decide to send them to OOS or not, *METR_Prevent_Sent_OOS* SOC option check is required, since Bangladesh behaves differently.

- For Bangladesh market, state of *METR_Prevent_Sent_OOS* is ON which means that recycled meters are not sent to OOS.

4.2.4.3 ONP and Swact Support

This feature changes the behavior of ONP as follows;

- MTRDEASS table is not transferred during ONP, instead this during transfer of meter blocks, for deassigned meters in meter block a new entry is added into MTRDEASS table. By this way, MTRDEASS is re-datafilled and date information reflects the date of ONP.
- During transfer of meter blocks in MASPECT stage of SWACT, meter counts of deassigned meters are transferred too.

4.2.5 Billing File Generation

Billing file is used to generate billing record for metered lines. Storage of meter billing records are to an external store type such as disk or tape.

Billing file includes both OOS meters and inservice meters. OOS meters are written into file first, then inservice meters are appended. To distinguish OOS meters and inservice meters a separator is used. An example for content of billing file is as follows;

```
BILLING IS TAKEN .....
R021112132202BIL
>mtrprint R021112132202BIL
DN              DATE   METER NAME  COUNT    WRAP
-----------------------------------------------
1027838888    02/11/12 FEATURE     00000009  NO
1027838888    02/11/12 LOCAL       00000005  NO
1027838888    02/11/12 TOLL        00000008  NO
9999999999    99/99/99 * END OOS * 99999999  NO
1027835572    02/11/12 FEATURE     00000084  NO
1027835572    02/11/12 LOCAL       00000018  NO
1027835572    02/11/12 TOLL        00000000  NO
```

With this functionality, deassigned meters are also included in billing file. But the section where deassigned meters are included differs in Bangladesh and TRNC market.

- In Bangladesh market, deassigned meters are included within inservice meters section since they are not sent to OOS.
- In TRNC market, deassigned meters are included within OOS meters section.

There is no indication for deassigned meters in billing file, they are distinguished from INUSE meters by the help of another report that has been reported manually to billing center or by checking unchanged meter counts during billing periods.

When *METR_Prevent_Sent_OOS* SOC is ON, OOS file is not included in billing file although it contains OOS meters.

4.2.6 Log Generation

A new log report MTR150 is added to the MTR log system. This log is generated when there is no space available in MTRDEASS table for a new tuple.

An example of the log format is as follows:

```
MTR150 APR1 12:00:13 1234 INFO MTRDEASS DATA LOST
DN:7835401 METER NAME: LOCAL USER:ADMIN
METER COUNT: 00000012 WRAP:N
NO FREE SPACE IS AVAILABLE IN MTRDEASS TABLE
```

This log is generated for each assigned meter of DN.

User is also warned by a warning message which is displayed while deleting MOG option from DN. By the help of this warning message, user can give up deleting MOG option.

In existing structure, when MOG option is removed, MTR153 log is generated while deallocating the meter block or when clearing all recycle meters. MTR153 log is an information log, whose text is as follows;

```
MTR153 APR1 12:00:13 1234 INFO METER DELETED
DN:000001027835401
MANUALLY DELETED METERS ARE RECORDED ON OOS JOURNAL FILE
METER NAME: LOCAL METER COUNT: 0000 0012
```

For deassigned meters which are not sent to OOS with this feature, MTR153 log is generated with a different text.

```
MTR153 APR1 12:00:13 1234 INFO METER DELETED
DN:000001027835401
MANUALLY DELETED METERS ARE RECORDED ON MTRDEASS TABLE.
METER NAME: LOCAL METER COUNT: 0000 0012
```

In TRNC market, deassigned meters are sent to both OOS and MTRDEASS tables. In these cases, MTR153 log is generated as following:

```
MTR153 APR1 12:00:13 1234 INFO METER DELETED
DN:000001027835401
MANUALLY DELETED METERS ARE RECORDED ON MTRDEASS TABLE
AND OOS JOURNAL FILE.
METER NAME: LOCAL METER COUNT: 0000 0012
```

4.2.7 New NONRES Command DEASSCLR

This is a NONRES command and it is accessed by TOOLSUP. It is used for deleting all content of MTRDEASS table.

There is no need to add a help option to DEASSCLR command since a detailed warning message is displayed to inform the user about result of executing this command.

> DEASSCLR

A warning message is displayed first when DEASCLR command is run.

```
************************************************
DANGER: LOSS OF METERING DATA IN MTRDEASS TABLE
        This command deletes all tuples in
        MTRDEASS table.
************************************************
```

Then a YES/NO prompt is displayed. If user select Y, command is executed, otherwise user gives up to continue.

This command is referenced when all DN numbers is to be changed. In such a case all DNs are needed to be removed from system and added again. In this period, number of tuples in MTRDEASS table can reach maximum limit. By using this command, all content of MTRDEASS table is cleared.

4.2.8 Enhanced ZAPMTRS Command

ZAPMTRS command clears meter counts of all software meter including recycled meters.

When this feature is functional, if ZAPMTRS command is executed, meter counts of deassigned meters are cleared too. Since meter counts of deassigned meters are cleared, there is no need to keep a tuple associated with these deassigned meters. So all content of MTRDEASS table is cleared during process of ZAPMTRS command.

4.3 Hardware Requirements or Dependencies

None.

4.4 Software Requirements or Dependencies

None.

4.5 Limitations and restrictions

- Maximum number of entries in MTRDEASS table is 65520.
- Limitations and restrictions of metering system exists for this feature.
- *METR_Prevent_Sent_OOS* can not be activated when state of *METR_Deassigned_Support* is IDLE.
- Metering OOS enhancements are not supported for meter trunk agent.

- Number of deassigned DNs and INUSE DNs can not exceed 120000.
- Adding or deleting a tuple into MTRDEASS table via RESTAB tool is restricted.
- Journal file is not updated during adding/deleting a tuple to/from MTRDEASS table since they are done internally.
- Maximum number of entries in recovery table is 2048, when it exceeds this size, meter counts of these meter blocks are lost.

4.6 Interactions

- Feature is not affected by ENABLE_METERING parameter in OFCENG table.
- Feature is not affected by ACT.59022090 “Excessive Metering Detection”

4.7 Applicable customer facing sections

Fault Management

Logs	__X__
Alarms	_N/A_

Configuration

Data Schema	__X__
User Interface	__X__
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_

Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

4.8 Glossary

Term	Description
OOS	Out of Service
TRNC	Turkish Republic of Northern Cyprus
ONP	One Night Process

Term	Description
MOG	Meter Origination Group
SOC	Software Optionality Control
SO	Service Order
ETSI	European Telecommunications Standards Institute

5: Functional Description (FN): A00001921

5.1 Feature name

SN07-Activity ACT.A00001921 “CIS Toll Call Ringing”

5.2 Description

When a call request comes from toll exchange over any incoming trunk to a line, a distinct ringing is applied to the called subscriber indicating that it is a toll call. This functionality is provided by existing feature AU3129 Long Distance Alert (LDA). With this activity ACT.A00001921 “CIS Toll Call Ringing”, the existing LDA feature is enhanced to provide CIS market requirements. Refer to AU3129FN.AB06 in PLS DOC Library for existing LDA feature details.

There are three enhancement items to apply toll call ringing for CIS market requirements:

- Existing LDA feature is still working with C, S, F, C30, CSR, C3C ringing schemes. The new ringing scheme C6R for CIS market will be added with this activity.
- Existing office parameters LDA_ENABLED, LDA_DEFAULT_CALLTYPE, LDA_OM_ENABLED, LDA_ALERT_NO_CLID, LDA_CWT_TIMEOUT, LDA_PATTERN in table OFCENG are moved to the new tuple “LONG_DIST_ALERT” in table ISERVOPT.
- Existing datafill sequence for LDA option in table TRKOPTS will be changed to apply toll call ringing for incoming ETSI ISUP V2+ trunk group using the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message.

The new ringing scheme “C6R” is defined to provide the required values for CIS in this activity. Toll call ringing cadence will be different from the local call ringing cadence.

According to reference document AU3129FN.AB06 in PLS DOC, in page 15 Figure 1 Functional flow diagram for Toll call recognition:

- Part of “CPC is Operator” is not provided in existing functionalty.
- The office parameter LDA_DEFAULT_CALL_TYPE in table OFCENG and CALLTYPE field in table LDASCRN can take any value of LONG_DISTANCE or NORMAL.

5.2.1 CIS Ringing Patterns

Physical ringing is the application of an alternating current (AC) applied between the tip (A lead) and the ring (B lead) of the line loop. The frequency

of the alternations and the voltage are distinctive parameters of the ringing. The waveform of the AC current is usually sinusoidal. The overall timing envelope of these current pulses is termed the cadence. The initial pattern repeats and the time needed to complete one iteration is termed the cycle time. The complete toll call ringing signal specification is:

Frequency: 25 +/- 2 Hz

Output level: 95 +/- 5 V

Cadence: 1.2 sec on (+/- 0.12), 2 sec off (+/- 0.2)

The toll call ringing cadence required for CIS is 1.2 seconds on, 2 seconds off, giving a cycle time of 3.2 seconds. However, due to the fact that actual cycle time of the Ringing Generator to be used in CIS (6X30AA, 6x30CA for ILCM, 6x60CA for RLCM) is 6 seconds, actual pattern will be 1 seconds on, 2 seconds off, 1 seconds on, 2 seconds off. This cadence lies well within 10% tolerance of the CIS.

Field RNGTYPE for related frame in table LCMINV and V5SIG must be datafilled to the new ring type “C6R” in order to provide ringing cadence required for CIS market.

DMS-100i standard ringing cadence which is 2 seconds on, 4 seconds off is used for local call ringing. The actual toll call ringing and local call (standard) ringing cadences provided for CIS are shown in Figure1.

Figure 1 CIS Ringing Cadences

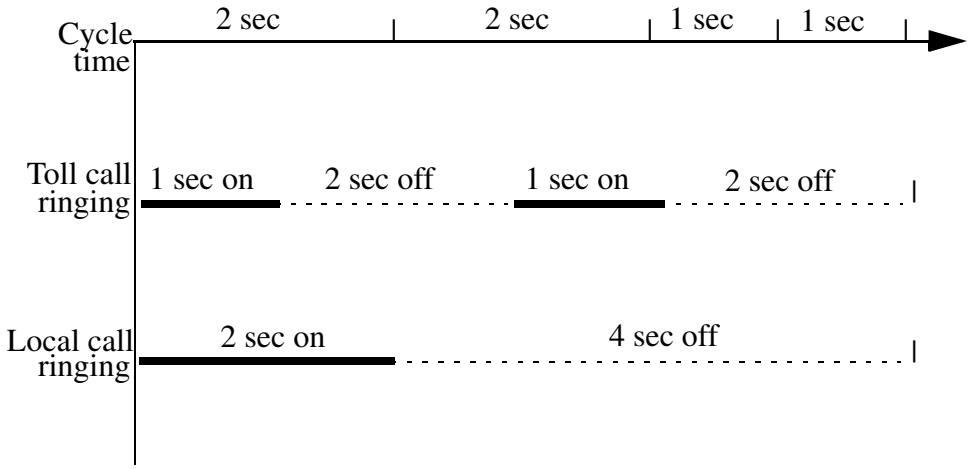


Table 1 Standard Ringing Specification

RING CODE	RING TYPE	DESCRIPTION	CADENCE (Seconds)
P(0)	C6R	Standard ringing	2 s ON, 4 s OFF
P(4)	C6R	Toll Call Ringing	1 s ON, 2 s OFF, 1 s ON, 2s OFF

5.2.2 Enhancement of existing LDA feature to apply Toll Call Ringing

There are three enhancement item to apply toll call ringing:

- Existing LDA feature is still working with C, S, F, C30, CSR, C3C ringing schemes. The new ringing scheme C6R will be added with this activity.
- Existing office parameters LDA_ENABLED, LDA_DEFAULT_CALLTYPE, LDA_OM_ENABLED, LDA_ALERT_NO_CLID, LDA_CWT_TIMEOUT, LDA_PATTERN in table OFCENG are moved to the new tuple “LONG_DIST_ALERT” in table ISERVOPT.

Refer to section 13.1.2.2 of Configuration document of this activity for this item details.

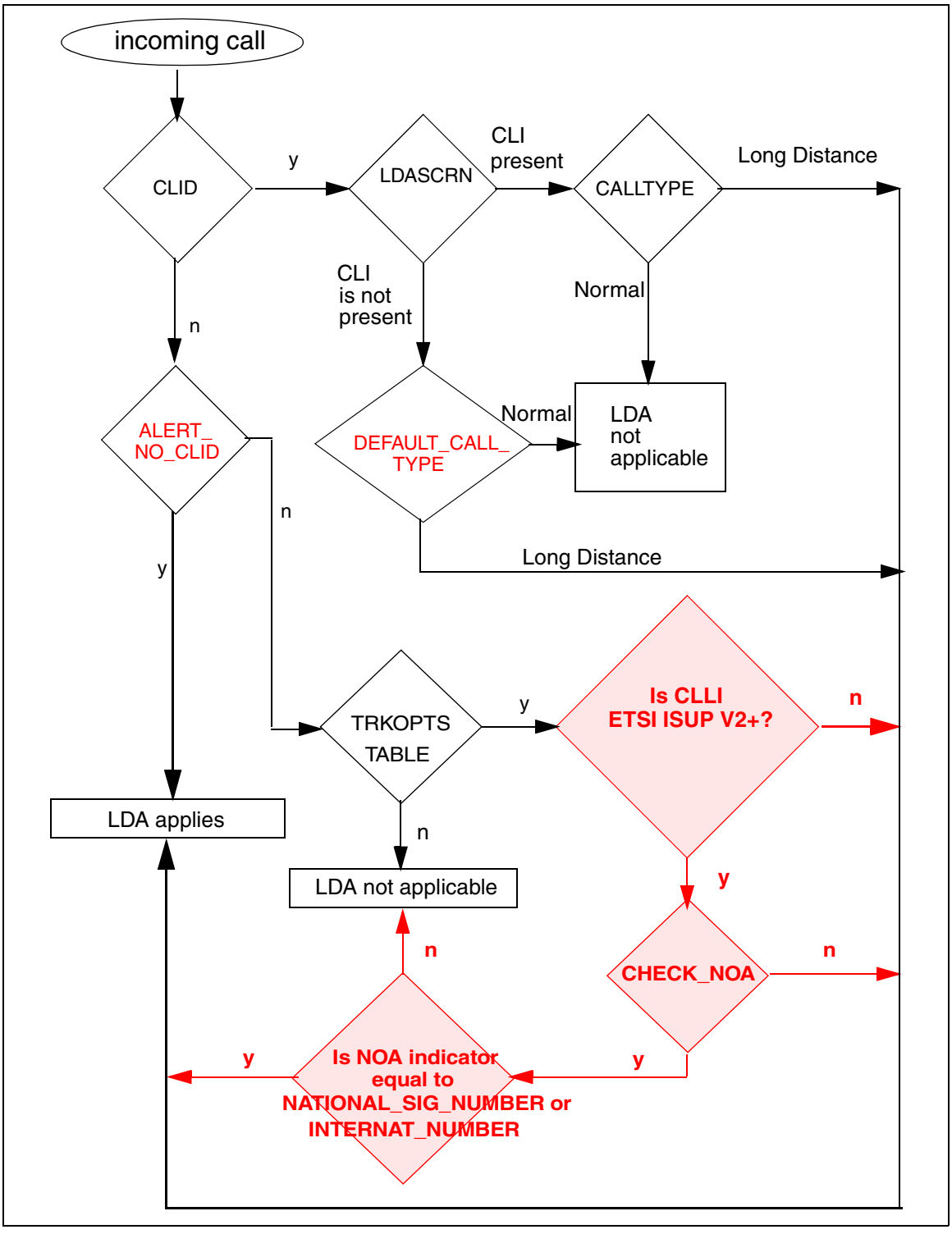
- Existing datafill sequence for LDA feature in table TRKOPTS will be changed to apply toll call ringing for incoming ETSI ISUP V2+ trunk group using the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message. The new field CHECK_NOA for LDA option in table TRKOPTS is defined to supply CIS market requirement. If dedicated trunk group with LDA option in table TRKOPTS is datafilled any kind of ETSI ISUP V2+, the value of CHECK_NOA is used to apply toll ringing. If this value is Y, local terminating exchange checks the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message and applies toll call ringing patterns to terminating line if NOA is equal to:
- National Number
- International Number

Otherwise, local ringing pattern is applied to the terminating line.

If the value of CHECK_NOA field is N, toll call ringing pattern is applied to the terminating line.

Refer to section 13.1.2.1 of Configuration document of this activity for this item details.

Figure 1 Functional flow diagram for Toll call recognition



The red parts of functional flow diagram in Figure 1 are improved with this activity.

Toll call can be recognized by the following methods. Please refer to “Figure1 Functional flow diagram for Toll call recognition” on page 31.

- Screening (If the CLI is delivered)
- Dedicated Toll Trunks (If CLI is not delivered)

5.2.2.1 Screening

This method is applicable only if the CLI is delivered. Existing table LDASCRN is used to screen the incoming CLI against a CLI_RANGE of numbers and identify the call type (Long Distance or Normal)

If the CLI of an incoming call cannot be screened with the Table LDASCRN, the call type will be the value of DEFAULT_CALL_TYPE field of LONG_DIST_ALERT tuple in table ISERVOPT.

By default DEFAULT_CALL_TYPE is LONG_DISTANCE.

5.2.2.1.1 Table LDASCRN

The existing table LDASCRN has fields ZONE, CLI_RANGE and CALLTYPE. For MBS sets, an additional field KEYLIST is added. The fields ZONE as well as CLI_RANGE will be used as the key for searching the table.

ZONE

This field is a part of the key used to search the LDASCRN table. The ZONE sub-option of the LDA option in the terminating line, will be used to index into this table. Logically, this field is a representation of the Called DN range.

CLI_RANGE

This field represents the range of Calling Line Id (CLI) to be screened for the corresponding ZONE. It is divided into 2 subfields:

FROMDIGS, specifying the starting number of the CLI_RANGE

TODIGS specifying the ending number of the CLI_RANGE.

This field also forms a part of the key to search in the LDASCRN table.

CALLTYPE

It can take any value of LONG_DISTANCE or NORMAL. This field has the call type for the corresponding ZONE.

This list contains the key numbers of the DNs to which the LDA feature applies. All of the DNs must belong to the same ZONE.

Method of Determination:

1. The ZONE of the terminating station is obtained from the ZONE sub-option in it's LDA line option.

2. This ZONE as well as the calling DN(CLI) is used as the key to search in the table LDASCRN.

3. If the search is successful, the type of the call will be the CALLTYPE of the tuple matched.

4. If the search fails, the check for CPC will be made to determine if the caller is an operator.

5. If the search fails and the caller is not operator, the type of the call will be that of DEFAULT_CALL_TYPE of LONG_DIST_ALERT tuple in table ISERVOPT.

5.2.2.2 Dedicated Toll Trunk

If CLI is not available then the toll call recognition is done depending on the value of ALERT_NO_CLID field of LONG_DIST_ALERT tuple in table ISERVOPT.

If it's value is Y, then distinctive alerting is provided to the terminating line.

If it's value is N, feature processing will continue to check table TRKOPTS for an alerting indication. Incoming trunk CLLI with LDA option is searched in the table TRKOPTS for toll call determination.

If dedicated trunk group with LDA option in table TRKOPTS is datafilled any kind of ETSI ISUP V2+, the value of CHECK_NOA is used to apply toll ringing. If this value is Y, local terminating exchange checks the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message and applies toll call ringing patterns to terminating line if NOA is equal to:

- National Number
- International Number

Otherwise, local ringing pattern is applied to the terminating line.

If the value of CHECK_NOA field is N, toll call ringing pattern is applied to the terminating line.

5.3 Hardware Requirements or Dependencies

The ring generators are partly controlled by four internal 8-section Dual-In-Line Package (DIP) switches. The DIP switches control the ringing subcycle length, ringing frequency and amplitude, and direct current (DC) offsets of ringing voltages. Each DIP switch controls the characteristics of each subcycle, there being four subcycles in a ringing cycle.

For CIS, the switches on the 6X30AA need to be set as follows :

Table 2 The switches on the 6X30AA for CIS market

SWITCH	SETTINGS	VOLTAGE	FREQ	SLOT SUBCYCLES
(SW1-4)	8 7 6 5 4 3 2 1	AC / DC	(HZ)	(SECONDS)
1 to 4	X 1 1 1 0 1 0 0	82 / -52	25	2 2 1 1

NOTE: The symbols under the heading SETTINGS are interpreted as:

0 = ON,1 = OFF, X = either ON or OFF.

The arrow on the DIP switch indicates the ON direction.

The Ringing will be supported over the following peripherals:

- Line Concentrating Module (LCM).
- Remote Line Concentrating Module (RLCM)

5.4 Software Requirements or Dependencies

The new ringing scheme datafilled in table LCMINV can be downloaded to LCM during RTS as part of the static data. The static data for the ringing scheme for the CIS market are defined in a separate new WT module “C6RRGINI”.

5.5 Limitations and restrictions

For CIS, the office parameter IMMEDIATE_RING_ENABLE in table OFCENG will be set to “Y” since immediate physical ringing is required. But immediate physical ringing is not working for long distance calls.

5.6 Interactions

N/A.

5.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema ___x__

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

5.8 Glossary

Term	Description
CIS	Commonwealth of Independent States
DMS	Digital Multiplex System
DMS-100i	DMS-100 International
LCM	Line Concentrating Module
XPM	Extended Peripheral Module
GPP	Global Peripheral Platform
DRU	Development Release Unit
CND	Calling Number Delivery
ISUP	ISDN User Part
CPE	Customer Premises Equipment
NOA	Nature of Address
DIP	Dual In-Line Package
AC	Alternating Current
DC	Direct Current
LCE	Line Concentrating Equipment

Term	Description
RSC	Remote Switching Center
LCME	Enhanced ISDN Line Concentrating Module
RLCM	Remote Line Concentrating Module
MBS	Meridian Business Set
CLID,CLI	Calling Line ID
CLLI	Common Language Location Identifier
ETSI	European Telecommunication Standard Institute
IBN	Integrated Business Network
LDA	Long Distance Alert
LCM	Line Concentrating Module
MBS	Meridian Business Set
VLCM	Virtual LCM

6: Functional Description (FN): A00001923

6.1 Feature name

CIS Subscriber Categories

6.2 Description

6.2.1 Introduction

This feature is to support subscriber categories for CIS market. In this way:

- Existing Calling Party Category (CPC) line options feature which assigns subscriber category to IBN line is used,
- CPC line options feature is also extended to assign subscriber category to BRI lines,
- CPC option is also given as customer group option,
- Subscriber category based authentication in CIS network is implemented.

6.2.2 Overview

In CIS telephony network, subscribers are categorized according to network access privileges. Subscriber categories are the ten privilege categories according to the rights such as accessing to intrazonal, interzonal, international networks and to special services out of local network. CIS Subscriber categories with their definition are given in Please refer to “Table 1 CIS Subscriber Categories” on page 100..

Table 1 CIS Subscriber Categories

CATX	Definition
CAT1	Apartment or enterprise telephone, having access rights to intrazonal, interzonal and international networks.
CAT2	Hotel telephone, having access rights to intrazonal, interzonal and international networks.
CAT3	Apartment, enterprise or hotel telephone, for local calls only.
CAT4	Enterprise telephone, having access rights to intrazonal interzonal and international networks, and to special services out of local network. Although it is not supported as DMS tool, a priority is ensured waiting for free resources in connections with intrazonal and interzonal networks.
CAT5	Enterprise tel.for offices of Ministry of Communication, having access rights to intrazonal, interzonal, and international networks, and to special services out of local network.

CATX	Definition
CAT6	Interzonal or universal pay station, having access rights to intrazonal, interzonal, and international networks, and to special services out of local network.
CAT7	Apartment or enterprise telephone, having access rights to intrazonal, interzonal and international networks, and to special services out of local network.
CAT8	Enterprise telephone with data transmitting devices, facsimile facilities and electronic mail, having access rights to intrazonal, interzonal, and international networks.
CAT9	Local pay stations, for local calls only.
CAT0	Reserved

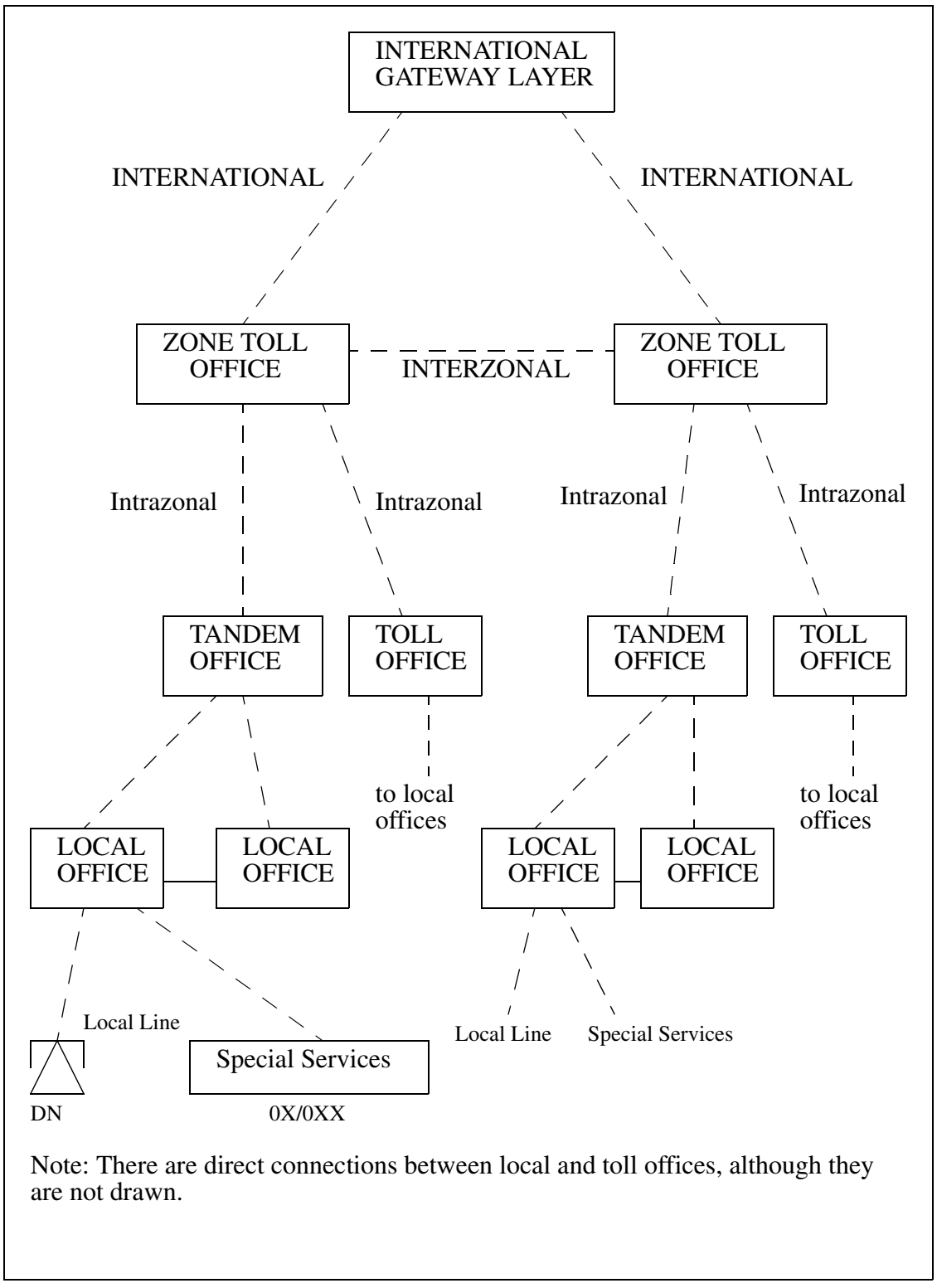
Figure 1 gives a concise view of CIS network. Network types in CIS network are

- International network
- Interzonal network
- Intrazonal network
- Local network

Groups of local offices build areal zones. There can be several toll offices serving local networks in a zone but there is one zone toll office, which is a gateway to the zone such that provides intrazonal, interzonal, international, intrazonal special services and interzonal special services calls. Local offices provide local calls and local special service calls.

There are no restrictions for local calls, and operator calls. All other types of toll routed calls have restrictions differing from one subscriber category to another.

Figure 1 CIS Telephony Network Topology



Note: There are direct connections between local and toll offices, although they are not drawn.

This feature consists of the following main parts:

- Assigning subscriber categories as line or customer group option, and mapping CIS Subscriber Categories to Calling Party Categories (CPC).
- Definition and evaluation of authorization for the categories in zone toll offices of CIS network.

6.2.3 Assigning Subscriber Category (CPC)

In feature CPC line options, CPC value can be assigned as line option for IBN lines, and in this feature, this functionality is extended for BRI lines. Additionally, CPC value can be assigned to customer group option of the line. CPC line option has priority on customer group CPC option, and if line option CPC is assigned then customer group CPC option will be ignored. When CPC line option and CPC option of line's customer group are not assigned, default CPC values are assumed to be valid and their corresponding values are sent in outgoing trunk message.

CPC name is assigned as line or customer group option. To assign a CPC value to a line, SERVORD commands are used (refer to SO section of Configuration document, optcn). CPC names are shown in Please refer to "Table 2 CPC names to assign as line or customer group options and their definitions" on page 103.. CPC name RSRVD is defined in this feature to meet CIS market requirement for CAT0 (reserved).

Table 2 CPC names to assign as line or customer group options and their definitions

CPC names (MMP)	Description
UNKNOWN	unknown subscriber
ORD	ordinary subscriber
PRIOR	subscriber with priority
MAINT	test call
SPM	pay phone
OPER	national operator
TRAN	data call
ITDN	subscriber with special services
FOC	free of charge subscriber
METER	local pay phone
VIS	voice information services subscriber
LOCAL	local network subscriber

Table 2 CPC names to assign as line or customer group options and their definitions

CPC names (MMP)	Description
CNDB	subscriber owner of CNDB
HOTEL	hotel subscriber
AU_ORD	automatic subscriber without priority
AU_PRIO	automatic subscriber with priority
RSRVD (new)	Reserved (newly added type to support CIS Subs. Cat. 0)

To assign as customer group option, table control commands are used for table CUSTSTN (refer to DS section of Configuration document, optcn). In Please refer to "Figure 2 Example CUSTSTN datafill for customer group option CPC" on page 104., customer group CPC option example datafill is shown.

Figure 2 Example CUSTSTN datafill for customer group option CPC

```
TABLE: CUSTSTN
CUSTNAME OPTNAME OPTION
-----------------------------------------------
CUST783 CPC CPC ORD
```

In this feature, CIS Subscriber Categories (CAT**X**, X: 0 to 9) are mapped to CPC values and corresponding CPC values are assigned as subscriber categories. This mapping is shown in Please refer to "Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping" on page 105.. When a CPC value not shown in Please refer to "Table 3 CIS Subscriber Categories and their corresponding CPC values for MMP" on page 104.is assigned in CIS network, its corresponding CIS subscriber category is assumed to be CAT1 (CPC assumed to be ORD). But, when CPC values not shown in Please refer to "Table 3 CIS Subscriber Categories and their corresponding CPC values for MMP" on page 104.are assigned at zone toll offices and line screening is enabled, each CPC's privilege is evaluated itself (not as ORD).

Table 3 CIS Subscriber Categories and their corresponding CPC values for MMP

CIS Subs. Cat.	CPC value (MMP)
CAT1	ORD
CAT2	HOTEL
CAT3	LOCAL

Table 3 CIS Subscriber Categories and their corresponding CPC values for MMP

CIS Subs. Cat.	CPC value (MMP)
CAT1	ORD
CAT4	PRIOR
CAT5	FOC
CAT6	SPM
CAT7	ITDN
CAT8	TRAN
CAT9	METER
CAT0	**RSRVD (new)**

In CIS Subscriber Categories feature, only Russian ISUP V2+ trunk is supported that is unsimilar to CPC line options feature which also supports FDCP trunks. CPC values are mapped to Russian ISUP CPC values internally in software. In Please refer to "Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping" on page 105., CPC name, corresponding CIS Subscriber Category and Russian ISUP CPC mapping is shown for Russian ISUP v2+ trunks.

Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping

CPC name	CIS Subs. Cat.	Russian ISUP CPC
UNKNOWN*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
ORD	CAT1	ISUP_CPC_SUBSCRIBER_1 (#0A)
PRIOR	CAT4	ISUP_CPC_PRIORITY (#0B)
MAINT*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
SPM	CAT6	RISUP_TOLL_PAYPHONE (#0F)
OPER*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
TRAN	CAT8	ISUP_CPC_DATA_CALL (#0C)
ITDN	CAT7	RISUP_SUBSCRIBER_W_ACCESS_SS (#E3)
FOC	CAT5	RISUP_SUBSCRIBER_FREE_OF_CRG (#E2)
METER	CAT9	RISUP_LOCAL_PAYPHONE (#E5)
VIS*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
LOCAL	CAT3	RISUP_LOCAL_NETWORK_SUBSCRIBER (#E4)
CNDB*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)

Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping

CPC name	CIS Subs. Cat.	Russian ISUP CPC
HOTEL	CAT2	RISUP_HOTEL_SUBSCRIBER (#E1)
AU_ORD*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
AU_PRIO*	(CAT1)	ISUP_CPC_SUBSCRIBER_1 (#0A)
RSRVD (new)	**CAT0**	RISUP_SUBSCRIBER_CATEGORY_0 (#E0)

* These CPC values are assignable but don't have their own CIS Subs. Cat. equivalent. Therefore, their corresponding CIS categories are assumed to be CAT1 and they are equivalent to CPC value ORD (ORDinary).

6.2.4 Authorization at Zone Toll Offices of CIS Network

Subscriber category based authorization is controlled at zone toll offices of CIS network.

This feature introduces two new boolean parameter on ISERVOPT table to control category screening on zone toll offices. A zone toll office is the one whose zone toll screening functionality is set to YES. The second parameter is defined to control screening of subscribers which are connected to office. When this parameter is set to YES, zone toll screening is done for calls of subscribers connected to zone toll office.

The parameters are set with table control commands in table ISERVOPT by system engineering (refer to DS section of Configuration document, optcn). In Please refer to "Figure 3 Example ISERVOPT datafill for CIS market" on page 106., an example tuple datafill is shown.

Figure 3 Example ISERVOPT datafill for CIS market

```
TABLE: ISERVOPT
SOPTSKEY SOPTNAM ZONETOLL_SCRN LINE_SCRN
------------------------------------------------------------------------------
zonetoll_scrn zonetoll_scrn Y/N Y/N
```

At the zone toll office, ISUP CPC of originator (call coming from incoming trunk or zone toll office itself) is inverse mapped to CPC value. Hence, corresponding CIS subscriber category for this CPC value can also be obtained (Please refer to "Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping" on page 105.).

Network and service access privileges of each subscriber category are given in Please refer to "Table 5 Network and Service Access Privileges of

Categories (Y: allowed, N: not allowed)" on page 107.. These are derived from subscriber category definitions.

Table 5 Network and Service Access Privileges of Categories (Y: allowed, N: not allowed)

Categories		Network Types /Inter- and Intrazonal Special Services			
CPC value	**CIS Subs. Cat.**	**Intrazonal Network**	**Interzonal Network**	**International Network**	**Inter-/ Intrazonal Sp. Serv. Calls**
ORD	CAT1	Y	Y	Y	N
HOTEL	CAT2	Y	Y	Y	N
LOCAL	CAT3	N	N	N	N
PRIOR	CAT4	Y	Y	Y	Y
FOC	CAT5	Y	Y	Y	Y
SPM	CAT6	Y	Y	Y	Y
ITDN	CAT7	Y	Y	Y	Y
TRAN	CAT8	Y	Y	Y	N
METER	CAT9	N	N	N	N
RSRVD	CAT0	N	N	N	N

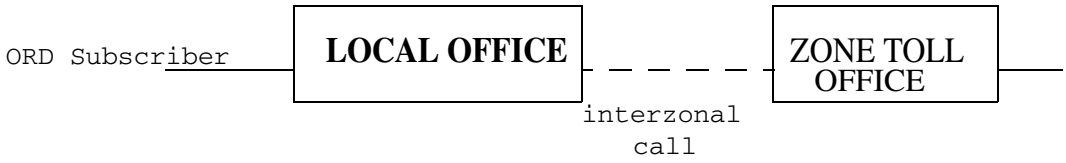
This feature implements network and service access privileges of CIS subscriber categories in terms of call translation classes. A two dimensional table which is indexed with CPC name (CIS Subs. Cat.) and call translation class is used to obtain privileges of CIS subscriber categories. This table is named CISCPCPR (CIS CPC PRivileges, refer to DS section of Configuration document, optcn). It is datafillable for all CPC values. Default values are empty, and no restriction is applied to subscriber categories having no tuple. In Please refer to "Figure 4 Example CISCPCPR datafill for CIS market" on page 107., an example datafill for table CISCPCPR is shown. In this example, subscriber category ORD has privilege YES for all call translation classes. YES means call routing is allowed at zone toll office. All CPC values can be datafilled to table CISCPCPR. When line screening is enabled at table ISERVOPT, all assignable 17 CPC values are checked for their privilege at table CISCPCPR. But, CPC values from incoming Russian ISUP v2+ trunk are expected to be the ones in Please refer to "Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping" on page 105..

Figure 4 Example CISCPCPR datafill for CIS market

```
TABLE: CISCPCPR
CPC_NAME
                                                    OPTIONS
-------------------------------------------------------------------------------
ORD (unknown) (iagrp) (attend) (dial_att) (local) (special)
(emergency) (national) (continental) (intercontinental) (international)
(operator_assisted) (intl_op_assisted) (rural) (collect) (cellular) $
```

Table CISCPCPR is used to authorize the call at zone toll office. By using CIS Subs. Cat. (CPC name) and call translation class on table CISCPCPR, zone toll office decides to route the call. When privilege is okay, the call is routed to destination. Otherwise, toll denied treatment is sent to originator. An example situation is illustrated in Figure 5.

Figure 5 Subscriber category based authorization in CIS network



The interzonal call originated by an ORD category subscriber is queried on table CISCPCPR at zone toll office for privilege check. If privilege is okayed, the call is routed. Otherwise, toll denied treatment is sent to originator.

6.3 Hardware Requirements or Dependencies

N/A

6.4 Software Requirements or Dependencies

N/A

6.5 Limitations and restrictions

- CPC line and customer group option feature is applicable only for IBN, BRI and coin lines. Lines which are connected with v5.2 link can also be given CPC option.
- Pphones can not be assigned CPC line option.
- CPC line option has priority on CPC customer group option. When both of them are not assigned, default values are sent.

- In CPC options feature, sending CP Activity over FDCP outgoing trunk is only supported for default variant. Non-default variant(s) (today, China market) is/are not supported.
- In CIS network, CPC screening at zone toll office is done for incoming Russian ISUP V2+ trunk calls, and can also be enabled for calls originated from lines connected to zone toll office.
- When ISUP CPC values except from ones in Please refer to "Table 4 CPC name, CIS Subscriber Category and Russian ISUP CPC mapping" on page 105.come to zone toll office from Russian ISUP v2+ trunk, it is treated as CPC value of ORD. Hence, no restriction is applied to such calls.

6.6 Interactions

N/A

6.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X
Office Parameters	N/A

Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

Glossary

Term	Description
CIS	Commonwealth of Independent States
CISCPCPR	CIS Calling Party Category access PRivileges Table

6.8 Recommended Reading/References

1 TA0122 CIS Subscriber Categories

2 A59032371 CPC Line Options

3 TA0073 USSR Signalling Specifications

7: Functional Description (FN): A00001929

7.1 Feature name

RUSSIAN ISUP-ISDN Interworking.

7.2 Description

This activity addresses the ability to support ETSI BRI -RUSSIA ISUP V2+, and ETSI PRI - RUSSIA ISUP V2+ interworkings on the DMS. It is implemented in ISN07.

Please note that for the rest of this document, the following short forms are used:

— R_ISUP for RUSSIA ISUP V2+

— BRI for ETSI BRI

— PRI for ETSI PRI

This activity is based on the existing ETSI ISUP V2 - ISDN interworking (Please see reference 3. AJ4323-ETSI ISUP V2 ISDN INTERWORKING (PRI/BRI) FN Document).

In addition to the existing functionality described in this reference activity , the following BRI/PRI-R_ISUP interworking requirements are implemented on DMS switches for call processing:

- Handling of Russia specific ISUP messages (CCL, RNG).
- Handling of CRG and FAC messages.
- Handling of network initiated SUS message which is received from the network.

Assignment of Calling Party Categories to BRI lines and mapping of these CPC values to ISUP CPC values is implemented by ISN07 activity A00001923 - ‘CIS SUBSCRIBER CATEGORIES’.

TBI is not supported by this activity. TBI support is provided by ISN07 activity A00002100 ‘ISUP-R 2000 OPERATOR CALL ON BUSY SUBSCRIBER (TBI) ENHANCEMENT’.

7.3 BRI - R_ISUP interworking

7.3.1 Handling R_ISUP Specific Messages

7.3.1.1 Calling Line Clear (CCL) Message

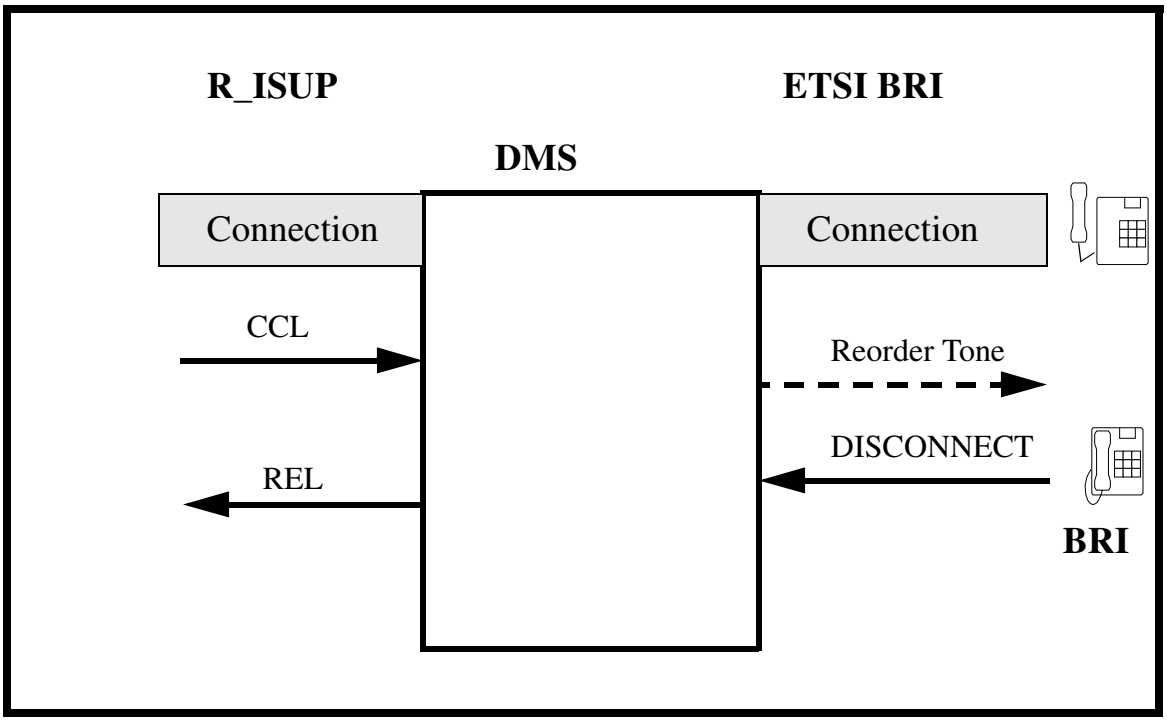
Generation:

CCL message is not generated in BRI to R_ISUP interworking.

Reception:

When CCL message is received instead of REL message, DMS stops billing speech path is disconnected, reorder tone is applied to BRI line, lines and trunks are held until terminating line is on hook. When the terminating line is on hook, REL message is sent backward, lines and trunks are released.

Figure 1 Call Clearing with CCL message: BRI Termination



7.3.1.2 Ring (RNG) message

Generation:

RNG message is not generated in BRI to R_ISUP Interworking.

Reception:

DMS ignores RNG message in cases it is received at terminating exchange.

7.3.1.3 Handling Charge (CRG) Message

Generation:

CRG message is not generated in BRI to R_ISUP Interworking.

Reception:

DMS ignores CRG message in cases it is received.

7.3.1.4 Handling Facility (FAC) Message

CFN message will be sent as a reply if FAC is received from an R_ISUP trunk in R_ISUP to BRI interworking.

7.3.2 ISUP INR/INF and IDR/IRS Messages

Figure 2 Default Tuple in table ISUPSVC

```
>table ISUPSVC
RUSSIA_EIV2
(INR_INF GENERATION_AND_RECEPTION (CGN_REQUESTED) $)
(IDR_IRS RECEPTION ) $
```

Default tuple in ISUPSVC table for R_ISUP V2 is given in Figure 2 ‘Default Tuple in table ISUPSVC’.

ETSI ISUP variants use their default tuples while determining how to process IAM messages without CLI (or CPC = UNKNOWN), or INR/IDR messages.

The default tuple can be modified, or new tuples for Russia ISUP V2+ can be added by table control commands.

The entries within ISUPSVC table should be referenced within TRKOPTS table in order to assign the specified behavior in the ISUPSVC tuple to a certain trunk group **in cases where default Russia tuple will not be used.**

Figure 3 “Example TRKOPTS Datafill”gives an example TRKOPTS datafill.

Figure 3 Example TRKOPTS datafill

```
>table TRKOPTS
OPTKEY OPTINFO
--------------
ICRSISUP ISUPSVC ISUPSVC RUSSIA_ALTERNATIVE_TUPLE
BOTTOM
```

Additionally, the trunk groups can be configured in order not to request any information (i.e. not send any IDR or IRS) by datafilling these tables. With the datafills given in Figure 4 “ISUPSVC and TRKOPTS datafills for preventing INR/IDR generation”

Figure 4 ISUPSVC and TRKOPTS datafills for preventing INR/IDR generation

```
DATAFILL FOR PREVENTING INR/IDR GENERATION FOR A CERTAIN
TRUNK GROUP.

ISUPSVC
RUSSIA_AVOID_REQUESTS  (INR_INF  (RECEPTION))  (IDR_IRS
(RECEPTION))$

TRKOPTS
2WRSISUP ISUPSVC ISUPSVC RUSSIA_AVOID_REQUESTS
```

The behavior for incoming and outgoing Russia ISUP V2+ trunks is explained in Table 1 “Possible ISUPSVC configurations and corresponding behavior for incoming trunks” and in Table 2 “Possible ISUPSVC configurations and corresponding behavior for outgoing trunks”

Table 1 Possible ISUPSVC configurations and corresponding behavior for incoming trunks.

IC Trunk Configuration		IC Trunk Behavior
INR-INF	**IDR-IRS**	**ISUP -to- BRI**
Generate & Receive	Receive	Generate INR to request information from originator. Process INF message.
	OR	
	None	Do not generate IDR

IC Trunk Configuration		IC Trunk Behavior
INR-INF	**IDR-IRS**	**ISUP -to- BRI**
Receive OR None	Receive OR None	Do not generate INR Do not generate IDR
	Generate & Receive	Generate IDR to request information from originator, if the connected agent has MCID assigned. Process IRS message Do not generate INR

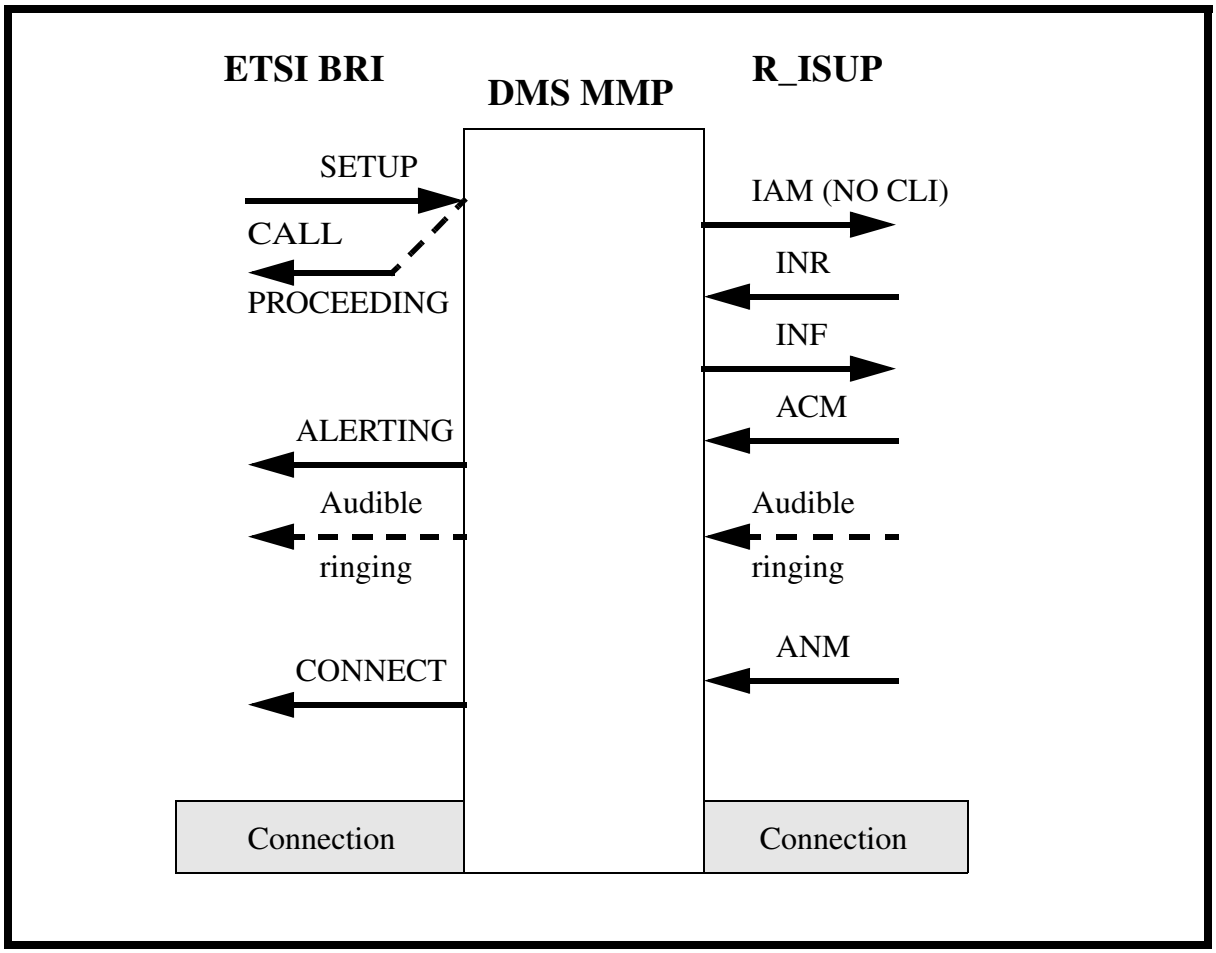
Table 2 Possible ISUPSVC configurations and corresponding behavior for outgoing trunks

OG Trunk Configuration		OG Trunk Behavior
INR-INF	**IDR-IRS**	**BRI -to- ISUP**
Generate & Receive OR Receive	None	Ignore IDR messages received from the terminating side Process INR message received from the terminating side and send back INF with the available information.
None	Generate & Receive OR Receive	Process IDR message received from the terminating side and send back IRS. Send an INF message to the terminating side which includes no information, if an INR message is received.

OG Trunk Configuration		OG Trunk Behavior
INR-INF	**IDR-IRS**	**BRI -to- ISUP**
Generate & Receive	Receive	Process IDR message received from the terminating side and send back IRS. Process INR message received from the terminating side and send back INF with the available information.
Receive	Generate & Receive	

Figure 5 shows an example for the INR/INF messaging according to the default datafill in Figure 2 “Default tuple in table ISUPSVC”

Figure 5 Call setup, CLI is absent, INR message is sent for CLI request



7.3.3 Handling SUS Message

User initiated SUS and RES messages are ignored when received.

Generation:
R_ISUP does not send SUS message when terminating line goes on hook.

Reception:

If a network initiated SUS message is received from network, call is released immediately. REL with “Normal Call Clearing” cause is sent back.

Figure 6 Call releasing to Network Initiated SUS Message in BRI->R_ISUP Interworking

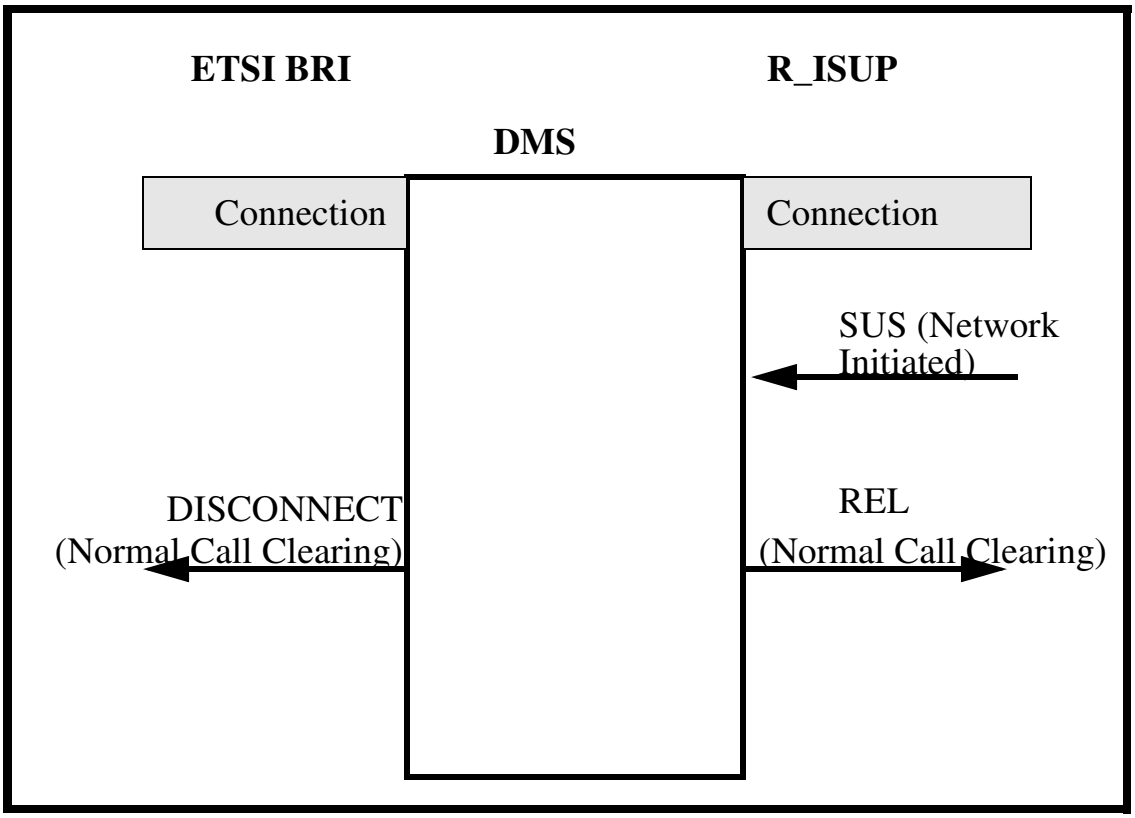
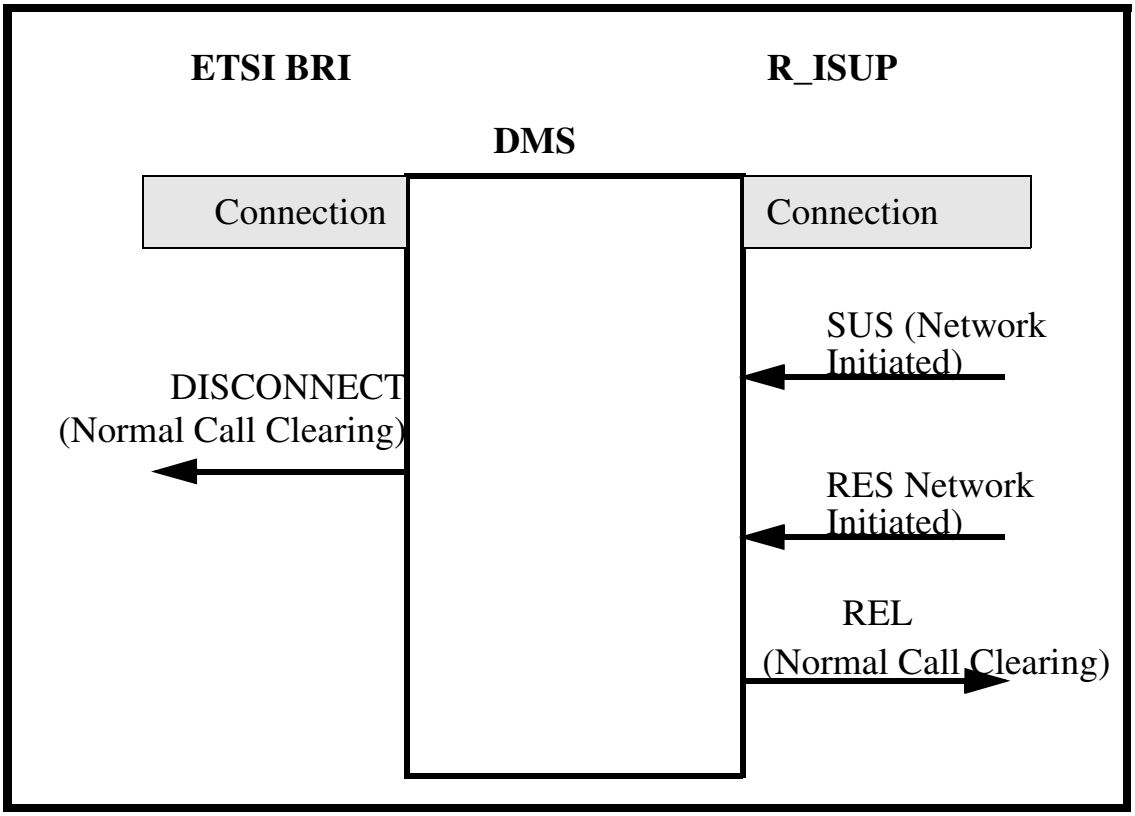


Figure 7 Call releasing when network initiated RES message is received after network initiated SUS message



7.3.4 Nature of Address Indicator parameter

Table 3“NOA values of Calling Party Number for different call types” shows the call types and the corresponding ‘Nature of Address Indicator’ (NOA) values in the IAM message for BRI to R_ISUP interworking.

Table 3 NOA values of Calling Party Number for different call types

Call Types	Nature of Address Indicator
Local Calls	National (significant) Number
National Calls	National (significant) Number
International Calls	National (significant) Number

Table 4“NOA values of Called Party Number for different call types” shows the call types and the corresponding ‘Nature of Address Indicator’ (NOA) values in the IAM message for BRI to R_ISUP interworking.

Table 4 NOA values of Called Party Number for different call types

Call Types	Nature of Address Indicator
Local Calls	Subscriber Number
National Calls	National (significant) Number
International Calls	International Number

7.3.5 Assignment and Mapping of CPC values

Assignment of Calling Party Categories to BRI lines and mapping of these CPC values to ISUP CPC values is implemented by ISN07 activity A00001923- ‘CIS SUBSCRIBER CATEGORIES’.

7.4 PRI- R_ISUP Interworking

7.4.1 Handling R_ISUP Specific Messages

7.4.1.1 Calling Line Clear (CCL) Message

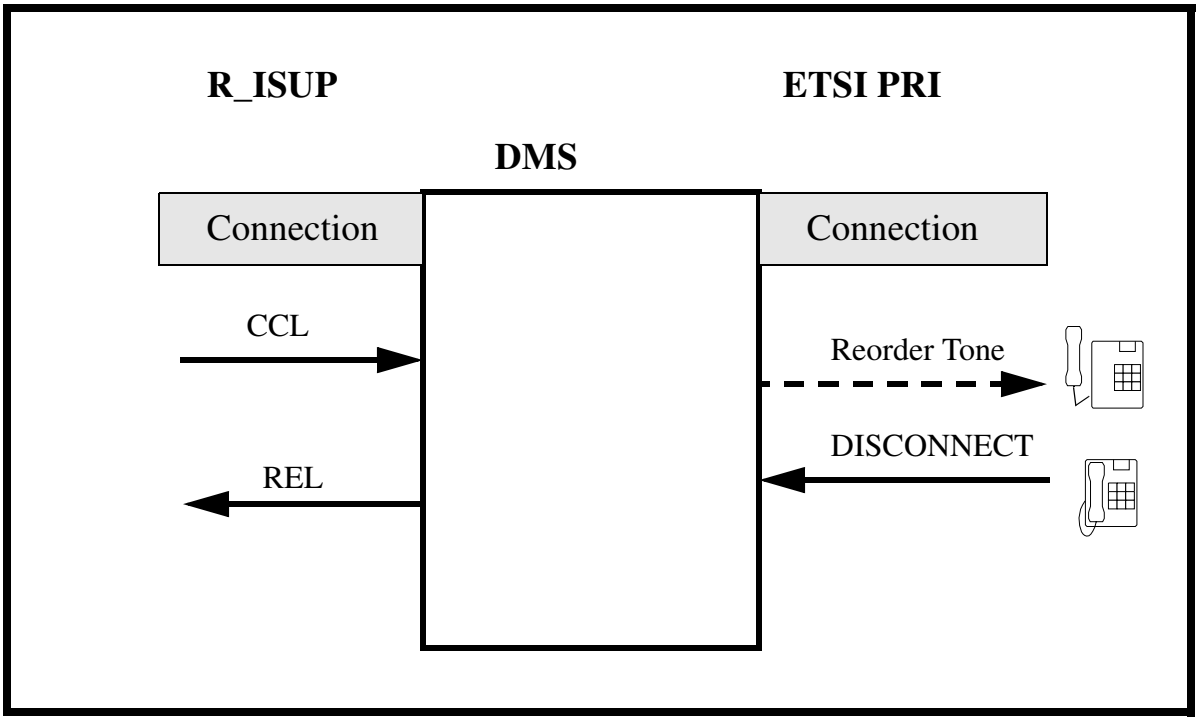
Generation:

CCL message is not generated in PRI to R_ISUP Interworking.

Reception:

When CCL message is received from R_ISUP, DMS stops billing, reorder tone is applied to PRI side, speech path is disconnected, lines and trunks are held. When release message is received from PRI, lines and trunks are released.

Figure 8 Call clearing with CCL: PRI Termination



7.4.1.2 Ring (RNG) Message

Generation:

RNG Message is not generated in PRI to R_ISUP Interworking.

Reception:

DMS ignores RNG message in cases it is received at terminating exchange.

7.4.1.3 Charge (CRG) Message

Generation:

CRG message is not generated in PRI to R_ISUP Interworking.

Reception:

DMS ignores CRG message in cases it is received.

7.4.1.4 Handling Facility (FAC) Message

CFN message will be sent as a reply if FAC is received from an R_ISUP trunk in R_ISUP to PRI interworking.

7.4.2 ISUP INR/INF and IDR/IRS Messages

The behavior for incoming and outgoing Russia ISUP V2+ trunks is explained in Table 3“Possible ISUPSVC configurations and corresponding behavior for incoming trunks” and in Table 4“Possible ISUPSVC configurations and corresponding behavior for outgoing trunks”

Table 5 Possible ISUPSVC configurations and corresponding behavior for incoming trunks

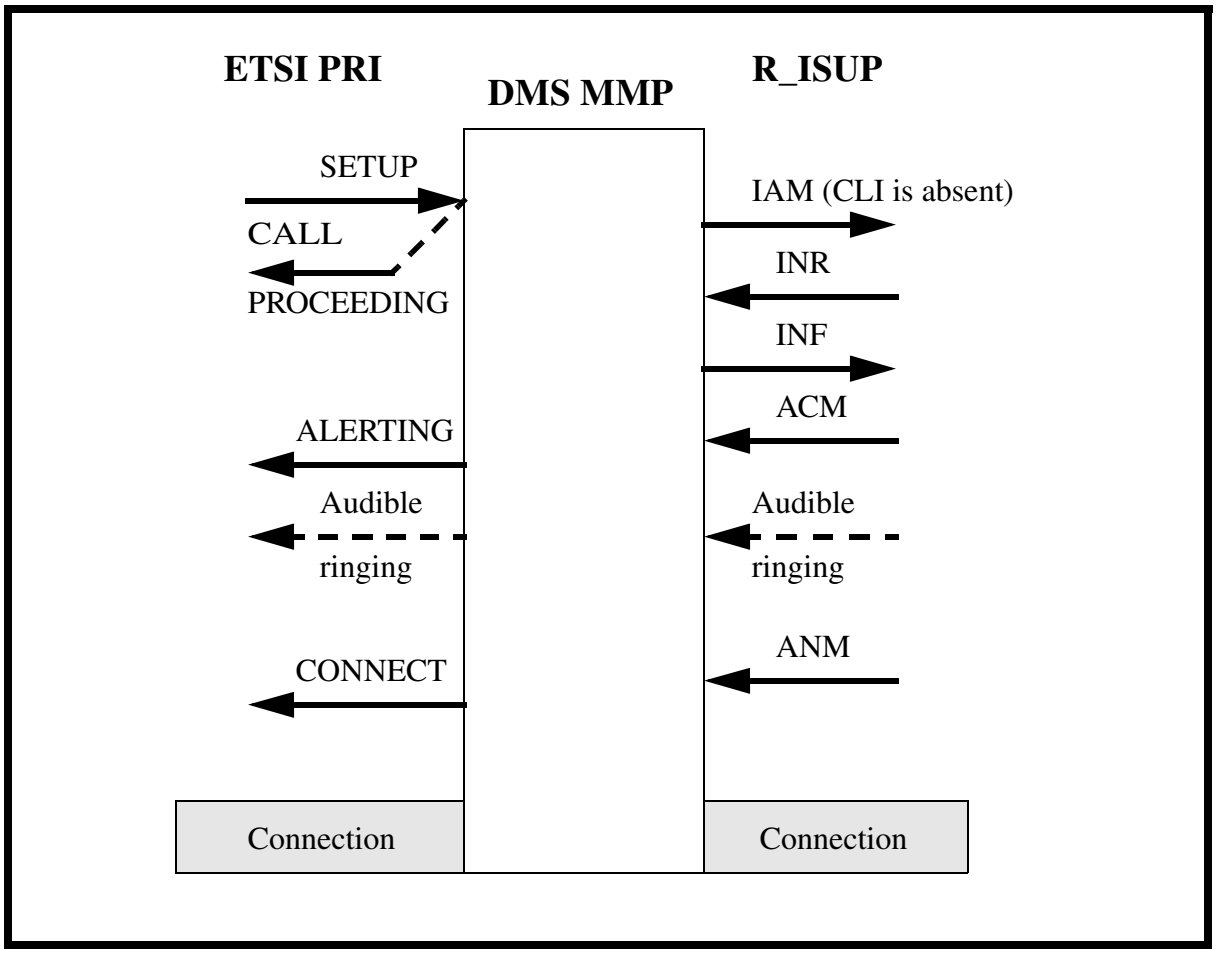
IC Trunk Configuration		**IC Trunk Behavior**
INR-INF	**IDR-IRS**	**ISUP -to- PRI**
Generate & Receive	Receive OR None	Generate INR to request information from originator. Process INF message. Do not generate IDR
Receive OR None	Receive OR None	Do not generate INR Do not generate IDR
	Generate & Receive	Generate IDR to request information from originator, if the connected agent has MCID assigned. Process IRS message Do not generate INR

Table 6 Possible ISUPSVC configurations and corresponding behavior for outgoing trunks

OG Trunk Configuration		OG Trunk Behavior
INR-INF	**IDR-IRS**	**PRI -to- ISUP**
Generate & Receive OR Receive	None	Ignore IDR messages received from the terminating side Process INR message received from the terminating side and send back INF with the available information.
None	Generate & Receive OR Receive	Process IDR message received from the terminating side and send back IRS. Send an INF message to the terminating side which includes no information, if an INR message is received.
Generate & Receive	Receive	Process IDR message received from the terminating side and send back IRS. Process INR message received from the terminating side and send back INF with the available information.
Receive	Generate & Receive	

Figure 9 shows an example for the INR/INF messaging according to the default datafill in Figure 2 “Default tuple in table ISUPSVC”

Figure 9 Call Setup, CLI is absent, INR and INF messages are sent



7.4.3 Handling SUS Message

User initiated SUS and RES messages are ignored when received.

Generation:
R_ISUP does not send SUS message when terminating line goes on hook.

Reception:
If a network initiated SUS message is received from the network, REL with "Normal Call Clearing" cause is sent back and a DISCONNECT message with also "Normal Call Clearing "cause is sent to PRI side.

Figure 10 Disconnection when network Initiated SUS is received

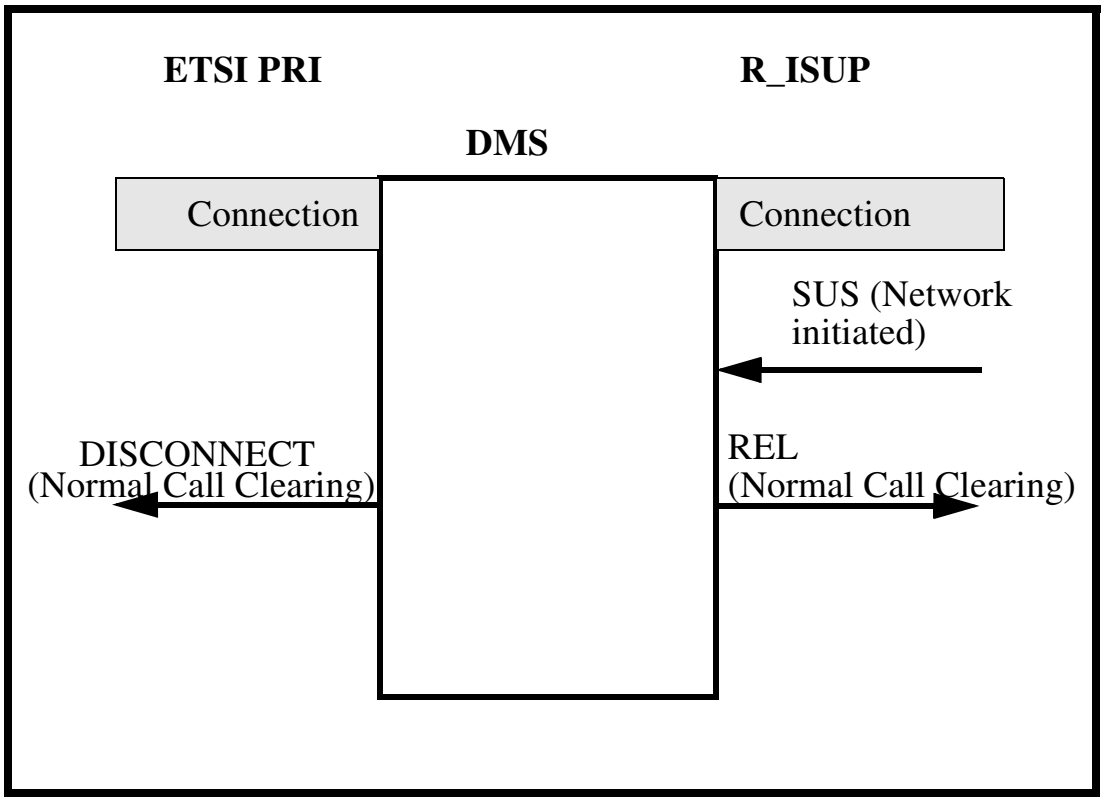
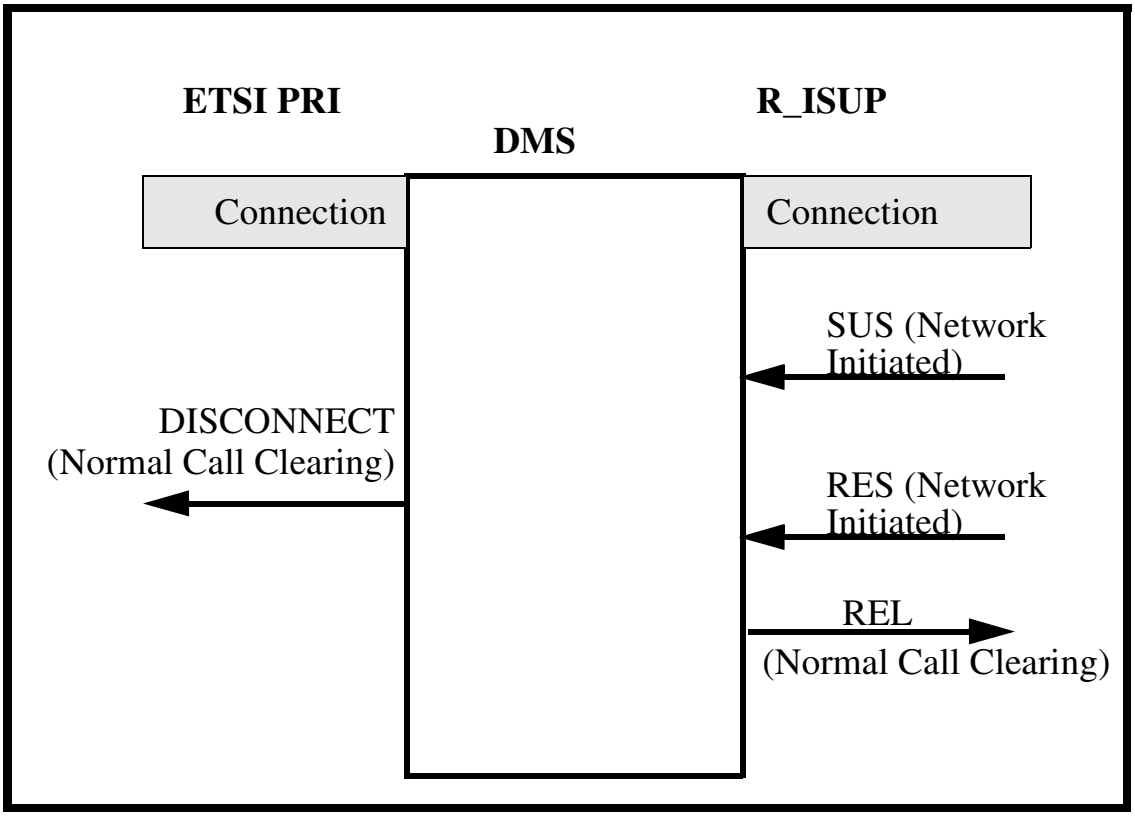


Figure 11 Call releasing when network initiated RES message is received after network initiated SUS message



7.4.4 Nature of Address Indicator parameter

Table 7“NOA values of Calling Party Number for different call types” shows the call types and the corresponding ‘Nature of Address Indicator’ (NOA) values in the IAM message for PRI to R_ISUP interworking.

Table 7 NOA values of Calling Party Number for different call types

Call Types	Nature of Address Indicator
Local Calls	National (significant) Number
National Calls	National (significant) Number
International Calls	National (significant) Number

Table 8“NOA values of Called Party Number for different call types” shows the call types and the corresponding ‘Nature of Address Indicator’ (NOA) values in the IAM message for PRI to R_ISUP interworking.

Table 8 NOA values of Called Party Number for different call types

Call Types	Nature of Address Indicator
Local Calls	Subscriber Number
National Calls	National (significant) Number
International Calls	International Number

7.4.5 Assignment and Mapping of CPC values

CPC values cannot be assigned to PRI trunks.

For PRI -> R_ISUP Interworking, Normal Calling Subscriber (Subscriber Category 1) is sent as the CPC parameter in the outgoing IAM message.

For R_ISUP-> PRI Interworking the CPC parameter in the IAM message is ignored.

7.5 Hardware Requirements or Dependencies

Russia ISUP V2+ is supported only on PDTCs which are equipped with SX05.

7.6 Software Requirements or Dependencies

N/A

7.7 Limitations and restrictions

No specific implementation is done for BRI-R_ISUP interworking cause value mappings with this feature. Cause value mappings are the same as BRI-ISUP_V2 interworking.

7.8 Interactions

Assignment of Calling Party Categories to BRI lines and mapping of these CPC values to ISUP CPC values is implemented by ISN07 activity A00001923- ‘CIS SUBSCRIBER CATEGORIES’.

7.9 Applicable customer facing sections

Fault Management

Logs N/A_____

Alarms N/A_____

Configuration

- Data Schema N/A_____
- User Interface N/A_____
- Element Management N/A_____
- Security N/A_____
- Service Order N/A_____
- Office Parameters N/A_____

Accounting (includes AMA billing) N/A_____

Performance (includes operational measurements) N/A_____

7.10 Glossary

Term	Description
BRI	Basic Rate Interface
CCL	Calling Line Clear
CLI	Calling Line Information
DMS	Digital Multiplexed System
ETSI	European Telecommunications Standards Institute
IAM	Initial Address Message
IDR	Identification Request
INF	Information
INR	Information Request
IRS	Identification Response
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
PRI	Primary Rate Interface
REL	Release
RNG	Ring

Term	Description
SUS	Suspend
TBI	Toll break in

7.11 References

1. ISUPR2000 “Summary of Differences Between ISUP-R-2000 and MMP17 Base ETSI ISUP V2”
2. AT.00000937 - “RUSSIA ISUP V2+ - Phase.1”
3. AJ4323 - ETSI ISUP V2 ISDN INTERWORKING (PRI/BRI)
4. A59023814 - “INR/INF (IDR/IRS) Platform”
5. ISN04 (TDM) Product Description Switch Capabilities Version: Issue ISN04TDM.3 (approved):
   - Chapter D13 ISDN BRI Access Interface
   - Chapter D14 ISDN PRI Interface
   - Chapter E17 ISDN Supplementary Services
6. Activity ID: 10-97-0052 NIS number: S223-1 01.02 "ETSI BRI(S/T) Specification DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the S/T Reference Point"
7. Activity ID: 10-97-0052 NIS number: S223-2 01.02 "ETSI BRI(T) Specification DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the T Reference Point"
8. Activity ID: 10-02-0040 NIS number: A215-1 "ETSI PRI(T) Specification ISN04/ISN04 (TDM) Implementation of the ETSI ISDN Primary Rate Interface at the T Reference Point"

8: Functional Description (FN): A00001930

8.1 Feature name

Last and Total Call Meter Inquiry Services

8.2 Description

8.2.1 Introduction

The purpose of this activity is providing Last and Total Call Meter Inquiry (CMI) services.

- **LCMI (Last Call Meter Inquiry)** is a service which allows the subscriber to inquire about the meter count for the last call made, via dialing a predefined number. When the number is dialed, the meter count of the last call and the feature meter count of the last call (if exists) is announced in English. Please note that only answered calls and feature calls (i.e. subscriber activation, deactivation, interrogation calls and feature usage) are taken into consideration for the announcement provided to LCMI service.

In case last call meter count is equal to zero, it is announced to indicate that last call was a free call. However feature meter count is not announced if it is equal to zero.

- Like LCMI, **TCMI (Total Call Meter Inquiry)** allows the subscriber to inquire about the total meter count, via dialing a predefined number. When the number is dialed, total of all assigned meters of the subscriber is announced in English[1].

CMI services are supported for IBN lines with FPS or MOG option, and ETSI BRI lines with MOG option. Please note that FPS (Fixed Price Service) option can be assigned to IBN lines only. Refer to the activity A89007209 “Fixed Price Service for Bangladesh” for further information on FPS.

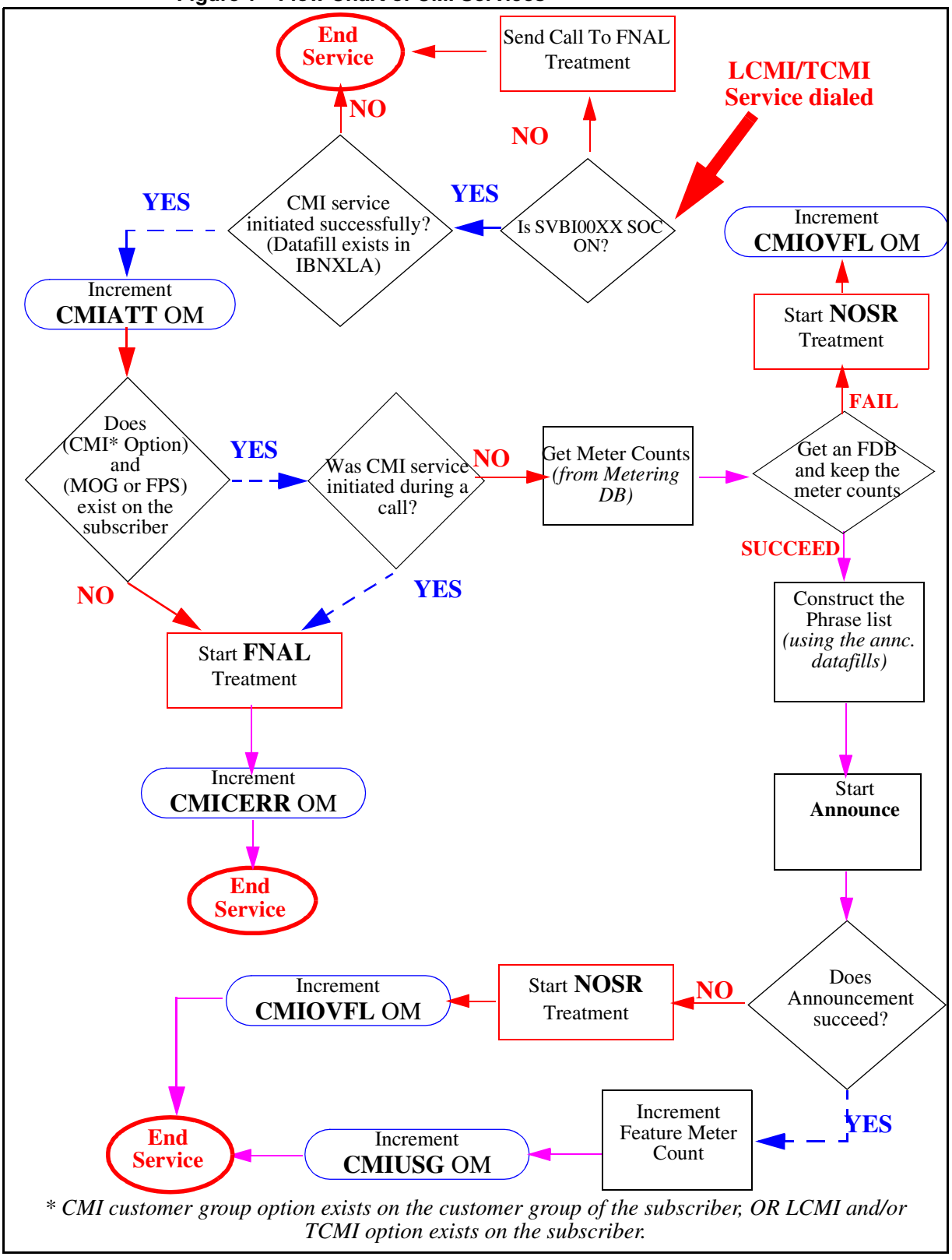
CMI services can be used by subscribers who use hardware metering (i.e. SPM and COIN) as well as software metered subscribers.

This design is implemented in ISN07.

Figure 1 shows the steps followed when TCMI or LCMI service is initiated.

[1]In the total call meter announce for subscribers with FPS option, instead of MOG, remaining credits, not the total of meters, is announced.

Figure 1 Flow Chart of CMI Services



8.2.2 Activation of Feature

CMI services will be activated for a subscriber, only if the following are provided:

1. State of SVBI0033 SOC must be ON in the office.
2. Since this is a metering dependant service, MOG option must have been assigned to the line or FPS option must exist on the subscriber.
3. TCMI/LCMI option must exist on the subscriber or the CMI customer group option must exist on the customer group that the subscriber belongs to.

8.2.2.1 SVBI0033 SOC

In order to control the office wide functionality of the TCMI and LCMI services, one state SOC is designed, which is given the name SVBI0033 SOC. SVBI0033 SOC has two states: SOC_ON and SOC_IDLE. In the SOC_ON state, SVBI0033 SOC is fully functional. In the IDLE state, the LCMI and TCMI features can be provisioned, but the usage of the service is not enabled.

Table 1 SVBI0033 SOC

SOC Group	SVBI
SOC Option Name	SVBI0033
SOC Option Title	Call Meter Inquiry
SOC Option Control Type	State
New SOC Option?	Yes
Option defined in DRU	WT20
Affected Products	DMS100 - MMP

Default state of SOC is IDLE.

Activation/Deactivation of SOC is done by password control. The password is unique for each office.

However, datafilling tables (i.e IBNXLA, IBNLINES, CUSTSTN, etc.) does not depend on the state of the SOC. This means that datafills could be done even if SVBI0033 SOC is not ON. But note that CMI services can not be activated if SVBI0033 SOC is IDLE.

For all MOG and FPS subscribers, last call and last feature meter counts are initialized when state of SVBI0033 SOC is changed to IDLE.

State of SVBI0033 SOC can not be changed from ON to IDLE while one of DUMP, METERING RESTORE, or METERING LINE RECOVERY processes. One of following error messages are displayed:

“DUMP is in progress“

“METER LINE RECOVERY process is in progress“

“METER RESTORE is in progress“

and change state is aborted.

8.2.2.2 LCMI and TCMI Line Options

Two new line options TCMI and LCMI are introduced. CMI line options are boolean options, which means it has no subfields. For ETSI BRI lines, they are compatible with point to point and point to multi point mode.

CMI line options can be assigned/deassigned to subscriber via SERVORD software. When TCMI/LCMI line options are assigned to a line, datafill will be added into one of tables IBNLINES (for IBN lines) or KSETLINE (for ETSI BRI lines) depending on the line type.

8.2.2.2.1 Administrator Assignment

CMI line options can be assigned to IBN lines and ETSI BRI lines through SERVORD software via ADO (Add Option) and NEW commands. TCMI and LCMI line options can be assigned to IBN and ETSI BRI subscribers only (as a DN feature for ETSI BRI lines, and the assignment is only aplicable to the keys of ETSI BRI line that has a DN). In order to assign TCMI or LCMI option to a line, line should have a MOG or FPS option. Please note that FPS option is supported for IBN lines only.

```
ado $ <DN> TCMI $

ado $ <DN> LCMI $
```

If line has none of MOG or FPS options, new CMI option can not be assigned to the subscriber. In this case system will reply with one of the following error messages.

```
"Cannot add LCMI since line does not have MOG or FPS option"

"Cannot add TCMI since line does not have MOG or FPS option"
```

If MOG and CMI options are intended to be assigned at the same time, MOG option should be given first so that the feature metering of administrative assignment is done correctly. Please refer to section 2.2.5 Feature Metering for more information on feature metering.

LCMI and TCMI line options cannot be added via EST (Establih hunt group) command, since addition of MOG and FPS by EST is not allowed and LCMI and TCMI line options require MOG or FPS previously assigned.

8.2.2.2.2 Administrator Deassignment

The administrator may deassign CMI option by using the DEO (Delete Option) and OUT commands through SERVORD software.

```
deo $ <DN> TCMI $

deo $ <DN> LCMI $
```

8.2.2.2.3 Deassignment of MOG Option

If both MOG and CMI options are intended to be deassigned from a line at the same time, CMI option must be deassigned first, so that feature metering of administrator deassignment is done correctly. Please refer to section 2.2.5 Feature Metering for more information on feature metering.

```
deo $ <DN> LCMI MOG $

deo $ <DN> TCMI MOG $
```

MOG option deletion is prohibited if line has TCMI and/or LCMI option. The following error message is generated:

```
"Error: Cannot delete MOG since TCMI requires MOG option."

"Error: Cannot delete MOG since LCMI requires MOG option."
```

8.2.2.2.4 Deassignment of FPS Option

FPS option deletion is prohibited if line has LCMI and/or TCMI line options. The following error message is generated FPS option is attempted to be deassigned from a line which has LCMI/TCMI line option.

```
"Error: Cannot delete FPS since TCMI requires FPS option."

"Error: Cannot delete FPS since LCMI requires FPS option."
```

8.2.2.3 Interaction with SWAP and CLN Commands

Last call and last feature meter counts of FPS and MOG agents are preserved during SWAP and CLN operations. In other words, last call and last feature meter counts of old len will be moved to new len during SWAP and CLN.

The following example shows the behavior of CMI service when SWAP command is applied to FPS agent (Behavior of MOG agent is the same). Please note that CMI SOC is ON.

Figure 2 SWAP Example (FPS Subscriber)

```
Before SWAP
>qdn 7835401
------------------------------------------------------------
-------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:         CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    42
PM TERMINAL NUMBER :    4
OPTIONS:
DGT FPS MOG_1 FPS1 160

------------------------------------------------------------
>qdn 7835402
------------------------------------------------------------
DN:     7835402
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 05
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:         CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    42
PM TERMINAL NUMBER :    6
OPTIONS:
DGT FPS MOG_2 FPS2 203

------------------------------------------------------------
FPS:
>qfps all
WARNING: Query of all FPS counters may take a significant
amount of time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835401  MOG_ID: MOG_1             FPS1   160
Last Call Credit    : 10
Last Feature Credit : 3

DN:      1027835402  MOG_ID: MOG_2             FPS2   203
Last Call Credit    : 12
Last Feature Credit : 5

============================================================
TOTAL: 2 FPS subscriber(s) found
>
>swap $ 7835401 7835402 $ loop y y
```

```
After SWAP
>qfps all
WARNING: Query of all FPS counters may take a significant
amount of time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835402  MOG_ID: MOG_2             FPS2   203
Last Call Credit    : 12
Last Feature Credit : 5

DN:      1027835401  MOG_ID: MOG_1             FPS1   160
Last Call Credit    : 10
Last Feature Credit : 3

============================================================
TOTAL: 2 FPS subscriber(s) found

>qdn 7835401
------------------------------------------------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 05
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:         CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    42
PM TERMINAL NUMBER :    6
OPTIONS:
DGT FPS MOG_1 FPS1 160

------------------------------------------------------------
>qdn 7835402
------------------------------------------------------------
DN:     7835402
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:         CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    42
PM TERMINAL NUMBER :    4
OPTIONS:
DGT FPS MOG_2 FPS2 203

------------------------------------------------------------
>
```

8.2.2.4 Adding TCMI and LCMI Line Options to IBNXLA

TCMI and LCMI services are provisioned through translation table IBNXLA. The numbers to be dialed for TCMI and LCMI services are provisioned in table IBNXLA and can be datafilled by the customer. LCMI and TCMI

features are added to the FEATURE field of the FEAT TRanslations SELector (TRSEL) for table IBNXLA.

```
>add  NETXLA XXX FEAT N N LCMI
>add  NETXLA XXX FEAT N N TCMI
XXX - number to be dialed for the service
```

In the following example, 117 is used for TCMI, and 118 is used for LCMI provisioning.

Figure 3 Datafill Sample for Translation Table IBNXLA

```
>table IBNXLA
>pos NETXLA 117
>lis
KEY            RESULT
-----------------------------------------------
NETXLA 117     FEAT N N TCMI

>pos NETXLA 118
>lis
KEY            RESULT
-----------------------------------------------
NETXLA 118     FEAT N N LCMI
```

8.2.2.5 CMI Customer Group Option

CMI customer group option can be assigned to a customer group via CMI customer group option.

The CMI option has two suboptions: TCMI and LCMI. At least one suboption must be assigned while assigning the CMI customer group option. CMI Customer Group option is datafilled in table CUSTSTN.

8.2.2.5.1 Administrator Assignment

CMI customer group option can be assigned to customer groups via datafilling the CUSTSTN table. Since CMI customer group has two suboptions TCMI and LCMI, followings are possible:

```
table CUSTSTN

     add <CUSTNAME> CMI CMI TCMI $

     add <CUSTNAME> CMI CMI LCMI $
```

```
add <CUSTNAME> CMI CMI TCMI LCMI $
```

In case subscriber has TCMI or LCMI suboption assigned already, and existing option is attempted to be assigned again, one of the following error messages is displayed:

"Duplicate XXX option is not allowed."

"XXX option already exists."

XXX - LCMI or TCMI

However CMI customer group option can be assigned to customer group although all of the group members do not have MOG or FPS option. But in order to use CMI service, IBN/ETSI BRI subscriber must have MOG or FPS option.

8.2.2.5.2 Administrator Deassignment

The administrator may deassign CMI option completely by deleting the tuple using the DEL command.

```
del <CUSTNAME> CMI
```

Please note that removing CMI option from a customer group means that removing both LCMI and/or TCMI options from the customer group.

In order to remove one of TCMI or LCMI features, independent from the other, related tuple must be changed from CUSTSTN table.

```
cha <CUSTNAME> CMI XXX
```

XXX - LCMI or TCMI

8.2.2.6 Feature Metering

LCMI/TCMI services will be charged when an administrator assignment, deassignment or subscriber usage action of LCMI/TCMI line option occurs. This means feature meter of the subscriber is incremented when the administrator initiates an LCMI/TCMI line option assignment/deassignment to a line, or when the subscriber uses LCMI/TCMI services.

Like LCMI and TCMI line options, feature metering of the subscriber is incremented during the subscriber usage only.

Please note that feature metering is only supported for IBN lines. Feature metering on ETSI BRI lines is not supported. For IBN lines, MTRFEAT table must be datafilled properly for feature metering.

For subscribers with FPS option, feature meter count is decremented from subscriber's credit directly. Refer to the activity A89007209 "Fixed Price Service for Bangladesh" for further information on FPS.

In the announcement, provided by LCMI service, the feature meter count of the last call (if any) will be included. In other words, feature meter count increment, which is caused by the current usage of the LCMI service, will not be reflected to the announcement. Feature meter increments caused by the administrator assignment/deassignment of any feature are not reflected to the LCMI announcement (i.e. only increment of feature meter count caused by subscriber usage is announced).

8.2.2.7 CMI OM Group

CMI OM Group provides information about the successful and unsuccessful usage and performance of CMI features (SVBI0033 SOC must be ON). CMI OM group has four registers with names CMIATT, CMIUSG, CMIOVFL, and CMICERR. These OM registers are pegged by LCMI and TCMI features. CMI OM group is multi-tuple, which includes LCMI and TCMI tuples.

CMI Registers

- **CMIATT - CMI ATTEMPT**

This register counts the number of attempts for TCMI/LCMI service to be invoked. Generally this register is incremented each time LCMI or TCMI service is initiated. This means, LCMI/TCMI service is successfully translated through translation table IBNXLA and successfully activated.

- **CMIUSG - CMI USAGE**

This register counts the number of times LCMI/TCMI service is successfully completed. This register is incremented just after the announcement is successfully played.

- **CMIOVFL - CMI OVERFLOW**

This register counts the number of times LCMI/TCMI service can not be successfully completed due to insufficient system resources. It is incremented when the announcement can not be provided to the subscriber.

- **CMICERR - CMI CUSTOMER ERROR**

This register counts the number of times CMI service is not provided to the subscriber, due to illegal initiation (i.e. initiation of the CMI service during active call) of the service or subscriber is not allowed to use the service.

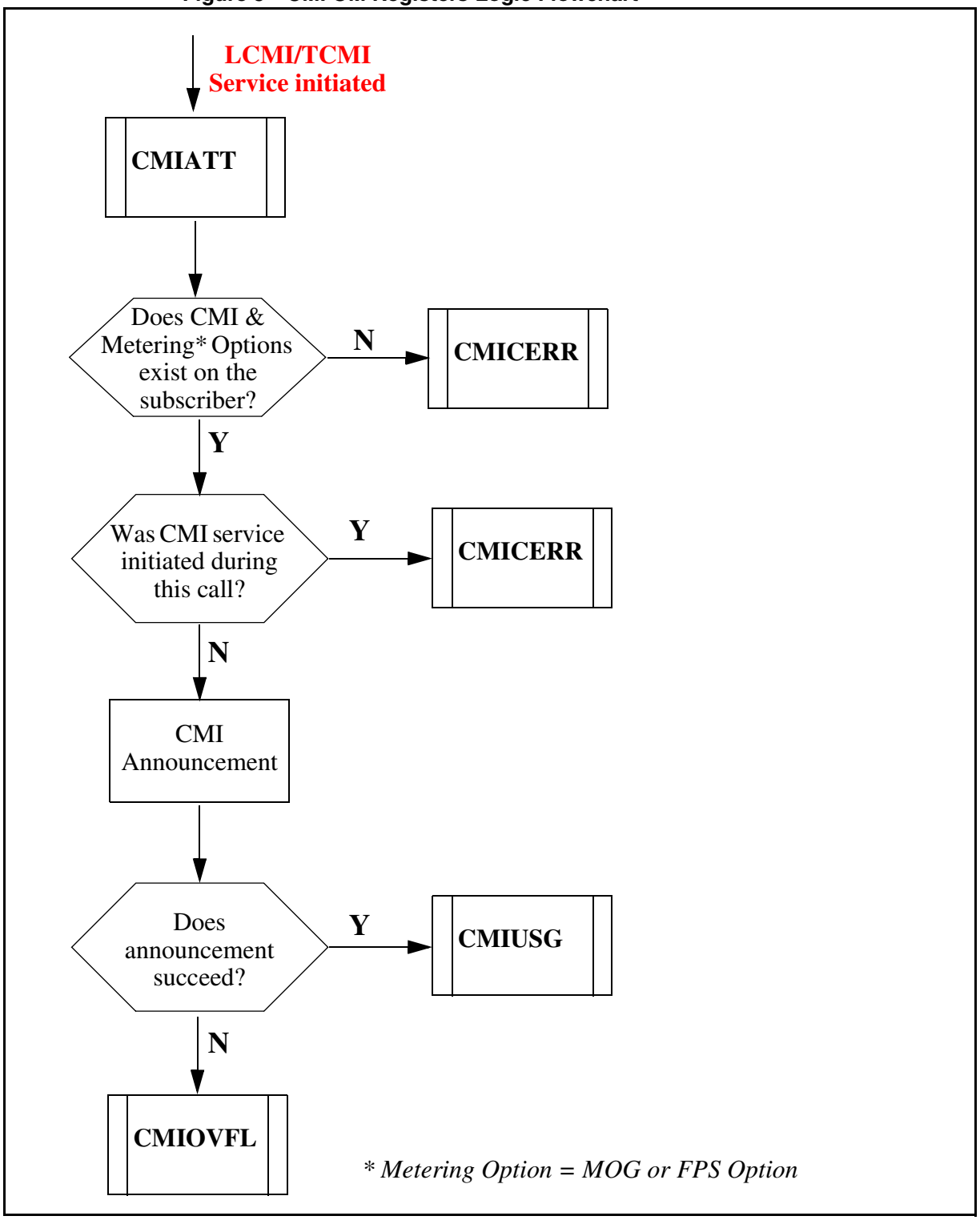
Following figure shows the map display of CMI OM registers.

Figure 4 Map display of CMI OM Registers

```
>omshow CMI active
CMI

CLASS:   ACTIVE
START:2003/05/25 12:00:00 SUN; STOP: 2003/05/25 12:01:47 SUN;
SLOWSAMPLES:          2 ; FASTSAMPLES:          11 ;
         KEY (CMI_OPTIONS)

                  CMIATT CMIUSG   CMIOVFL          CMICERR
         0 TCMI   4       2       1                1
         1 LCMI   10      9       1                0
```

See Figure 4 for pegging cases of CMI OM registers.

Figure 5 CMI OM Registers Logic Flowchart



8.2.2.8 Enhancement of MTRCOUNT Command

MTRCOUNT command, which displays the software meter counts of the subscriber having MOG, is enhanced in order to display the last call meter count, last feature meter count, and the total of all meter counts assigned to the subscriber when SVBI0033 SOC is ON (when used with “line” parameter). Map display is as follows:

Figure 6 Map Display for MTRCOUNT LINE command

```
>mtrcount LINE 7835406
************************************************************

DN     : 1027835406
DATE   : 03/07/18
MTR NAME: FEATURE           MTR COUNT:  00000000 WRAP: N
MTR NAME: LOCAL             MTR COUNT:  00000000 WRAP: N
MTR NAME: TOLL              MTR COUNT:  00000000 WRAP: N

          TOTAL             MTR COUNT: 000000000
          LAST CALL         MTR COUNT:  00000000
          LAST FEATURE      MTR COUNT:  00000000
************************************************************
```

When MTRCOUNT command is used with TRUNK/LMG (Line Meter Group) option, when SVBI0033 SOC is ON, TOTAL of assigned meter counts of trunk/lmg is displayed. Example map displays are as follows:

Figure 7 Map Display for MTRCOUNT TRUNK command

```
>mtrcount trunk 2WBDISP2AB
 ************************************************************

 TRUNK GROUP: 2WBDISP2AB
 DATE   : 04/03/05

 INCOMING CALLS
 --------------
 MTR NAME: METER1           MTR COUNT:  000000000000 WRAP:Y
 MTR NAME: METER2           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER3           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER4           MTR COUNT:  999999999999 WRAP:Y

           TOTAL            MTR COUNT: 6999999999997

 OUTGOING CALLS
 --------------
 MTR NAME: METER1           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER2           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER3           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER4           MTR COUNT:  999999999999 WRAP:Y

           TOTAL            MTR COUNT: 7999999999996

************************************************************
```

Figure 8 Map Display for MTRCOUNT LMG command

```
>mtrcount lmg 533
************************************************************

LOGICAL METERING GROUP: 533
DATE   : 04/03/05

INCOMING CALLS
--------------
MTR NAME: TLOCAL           MTR COUNT:  999999999999 WRAP:N
MTR NAME: TTOLL            MTR COUNT:  000000000134 WRAP:Y

          TOTAL            MTR COUNT: 2000000000133

OUTGOING CALLS
--------------
MTR NAME: TLOCAL           MTR COUNT:  000000000145 WRAP:N
MTR NAME: TTOLL            MTR COUNT:  000000000125 WRAP:Y

          TOTAL            MTR COUNT: 1000000000270
************************************************************
```

8.2.2.9 Enhancement of QFPS Command

QFPS FPS CI command, which displays the FPS credit of the subscriber having FPS, is enhanced in order to display the last call meter count, last feature meter count, and the total of all meter counts assigned to the subscriber when SVBI0033 SOC is ON. QFPS command with ZERO, UNUSEDFOR, DN and ALL options are enhanced by this activity. Map display is as follows:

Figure 9 Map Display for QFPS command

```
>qfps all
WARNING: Query of all FPS counters may take a significant amount of
time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835407  MOG_ID: MOG_2             FPS2   256
Last Call Credit    : 10
Last Feature Credit : 0

DN:      1027835401  MOG_ID: MOG_3             FPS1   176
Last Call Credit    : 20
Last Feature Credit : 2

DN:      1027835403  MOG_ID: MOG_2             FPS1   176
Last Call Credit    : 0
Last Feature Credit : 0

DN:      1027835402  MOG_ID: MOG_2             FPS2   256
Last Call Credit    : 0
Last Feature Credit : 10

================================================================
TOTAL: 4 FPS subscriber(s) found

>qfps dn 7835407
----------------------------------------------------------------
DN: 7835407     MOG_ID: MOG_2             FPS2   256

Last Call Credit         : 10
Last Feature Credit      : 0
>

>qfps unusedfor 1
WARNING: Query of all FPS counters may take a significant amount of
time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835403  MOG_ID: MOG_2             FPS1   176
Last Call Credit    : 0
Last Feature Credit : 0

================================================================
TOTAL: 1 FPS subscriber(s) found
```

8.2.2.10 CMI Announcements

CMI announcements are custom announcements that consist of a number of simple phrases, in English, datafilled in table ANNPHLST (See Appendix B for sample announcement datafill). Each simple phrase has a corresponding recording on the EDRAM card.

Feature meter count announce is provided by datafilling table ANNPHLST properly. CMIFTRANN_START phrase idicates the start of feature announce sentence, while CMIFTRANN_STOP indicates the end of the feature announce sentence.

Please note that announcement sequence strictly depends on the datafill in table ANNPHLST. If it is not datafilled properly, announcement will be provided in wrong sequence.

8.2.2.10.1 Simple Phrase Names Used in CMI Announcement

The simple phrase names provided for CMI service for English language and the corresponding phrases recorded on the EDRAM are shown in table below. These are assigned on a EDRAM using the ASSIGN command. Please refer to “APPENDIX A Assigning EDRAM Phrases Using DRAMREC CI Command”.

Table 2 List of English Phrases in CMI Service

Phrase Name	Recording	Phrase Name	Recording
CMIENG1	Your	CMIENG2	Last Call
CMIENG3	Total	CMIENG4	Meter Count is
CMIENG37	Last Feature	CMIENG5	Thank you for your calling
CMIENG39	Credit is	CMIENG38	Remaining
CMIENG6	One	CMIENG7	Two
CMIENG8	Three	CMIENG9	Four
CMIENG10	Five	CMIENG11	Six
CMIENG12	Seven	CMIENG13	Eight
CMIENG14	Nine	CMIENG15	Ten
CMIENG16	Eleven	CMIENG17	Twelve
CMIENG18	Thirteen	CMIENG19	Fourteen
CMIENG20	Fifteen	CMIENG21	Sixteen
CMIENG22	Seventeen	CMIENG23	Eighteen
CMIENG24	Nineteen	CMIENG25	Twenty
CMIENG26	Thirty	CMIENG27	Forty
CMIENG28	Fifty	CMIENG29	Sixty

Phrase Name	Recording	Phrase Name	Recording
CMIENG30	Seventy	CMIENG31	Eighty
CMIENG32	Ninety	CMIENG33	Hundred
CMIENG34	Thousand	CMIENG35	Million
CMIENG36	Zero	**CMIENG**	Language delimiter (optional)
CMIENGFTRANN_ START	delimiter for feature announce starting	**CMIENGFTRANN_ STOP**	delimiter for feature announce stopping
CMIENG_MTR_CREDIT	meter count/credit	CMIENGCNT_LSTFTR	last feature meter count
CMIENGCNT_LSTOT	last/total/remaining	CMIENGLSTOT	last//total

Red - Main phrases

Blue - Number Phrases

Black - Compound Phrases

Green - delimiters

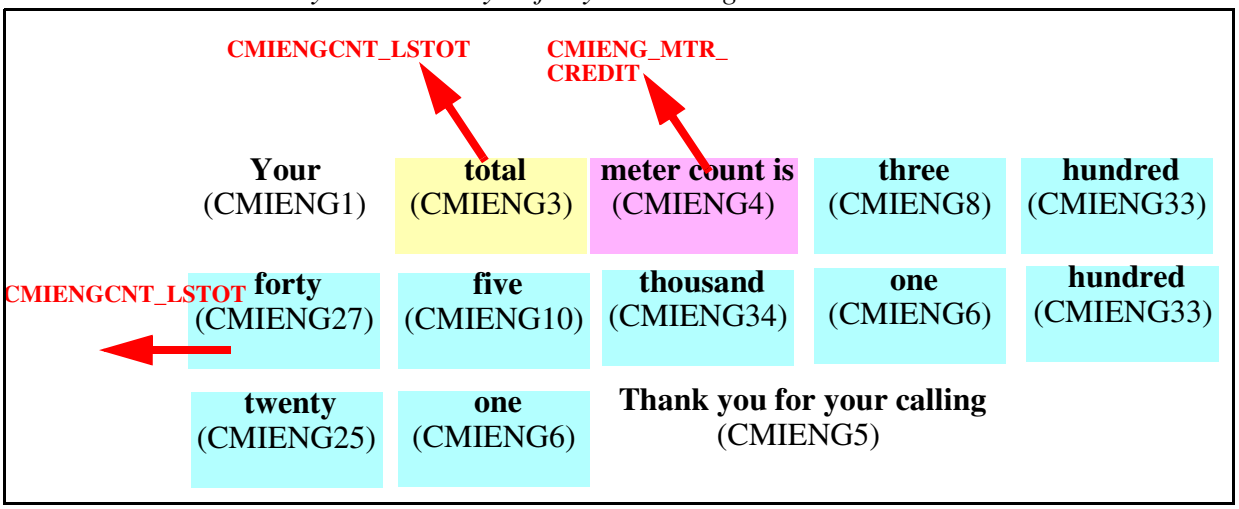
Please note that compound phrases and delimiters should not be recorded manually. Corresponding phrases are decided dynamically at run time.

8.2.2.10.2 CMI Announcement Example

Examples of announcements for CMI service is shown in the following table, announcing:

- **Example 1: TCMI announcement provided to subscriber having MOG option.**

"Your total meter count is three hundred forty five thousand one hundred twenty one. Thank you for your calling."

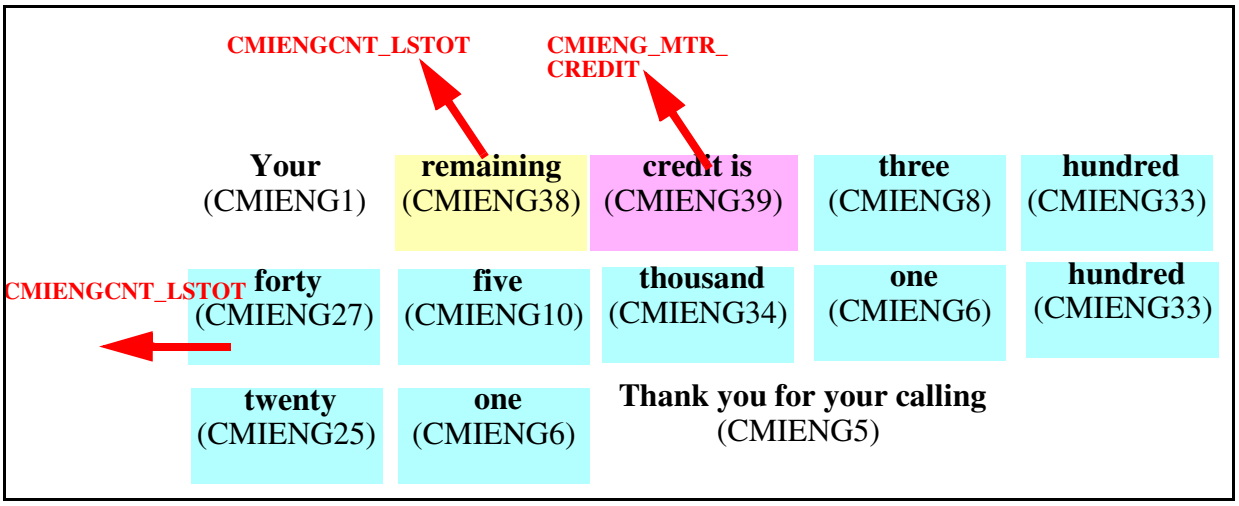


- **Example 2: TCMI announcement provided to subscriber having FPS option.**

"Your remaining credit is three hundred forty five thousand one hundred twenty one. Thank you for your calling."

- **Example 3: TCMI announcement provided to subscriber having FPS option.**

"Your remaining credit is three hundred forty five thousand one hundred twenty one. Thank you for your calling."



8.3 Hardware Requirements or Dependencies

This feature uses the Enhanced Digital Recorded Announcement Machine (EDRAM) to provide the announcement for CMI service. The CMI simple phrases are loaded into EDRAM as voice files.

8.4 Software Requirements or Dependencies

Software and hardware metering should be enabled via office parameter ENABLE_METERING. ENABLE_METERING must be YES in order to use CMI services.

8.5 Limitations and Restrictions

1. The total recording time for all the phrases is limited by the EDRAM hardware. All phrases making up CMI announcement must exist on one physical EDRAM card. NTP-297-1001-527 contains the complete description on EDRAM.
2. Hardware and software metering should be enabled via office parameter ENABLE_METERING. In case ENABLE_METRING is NO, meter counts are not updated after each call, and CMI announcement does not reflect the correct values of meter counts.
3. LCMI and TCMI services can not be initiated during an active call.
4. Last call meter count and last feature count of MOG Subscribers are preserved during warm, cold and reload restarts, since these counts are saved in DSPROT memory. But these counts are not survived during office reboot.But please note that last call meter count and last feature count of FPS subscribers are preserved during WARM restarts only.
5. State of SVBI0033 SOC can not be changed to IDLE state from ON state, while one of DUMP, METERING RESTORE, or LINE RECOVERY processes are running.

8.6 Interactions

Please note that only the features that CMI service has interaction with are explained below.

8.6.1 Call Diversion

Call diversion to LCMI and TCMI services is allowed. But, in case a subscriber diverts his phone to LCMI/TCMI service, others calling the diverting DN hears the BUSY tone. However, diverting subscriber himself will be able to call LCMI/TCMI service.

8.6.2 Hunt Groups

CMI services are supported for DNH, DLH and MLH Hunt Groups. In the last meter count announce for MLH and DLH members, meter counts of the last call made by “any member” (i.e subscriber himself or anybody else) is included.

In the total meter count announce, total of all meters assigned to the hunt group is included.

8.6.3 MSN on ETSI BRI

CMI and MSN on ETSI BRI interaction behavor is just like the behavior of CMI and Hunt groups.

8.6.4 Reverse Charging

LCMI service is compatible with reverse charging. In case originating agent initiates LCMI service after a reverse charged call, “last call meter count =0” is announced to the subscriber. In case LCMI service is initiated by the terminating agent (i.e charged party), subscriber is announced the actual value of the meter count, consumed during the last call.

8.6.5 FNT (Free Number Terminating)

CMI services arecompatible with FNT option. Last call/feature meter counts of IBN/ETSI BRI agent are updated as zero after answered free call (i.e.If IBN/ ETSI BRI agent initiates LCMI service after a free call, last call meter count of the agent is announced as zero). Please note that feature meter count increments (due to usage or activation of any metered feature) during FNT call are not reflected to the last call meter count.

8.6.6 HOLD

LCMI announcement is released when LCMI announcement is held, in order not to cause any troubles during complex call scenarios in ETSI BRI lines (i.e. 3PTY etc).

8.6.7 Basic Call & Complex Call CMI Interaction

- Consider the following scenario:

Action	Last Call Meter Count	Last Feature Meter Count	Announcement
1. Any Call	4	3	-
2. Subscriber initiates LCMI Service	4	2	Last Call Meter Count = 4 last feature meter Count = 3
3. Subscriber initiates LCMI Service	0	2	Last Call Meter Count = 4 last feature meter Count = 2

In the subscriber’s first initiation of LCMI service, meter counts of the last call is announced to the subscriber. After the announcement, last feature meter count is incremented due to the usage of LCMI service.

In the second initiation of LCMI service, last call meter count of the previous call is preserved, and last feature meter count was two. And again last feature meter count is incremented due to usage of LCMI service.

- In complex call scenarios that contain more than one leg (i.e. Call Transfer, Three Way Call and Six Way Call), meter count of the latest disconnected leg is announced to the charged agent. Consider the following scenario of 3WC:

1. Agent A has 3WC option.
2. Agent A calls Agent B.
3. Agent B answers the call.
4. Agent A flashes, and calls Agent C. (A-B call on hold)
5. Agent C answers. (A-C call active)

For possible scenarios after this step, lately disconnected leg's meter count is reflected to the announcement provided to Agent A (i.e. charged agent), since last call meter count is updated when all of the connected calls are released.

8.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	__X__
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	__X__
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	__X__

8.8 Glossary

Term	Description
BRI	Basic Rate Interface
CMI	Call Meter Inquiry
DLH	Distributed Line Hunting
ETSI	European Telecommunications Standard Institute
FNAL	Feature Not Allowed
FPS	Fixed Price Service
LCMI	Last Call Meter Inquiry
MLH	Multi-line Hunting
MOG	Metering Origination Group
MSN	Multiple Subscriber Number
OM	Operational Measurement
SO	Service Order
SOC	Software Optionality Control
SPM	Subscriber’s Private Meter
TCMI	Total Call Meter Inquiry

8.9 APPENDIX A Assigning EDRAM Phrases Using DRAMREC CI Command

This section explains the command required to assign an internal recording on EDRAM to an external phrase name (up to 16 alpha numerics) in order to datafill table ANNPHLST. The internal recordings in the corresponding voice files are downloaded already to the EDRAM. *RECORD* is a subcommand under DRAMREC utility. For complete information, refer to NTP-297-1001-527 *Digital Recorded Announcement Machine DRAM and EDRAM Guide.*

Table 3 ASSIGN Phrase Names to Internal EDRAM Recordings

Command Name	EXTERNAL PHRASE NAME	LENGTH	PAD	DRAM	CARD	INTERNAL PHRASE #	Force
record	cmieng1	1	pad	1	4	9	force
record	cmieng2	1	pad	1	4	10	force
record	cmieng3	1	pad	1	4	11	force
record	cmieng4	2	pad	1	4	12	force
record	cmieng5	2	pad	1	4	14	force
record	cmieng6	1	pad	1	4	16	force
record	cmieng7	1	pad	1	4	17	force
record	cmieng8	1	pad	1	4	18	force
record	cmieng9	1	pad	1	4	19	force
record	cmieng10	1	pad	1	4	20	force
record	cmieng11	1	pad	1	4	21	force
record	cmieng12	1	pad	1	4	22	force
record	cmieng13	1	pad	1	4	23	force
record	cmieng14	1	pad	1	4	24	force
record	cmieng15	1	pad	1	4	25	force
record	cmieng16	1	pad	1	4	26	force
record	cmieng17	1	pad	1	4	27	force
record	cmieng18	1	pad	1	4	28	force
record	cmieng19	1	pad	1	4	29	force
record	cmieng20	1	pad	1	4	30	force
record	cmieng21	1	pad	1	4	31	force
record	cmieng22	1	pad	1	4	32	force
record	cmieng23	1	pad	1	4	33	force
record	cmieng24	1	pad	1	4	34	force
record	cmieng25	1	pad	1	4	35	force
record	cmieng26	1	pad	1	4	36	force
record	cmieng27	1	pad	1	4	37	force
record	cmieng28	1	pad	1	4	38	force
record	cmieng29	1	pad	1	4	39	force
record	cmieng30	1	pad	1	4	13	force

Table 3 ASSIGN Phrase Names to Internal EDRAM Recordings

Command Name	EXTERNAL PHRASE NAME	LENGTH	PAD	DRAM	CARD	INTERNAL PHRASE #	Force
record	cmieng31	1	pad	1	6	14	force
record	cmieng32	1	pad	1	6	15	force
record	cmieng33	1	pad	1	6	16	force
record	cmieng34	1	pad	1	6	17	force
record	cmieng35	1	pad	1	6	18	force
record	cmieng36	1	pad	1	6	19	force
record	cmieng37	2	pad	1	6	20	force
record	cmieng38	1	pad	1	6	22	force
record	cmieng39	2	pad	1	6	23	force

8.10 APPENDIX B Datafill for CMI Announcements

This appendix describes changed datafill required for CMI announcements on an EDRAM card. For complete information, refer to NTP-297-1001-527 *Digital Recorded Announcement Machine DRAM and EDRAM Guide.*

The sequence to datafill EDRAM and CMI related tables are shown below.

8.0.9.1 Table TMINV

This table defines the location of two EDRAM hardware cards within the Maintenance Trunk Module (MTM).

Figure 10 Table DTMINV - Sample Datafil

```
 TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS        LKDATA  EQPEC
    LOAD   EXECS                                SCTMLOC
-----------------------------------------------------------------
       DTM    0    TME    0    51     1   B     3   0 10 12  0 1X80AA
EDRMAE47   MTMEX         SINGLE_CARD         MTM     2 12
```

8.0.10.2 Table DRAMS

This table contains the information about two physical EDRAM cards and the arrangement of speech memory. Each physical card can be divided into 8 single-density virtual cards or 4 double-density virtual cards. The datafill below divides one physical card into 4 double-density virtual cards.

Figure 11 Table DRAMS - Sample Datafil

```
DRAMCARD TMTYPE TMNO TMCKT  CARDCODE
                                                              CARDINFO
-----------------------------------------------------------------
    1  0    DTM    0     0    1X80AA
                                                  CTLR          DRAM1

    1  2    DTM    0     2    1X80AA
RAM (1) $

    1  4    DTM    0     4    1X80AA
RAM (2) $

    1  6    DTM    0     6    1X80AA
RAM (3) $
```

8.0.11.3 Table EDRAMINV

This table contains the voice file information fort he EDRAM. Voice files contain internal recordings for simple phrases. Up to 8 single-density voice files or 4 double-density voice files can be downloaded to a specific EDRAM card.

Table 1 Table EDRAMINV - Sample Datafill

EDRAMNM	TUPINFO	
DTM 0 3	ANN	CMIANN1
DTM 0 4	ANN	CMIANN2

Four voice files, CMIANN1 to CMIANN2 contain English phrases.

After datafilling table EDRAMINV, DTM must be reloaded with announce files. Then the phrases must be assigned.

8.0.11.4 Table CLLI

This table is used to define new CLLIs for two announcement groups. Field TRKGRSIZE defines the total number of members in each group.

Table 2 Table CLLI - Define Announcement CLLI

CLLI	ADNUM	TRKGRSIZE	ADMININFO
CMIENG	800	10	CALL_METER_INQUIRY_ENGLISH

8.0.11.5 Table ANNS

This table assigns the CLLI name defined in table CLLI to an announcement type. Field CLLI contains the CLLI name. For CMI service, field ANTYPE must be datafilled with *CMI*. The value in field MAXCONN has no impact to custom announcements such as CMI since for a custom announcement, the maximum number of simultaneous connections that can be made to one announcement is hard-coded to 1. CMI Announcement is repeated for number

Table 3 Table ANNS - Sample Datafill

CLLI	ANTYPE	TRAFSNO	MAXCONN	CYTIME	MAXCYC
CMIENG	***CMI***	25	1	0	2

of times defined by MAXCYC field. But please note that once you datafill this tuple, it is very hard to change it.

8.0.11.6 Table ANNMEMS

This table contains the assignments for each announcement member in the announcement group defined in table ANNS. Each tuple here corresponds to one trunk member in its group at MAP TTP level. For custom announcement such as CMI, hardware type must be DRAM, only one track can be datafilled in field TRACKLIST and the track number must be 0. For each EDRAM card, e.g. DTM 2, only up to 29 members (1 to 29 at the last column) can be datafilled.

Table 4 Table ANNMEMS - Sample Datafill

ANNMEM		HDWTYPE	CARD	TRACKLIST			
CMIENG	0	DRAM	DRA	0	DTM	0	14

8.0.11.7 Table ANNPHLST

Each tuple in this table defines one custom announcement. For CMI service, the announcement number (the second field of USERANN) must be unique. Phrase list to be announced is generated dynamically at runtime. Adviced datafill for CMI announcement is like the following if feature meter count will be announced in the LCMI announcement:

Figure 12 Sample Datafill For CMI Announcement, Announcing Last feature also meter count

```
ANNPHKEY          PHSLIST
-------------------------------------------------------------------
CMIENG        1   CMIENG   CMIENG1   CMIENGLSTOT   CMIENG_MTR_CREDIT
CMIENGCNT_LSTOT

CMIFTRANN_START       CMIENG1       CMIENG37       CMIENG_MTR_CREDIT
CMIENGCNT_LSTFTR CMIFTRANN_STOP

CMIENG5 $
```

TCMI announcement with the above datafill will be like the following for **MOG subscriber**:

"Your total meter count is three hundred forty five thousand one hundred

twenty one. Thank you for your calling."

For the **FPS subscribers**. it will be:

"Your remaining creadit is three hundred forty five thousand one hundred

twenty one. Thank you for your calling."

LCMI Announcement for **MOG subscribers**(feature meter count is not equal to 0) will be:

"Your last call meter count is three hundred forty five thousand one hundred

twenty one. Your last feature meter count is five. Thank you for your calling."

For FPS subscribers(feature meter count is not equal to 0) will be:

"Your last call credit is three hundred forty five thousand one hundred

twenty one. Your last feature meter credit is five. Thank you for your calling."

If last feture meter count of the subscriber is equal to zero, feture meter is not announced.

Adviced datafill for CMI announcement is like the following if feature meter count will be announced in the LCMI announcement:

Figure 13 Sample Datafill For CMI Announcement, without last feature meter count announcing

```
ANNPHKEY          PHSLIST
-----------------------------------------------------------------
CMIENG        1   CMIENG   CMIENG1   CMIENGLSTOT   CMIENG_MTR_CREDIT
CMIENGCNT_LSTOT

CMIENG5 $
```

Last feature meter count is not announced in LCMI announcement (even if last fetature meter count is different than zero), while TCMI announcement remains the same. This time,

LCMI Announcement for **MOG subscribers** will be:

"Your last call meter count is three hundred forty five thousand one hundred

twenty one. Thank you for your calling."

For **FPS subscribers** it will be:

"Your last call credit is three hundred forty five thousand one hundred

twenty one. Thank you for your calling."

If more than one tuple is datafilled for CMI service in this table, only the first, decided by the unique announcement numbers (e.g. 1 in the above table), is used for announcement playing on each cycle.

The announcement number in this table can be from 1 to 255. For better real time performance, it's recommended to assign the announcement number from 1 up.

9: Functional Description (FN): A00001935

9.1 Feature name

Provisioning Support for Centrex-IP Nodes and Lines

9.2 Description

Feature A0001935 will deliver the lines flow through and pre-provisioning functionality in the Succession Element and Sub-element Manager (SESM) required for the Centrex IP Client Manager (CICM) integration with Succession. The design will be split into Nodes provisioning for CICM Gateways (GWs), and lines provisioning for CICM terminations.
The Nodes provisioning feature component will provide for the provisioning of CICM GWs. Nodes provisioning will also provide functionality to pre-provision the CICM terminations in the GWC-EM and to pre-provision LENs (Line Equipment Numbers) in XACore table LNINV. The Lines Provisioning component will provide flow through of service information entered at OSSGate (SERVORD+ commands). New line provisioning functionality will be delivered to allow line data to be transmitted to the CICM Element Manager (CICM-EM).

9.3 Hardware Requirements or Dependencies

Not applicable.

9.4 Software Requirements or Dependencies

Not applicable.

9.5 Limitations and restrictions

None.

9.6 Interactions

This feature will integrate the Centrex-IP client provisioning with the existing Succession SERVORD+ system. Centrex-IP client ommands/data will distributed to the CICM-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the CICM-EM from SESM SERVORD+:

- NEW, EST, ADD, OUT, DEL, CDN, CHDN, CLN/CTP, CKLN/CKTP, ADO, DEO, CHF

This list is subject to change until final DSUM approval.

9.7 Applicable customer facing sections

Fault Management

- Logs __N/A_
- Alarms __N/A_

Configuration

- Data Schema ___X__
- User Interface __N/A_
- Element Management __N/A_
- Security __N/A_
- Service Order ___X__
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

9.8 Glossary

Term	Description
New term	Definition

10: Functional Description (FN): A00001965

10.1 Feature name

H.323 DPNSS Tunnelling on CS2K

10.2 Description

This SN06 activity, A00001965, provides the capability to connect DPNSS PBXs to the CS2K and provide Carrier Hosted VPN service to the PBX using DPNSS networked feature signalling between extensions on the PBXs and CS2K hosted Lines[1]. The same level of service is provided for network calls between PBXs and Lines connected to different CS2K call servers.

This feature is only available in the International CS2K software load.

The proposed system uses a customer premise located Gateway which interfaces to TDM DPNSS trunks from the PBX and tunnels the DPNSS signalling over a H323 IP connection to the CS2K. The Gateway to be used is the Westell iQ2030.

The DPNSS signalling from the Westell H.323 DPNSS interface is tunnelled transparently by the CS2K to either:

- another DPNSS PBX connected to the CS2K via a Westell H.323 gateway or
- IBN7 trunks supporting the existing Nortel proprietary DPNSS feature transparency capability (DFT).

This tunneling capability supports end to end transparency of DPNSS Real Calls (Basic Call Service & Call Associated Services (CAS)) and DPNSS Virtual Calls (Non-Call Associated Services (NCAS)) in the above call scenarios as if the intermediate H323 and IBN7 trunks were not present.

The same level of service is provided as for TDM DPNSS trunk connected to a DMS MMP.

Figure 1 shows possible configurations that are supported in CS2K for the deployment of H.323 Westell Gateway by this feature for DPNSS tunnelling applications.

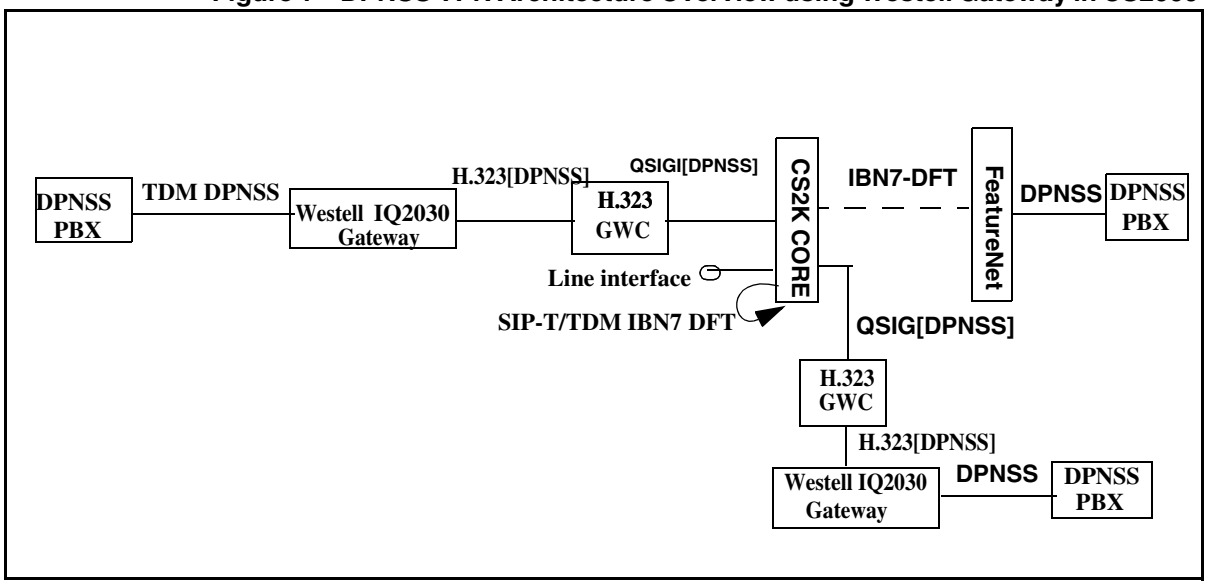
[1]Direct interworking of the H.323 DPNSS interface to CS2K hosted lines will not support DPNSS transparency in SN06. In SN06, calls between H.323 DPNSS interfaces and CS2K hosted lines need to be routed via an IBN7 looparound (TDM or SIP-T) to support DPNSS feature transparency.

The following call scenarios are supported:

- Westell To Westell H.323-QSIG[DPNSS] tunnelled calls.
- Westell call to CS2K and over IBN7-DFT to FeatureNet.
- Westell call to Madiatrix line (off CS2K) over SIP-T or IBN7 looparound.

The H.323 GWC performs also the function of H.323 Gatekeeper.

Figure 1 DPNSS VPN Architecture Overview using Westell Gateway in CS2000



10.2.1 Operational Overview

The H.323 Gateway component of the H.323 system uses H.225 basic call control messaging protocol which is based on Q.931/Q.932 message and H.450.1 service signalling mechanism.

To support both call related and Call Independent, Connection-Oriented signalling supplementary services (CAS and NCAS) which are required by this feature, the feature aligns itself with Q.932 Generic Functional Protocol for VPN applications and its use of Facility Information Element.

Furthermore, the DPNSS message is tunnelled using Westell defined manufacturer specific Operations as part of the h4501SupplementaerService field of the H323-UserInformation PDU.

This information in turn is mapped into Q.932 defined Facility Information element as part of ASN.1 PER encoded serviceAPDU element in H.450 Supplementary Service APDU using Nortel defined H.323 Operation.

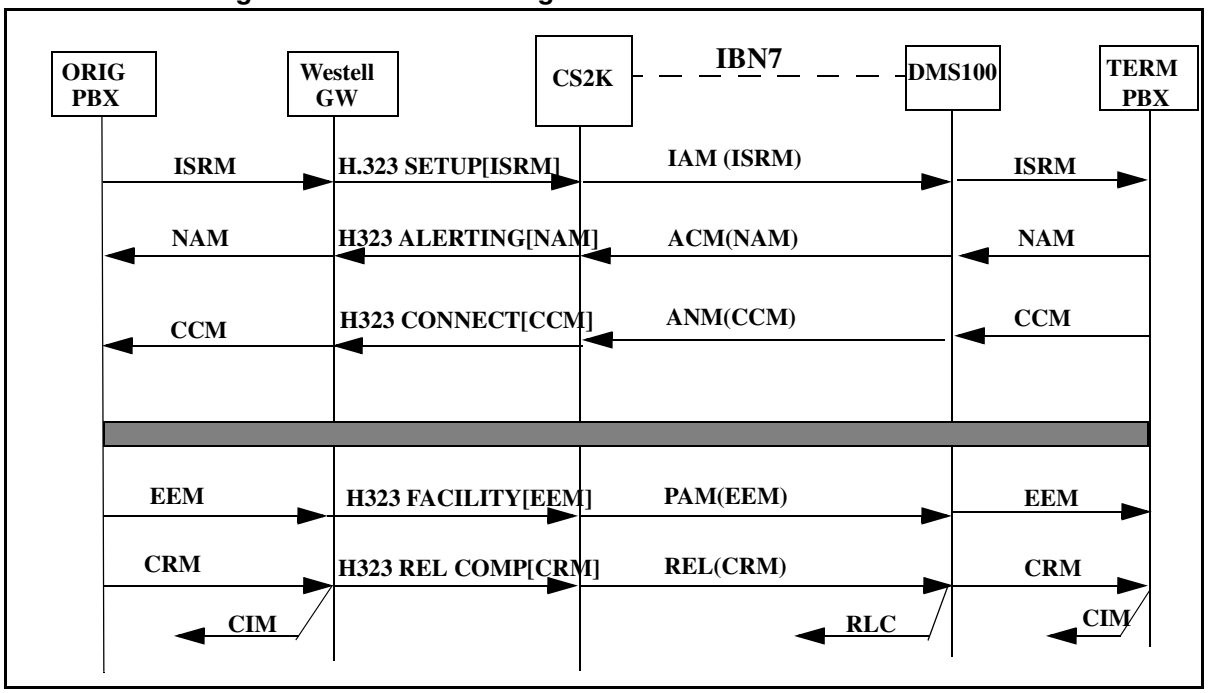
As per Westell H.323 Tunnelling specification, the DPNSS service strings are included in the Transparency service APDU and the number parameters (e.g CLI) are included in Address Service APDU.

10.2.2 External Message Interface

The following are the decomposition of messages and the external interfaces that are provided by CS2K as a transit node.

DPNSS real call includes support for basic call in addition to support for DPNSS services which require bearer channel (e.g: route optimization, executive intrusion, call diversion) and other centrex type of services. The DPNSS services supported are as part of DPNSS transit node functionalities.

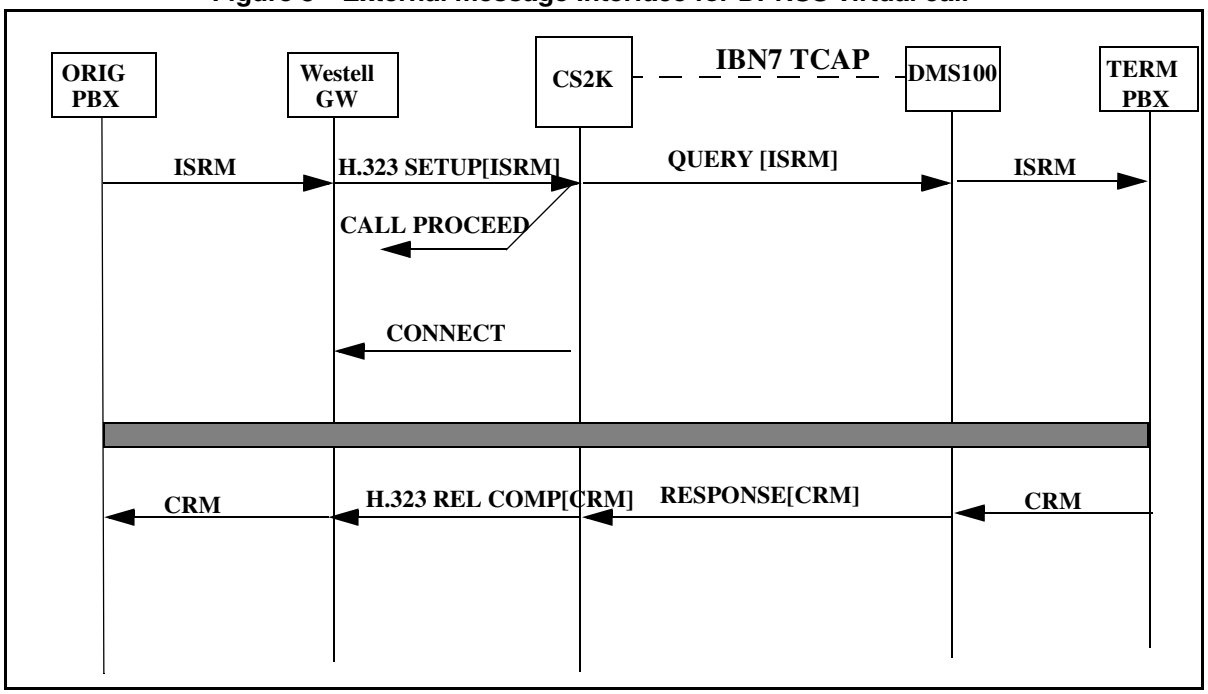
Figure 2 External message Interface for DPNSS real call



The DPNSS virtual calls, or NCAS calls, are bearer independent and include supporting services such as Call Back When Free, Message Waiting Indicator.

To support DPNSS virtual calls, this feature uses the IBN7 TCAP and existing INTERWRK subsystem (as part of SCCP) as used by TDM DFT. However a new architecture is introduced to interface the incoming H.323-QSIG[DPNSS] NCAS messages to IBN7 TCAP, and for the incoming IBN7 TCAP messages, to direct them to the QVPN VID starter instead of DPNSS feature starter.

Figure 3 External message Interface for DPNSS virtual call



The external interface to CS2K on the H.323 IP side for Interworking/Transit of DPNSS signalling over QSIG/IP networks, are provided by Westell gateway [15]. On the network side, the external interfaces shown are as those provided by [7] and [8] for Real and Virtual calls respectively.

10.2.3 Trunks Provisioning

The QSIG H.323 trunk is provisioned as Variant QSIGPRI, Issue ISO1996 in table LTDEF. In addition, the service option H323 in table LTDATA is added to the LTID of the QSIG trunk (as introduced by feature A00001895).

In addition, the existing DFT option in table NCOS is re-used This option is accessed via table LTCALLS against the QSIG trunk for QSIG to IBN7 DFT calls. For IBN7 DFT to QSIG calls, the same DFT option is used in table NCOS.

This feature does not introduce a new datafill of its own.

Please See “Appendix A: Basic call Setup” on page 168. for the datafill information related to Basic Calls.

Please See “Appendix B: Datafills for DPNSS CBWF and MWI” on page 175. for the datafills for CBWF and MWI

10.2.4 SOC Functionality

As part of H.323 base functionality, this feature supports both state and usage SOC functions.

The state SOC, controls (enables) the provisioning of the QSIG H.323 trunks.

The usage SOC, limits the maximum number of H.323 endpoints that can be datafilled on a CS2K as represented by the H.323 QSIG trunk members.

The H.323 SOC ordercode is: CS2B0004.

For further details on SOC functionality as supported by this feature, refer to A00001895 and A00002225.

10.2.5 Support for Netinfo

The Netinfo parameter consisting of customer group and NCOS, as supporetd in the DMS100 can optionally be used by this feature.

In order to be able to generate the Netinfo parameter on the H.323-QSIG trunk, option XLARTE is required to be added in table LTCALLS.

10.3 Hardware Requirements or Dependencies

The proposed system to support H.323 DPNSS tunnelling, uses a customer premise located Gateway which interfaces to TDM DPNSS trunks from the PBX and tunnels the DPNSS signalling over a H.323 IP connection to the CS2K. The Gateway used is the Westell iQ2030.

10.4 Software Requirements or Dependencies

This feature is as part of the group of features introduced in SN06 (and SN06.1) to support H.323 IP connections in the CS2K.

This feature has dependency with the following activities:

A00001895	H.323 Base Application(GWC9.1)
A00002358	H.323 QSIG(GWC9.1)
A00002225	H.323 Provisioning
A00001913	H.323 OAM(SESM6.1)

10.5 Limitations and restrictions

As stated earlier, this feature provides VPN transit functionalities for the hosted CS2K. Therefore, any originating or end node functionalities that relate to DPNSS features are not supported by the host CS2K. Any support for originating/terminating DFT as end-node functionalities on CS2k Madiatrix lines, require DFT (IBN7 TDM/SIP-T) looparounds.

Direct BTUP inteworking for PSTN breakout calls from the CS2K are also not supported. DFT looparounds will be required for such calls.

ROP functionality as required by the transit exchange is supported. However The ROP billing as a DPNSS feature is not supported over the QSIG trunk.

Billing records in general will be based on the incoming QSIG trunk rather than the DPNSS.

Data calls are not supported by Westell gateway.

Name Display service is not supported (as currently is not supported in DMS100 for DPNSS).

Tables TMTMAP and FAILMSG are not supported by QSIG. This results in not being able to provide flexible treatments and cause mapping in IBN7/ QSIG interworking call scenarios. This implies that we can not use table TMTCNTL in conjunction with table TMTMAP to be able to flexibly apply annoncements locally by the CS2K, while letting the tones to be applied remotely by the PABX based on specific causes. This restriction together with H.323 gateway limitation in applying tones such as user_busy, means that we should always set the AUDTRMT option in table LTDATA to 'N'.

Westell gateway (together with other current H.323 gateways) can not be made to apply RingBack tone after the Connect. This means for certain services which rely on CS2K to apply the RingBack tone after connection, the CS2K will not be able to apply the tone.

10.6 Interactions

None.

10.7 Applicable customer facing sections

Fault Management

Logs	___N/A__
Alarms	___N/A___

Configuration

Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) __N/A____

10.8 Glossary

Term	Description
ANM	Answer message
ACM	Address Complete message
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation one
CAS	Call Associated Signalling
CCM	Call Connect message
CIM	Clear Indication message
CRM	Clear request message
CS2K	Call Server 2000
DFT	DPNSS feature transparency
DPNSS	Digital Private Network Signalling System
EEM	END to End Message
FIE	Facility Information element
GW	Gateway
HNI	Hybrid Network Information
IP	Internet Protocol
ISRM	Initial Service Request Message
IAM	Initial Address Message
INF	Information message
NAM	Number Acknowledge message
NCAS	Non-Call Associated Signalling
NIM	Network Indication message
NTP	Network Transport Parameter
PAM	Pass along message
QSIG	Q-reference Point Signalling (also known as PSS1)
ROSE	Remote Operation Service Element

Term	Description
SS	Supplementary Service
SCCP	Signalling Connection Control Protocol
UU	H.323 User-user Information element
VPN	Virtual Private Network

10.9 References

1. H.323 Packet-Based Mulimedia Communication Systems.
2. H.225 Call Signalling Protocols and media stream packetization for Packet-based Multimedia Communication Systems.
3. H.450.1 Generic Functional protocol for the Support of Supplementary Services in H.323.
4. Q.932 DSS1 Generic Procedures for the Control of Supplementary Services.
5. Q.931 ISDN Layer 3 Protocol
6. BTNR 188 DPNSS . Digital Private Network Signalling System No.1
7. AE0909 DPNSS Transit DFT - Real Call
8. AE0910 DPNSS Transit - Virtual Call
9. AD1673 PRA/SS7 TCAP Interworking
10. AE1312 DPNSS Excellence!
11. A00001895 H.323 Base Application
12. A00002358 H.323 QSIG
13. A00002225 H.323 Provisioning
14. A00001913 H.323 OAM
15. Interworking/Transit of DPNSS Signalling Over QSIG and IP Networks - WP-13-000-016.012

10.10 Appendix A: Basic call Setup

The example gives below the the translations and the setup for a basic all originating from TDM switch over DPNSS-WESTELL connected to CS2K switch. The incoming Trunk on CS2K is QSIG and it goes over SIP-T looparound to land on the Mediatrix line on CS2K.

Important Points for setting up the translations for a Basic DPNSS-WESTELL-QSIG-SIP-T - Line call in CS2K switch:

- The Customer Group/NCOS combination of the Terminating line should have DFT option in table NCOS.
- When travering from QSIG trunk to SIP-T trunk, the CFT selector should get hit.
- The NCOS/Customer Group combination of the QSIG trunk should have DFT option in table NCOS.
- In table LTDATA, for the QSIG trunk, the PRI_IP_PROT option and H323 as the VOIP Protocol for that option should be added.

The details below are from TDM Switch.

```
>qlen 8104070
------------------------------------------------------------------------------
LEN:     HOST  01 0 00 21
TYPE: SINGLE PARTY LINE
SNPA: 181
DIRECTORY NUMBER:     8104070
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:   QUEENSX00MEL     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  6X17BA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    82
PM TERMINAL NUMBER :    22
DNGRPS OPTIONS:
NETNAME:  QUEENSNET
ADDRESS:             DDD810NNNN
NETNAME:     PUBLIC
ADDRESS:             NNN810NNNN
OPTIONS:
3WC RAG LNR DGT
------------------------------------------------------------------------------
>traver l 8104070 68124322 b
TABLE IBNLINES
HOST 01 0 00 21 0 DT STN IBN 8104070 QUEENSX00MEL 0 0 181 (3WC) (RAG) (LNR) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
181 810 4070 4070
   (QUEENSNET ( ADDRESS DDD 810 NNNN) $)
   (PUBLIC ( ADDRESS NNN 810 NNNN) $)$
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.
```

TABLE NCOS
QUEENSX00MEL 0 0 0 LINE (DFT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
QUEENSX00MEL NXLA QNSXXLA QNSXFET 0 QNSXDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME QNSXXLA
QNSXXLA 6 NET N N 0 N NDGT N Y DOD N 200 181_NPRT_10 NLCA_NILLA_10 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
200 IBN NONE NT 0 0 NILSFC 0 PX QNSXPX NIL 00 181_NPRT_10 NLCA_NILLA_10 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
181_NPRT_10 NSCR 181 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_10 NLCA NIL NILLATA $
TABLE PXHEAD
QNSXPX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 68124322
TABLE PXCODE
QNSXPX 6812 6812 RTE (PF 1) (MM 2 20) (DEST 20)$
TABLE: PXRTE
KEY: QNSXPX 20
. S WESTDPNSSA
EXIT TABLE PXRTE
Originator is not an EIN agent, therefore EIN info is not processed.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 WESTDPNSSA 8124322 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 ANNC006
2 LKOUT

+++ TRAVER: SUCCESSFUL CALL TRACE +++

The Details below are from CS2K Switch.
>qlen 8124322

```
--------------------------------------------------------------------------------
LEN:     LG    00 1 00 19
TYPE: SINGLE PARTY LINE
SNPA: 208
DIRECTORY NUMBER:     8124322
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:   ETB3PRIVGRPA     SUBGRP: 0  NCOS: 10
SIGNALLING TYPE:  DIGITONE
CARDCODE:  GWLPOT    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    37
PM TERMINAL NUMBER :    25
OPTIONS:
LNR DGT
--------------------------------------------------------------------------------
Table NCOS
>pos ETB3PRIVGRPA 10
ETB3PRIVGRPA 10 LINE 0 0 (XLAS E3A10XL NXLA E3ADIG) (DFT ) $

>traver tr h323qsiga 8124322 b
TABLE TRKGRP
H323QSIGA PRA 0 NPDGP NCRT MIDL N (QSIG 4) $ $
TABLE LTCALLS
QSIG 4 PUB XLALEC 3 208_NPRT_1 NLCA_NILLA_2 $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE LINEATTR
3 IBN NONE NT 0 0 NILSFC 0 PX E3APX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
208_NPRT_1 NSCR 208 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_2 NLCA NIL NILLATA $
TABLE PXHEAD
E3APX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8124322
TABLE PXCODE
E3APX 812 812 RTE ( PF 3) ( MM 2 20) ( DEST 456)$
TABLE: PXRTE
KEY:    E3APX  456
 . T IBNRT3 11
 .  . TABLE IBNRT3
 .  .   11 CFT N N N N SIPTVPNSHARED 0
```

```
 .  . EXIT TABLE IBNRT3
EXIT TABLE PXRTE
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN ETB3INAP)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES


This route is a DPT
1 SIPTVPNSHARED        4322            ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++

> traver tr SIPTVPNSHARED 4322 b
TABLE TRKGRP
SIPTVPNSHARED IBNT2 0 NPDGP NCRT VPNSHARED 0 ASEQ 90 N ANSDISC 0 Y N
N N N N N 0
   0 N 0 0 0 0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
VPNSHARED 90 0 0 SIPTRK ( XLAS SIPTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND
DIGCOL
VPNSHARED NXLA VPNXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME SIPTXLA
TUPLE NOT FOUND
Default is to go to next XLA name.
CUST PRELIM XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME VPNXLA
TUPLE NOT FOUND
Default from table XLANAME:
```

```
VPNXLA
   (NET N N 0 N NDGT Y Y DOD N 10 101_NPRT_1 NLCA_NILLA_0 NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
10 IBN NONE NT 0 0 NILSFC 0 PX VOIPPX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
101_NPRT_1 NSCR 101 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
VOIPPX DFLT CONT ( XLT OFC OFCLINE)$ DFOP ( CLASS NATL)$ NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    4322
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
OFCLINE SDFLT NODFOP NOCON 9
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    4322
TABLE OFCCODE
OFCLINE 4 4 DNRTE ( MM 4 4) ( CLASS NATL) ( DN 208 812)$
TABLE TOFCNAME
208 812 $
TABLE DNINV
208 812 4322 ILC LG 00 1 00 19
TABLE DNFEAT
TUPLE NOT FOUND
TABLE DNATTRS
208 812 4322
   (PUBLIC ( NAME ERNEST_PENFOLD) $)
   (ETB3PRIVNET ( NAME ERNEST_PENFOLD) $)$ $
TABLE DNGRPS
208 812 4322 4322
   (PUBLIC ( ADDRESS DDD 812 NNNN) $)
   (ETB3PRIVNET ( ADDRESS DDD 812 NNNN) $)$
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN ETB3INAP)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
INAP Termination Attempt TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES
```

```
1 LINE              2088124322        ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++



2003/07/02 09:44 *** ETB3 PSNW06BZ built on 05 JULY 2003 ***
TABLE: LTDATA
>pos QSIG 4 SERV SERV
QSIG 4 SERV SERV N Y ALWAYS ALWAYS (PRI_IP_PROT H323) $
>
2003/07/02 09:44 *** ETB3 PSNW06BZ built on 05 JULY 2003 ***
TABLE: LTCALLS
>pos QSIG 4 PUB
QSIG 4 PUB XLALEC 3 208_NPRT_1 NLCA_NILLA_2 $
>pos QSIG 4 PVT
QSIG 4 PVT XLAIBN 3 208_NPRT_1 NLCA_NILLA_2 ETB3PRIVGRPA 0 10 $
>
```

10.11 Appendix B: Datafills for DPNSS CBWF and MWI

```
-------------------------------------------------------------
CBWF Datafill:
--------------

TABLE: MSGRTE
MSGRTKEY MSGRTRES
-----------------
ETB3PRIVNET 9440 94499 (DPNSS SIPTVPNSHARED 1 N $) $
ETB3PRIVNET 440 4499 (SS7 ANSILOOPRS1 0 9 $) $
ETB3PRIVNET 812 812 (SS7 ANSILOOPRS1 0 9 $) $
ETB3PRIVNET 9812 9812 (DPNSS SIPTVPNSHARED 1 N $) $

Table CUSTNTWK:
---------------
ETB3PRIVGRPA ETB3PRIVNET 20 $ (NTWKRAG 60 5 10 6 2 40 OFFNET)
(CLID OFFNET)(NASOPT ( NACR ) (NACO 25 N) (NBVL ) $) (COSMAP NIL E3AOUT) (COF )
(REDIR 30) (EI ) (RNID OFFNET) (DTKROP ( TERMROP ) $)$

>qlen 8124322
-----------------------------------------------------------------------
LEN:     LG    00 1 00 19
TYPE: SINGLE PARTY LINE
SNPA: 208
DIRECTORY NUMBER:     8124322
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:   ETB3PRIVGRPA     SUBGRP: 0  NCOS: 10
SIGNALLING TYPE:  DIGITONE
CARDCODE:  GWLPOT    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    37
PM TERMINAL NUMBER :    20
DNGRPS OPTIONS:
NETNAME:     PUBLIC
ADDRESS:              DDD812NNNN
NETNAME:ETB3PRIVNET
ADDRESS:              DDD812NNNN
OPTIONS:
CWT 3WC RAG CWI DCPU LNR HLD DGT CNAMD NOAMA NAME PUBLIC ERNEST PENFOLD
ETB3PRIVNET ERNEST PENFOLD CFD P 68124427 A CFB P 68124327 I
-----------------------------------------------------------------------

MWI Datafill:
--------------

1. Add MWI option to line.

2. TABLE OFCENG
   DPNSS_MWI_CAPABILITY

3. TABLE NSIMAP
add N N 1 MWIACT
add N N 0 MWICANC

Procs:
NSI_STRING_PARSE
NSI_END_FUNCTIONALITY
NSI_MWI_ACT

CI test tool:
MWQ
QUEUE 8104070 1 8104071
```

```
Scenario:
---------
Pty A -> SIPT -> CS2K -> QSIG H323 -> Westell -> DMS (DPNSS) -> Pty B

Travers on CS2K:
----------------

traver l 8124427 68104070 b
TABLE IBNLINES
LG 00 2 00 24 0 DT STN IBN 8124427 ETB3PRIVGRPA 0 10 208 (RAG) (LNR) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
208 812 4427 4427
    (ETB3PRIVNET ( ADDRESS DDD 812 NNNN) $)
    (PUBLIC ( ADDRESS DDD 812 NNNN) $)$
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE NCOS
ETB3PRIVGRPA 10 0 0 LINE ( XLAS E3A10XL NXLA E3ADIG) ( DFT )$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
ETB3PRIVGRPA NXLA E3AXLA E3AFET 0 E3ADIG
TABLE DIGCOL
E3ADIG 6 COL L 7
TABLE IBNXLA: XLANAME E3A10XL
TUPLE NOT FOUND
Default is to go to next XLA name.
CUST PRELIM XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME E3AXLA
E3AXLA 6 NET N N 0 N NDGT N Y DOD N 5 101_NPRT_1 NLCA_NILLA_0 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
5 IBN NONE NT 0 0 NILSFC 0 PX E3APX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
101_NPRT_1 NSCR 101 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
E3APX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        68104070
TABLE PXCODE
E3APX 6810 6810 RTE ( MM 2 20) ( DEST 456)$
TABLE: PXRTE
KEY:    E3APX  456
 . T IBNRT3 20
 .  . TABLE IBNRT3
 .  .   20 S N N N N SIPTVPNSHARED
 .  . EXIT TABLE IBNRT3
EXIT TABLE PXRTE
Originator is not an EIN agent, therefore EIN info is not processed.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES
This route is a DPT
1 SIPTVPNSHARED         68104070           ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER
2 LKOUT
```

```
Scenario:
---------

Pty A -> SIPT -> CS2K -> QSIG H323 -> Westell -> DMS (DPNSS) -> Pty B

Travers on CS2K:
----------------

traver tr SIPTVPNSHARED 68104070 b

TABLE TRKGRP
SIPTVPNSHARED IBNT2 0 NPDGP NCRT VPNSHARED 0 ASEQ 90 N ANSDISC 0 Y N N N N N N 0
    0 N 0 0 0 0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
VPNSHARED 90 0 0 SIPTRK ( XLAS SIPTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
VPNSHARED NXLA VPNXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME SIPTXLA
SIPTXLA 681 NET N N 0 N NDGT N Y DOD N SIPTLNTR 101_NPRT_1 NLCA_NILLA_0 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
SIPTLNTR IBN NONE NT 0 0 NILSFC 0 PX SIPTPX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
101_NPRT_1 NSCR 101 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
SIPTPX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        68104070
TABLE PXCODE
SIPTPX 6810 6810 RTE ( PF 1) ( MM 2 20) ( DEST 810)$
TABLE: PXRTE
KEY:   SIPTPX  810
 . S H323QSIGA
EXIT TABLE PXRTE
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN ETB3INAP)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 H323QSIGA                  N CDN  E164  L  8104070 NIL_NSF   BC SPEECH


TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

```
Scenario:
---------

Pty A -> DMS (DPNSS) -> Westell-> CS2K(QSIG H323) ->SIPT -> Pty B

traver tr h323qsiga 8124427 b

TABLE TRKGRP
H323QSIGA PRA 0 NPDGP NCRT MIDL N (QSIG 4) $ $
TABLE LTCALLS
QSIG 4 PUB XLALEC 3 208_NPRT_1 NLCA_NILLA_2 $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE LINEATTR
3 IBN NONE NT 0 0 NILSFC 0 PX E3APX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
208_NPRT_1 NSCR 208 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_2 NLCA NIL NILLATA $
TABLE PXHEAD
E3APX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8124427
TABLE PXCODE
E3APX 812 812 RTE ( PF 3) ( MM 2 20) ( DEST 456)$
TABLE: PXRTE
KEY:    E3APX  456
 . T IBNRT3 20
 .  . TABLE IBNRT3
 .  .   20 S N N N N SIPTVPNSHARED
 .  . EXIT TABLE IBNRT3
EXIT TABLE PXRTE
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN ETB3INAP)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES


This route is a DPT
1 SIPTVPNSHARED         4427               ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

```
Pty A -> DMS (DPNSS) -> Westell-> CS2K(QSIG H323) ->SIPT -> Pty B

traver tr SIPTVPNSHARED  4427 b
TABLE TRKGRP
SIPTVPNSHARED IBNT2 0 NPDGP NCRT VPNSHARED 0 ASEQ 90 N ANSDISC 0 Y N N N N N N 0
    0 N 0 0 0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
VPNSHARED 90 0 0 SIPTRK ( XLAS SIPTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
VPNSHARED NXLA VPNXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME SIPTXLA
TUPLE NOT FOUND
Default is to go to next XLA name.
CUST PRELIM XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME VPNXLA
TUPLE NOT FOUND
Default from table XLANAME:
VPNXLA
    (NET N N 0 N NDGT Y Y DOD N 10 101_NPRT_1 NLCA_NILLA_0 NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
10 IBN NONE NT 0 0 NILSFC 0 PX VOIPPX NIL 00 101_NPRT_1 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
101_NPRT_1 NSCR 101 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
VOIPPX DFLT CONT ( XLT OFC OFCLINE)$ DFOP ( CLASS NATL)$ NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              4427
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
OFCLINE SDFLT NODFOP NOCON 9
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              4427
TABLE OFCCODE
OFCLINE 4 4 DNRTE ( MM 4 4) ( CLASS NATL) ( DN 208 812)$
TABLE TOFCNAME
208 812 $
TABLE DNINV
208 812 4427 ILC LG 00 2 00 24
TABLE DNGRPS
208 812 4427 4427
    (ETB3PRIVNET ( ADDRESS DDD 812 NNNN) $)
    (PUBLIC ( ADDRESS DDD 812 NNNN) $)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 LINE                  2088124427         ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 UKREORDER
```

10.12 Appendix C: Westell Gateway Configuration

The number routing between Gateway and Gatekeeper is not been deployed. This functionality as specified by the Gateway and uploaded to gatekeeper, would enable the gatekeeper to route the incoming calls based on the prefix (for example) to the Gateway. Instead, the CS2K translation enables the function of call routing required to each Gateway (for example as governed by the trunk group).

10.13 Appendix D: SN06.2: Supported DPNSS/Centrex Features over Westell.

The following tables represent the set of DPNSS and Centrex services tested as part of the SN06.2 ICAF activity: A00004897

The list of DPNSS services is exhaustive.

All end-node functionality (calling and called) has been tested by going over an ANSI SIPT DFT looparound.

Table 1 DPNSS Services

DPNSS Service	Nodal[a] Transit	Network Transit[b]	End Node Calling/Called	Comment
CLI Display	Y	Y	Y	
Busy Information	Y	Y	Y	
CBWF	Y	Y	Y	
Executive intrusion	Y	Y	Y	The feature is been blocked and not supported for lines where the intruded party is on the CS2K.
Divert on No Reply	Y	Y	Y	Both with/without drop-back diversion
Divert on Busy	Y	Y	Y	Both with/without drop back diversion
Divert-Immediate	Y	Y	Y	Both with/without drop-back diversion
HOLD	Y	Y	Y	
Call Offer	Y	Y	Y	

Table 1 DPNSS Services

Call Waiting	Y	Y	Y	The service has been tested with respect to Centrex but the DPNSS specific signalling has not been verified.
ROP	Y	Y	Y	With exception of ROP Billing
MWI[c]	Y	Y	Y	Not been tested with actual voice mail box
				Services that can be expected to be "broadly" supported in CS2K but have not been explicitly tested/verified in CS2K as part of this feature.
Three Party Call	Y	Y	Y	The functionally equivalent Centrex 3WC has been verified. With the same limitations in terms of the required DPNSS specific signalling as in TDM.
Non-Specified Information	Y	Y	Y	
Service-Independent strings	Y	Y	Y	
Redirection	Y	Y	Y	
Series Call	Y	Y	Y	
Night Service	Y	Y	Y	
Centralised Operator	Y	Y	Y	
				Services that can be expected to be supported in TRANSIT but have not ben explicitly tested / verified by this feature.
Extension Status	Y	Y	N	
Controlled Diversion	Y	Y	N	
Three Party takeover	Y	Y	N	
Remote Alarm Reporting	Y	Y	N	
Add-on Conference	Y	Y	N	
Time Synchronization	Y	Y	N	
Call Back When Next Used	Y	Y	N	
Do not Disturb	Y	Y	N	

Table 1 DPNSS Services

Remote Registration of Diversion	Y	Y	N	
Remote Registration of Do not Disturb	Y	Y	N	
Priority Breakdown	Y	Y	N	
Call Back Messaging	Y	Y	N	
Loop Avoidance	Y	Y	N	
Forced Release	Y	Y	N	
Text Message	Y	Y	N	
Charge Reporting	Y	Y	N	
Network Address Extension	Y	Y	N	
Call Park	Y	Y	N	
Call Distribution	Y	Y	N	
Route Capacity Control	Y	Y	N	
Wait on Busy	Y	Y	N	
Call Pick-up	Y	Y	N	
Travelling Class of Service	Y	Y	N	
Number Presentation Restriction	Y	Y	N	

a. Nodal Transit is referred as transit configuration where CS2K acts as ‘pure transit’ with Westell gateway(s) serving both Ingress and Egress gateways.
b. Network transit is referred as supporting DPNSS signalling transparently (DFT) across the network via IBN7 DFT (or SIP-T) proprietary signalling.
c. Nortel’s Proprietary

The following list of centrex services is not exhaustive, but represents the set of services that have been tested and verified.

Table 2 Centrex Services

Centrex Service	Nodal Transit	Network Transit	End Node Calling/Called	Comment
Meet Me Conference (Flash only)	Y	Y	Y	

Station Controlled Conference	Y	Y	Y	
Permanent hold	Y	Y	Y	
Three Way Call	Y	Y	Y	
Call waiting (Direct Answer)	Y	Y	Y	
Make set Busy	Y	Y	Y	
Malicious call hold	Y	Y	Y	
Blind Call Transfer	Y	Y	Y	
Call Transfer	Y	Y	Y	
Call Park	Y	Y	Y	
Call Park Retrieve	Y	Y	Y	
Call Pick-up	Y	Y	Y	
Call Forward Don't Answer	Y	Y	Y	The forwarding is done over UKISUP
Call Forward Immediate	Y	Y	Y	The forwarding is done over UKISUP
Call Forward Busy	Y	Y	Y	The forwarding is done over UKISUP
Business set Camp On				**These services have not been tested/verified on the CS2K**
Malicious Call Hold with Call Forward				
MADN Hold - Activate				
MADN Hold - Cancel				
Preset Conference (CS2K as nodal transit)				
Call Waiting (Flash Feature Code Answer)				
Call Forward Universal chaining (with no DPNSS diversion)				
Make Set Busy Intra-Group				

11: Functional Description (FN): A00002053

11.1 Feature name

A00002053 “AMA Records for Metered Features”

11.2 Description

The purpose of this activity is to provide detailed information for feature subscriber’s metered functions by generating an AMA record and an optional AMA log.

This feature developed in ISN07 (MMP20) release is an enhancement of the MMP15 activity AT.59022215 ‘Log For Cept Subscriber Functions’ which generates MTR156 log when the feature metering is done successfully due to usage of the feature actions such as assign, usage, deassign, activation, deactivation or interrogation etc.. In this feature, generation of the MTR156 log is made dependent on the SOC option RBIL0014. (For detailed information about this option, please refer to the activity A59013592). When the RBIL0014 is ON, the MTR156 log is not generated and the same information is supplied by a new AMA record (FTR) and its AMA log (AMAB156).

The new FTR record enables to keep the feature usage information by using DIRP (Device Independent Recording Package) and to use them in the downstream billing process. Thus, it allows telco personnel to give detailed information about feature meter count in the customer’s detailed bill.

The AMAB156 log is optionally generated depending on the existing AMA parameter LOGAMA in table AMAOPTS. If this parameter is set to ON, then this log is printed whenever the FTR record is generated.

The generation of the FTR record for the metered actions of ICR feature option depends on the new office parameter FTR_RECORD_FOR_ICR_OPT in table OFCVAR. This parameter is created in this feature to make the generation of FTR record optional when the subscriber is charged for the ICR operations assignment / deassignment / usage.

This feature applies to meterable IBN lines only.

11.2.1 Background

11.2.1.1 Existing MTR156 log

When feature metering is done successfully due to usage of the feature actions, then the existing MTR156 log is generated in the log system with the following information:

- Calling number (10 digits)
- Date (6 digits)
- Time (6 digits)
- Feature code(2 digits)
- Action type (2 digits)
- Feature Metering Count (2 digits)

Calling Number represents the IBN line agent which is metered for feature actions.

Feature Code is datafilled in table MTRFEAT by Telco Personnel and each meterable feature is represented by a feature code.

Action Code is used for the feature activation types which are Assign, Deassign, Usage, Interrog, Admact, Admdeact, Admproc, Subact, Subdeact, Subproc and datafilled in the table ISERVOPT.

For more detailed information, please refer to FN and DS documents of the activity A59022215 in the FMDOC library.

An example for the MTR156 log can be seen in Figure 1.

Figure 1 MTR156 Log Example

```
MTR156 MAR12 10:42:36 6704 INFO LOG
CALLING NUMBER: 1027835489   FEATURE CODE: 21
ACTION: 45                   COUNT: 32
TIME: 10:42:36               DATE: 03/03/12
```

In this activity, MTR156 log generation is made dependent on the SOC option RBIL0014. If this option is set to ON, instead of MTR156 , FTR record and its optional AMAB156 log are generated with the same information as MTR156.

11.2.1.2 Existing AMA record components used in this feature

An AMA record consists of a base Structure Code and optional Module Codes containing specific information relevant to the call. (In this feature, an existing structure code SCI_00514 with call code CCI_006 and the existing module code MCI_612 with context_id 80040 are used to generate the new record.)

Structure code SCI_00514 with call code CCI_006 has already been present in DMS MMP software with the following fields:

Structure code 00514 fields information	Field number
Record descriptor word	000
Hexadecimal identifier	00
Structure code	0
Call type codes	1
Sensor type	2
Sensor identification	3
Recording office type	4
Recording office identification	5
Date	6
Timing indicator	7
Study indicator	8
Called party off-hook	9
Service observed, traffic sampled	10
Operator action	11
Service feature	12
Significant digits in next field	55
Originating open digits 1	500
Originating open digits 2	501
Originating charge information	504
Domestic/international indicator	505
Significant digits in next field	55
Ext terminating open digits 1	126
Ext terminating open digits 2	126
Connect time	18
Elapsed time	19
Completion indicator	280
Module code	88

For detailed information about the SCI_00514 fields, please refer to the NTP documents 297-1001-830 and 297-9051-800. For the new FTR record, only the following fields of SCI_00514 are taken into consideration:

- **Hex ID:** Hex ID field indicates whether the record is successfully populated. “AA” indicates complete record while “AB” indicates resource failure.
- **Structure Code:** In EBAF environment more than one structure codes exist which means different base fields for AMA recording. This field is filled by 40514 for this structure code. The ‘4’ digit in the field indicates that module codes are attached to the base structure code.
- **Call Type Code:** This field is used to differentiate call types. The default AMA record contains the value 006.
- **Date:** Please refer to Table 1 “Date field explanation” below for field mapping.

Table 1 Date field explanation

BCD Char	Meaning
1	Last Digit of Year
2-3	Month
4-5	Day
8	Sign (hex C)

- **Originating Open Digits 1:** This field contains the first 11 digits of the calling number. If there are less than 11 digits, the number is right-justified and padded with 0s.
- **Connect Time:** Please refer to Table 2 “Connect time field explanation.” below for field mapping.

Table 2 Connect Time field explanation

BCD Char	Meaning
1-2	Hours
3-4	Minutes
5-6	Seconds
7	Tenths of Seconds
8	Sign (hex C)

Currently, the structure code SCI_00514 is used with the module code MCI_612 (with context_id 80040) for the ICAMA, IAA and ICR records when SOC option RBIL0014 is ON. (Please refer to the activity A59013592 for the ICAMA and IAA records, and the activity A59021950 for ICR record.) By this activity, the new record type FTR is added to these records for the metered feature actions.

MCI_612 has already been present in MMP software as a Generic Module Code and contains two strings of 15 BCD positions each. Field description of this module code is given in the Table 3.

Table 3 MCI_612 field description

Information	Number of BCD Chars
Module code 612	4
Generic Context Identifier	8
Generic Digit String 1	16
Generic Digit String 2	16

When the SOC option RBIL0014 is ON, the context identifier 80040 is used with the fields shown in the Table 4 and 5.

Table 4 Generic Digits String 1 explanations

BCD Char	Meaning
1-2	Record Code 00 ICAMA / 01 IAA / 02 ICR
3-4	Call Class
5-6	Call Info
7	Unused
8-15	Pulse Count
16	Sign (hex C)

Table 5 Generic Digits String 2 explanations

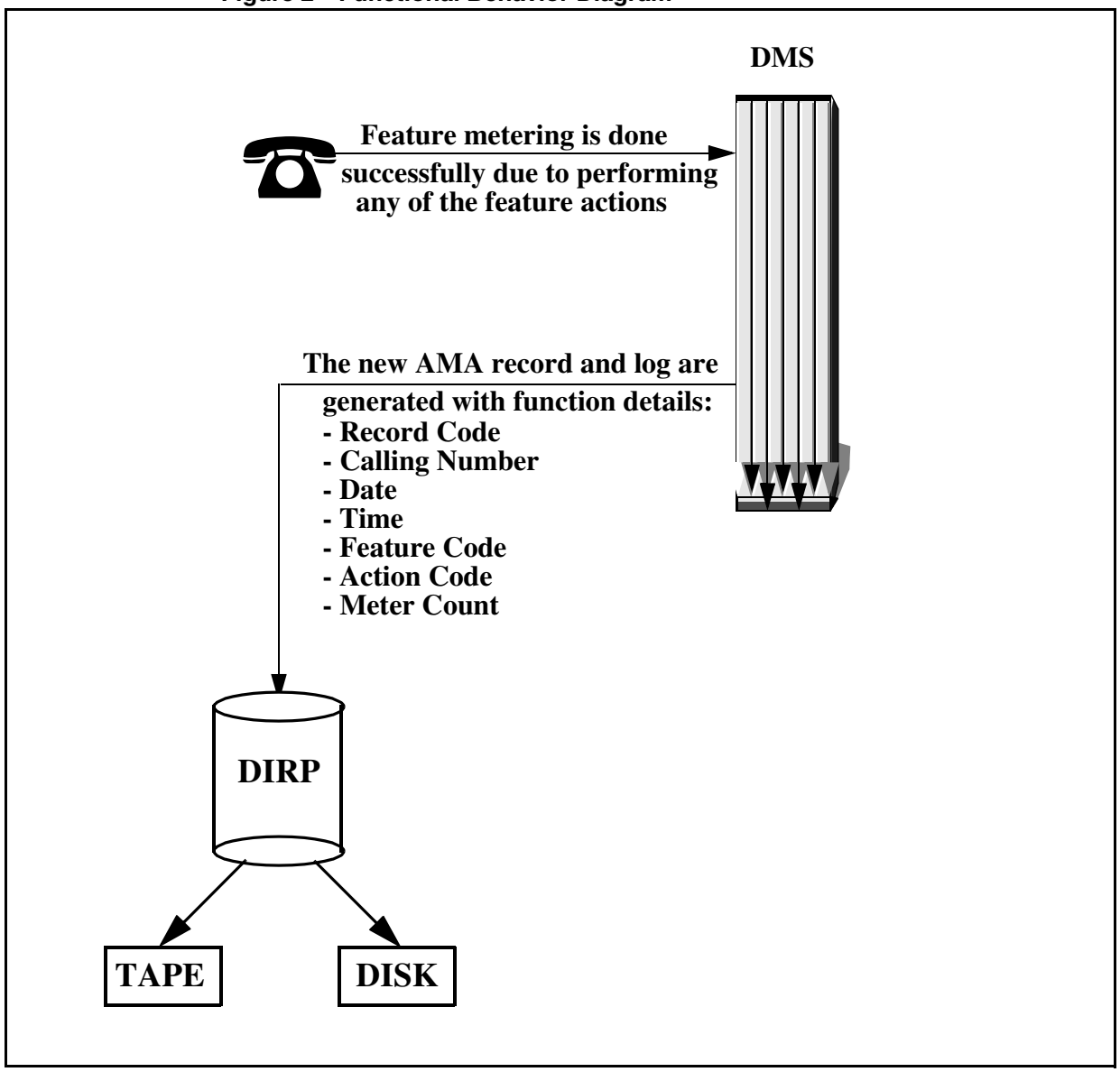
BCD Char	Meaning
1-6	Start Date
7-13	End Time
14	Unused
16	Sign (hex C)

This context_id was created by the activity A59013592 ‘AMA Billing Enhancements for Turkey’. For detailed information, please refer to the documents of this activity in the FMDOC library.

11.2.2 The new AMA record, FTR

The new FTR record is generated in the cases that the MTR156 log is generated (i.e, whenever a feature action is metered) as in the Figure 2, and contains the same information as MTR156 log.

Figure 2 Functional Behavior Diagram



This record consists of the structure code SCI_00514 with call code CCI_006 and module code MCI_612 with context identifier 80040. Since this record generated when the SOC option RBIL0014 is ON, it does not affect the other markets.

In the FTR record, Calling number, Date and Time information for metered feature actions are put in the SCI_00514 fields Originating Open Digits 1, Date and Connect Time respectively, as shown in below:

Calling Number -> ORIGINATING OPEN DIGITS 1

Date -> DATE

Time -> CONNECT TIME

ORIGINATING OPEN DIGITS 1 field in SCI_00514 contains 11 digits. But the Calling Number data of the IBN agent metered for feature actions has 10 digits. So, this data is put in this field as right-justified and the first digit filled by 0.

DATE field of SCI_00514 is filled by the Date data of the metered feature action in the following format:

Table 6 Date field explanation in SCI_00514

BCD Char	Meaning
1	Last Digit of Year
2-3	Month
4-5	Day
8	Sign (hex C)

CONNECT TIME field of SCI_00514 is used to place the Time at which the feature action is metered, as in below:

Table 7 Connect Time field explanation in SCI_00514

BCD Char	Meaning
1-2	Hours
3-4	Minutes
5-6	Seconds
7	Tenths of Seconds
8	Sign (hex C)

Note: Date and Time information are also displayed in the Generic Digits String 2 fields of the appended module code MCI_612 (80040). Please refer to Table 9.

In this feature, EXT TERM OPEN DIGITS 1 field of the SCI_00514 is filled by zeros for the Called DN.

Then the remaining information which are Record Code, Feature Code, Action Code and Feature Meter Count, are put in the Generic Digits String 1 fields of

the MCI_612 (80040) as in Table 8. In this table the usage changes are given in the bold format.

Table 8 Generic Digits String 1 usage for new FTR record

BCD Char	Content
1-2	Record Code **is filled as 03 for the new FTR record**.
3-4	Call Class **is not used and filled as 00 in the new FTR record.**
5-6	Call Info **is not used and filled as 00 in the new FTR record.**
7	Unused field (0).
8-15	Pulse Count **is used to hold the following information:**
	8-9 Feature Code
	10-11 Action Code
	12-13 Unused (00)
	14-15 Meter Count
16	Sign (hex C)

The Record Code field contains 2 digits Record Code data which uniquely identifies the type of the record to distinguish it from the other record types generated when SOC option RBIL0014 is ON. It is set to ‘03’ for the new FTR record since the existing record codes are ‘00’ for Turkish CAMA, ‘01’ for IAA and ‘02’ for ICR.

The Call Class (2 digits, from 3 to 4) and Call Info (2 digits, from 5 to 6) fields are not used in the new FTR record. So, these are filled by zero. Also the seventh digit is already unused and 0.

The Pulse Count field has 8 digits from 8 to 15, and for FTR record it is filled by the Feature Code, Action Code and Feature Meter Count information in the following order:

Feature Code (2 digits) -> Pulse Count (the first 2 digits)

Action Code (2 digits) -> Pulse Count (3 and 4th digits)

Space, 00 -> Pulse Count (5 and 6th digits)

Feature Meter Count (2 digits) -> Pulse Count (7 and 8th digits)

In the fields of the Generic Digits String 2 of 80040, the Date and Time values have already existed and they are continued to display in this FTR record with the same format as before (additional to Date and Time information put in the SCI_00514 fields DATE and CONNECT TIME). The explanations for the existing fields of the Generic Digits String 2 are given in Table 9.

Table 9 Existing Generic Digits String 2 fields

BCD Char	Meaning
1-6	Date
7-13	Time
14-15	Unused
16	Sign (hex C)

The example views of this record can be given as in Figure 3 for ‘calldump’ command and Figure 4 for ‘calldump full’ command.

Figure 3 The example view of the FTR Record.

```
> calldump

*HEX ID:AA  STRUCTURE CODE:40514C  CALL CODE:006C  SENSOR TYPE:036C
 SENSOR ID:0000000C  REC OFFICE TYPE:036C  REC OFFICE ID:0000000C
 DATE:30326C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:0C
 SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C
 SIG DIGITS NEXT FIELD:010C  ORIG OPEN DIGITS 1: 01027835406C
 ORIG OPEN DIGITS 2:FFFFFFFFFF  ORIGINATING CHARGE INFO:FFFF
 DOMESTIC/INTL INDICATOR:9C  SIG DIGITS NEXT FIELD:000C
 EXT TERM OPEN DIGITS 1:000000000000000C
 EXT TERM OPEN DIGITS 2:FFFFFFFFFFFFFFFF  CONNECT TIME:0923355C
ELAPSED TIME:000000000C COMPLETION INDICATOR:001C MODULE CODE:612C
 GENERIC CONTEXT ID:8004000C  GENERIC DIGIT STRING ONE:030000021450002C
 GENERIC DIGIT STRING TWO: 030326092335500C MODULE CODE:000C
```

Figure 4 The example view of the FTR Record.

```
> calldump full
*
 HEX ID:                    AA
 STRUCTURE CODE:                40514C
 CALL CODE:                   006C      STATION PAID
 SENSOR TYPE:                  036C      DMS 100F
 SENSOR ID:                  0000000C
 REC OFFICE TYPE:               036C      DMS 100F
 REC OFFICE ID:                0000000C
 DATE:                      30326C    MARCH 26, 2003
 TIMING IND:
    TIMING GUARD FLAG             0        UNUSED
    SHORT CLD PARTY OFF-HOOK IND  0        UNUSED
    LONG DUR/SERV PTY CAPABILITY IND 0       UNUSED
    UNUSED                    0
    UNUSED                    0C
 STUDY IND:
    STUDY TYPE A              0        UNUSED
    STUDY TYPE B              2        NETWORK COMPLETION
    STUDY TYPE C              0        UNUSED
    TEST CALL IND             0        UNUSED
    UNUSED                    0
    ORIG/TERM NANP NUM IND        0        UNUSED
    OPERATOR SERV IND             0C       UNUSED
 CLD PTY OFF-HK:                0C       CLD OFF-HOOK DETECTED
 SERVICE OBSERVED:              0C       NONE
 OPER ACTION:                  0C       ANI, CUSTOMER DIALED CALL
 SERVICE FEATURE:               000C      OTHER
 SIG DIGITS NEXT FIELD:          010C
 ORIG OPEN DIGITS 1:            01027835406C
 ORIG OPEN DIGITS 2:           FFFFFFFFFF
 ORIGINATING CHARGE INFO:        FFFF
 DOMESTIC/INTL INDICATOR:        9C       UNKNOWN
 SIG DIGITS NEXT FIELD:          000C
 EXT TERM OPEN DIGITS 1:         000000000000000C
 EXT TERM OPEN DIGITS 2:         FFFFFFFFFFFFFFFF
 CONNECT TIME:                  0923355C   09:23:35.5
 ELAPSED TIME:                000000000C 000000:00.0
 COMPLETION INDICATOR:           001C      COMPLETED: ANSWERED
 MODULE CODE:                  612C      GENERIC MOD: TWO DGT STR FMT
 GENERIC CONTEXT ID:
    PARSE RULES                80040     ICAMA FIELDS
    SIGNIFICANT DIGITS          00C       NIL
 GENERIC DIGIT STRING ONE:
    ICAMA-IAA DATA                 030000021450002C
 GENERIC DIGIT STRING TWO:      030326092335500C
 MODULE CODE:                  000C      FINAL MODULE
```

In these Figures, Generic Digits String 1 fields are interpreted as in below:

0300000**21**4**5**00**02**C

03: Record Code is FTR (first 2 digits)

00000: Unused space (5 digits after record code)

21: Feature Code (2 digits as 8th and 9th)

45: Action Code (2 digits as 10th and 11th)

00: Two space between Action Code and Meter Count (12th and 13th digits)

02: Meter Count (last 2 digits)

For the metered actions of ICR option (assignment / deassignment / usage), the generation of the FTR record is optional by the newly created office parameter FTR_RECORD_FOR_ICR_OPT in table OFCVAR. When the subscriber having ICR feature option is charged for the ICR operations in MTRFEAT table, the FTR record is generated if the FTR_RECORD_FOR_ICR_OPT is Y, not generated if the FTR_RECORD_FOR_ICR_OPT is N.

When the parameter FTR_RECORD_FOR_ICR_OPT is changed from “N” to “Y”, the following message is displayed;

“WARNING: FTR record generation for ICR feature is activated”

Opposite when FTR_RECORD_FOR_ICR_OPT is changed from “Y” to “N” the following message is displayed;

“WARNING: FTR record generation for ICR feature is deactivated”

11.2.3 The new AMA log, AMAB156

By this activity, the MTR156 log is generated only when the SOC option RBIL0014 is IDLE. If this option is set to ON, an FTR record is generated with an optional AMAB156 log, instead of MTR156. The AMAB156 log contains the same data as FTR record (i.e, MTR 156 data) and it is optionally generated depending on the existing AMA parameter LOGAMA in table AMAOPTS. If the LOGAMA option is ON, AMAB156 log is printed whenever the FTR record is generated.

Record Code is ‘BE’ in AMAB156 in spite of ‘03’ in FTR Record. Because the Record Code values BB, B8, BD are currently used in the AMA logs of the ICR, ICAMA, IAA records.

Please refer to Figure 5 for the example view of AMAB156 log.

Figure 5 AMAB156 LOG Format Example

```
RSNW4E06BK     AMAB156 MAR26 09:23:36 7216 INFO AMA RECORD DATA
          RECORD CODE = BE
          CALLING NUMBER = 1027835406   FEATURE CODE = 21
          ACTION = 45                   COUNT = 02
          TIME = 0923355                DATE = 030326
```

11.2.4 The provisioning for the new FTR record

For the generation of the FTR record and AMAB156 log on MMP load, the following datafills are required:

11.2.4.1 Office Wide Parameters:

1. The below presented datafill is already available in DMS MMP and is not a result of this activity. You can refer to NTP 297-9051-800, DMS 100 MMP AMA Reference Guide, for more information on provisioning of EBAF AMA Recording.

- In table OFCOPT, LAMA_OFFICE parameter is set to ‘Y’.
- In table OFCENG, UNIVERSAL_AMA_BILLING tuple is set to ‘Y’
- In table DIRPSSYS a tuple is required to enable DIRP subsystem to receive AMA records and transfer them onto a recording device.

  Sample entry:

  AMA, Y, 2, 1, AMAPOOL, $, CR, NA, NA, NA, 30, 30, $, N, NA, OPENED, NNNNNNN, 0, NOROTATE, NONE, NONE, N, 64, Y
- In table CRSFMT, the AMA Format is determined.

  Sample Entry:

  AMA, BCFMT, N, NIL_FM, N, N, 0
- In table CRSMAP, the stream associated with the format is defined.

  Sample Entry:

  LAMA AMA
  CAMA AMA

  Note: Other streams have to be associated with other formats instead of AMA. E.g SMDR SMDR.
- In table OFCENG, number of Recording Units to be allocated is determined by use of the following entries. Each entry has a default value

of 100. It is possible to allocate memory for recording units automatically by using table OFCAUT. Please refer to NTP documents 297-9051-855 (Office Parameters Volume 1 of 3 (OFCENG)) and 297-9051-351 (Data schema Reference Manual Volume 8 of 12) for information on provisioning of recording unit pools and auto-provisioning.

The difference between pools are the method of usage and the memory space allocated out of the pool for each recording unit. Different structure codes and module codes require different memory and therefore, they consume memory out of different memory pools.

Pool size default values in table OFCENG are as below:

CRS_PRU_POOL1_SIZE	100
CRS_PRU_POOL2_SIZE	100
CRS_PRU_POOL3_SIZE	100
CRS_SUBRU_POOL1_SIZE	100
CRS_SUBRU_POOL2_SIZE	100
CRS_SUBRU_POOL3_SIZE	100
CRS_SUBRU_POOL4_SIZE	100
CRS_SUBRU_POOL5_SIZE	100

2. To generate the FTR record, the existing SOC option RBIL0014 is set to ON.
3. To generate the AMAB156 log beside the FTR record, the existing LOGAMA parameter in table AMAOPTS is set to ON.
4. To deactivate generation of the FTR record and AMAB156 log, and to activate the MTR156 log generation, the SOC option RBIL0014 is set to IDLE.
5. The new office parameter FTR_RECORD_FOR_ICR_OPT is created in Table OFCVAR by this activity to make optional the FTR record generation for metered actions of the ICR feature. It is set to Y to generate FTR record for the charged ICR operations of subscribers (assign / deassign / usage).

Figure 6 The new OFCVAR parameter

```
> Table OFCVAR

PARMNAME PARMVAL
----------------------------
FTR_RECORD_FOR_ICR_OPT      Y
```

11.2.4.2 Provisioning for metering and record generation

The below presented datafill is already available in DMS MMP and is not a result of this activity. Please refer to the FN and DS documents of the activity A59022215 in the FMDOC library.

1. Only the feature functions of the subscribers having IBN lines and MOG option are metered. MOG option is assigned to the subscriber by SERVORD.
2. The Action Codes are datafilled in the ISERVOPT table. An example for the action codes are shown in Figure 7. In this example, the action codes '03 45 57 04 49 07 98 42 23 46' represent 'Assign DeAssign AdmAct AdmDeact AdmProg SubAct SubDeact SubProg Usage Interrog' respectively.
3. The Feature Codes and Charges for the feature actions are datafilled in the table MTRFEAT as in the example shown in Figure 8. In this example, 54 and 21 are feature codes for ICWT and CLF respectively. The numbers, next to the action codes, are the charge values or meter counts for that action.

   Note: Although the FTR_RECORD_FOR_ICR_OPT is Y in table OFCVAR to generate FTR record for metered actions of ICR feature option, the record is not generated unless a tuple exists for the ICR in table MTRFEAT.

Figure 7 Action Codes in the table ISERVOPT

```
> Table ISERVOPT

SOPTSKEY SOPTSVAR
----------------------------
FTRACT FTRACT 03 45 57 04 49 07 98 42 23 46
```

Figure 8 Feature Codes in the table MTRFEAT

```
TABLE MTRFEAT
KEY FTRCOD OPTIONS
-----------------------------
ICWT MOG_3 54 (ASSIGN 1) (DEASSIGN 2) (ADMACT 3) (ADMDEACT 4) (SUBACT 6)
(SUBDEACT 7) (USAGE 9) (INTERROG 10) $

CLF MOG_2 21 (ASSIGN 1) (DEASSIGN 2) (USAGE 5) $
```

11.2.4.3 Software Optionality Control

There is no new created Software Optionality Control by this feature. The existing SOC option RBIL0014 is used for this record. It was created by the feature AT.59013592 in MMP13 release. In this activity, for the metered feature actions, the FTR record and AMAB156 log are generated instead of the MTR156 log if the SOC option RBIL0014 is set to ON. When the SOC option RBIL0014 is IDLE, MTR156 log is generated as before.

11.3 Hardware Requirements or Dependencies

No new customer hardware requirements or dependencies are introduced in this feature.

11.4 Software Requirements or Dependencies

This feature uses the existing AMA/Billing framework and the existing components of this framework.

11.5 Limitations and restrictions

- This feature applies to IBN lines only.
- This record is generated for only meterable (having MOG option) feature actions.
- In order to generate the FTR record and AMAB156 log,
  - — the all datafills given in the section 2.2.4 have to be done,
  - — feature metering should be performed successfully.
- Feature Meter Count information is displayed by 2 digits in the FTR record and AMAB156 log. The data shown in this field reflects the value datafilled in the CHARGE field of table MTRFEAT and the range for the charge value has been defined as 0 to 255 in this table. Although 3 digits data is datafilled in the charge field of MTRFEAT table, the last 2 digits will be displayed in the FTR record and AMAB156 log, as in MTR156 log.
- The FTR record for metered actions (assign / deassign / usage) of ICR feature option is not generated unless the office parameter FTR_RECORD_FOR_ICR_OPT is set to Y in table OFCVAR.
- The AMAB156 log is not generated unless the parameter LOGAMA is set to ON in table AMAOPTS, although the FTR record is generated.
- The FTR Records are routed to ICR volume.
- The FTR Records are stored in disks/tapes by using Bellcore AMA Format.
- NT AMA Format is not supported on the MMP.

11.6 Interactions

- If the feature metering according to action type is done successfully then this record is generated.
- AMA in MMP is based on Bellcore AMA Format. This feature uses the existing AMA/Billing framework components with no change in their existing structures to realize customer's requirements. So, there is no effect on the existing AMA subsystem in the MMP load.

11.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	Y
Accounting (includes AMA billing)	Y
Performance (includes operational measurements)	N/A

11.8 Glossary

Term	Description
AMA	Automatic Message Accounting
CCI	Call Code Index
DIRP	Device Independent Recording Package
DMS	Digital Multiplex System
FTR	FeaTuRe
IAA	Inter Administration Accounting
ICAMA	International Centralized Automatic Message Accounting

Term	Description
ICR	International Charge Recording
MCI	Module Code Index
MMP	Multi Market Product
SCI	Structure Code Index
SOC	Software Optionality Control
Telco	Telecom Company

11.9 Recommended Reading/References

a. A59022215 - Log For Cept Subscriber Functions

b. A59013592 - AMA Billing Enhancements for Turkey

c. A59021950 - Meter Count Support in Billing Records (International Charge Recording)

d. NTP 297-9051-800 ‘DMS100 MMP AMA Reference Guide’

e. NTP 297-1001-830 ‘Bellcore Format AMA Reference Guide’

12: Functional Description (FN): A00002100

12.1 Feature name

ISUP_R_2000 (Russia ISUP V2+) Operator Call on Busy Subscriber (Toll Break In).

12.2 Description

12.2.1 Notation

The following notations are used throughout whole document:

Party C or called party: The party who is called by the operator when it is in talking state with party A.

Party A: The party who is in the talking state with party C.

Party B or operator: The party who is operator and tries to reach party C when party C is in talking state with party A.

Talking call: The call between party A and party C. This call can be originated by either parties.

Operator call: The call originated by party B (operator) to party C. This call waits called party's acceptance.

Waiting Tone: Call waiting tone

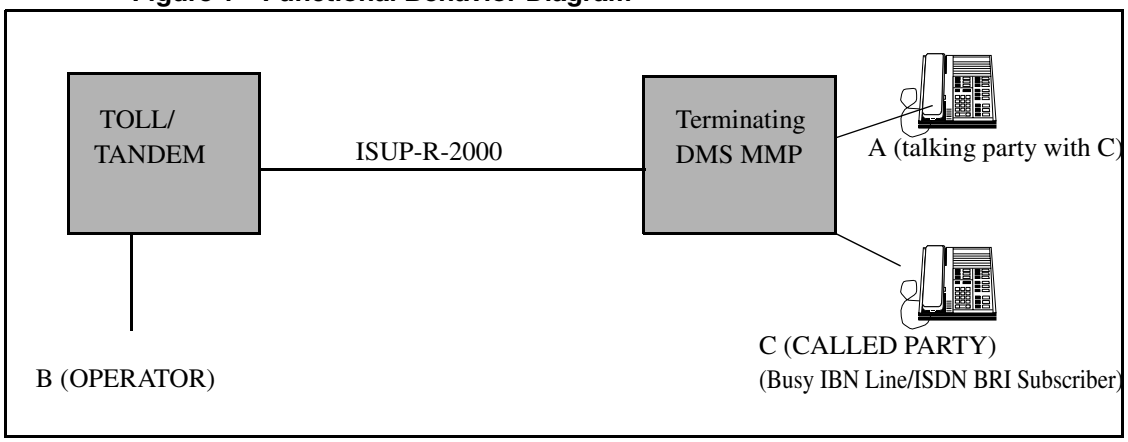
: is used to denote the numerical value instead of hexadecimal value in ISUP messages.
For example #19 denotes 19 as a numerical value, not 25 as hexadecimal value.

12.2.2 Feature Description

ISUP_R_2000 (Russia ISUP V2+) Operator Call on Busy Subscriber (Toll Break In) is implemented in ISN07.

With Russia ISUP V2+ signalling, it is required to establish operator calls to busy subscribers with Call Waiting service for both analogue and ISDN/BRI subscribers. CW is activated automatically and regardless of subscription status of CW, i.e whether the terminating line has CWT option or not.

Figure 1 Functional Behavior Diagram



"Toll Break In" allows a subscriber (party C) in the talking state (connected to a line or trunk, not to a tone or announcement) to be alerted by a call waiting tone when operator call (party B) is attempting to terminate to that line.

CW feature applies call waiting tone to the called party only. The operator side, party B, receives ring back tone during the sending of the call waiting tone to party C.But when TBI occurs, both the called subscriber (party C) and the operator side (party B) will receive the **call waiting tone**.

Operator, Party B, is allowed to wait up to a certain time period (TBI Timer). Within this period, called party C may ignore or reject the operator call and continue with the existing call, hold/release the existing call and answer the operator, party B.

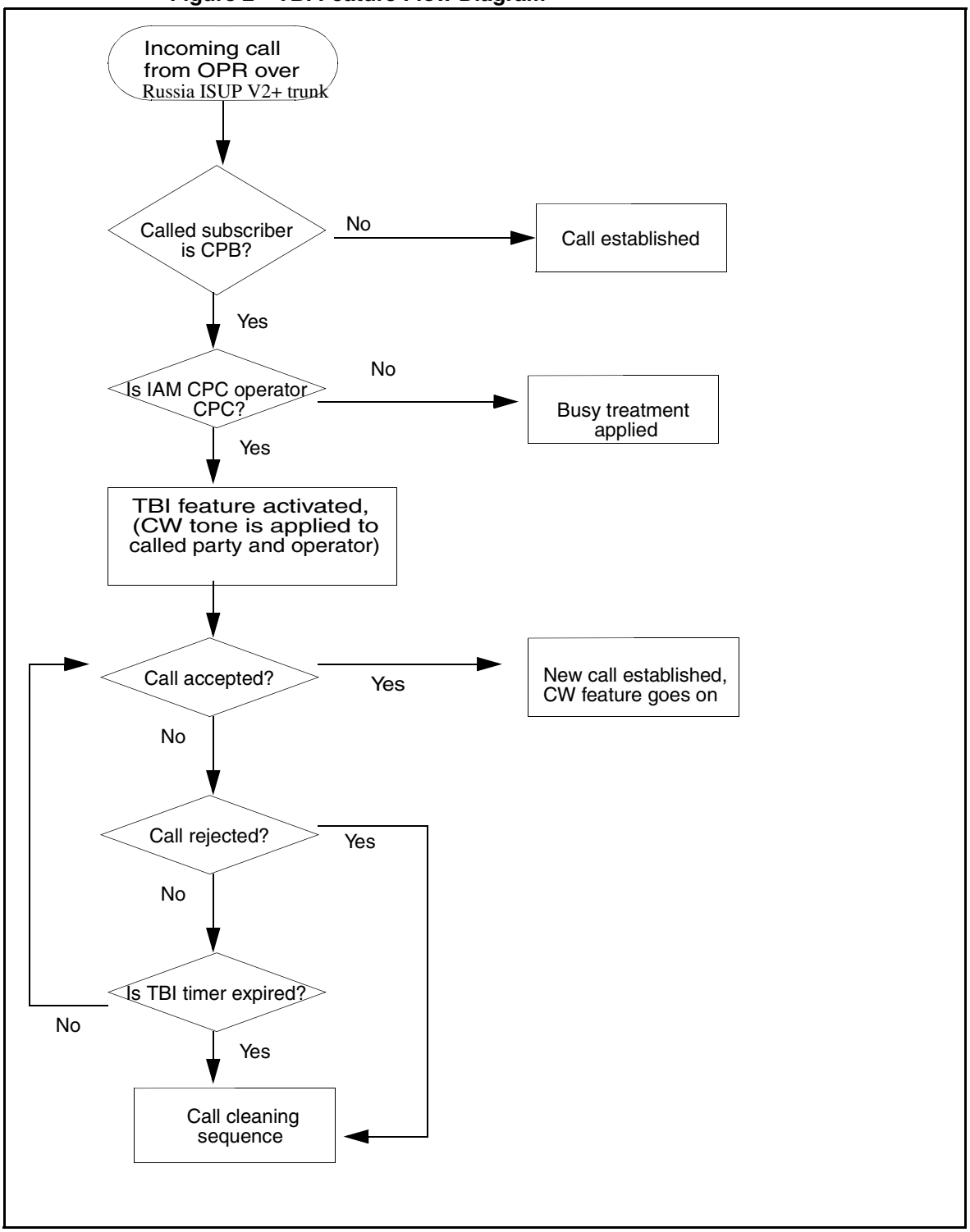
IBN Lines uses Cept CW feature and Cept CW timer is hardcoded as 30 sn. for Turkey. TBI timer will be hardcoded as 20 sn. for operator calls in Russia market. Cept CW Timer will not be changed and it remains 30 sn. for Russia.

ISDN/BRI lines uses ETSI CW feature and there is no specific CW timer for ETSI CW. When TBI occurs, we will use 20 sn. hardcoded TBI Timer for ISDN/BRI lines.

If the timer expires, the operator call is ignored, release message with cause value 'No answer from user / User alerted' is sent to the operator, party B.

Figure 2 illustrates such flow.

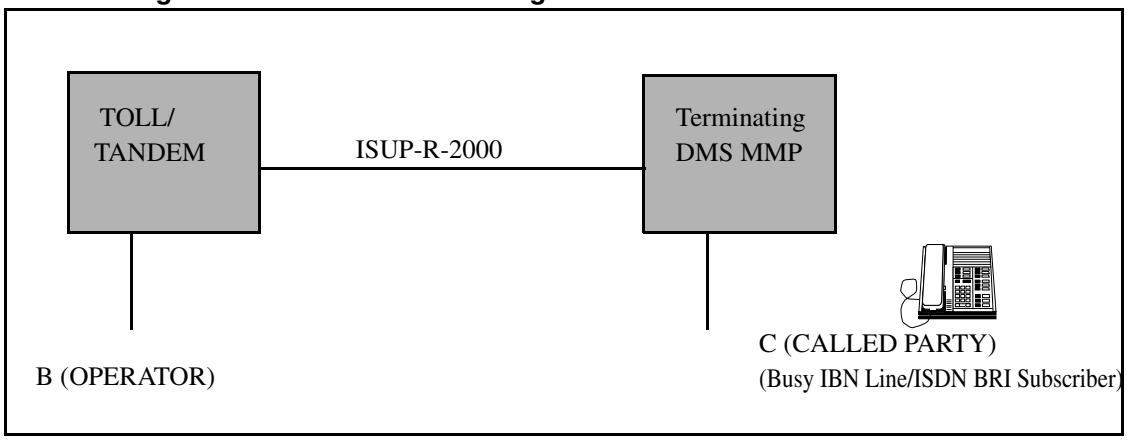
Figure 2 TBI Feature Flow Diagram



* TBI timer is hardcoded as 20 sn. for operator calls.

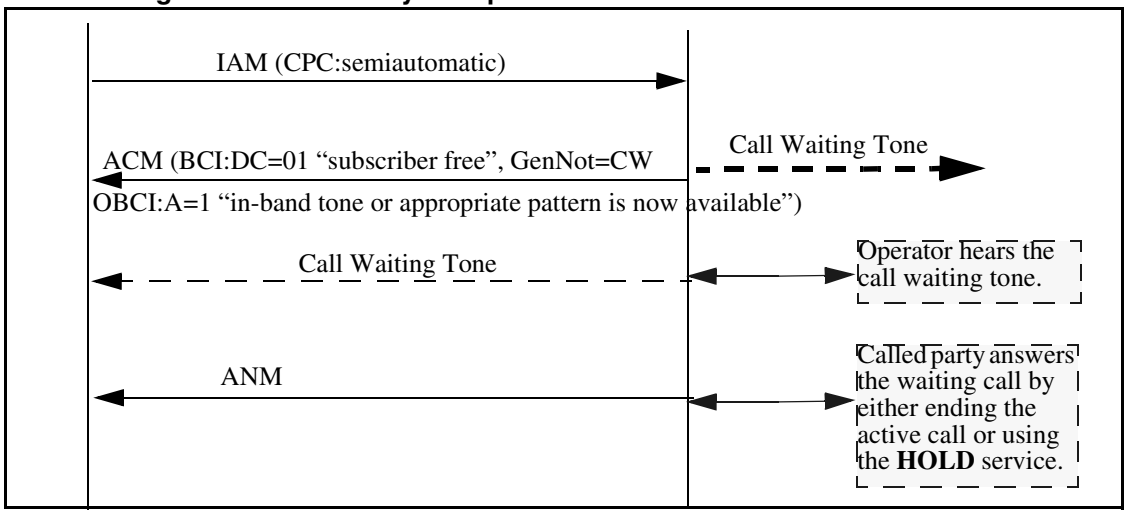
12.2.3 Desired Behavior Scenarios

Figure 3 Desired Behavior Diagram



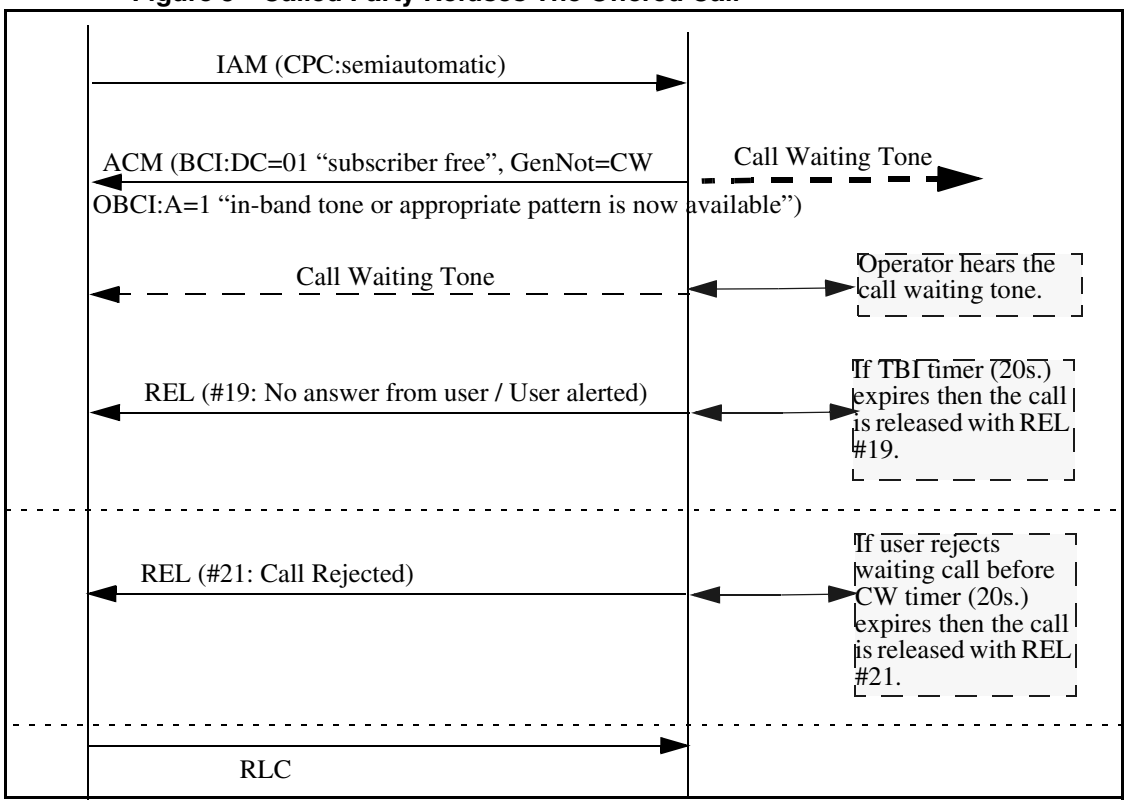
12.2.3.1 Russia ISUP V2+ Operator Calls to Busy IBN Line Subscribers

Figure 4 Called Party Accepts The Offered Call



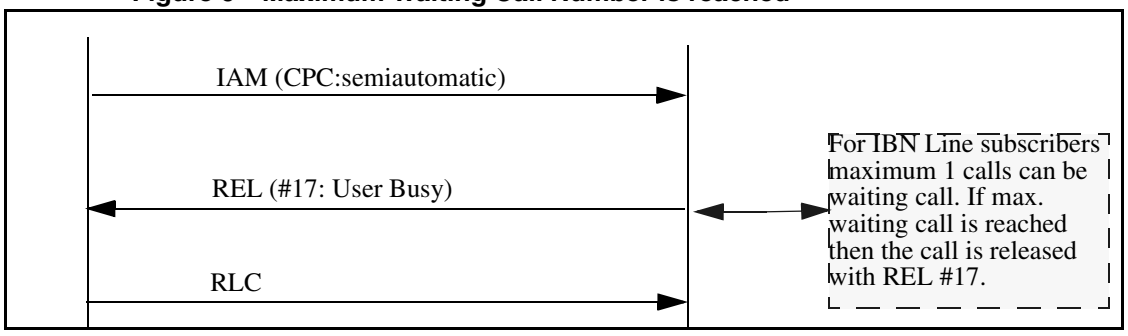
When operator call is answered by called subscriber, basic call procedures are applied as shown in Figure 3.

Figure 5 Called Party Refuses The Offered Call



When an operator call arrives for a busy subscriber (line is CPB), CW is activated automatically. Operator hears the "waiting tone".When called party refuses the offered call above scenario will be seen.

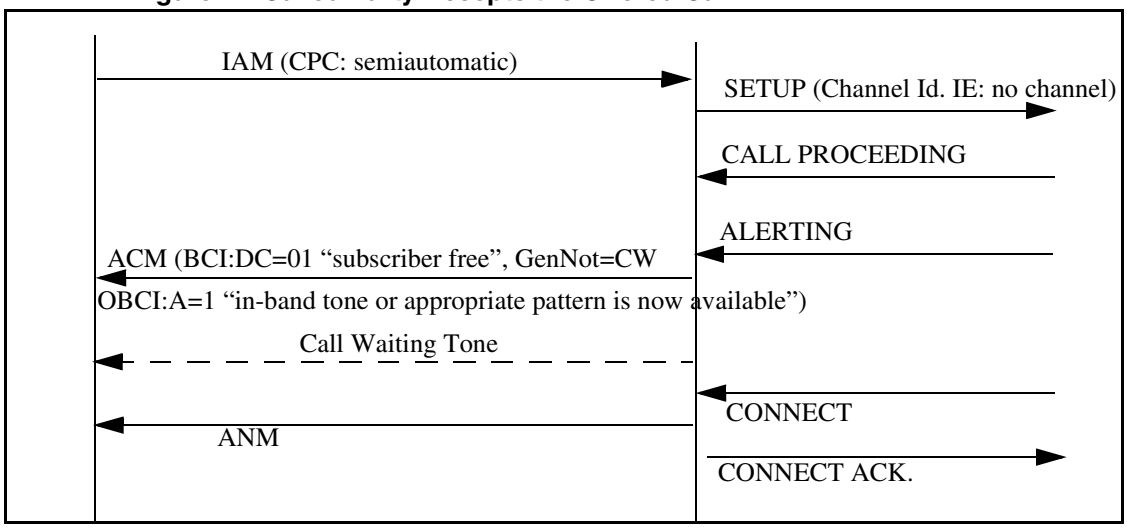
Figure 6 Maximum Waiting Call Number is reached



An IBN Line subscriber can have maximum one active call and one call in CW at the same time.Figure 5 shows the case when these limits are reached.

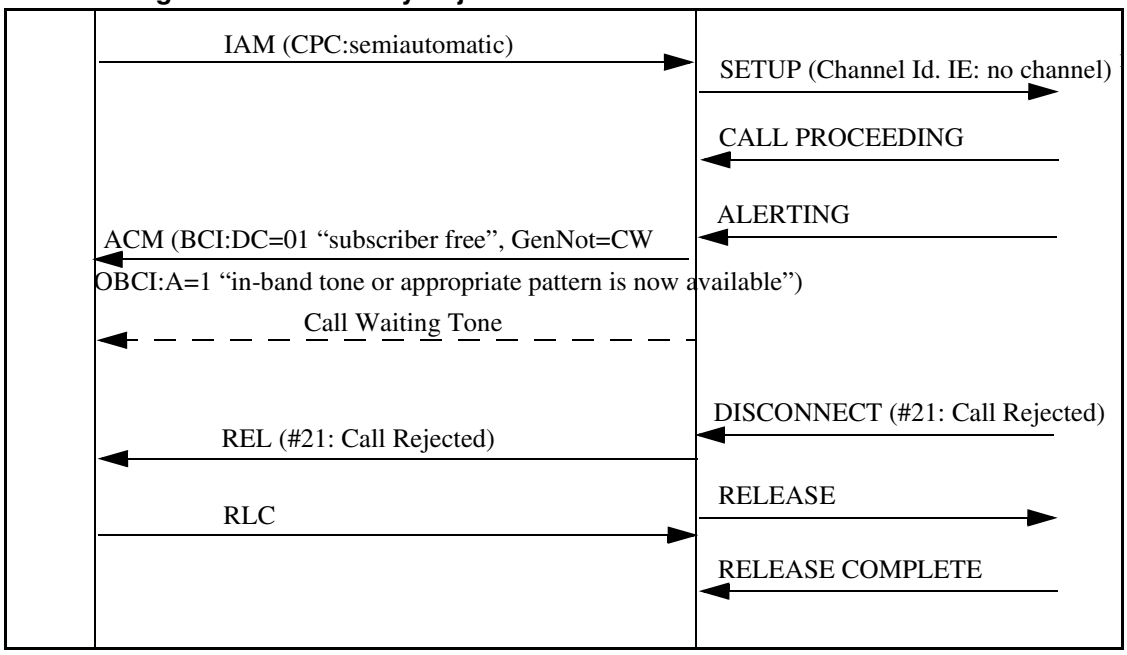
12.2.3.2 Russia ISUP V2+ Operator Calls to Busy ISDN BRI Subscribers

Figure 7 Called Party Accepts the Offered Call



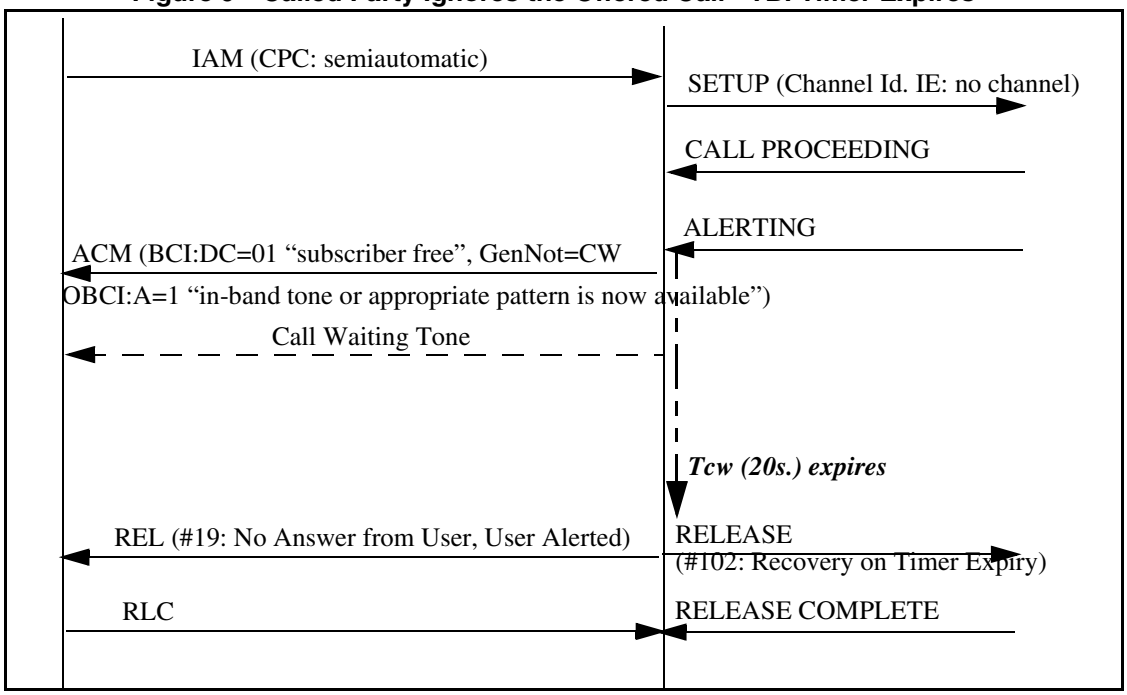
In Figure 7 , an operator call arrives at the terminating office for an ISDN BRI busy subscriber (both B-channels are busy), then the Call Waiting service is invoked and the call is offered to the subscriber with an indication that the channels busy condition exists. When the ALERTING message is received from the called subscriber, an ACM message is sent with the Call Waiting indication to the preceding office. After sending the ACM message, the terminating office applies the “Waiting Tone” to the preceding office. The called party can accept a waiting call either by releasing an existing call according to the basic call procedures or using the Call Hold supplementary service on an existing call.

Figure 8 Called Party Rejects the Offered Call



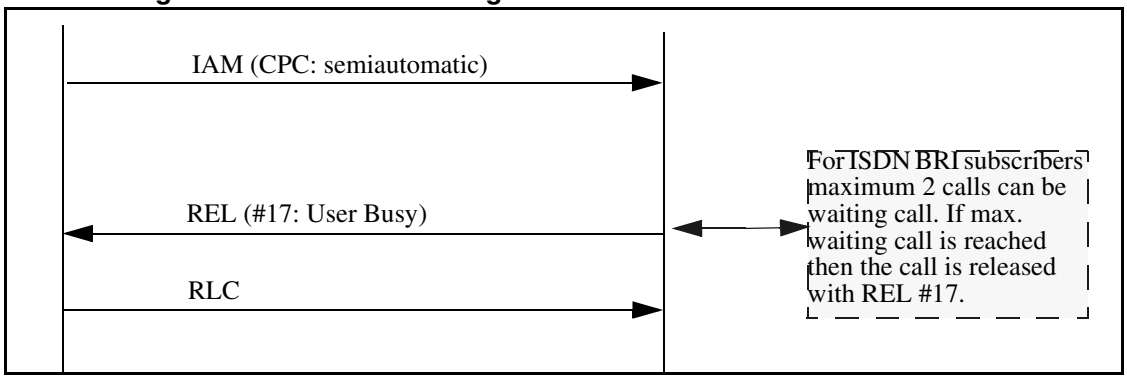
As described in Figure 8 , after the ALERTING message has been sent by the called party, this new waiting call can be rejected before CW timer (20 sec.) expires by sending a DISCONNECT (#21) message.

Figure 9 Called Party Ignores the Offered Call - TBI Timer Expires



In Figure 9 , after the ALERTING message has been sent by the called party, the subscriber decides not to react to this waiting call (neither accepting nor rejecting call). When CW timer (20 sec.) expires, then the network initiates clearing procedure.

Figure 10 Maximum Waiting Call Number is Reached



An ISDN subscriber can have maximum two active calls and two waiting calls at the same time. The called subscriber is considered as busy when the limit on the maximum number of calls which can be waiting has been reached. Any incoming call during this period is cleared by the network.

Figure 11 Called Party sends RELEASE COMPLETE (#17) message

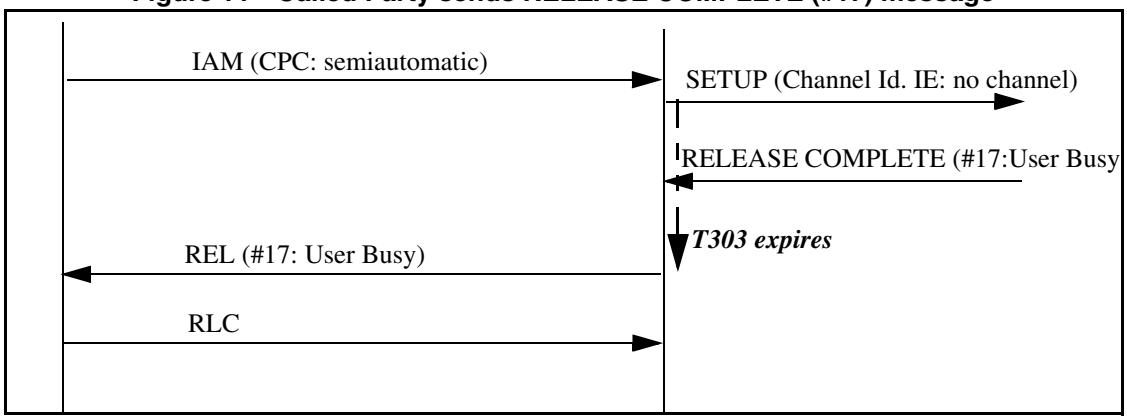


Figure 11 shows the case when the called party sends RELEASE COMPLETE (#17) message in response to SETUP message. If no other response is received from the other users and T303 expires, then the terminating office release the call by sending REL (#17) message to the preceding office.

Figure 12 Operator goes on-hook during call alerting

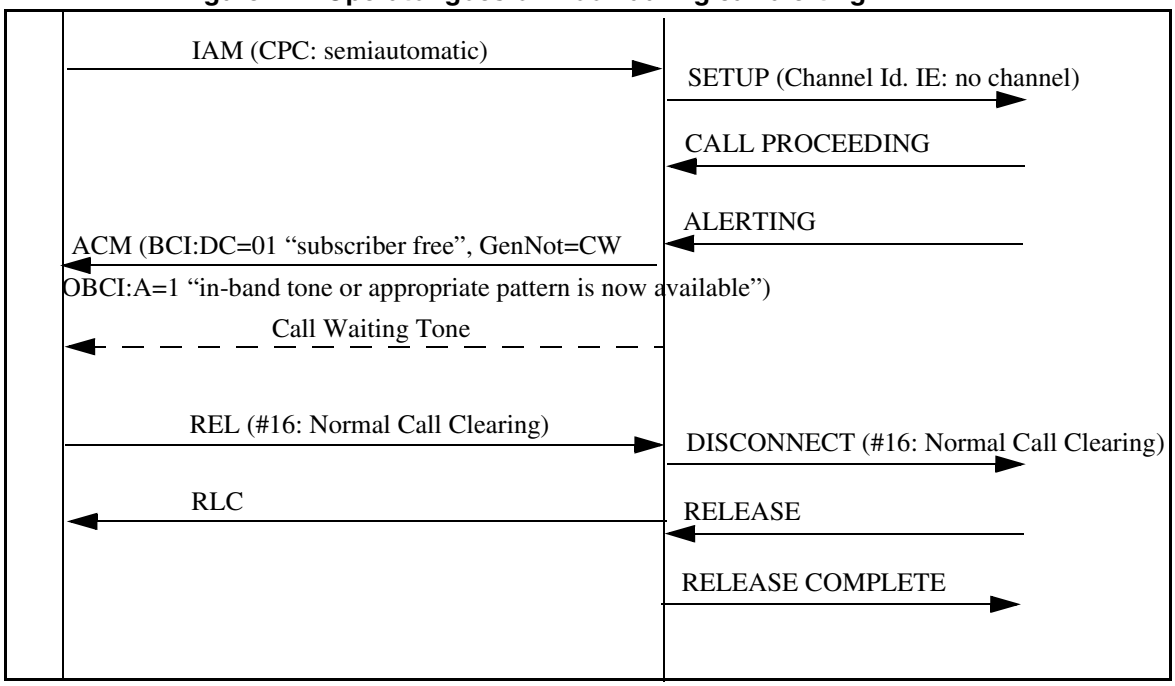


Figure 12 shows the case when the operator goes on-hook during call alerting phase. The basic call clearing procedure applies.

Figure 13 Called Party accepts but no B-channel available to complete the call

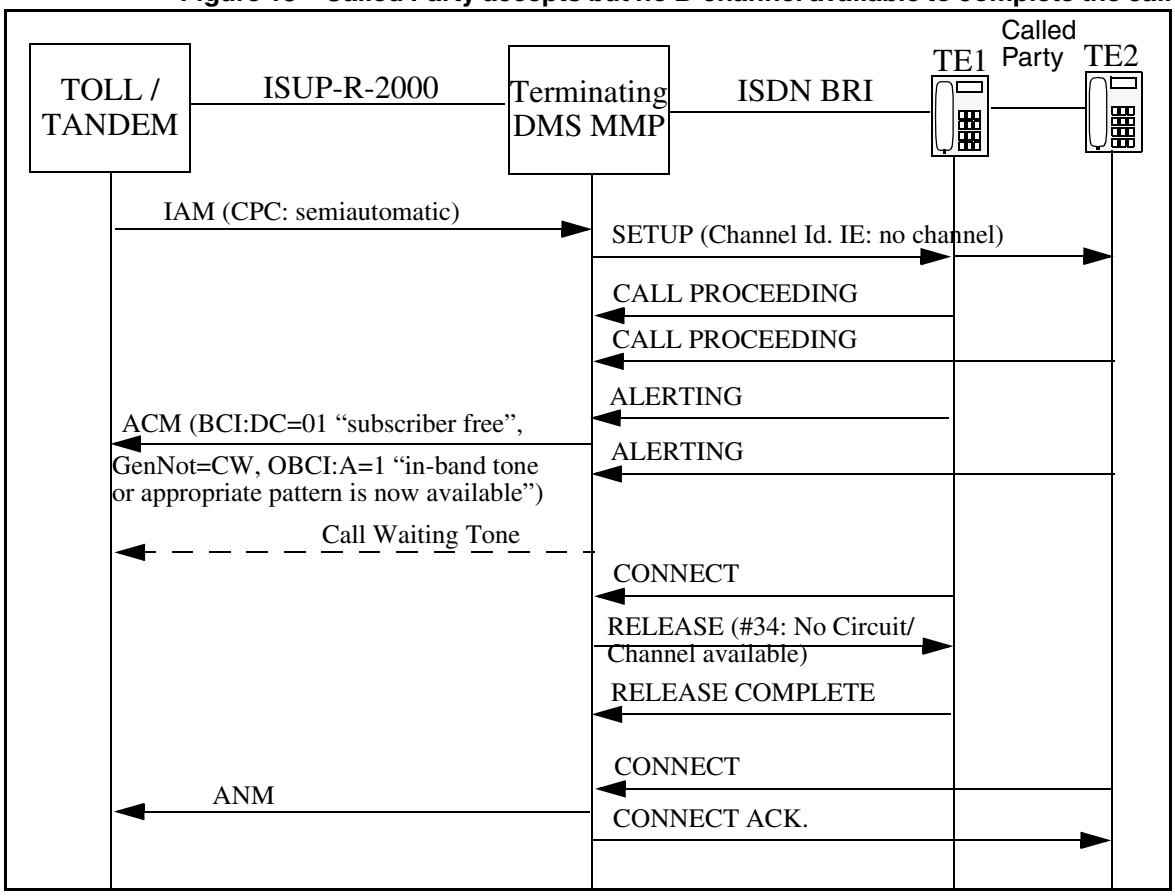


Figure 13 shows the case when a CONNECT message is received from the called party but no B-Channel available to complete the call. On receipt of a CONNECT message from the called party and if no B-channel is available to complete the call (i.e. no channel is free and no channel is reserved for use by this terminal), then the network clears the user and waits for another user B indication for acceptance.

The network shall indicate an error to called party with cause "no B-channels available" (#34). The network shall not clear the call but will wait for another user B indication for acceptance until the calling party clears the call or the CW timer expires.

Figure 14 Called Party accepts but Channel Id. info is not accepted by network

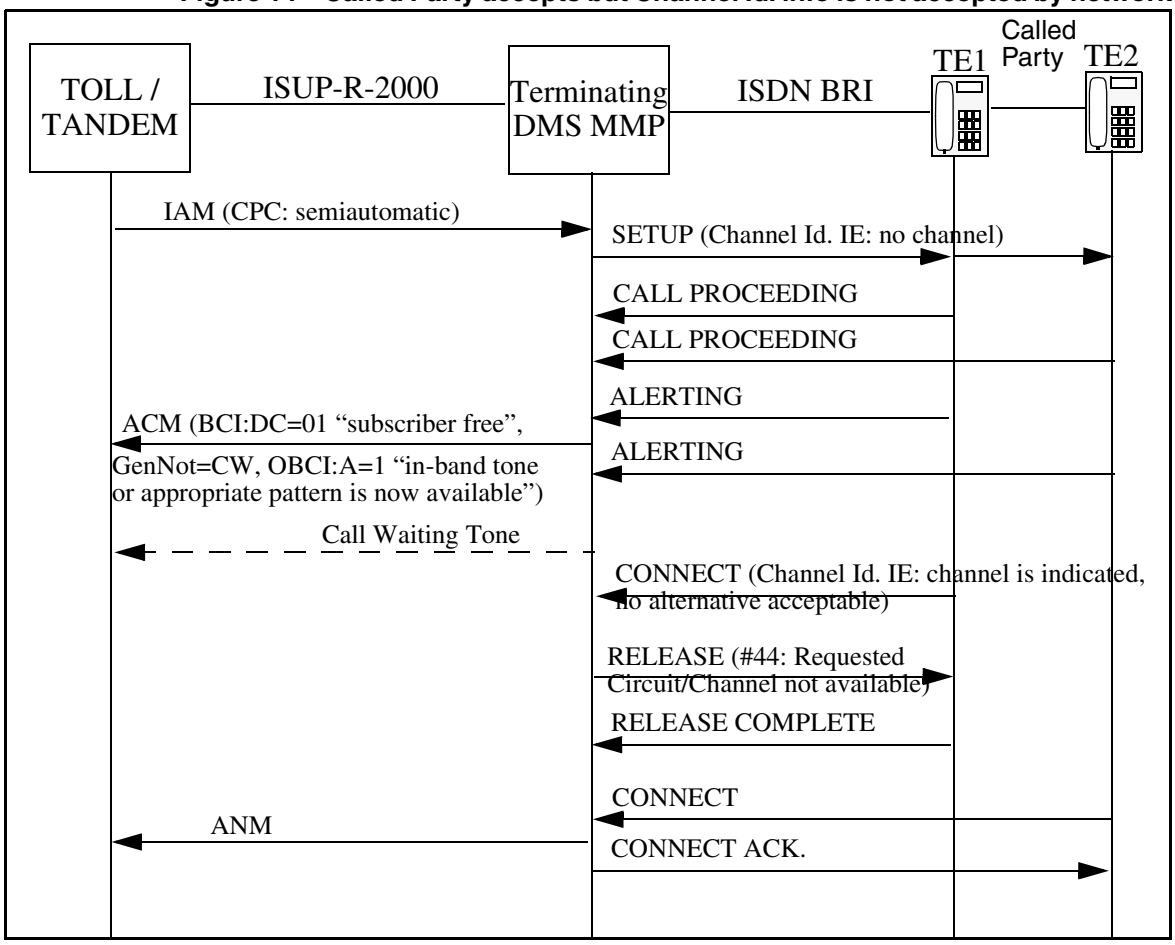


Figure 14 shows the case when the called party accepts the call by sending CONNECT message but the Channel Identification Information specified by the user is not accepted by the network.

If the user returns the Channel Identification Information element in the CONNECT message indicating "channel is indicated, no alternative acceptable" and if the network cannot accept the indicated B-Channel, then the network clears the user and waits for another user B indication for acceptance until the calling party clears the call or the CW timer expires

Figure 15 No message is received in response to SETUP message

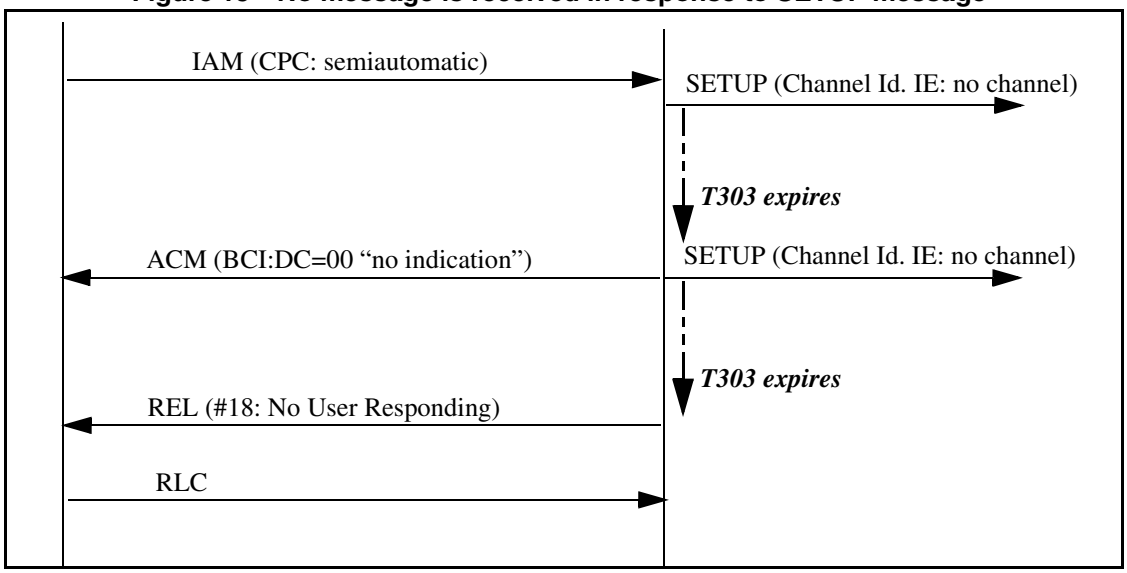


Figure 15 shows the case when no message is received in response to SETUP message.

Figure 16 No message is received after CALL PROCEEDING message

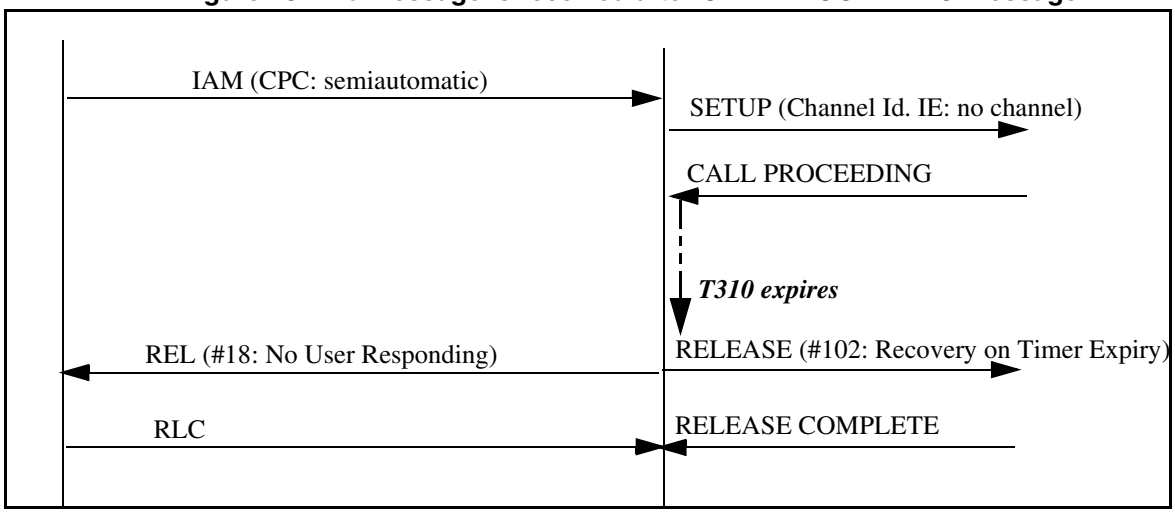


Figure 16 shows the case when no message is received after CALL PROCEEDING message.

12.0.1 Feature Activation

“Toll Break In” does not require any invocation from a subscriber. The feature may be invoked automatically on identification of the required conditions:

- incoming call is operator assisted
  i. Operator calls distinguished from other calls via the calling party parameter placed in IAM message.

ii. CPC (Calling Party Category) values specific to National Network of Russia are listed below:l

Operator Categories	ISUP Coding
Calling party's category unknown at this time **(see note 1)**	0000 0000
National operator	0000 1001
Semiautomatic call, category I OCC I	1111 0001
Semiautomatic call, category II OCC II	1111 0011
Semiautomatic call, category III OCC III	1111 0101
Semiautomatic call, category IV OCC IV	1111 0111

Note 1: This value is processed as semiautomatic call of category IV.

- the called party is busy (line is CPB)
- TBI is offered over Russia ISUP V2+ trunk.

"Toll Break In" activates Call Waiting feature regardless of the subscription status of the CW option.

12.0.1.1 Call Acceptance for IBN Lines

To allow IBN Lines to do some specific actions, R-CODEs are used. R-CODEs stand for flashing and dialing a single digit by controller. For only IBN lines, during the talking mode the subscriber can accept the operator call by dialing the following sequence:

(talking) RR SDT * RCODE

R-codes are data filled through table ISERVOPT as shown below:

Figure 17 R-CODE datafills

```
> table ISERVOPT

SOPTSKEY                                                    SOPTSVAR

RCODE  RCODE (RCODE0  TOGGLE) (RCODE1  DISC_ACT) (RCODE2  XFER) (RCODE3  CON_3WC) (RCODE4 DISC_HOLD) $
```

TOGGLE is used for call acceptance. IBN subscriber can accept operator call by Flash 0 with the above datafill.

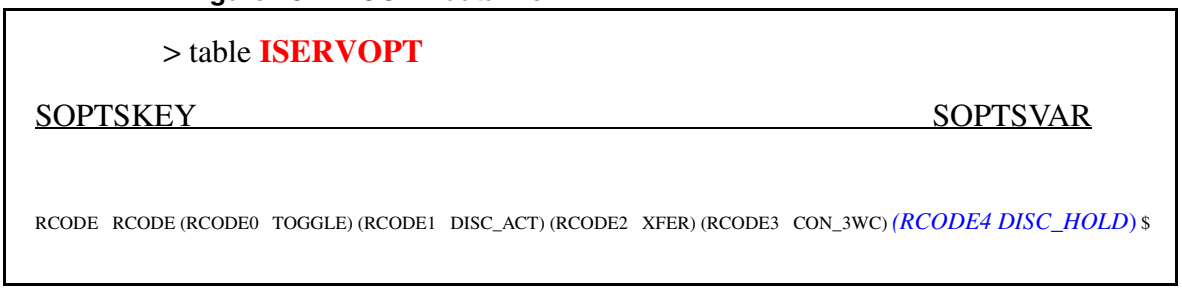
Note: To use R-Codes for IBN Lines, CEPT option must exist on the subscriber and on the customer group that the subscriber belongs to. Russia market uses CEPT by default option.

12.0.1.2 Call Rejection for IBN Lines

For IBN Lines, during the talking mode the subscriber can reject the operator call by dialing the following sequence:

(talking) RR SDT * RCODE

Figure 18 R-CODE datafills



DISC_HOLD is used for call rejection. IBN subscriber can reject operator call by Flash 4 with the above datafill.

12.0.2 Feature Metering and OM Pegs

Feature metering is a system used to charge feature meterable activities to subscribers initiated by either administrator or subscriber itself.

When TBI is active, feature metering for Call Waiting will not be incremented.Also Call waiting OM Pegs are not allowed to increase.

12.0.3 Tones

Following tones are used at various stages of an operator call on busy subscribers:

Call Waiting Tone: provides an indication that a call is being call waited. This tone is provided to the called party and the operator.

To be able to apply the Call Waiting Tone to the operator over Russia ISUP V2+ trunk, we need a CWT trunk defined on MTM device which has 3X68AB/ 3X68AC card on it. Additional datafills are needed as shown below:

Figure 19 Datafill to define a CWT trunk to apply CW Tone

```
>table stn
-------------------------------------------------------------------
SK TMTYPE TMNO TMCKTNO CARDCODE MAXCONN TRAFSNO
-----------------------------------------------
CWT 0 MTM 1 21 3X68AB 3 0
```

Hold Tone: provides an indication that a call is being held. This tone is provided to the held party.

12.1 Hardware Requirements or Dependencies

None

12.2 Software Requirements or Dependencies

None

12.3 Limitations and restrictions

The following limitations and restrictions apply to this feature:

- Only incoming operator calls on Russia ISUP V2+ trunks are supported
- Called party's line state must be CPB.
- TBI is denied if maximum waiting call number is reached for both IBN Lines (max. one active call and one waiting call) and ISDN/BRI lines (max two active calls and two waiting calls).
- TBI is denied to the Category-8 subscribers (Data/Fax Subscribers) for both IBN and ISDN/BRI lines.
- To apply call waiting tone to the operator side, datafill is required as shown in figure 19 on page 52.
- CEPT features are used by Russia market for IBN Lines. CEPT option must exist on the subscriber and on the customer group that the subscriber belongs to for IBN Lines.
- In addition to these, Cept CW limitations and restrictions are also applicable to this feature for IBN Lines.(Please refer to the FN document of activity A59019288 Section 2.4)

Note: CEPT CW restrictions includes **"coin and spm"** line restrictions especially. TBI is restricted to coin and spm lines, like Call Waiting.

- The CW supplementary service is used to support waiting calls on ISDN/BRI lines. The CW supplementary service limitations and restrictions are also applicable to this feature for ISDN/BRI lines. (Please refer to the FN document of activity AR2179HD Section 1.4.1)

12.4 Interactions

TBI feature uses Cept CW feature to provide operator calls on busy subscribers for IBN Lines in Russia Market. So all feature interactions of Cept CW feature are applicable to this feature.(Please refer to the FN document of activity A59019288 Section 2.5)

ISDN/BRI lines uses ETSI CW feature (not Cept CW). ISDN/BRI supplementary services and CW feature interactions will remain unchanged for TBI activity. (Please refer to the Section 4.3.2.9 of the HLD document of Activity AR2179HD)

The following table clarify the interactions between CEPT Call Waiting and other CEPT services. The following legend has been used to denote the interaction between a service A and a service B:

- Compatible-with No interactions (C-N): Services A and B can work together and do not have any interaction with each other.
- Compatible-with Interactions (C-I): Services A and B can work together, but may have some interactions with each other. These interactions may include cases such as service A taking precedence over service B, service A influencing service B in some way.
- Incompatible-not Provisionable (I-P): Services A and B cannot be provisioned together on the same line.
- Incompatible-at Activation time (I-A): Services A and B can be provisioned on the same line, but one should not be invoked while the other is active.
- Not Applicable (N/A): Service A cannot interact with service B.

Figure 20 CEPT Call Waiting interactions with other CEPT Services

Service	Call Waiting Interaction	Description
Automatic Line (AUL)	I-P	AUL and ICWT cannot be provisioned on the same line. So TBI is incompatible with AUL.

Call Completion to Busy Line (CCBS), Network Call Completion to Busy Line (NetCCBS)	C-I	Call Waiting takes precedence over CCBS/ NetCCBS. So TBI takes precedence over CCBS/Net CCBS.
Call Diversion to Operator (CDTO)	C-I	CDTO takes precedence over Call Waiting. With CDTO active, Call Waiting is impossible. So CDTO takes precedence over TBI.
Call Diversion To Announcement (CDTA)	C-I	CDTA takes precedence over Call Waiting. With CDTA active, Call Waiting is impossible. So CDTA takes precedence over TBI.
Call Forward on Busy Programmable (CFB Programmable)	C-I	Call Waiting takes precedence over CFB Programmable. After CWT time-out CFB Programmable is impossible. So TBI takes precedence over CFB Programmable.
Call Forward on Busy Fixed (CFB Fixed)	C-I	Call Waiting takes precedence over CFB fixed. After CWT time-out CFB Fixed is impossible. So TBI takes precedence over CFB fixed.
Call Forward Do not answer programmable (CFD programmable)	C-N	Since the call has not been answered yet, it is already impossible to do Call-Waiting. So it is impossible to do TBI.
Call Forward Do not answer fixed (CFD fixed)	C-N	Since the call has not been answered yet, it is already impossible to do Call-Waiting. So it is impossible to do TBI.
Call Forward Fixed (CFF)	C-I	CFF takes precedence over Call Waiting. With CFF active, Call Waiting is impossible. So CFF takes precedence over TBI.
Call Forward Remote Access (CFRA)	C-I	CFRA takes precedence over Call Waiting. With CFRA active, Call Waiting is impossible. So CFRA takes precedence over TBI.
Call Forward Universal (CFU)	C-I	CFU takes precedence over Call Waiting. With CFU active, Call Waiting is impossible. So CFU takes precedence over TBI.
Denied Origination (DOR)	C-N	
Hunt Group	I-P	Hunt Group and ICWT cannot be provisioned on the same line. So TBI is incompatible with hunt groups

International Call Transfer (ICT)	C-I	The controller may initiate his second call and transfer them if he has a ICT option. If the controller already has a waiting call, ICT is impossible.
Cept Do Not Disturb (CDND)	C-I	CDND takes precedence over Call Waiting. If CDND is active, Call Waiting is impossible, so TBI.
International Line Restriction (ILR)	C-N	
International Three Way Calling (I3WC)	C-I	If a talking call or incoming call is involved with Three Way Calling, then the Call Waiting feature will be disabled during the duration of that call. If the Call Waiting feature is active then the Three Way Calling capability of both non-controlling parties will be disabled if the calls are within the same office. If the non-controlling party is in a different office, the Three Way Calling and Call Waiting capabilities are not affected. In the CWT feature during the enquiry call, the controller may conference the held party, if he has a I3WC option data filled against his line. So if I3WC is in effect on the call, TBI will be denied.
Six Way Calling (I6WC)	C-I	if I6WC is in effect on the call, TBI will be denied.
International Wake-up Call (IWUC)	C-I	When a subscriber goes off-hook on a wake up call (ringing), the subscriber hears disconnect tone or announcement. Call Waiting would not alert the subscriber on a disconnect tone or announcement, the caller will receive busy treatment. Wake-up Call would not alert a subscriber in the talking state even if Call Waiting is available. Wake up Call can be considered to take precedence over Call Waiting. So TBI will be denied if a Wake up Call to an announcement is in progress.
Last Number Redial (LNR)	C-N	
Malicious Call Tracing (MCT)	C-I	MCT and ICWT can not be provisioned on the same line. So TBI is incompatible with MCT on the same line. But if party A calls party B who has MCT, party B can initiate MCT to trace party A even if Call Waiting is active on party A. In that case, party A is held and the waiting party (or held party) gets disconnect tone. When the call is held, Call Waiting cannot active.
Speed Call Short (SCS) / Speed Call Long (SCL)	C-N	

Warm Line (WML)	C-I	If party A (has ICWT and CEPT WML) hears call waiting tone can press Flash and dial ONLY single digit. After party C is accepted by party A, still only single digit can be handled after flash (second flash case). So CEPT feature programming interface can not be used in this stage for CEPT WML.

Figure 21 Other Feature Interactions with TBI

Service	Call Waiting Interaction	Description
Free Number Terminating(AUL)	I-P	FNT disables Call Waiting feature for trunk to line calls. So TBI is incompatible with FNT.
Cancel Call Waiting (CCW)	I-P	CCW activated on the terminating line prevents the operator to break in. So TBI is incompatible with CCW.
Essential Line (ELN)	C-N	
International Call Recording (ICR)	C-I	When a subscriber with ICR option, already involved in a TBI Call, releases the waiting call, then ICR should be produced.
Denied Termination (DTM)	I-P	TBI is incompatible with DTM.
Plug up-place on trouble intercept (PLP)	I-P	TBI is incompatible with PLP.
Suspend Service (SUS)	I-P	TBI is incompatible with SUS.
Flash Ignore (FIG)	I-P	SinceFIG option disables to make flash terminating line can not accept or reject the TBI call.
No Double Connect (NDC)	I-P	ICWT is incompatible with NDC, so TBI.

Applicable customer facing sections

Fault Management

Logs __N/A____

Alarms __N/A____

Configuration

Data Schema __N/A____

User Interface __N/A____

Element Management __N/A____

Security __N/A____

Service Order __N/A____

Office Parameters __N/A____

Accounting (includes AMA billing) __N/A____

Performance (includes operational measurements) __N/A____

12.5 Glossary

Term	Description
ACM	Address Complete Message
ANM	Answer Message
BCI	Backward Call Indicator (ACM)
CW	Call Waiting
CWT	Call Waiting Tone
GenNot	Generic Notification
IAM	Initial Address Message
OBCI	Optional Backward Call Indicator (ACM)
REL	Release Message
RR	Flash
TBI	Toll Break In

12.6 References

a. ISUPR2000 Spec - ISUP-R-2000 Operator Calls to Busy Subscribers

b. Interworking Specification of ISUP_R_2000 - ITU-T Recommendations I.253.1(1990) and Q.733.1(1992)

c. MMP17 ETSI BRI (S/T) Specification - ETSI ISDN BRI signalling

13: Functional Description (FN): A00002101

13.1 Feature name

'ALLOW ITX ONLY SSUTR2', which maps to actid A00002101 in ISN07.

13.2 Description

This activity,'A00002101-Allow ITX only SSUTR2*' in MMP20, provides a new IC/2W trunk option which allows the DMS Tandem Exchange :

- To transmit and report the received ITX messages.
- To block TAX and CHT messages.
- To allow ITX generation for indirect access calls, if NETAOCD datafill exists at DMS Indirect Access Node.

Regarding to SSUTR2 (reference-[a] ,section 3.2 Call Charging Procedures) ; Bacward Call Charging Scenarios has to be one of the three below: A-) No Backward charging message will be received , B-) TAX (possibly CHT) message(s) will be received , C-) One or several ITX message(s) will be received . Any other backward charging scenarios are not supported by this activity .

In order to ;

- block TAX/CHT and not report
- let the ITX(s) pass and report

to the originator side of the call the incoming (IC) FTUP trunk must hold the new option TELETAX_ITX_SIG .

This activity also enhances the DMS-XPM ITX generation mechanism to prevent zero count ITX generation, this individual behavior is submitted under case:030801-33578 .

13.2.1 Background information:

SSUTR2 defines three backward charging procedures using a combination of charging messages (TAX, CHT, ITX, TXA) to indicate the charging requirements to the billing switch. Please refer to Appendix, Section 2.10.3 for message formats.

At EUR010, TELETAXE_NOSIG option in table TRKOPTS has been provided by the activity AU3283-SSUTR2 SUPPORT FOR BACKWARD CHARGING to control sending of backwards charging messages at DMS Indirect Access Node.

For SSUTR2-SSUTR2 and SSUTR2-SPIROU tandem calls from an incoming trunk marked with the TELETAX_NOSIG option; backward charging messages received on the outgoing SSUTR2 trunk will not be tandemed. Instead , CHT and ITX messages acknowledged with a TXA. Besides, ITX generation is not allowed although NETAOCD datafill exists at DMS Indirect Access Node. Please refer to the section 2.2.2.3 and 2.2.2.4 for the behaviour when TELETAXE_NOSIG option is datafilled.

*__Note:__ SSUTR2 is the French national variant of the ITU-T Q.723 specification (TUP), commonly referred to as French Telephony User Part (FTUP). It is used for interconnection of France Telecom and other licensed domestic operators.

13.2.2 Backward Charging Functionality

Table 1 Backward Charging Functionality

OPTION datafilled for IC/2W trk in the TABLE TRKOPTS	No NETAOCD datafilled at DMS Tandem Exchange	NETAOCD datafilled at DMS Tandem Exchange
No option datafilled (i.e.None of the options TELETAXE_NOSIG and TELETAXE_ITX SIG)	*ITX, TAX and CHT messages are tandemed and reported to CM.* ***Please refer to Figures 1 and 2.***	*The ITX, TAX and CHT messages received are not tandemed, but reported to CM.* *ITX generation is allowed regarding existing tariff for NETAOCD datafills.* ***Please refer to Figures 3 and 4.***
TELETAXE	*ITX, TAX and CHT messages are tandemed and reported to CM.* ***Please refer to Figures 1 and 2.***	*The ITX, TAX and CHT messages received are not tandemed, but reported to CM .* *ITX generation is allowed regarding existing tariff for NETAOCD datafills.* ***Please refer to Figures 3 and 4.***
TELETAXE_NOSIG	*The ITX, TAX and CHT messages received are not tandemed, but reported to CM.. ITX and CHT messages are acknowledged by TXA messages.* ***Please refer to Figures 5 and 6.***	*The ITX, TAX and CHT messages received are not tandemed,but reported to CM. ITX and CHT messages are acknowledged by TXA messages.* *Although NETAOCD datafill exists at tandem exchange, ITX generation is not allowed.* ***Please refer to Figures 7 and 8.***

Table 1 Backward Charging Functionality

OPTION datafilled for IC/2W trk in the TABLE TRKOPTS	No NETAOCD datafilled at DMS Tandem Exchange	NETAOCD datafilled at DMS Tandem Exchange
TELETAXE_ITX_SIG	**The ITX messages received at tandem are tandemed and reported to the CM.** **The TAX and CHT messages received at tandem are not tandemed and not reported to CM, but CHT messages are acknowledged by TXA.** **Please refer to Figures 9 and 10.** **Handling of Charge Message(s) in rare-seen scenarios , under provision of TELETAX_ITX_SIG , is defined in figures 13 to 16.**	**The ITX messages received are not tandemed, but reported to CM.** **The TAX and CHT messages received are not tandemed, but reported to CM.** **ITX and CHT messages are acknowledged by TXA messages.** **ITX generation is allowed regarding existing tariff for NETAOCD datafills.** **Please refer to Figures 11 and 12.** **Handling of Charge Message(s) in rare-seen scenarios, under provision of TELETAX_ITX_SIG , is defined in figures 13 to 16.**

Note :The parts in *italic* in the Table 1 above represent the existing behaviour. The part in **bold** in the Table 1 above represents the new funtionality.

13.2.2.1 Any of the options (TELETAXE_NOSIG or TELETAXE_ITX_SIG) is not datafilled when NETAOCD datafill does not exist:**

Figure 1 ITX received by tandem with no NETAOCD datafill

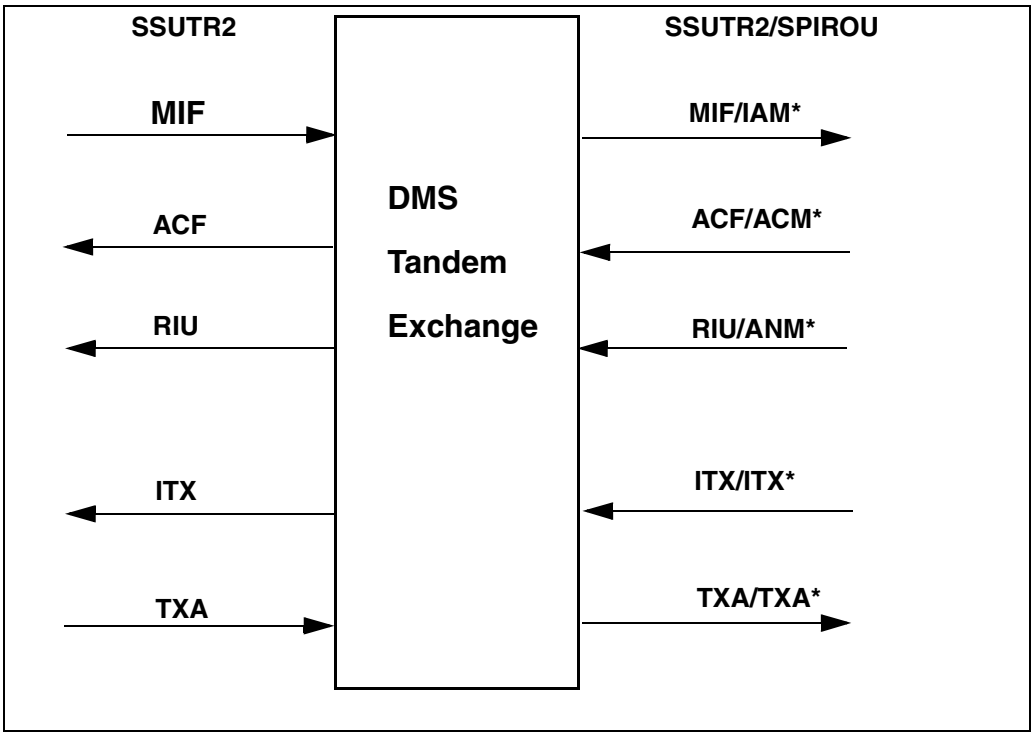
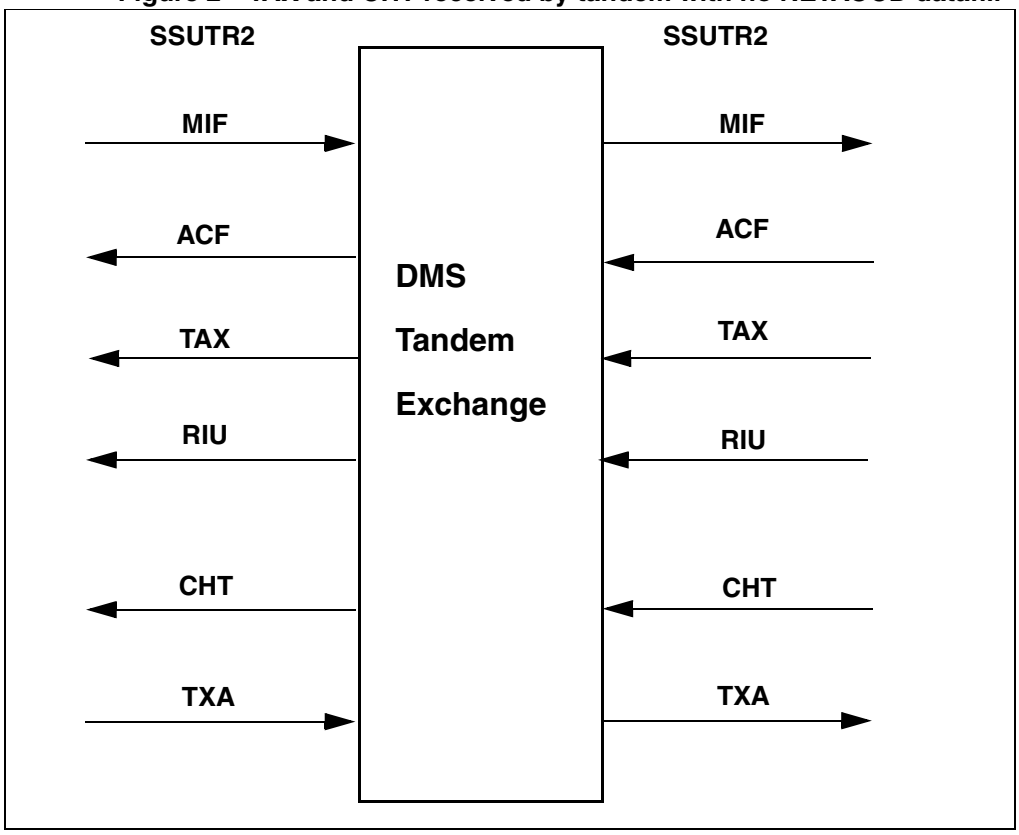


Figure 2 TAX and CHT received by tandem with no NETAOCD datafill



The ITX, TAX and CHT messages received at tandem will be tandemed and will be reported to the CM.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

****Note:*** Figure 1 and Figure 2 also represent the case where TELETAXE option is datafilled in Table 1.Any of the options (TELETAXE_NOSIG or TELETAXE_ITX_SIG) is not datafilled when NETAOCD datafill exists**:

Figure 3 ITX received by tandem with NETAOCD datafill

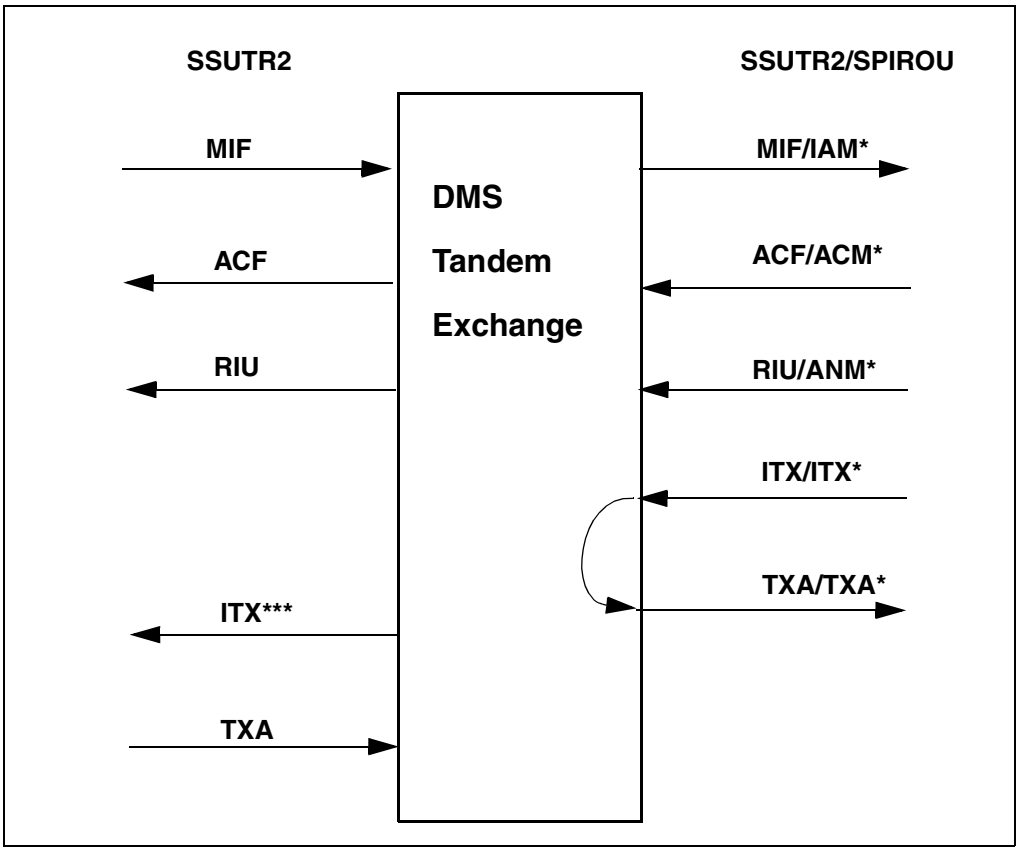
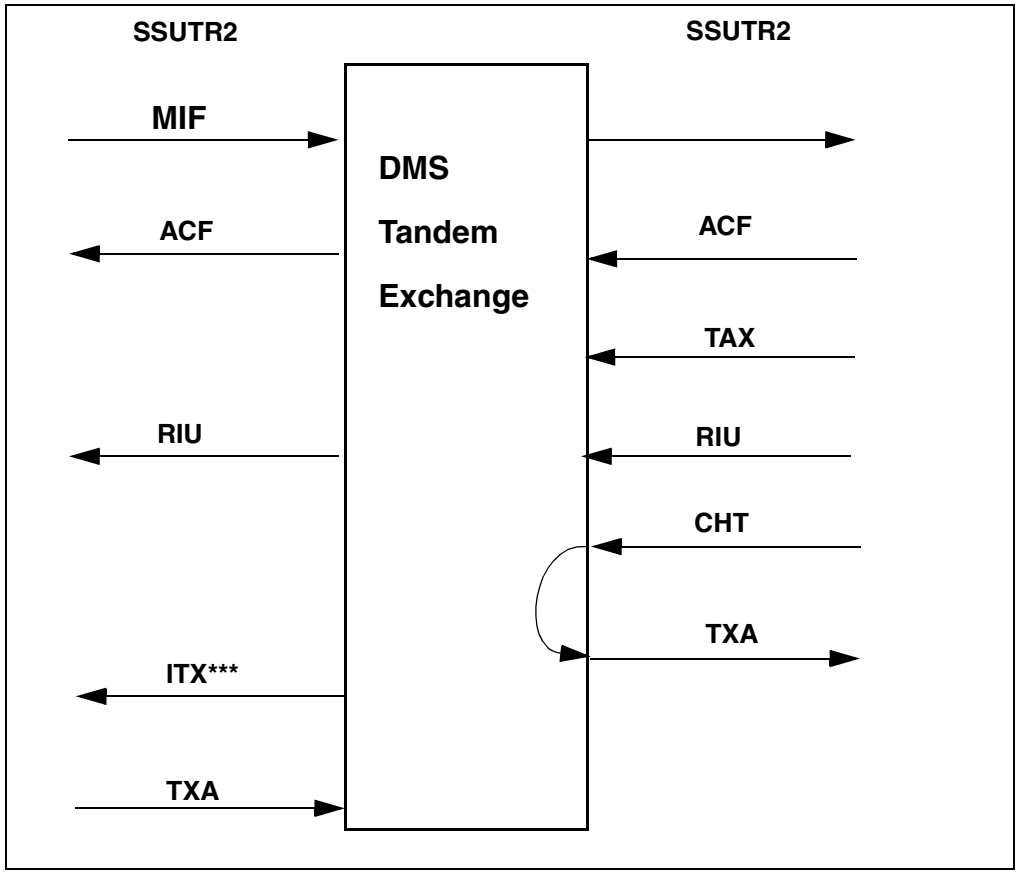


Figure 4 TAX and CHT received by tandem with NETAOCD datafill



The ITX, TAX and CHT messages received are not tandemed , but reported to CM.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

***Note:** Figure 3 and Figure 4 also represent the case where TELETAXE option is datafilled in Table 1.

***ITX generation is allowed regarding existing tariff for NETAOCD datafills

13.2.2.2 TELETAXE_NOSIG is datafilled when no NETAOCD datafill exists:

Figure 5 ITX received by tandem with no NETAOCD datafill

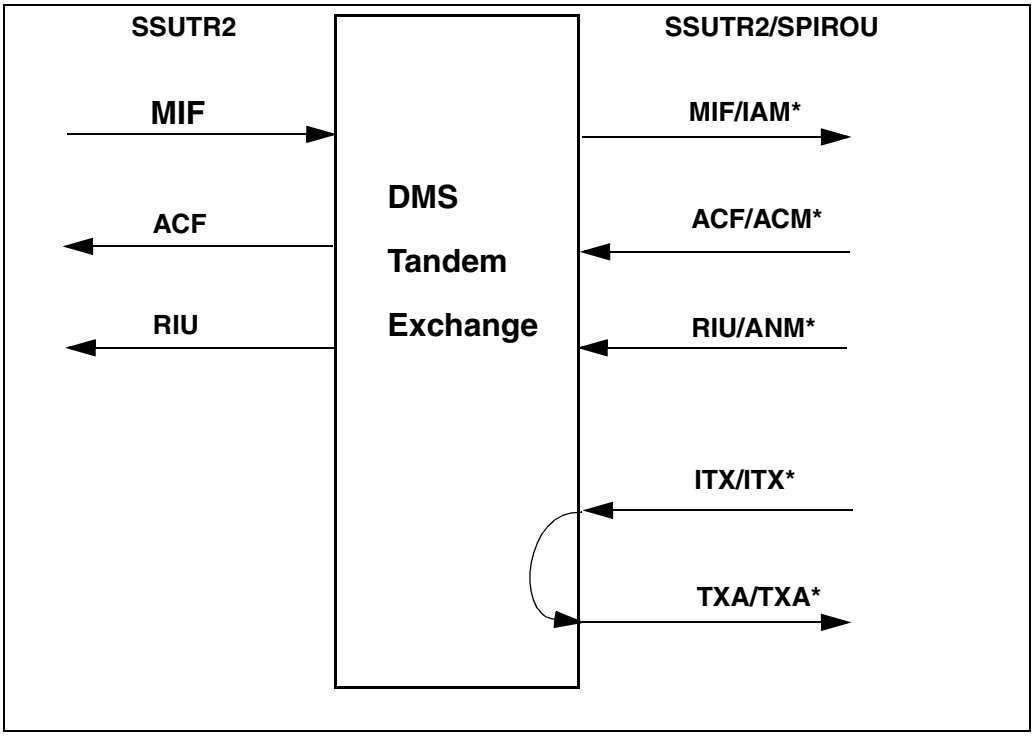
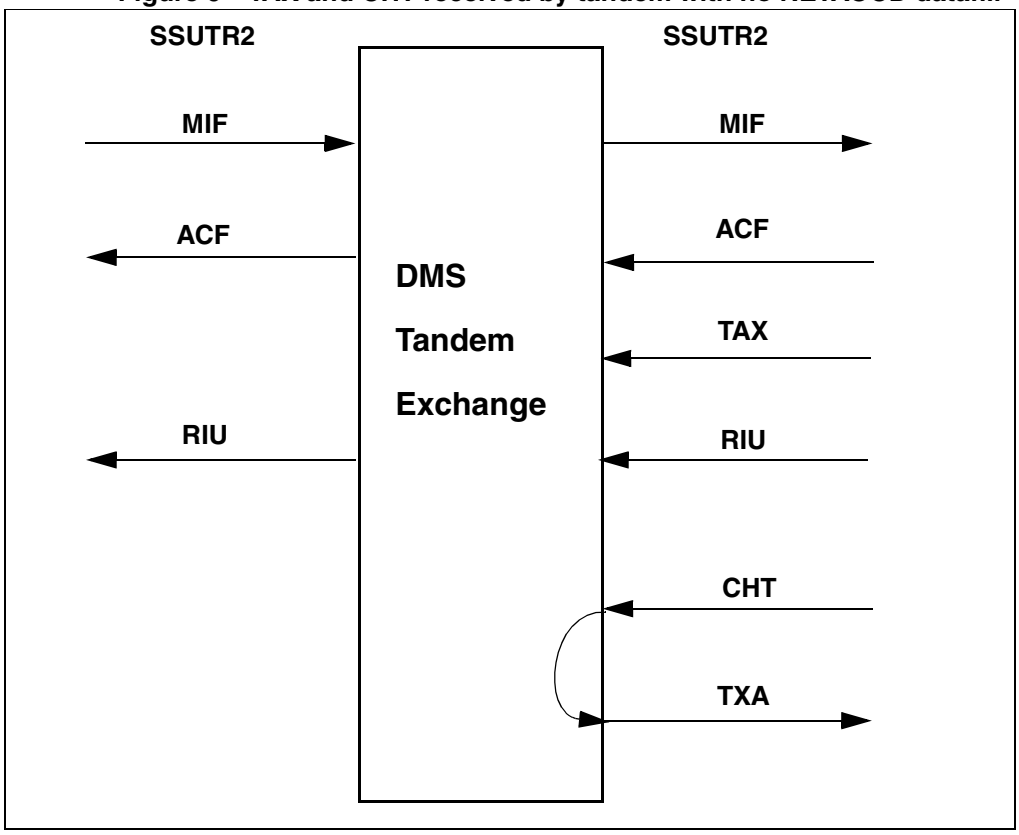


Figure 6 TAX and CHT received by tandem with no NETAOCD datafill



The ITX, TAX and CHT messages received are not tandemed , but reported to CM.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

13.2.2.3 Both TELETAXE_NOSIG and NETAOCD are datafilled:

Figure 7 ITX received by tandem with NETAOCD datafill

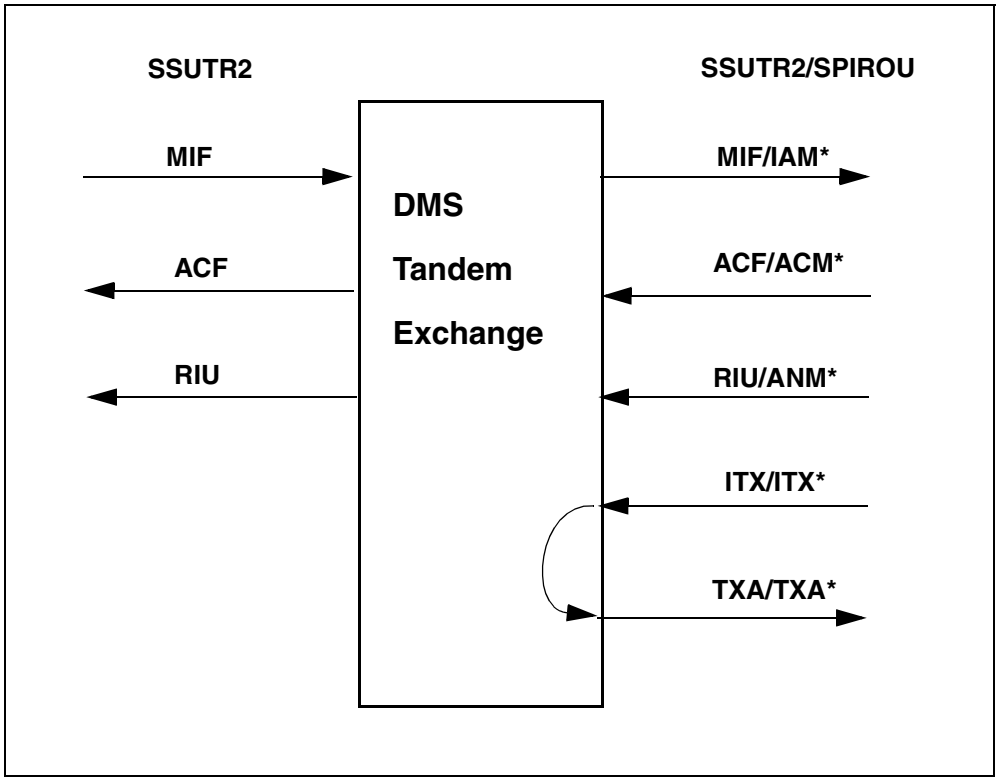
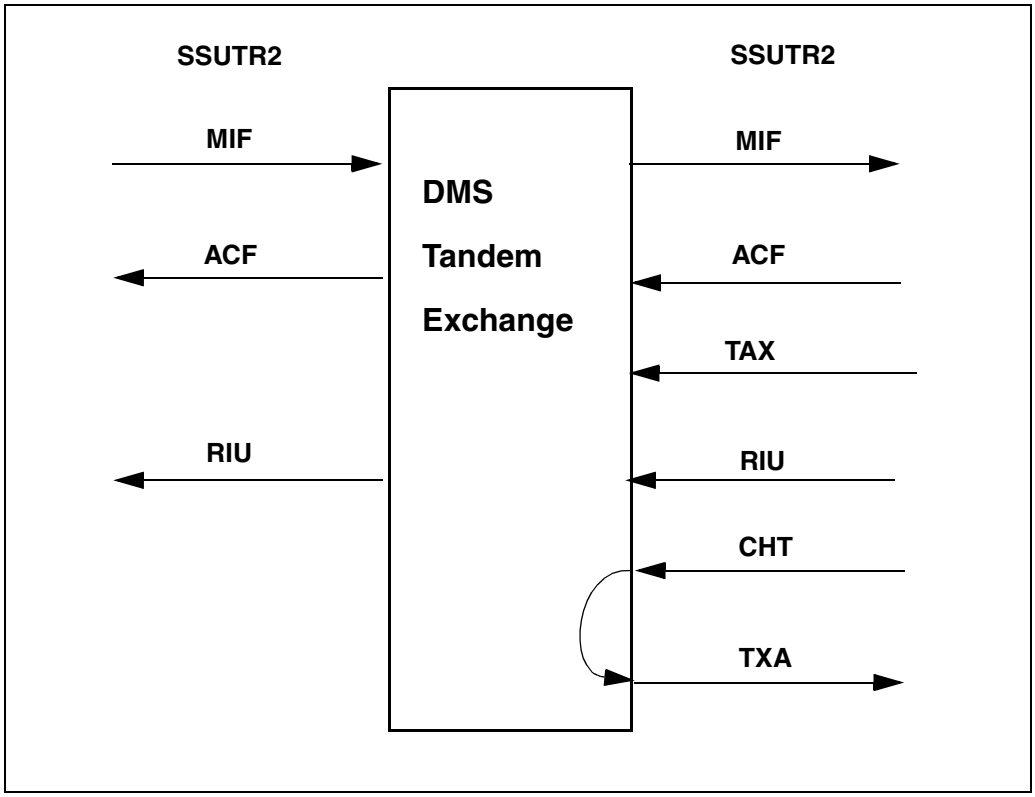


Figure 8 TAX and CHT received by tandem with NETAOCD datafill

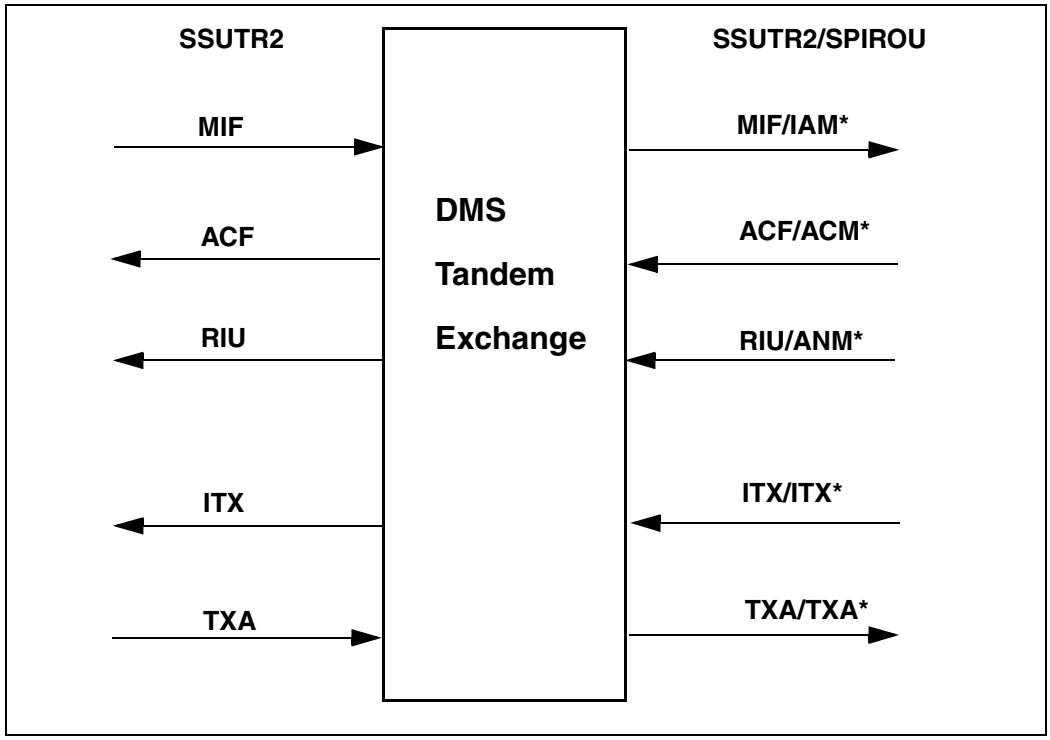


The ITX, TAX and CHT messages received are not tandemed , but reported to CM. ITX and CHT messages are acknowledged by TXA messages. Even if NETAOCD datafill exists at tandem exchange, ITX generation is not allowed.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

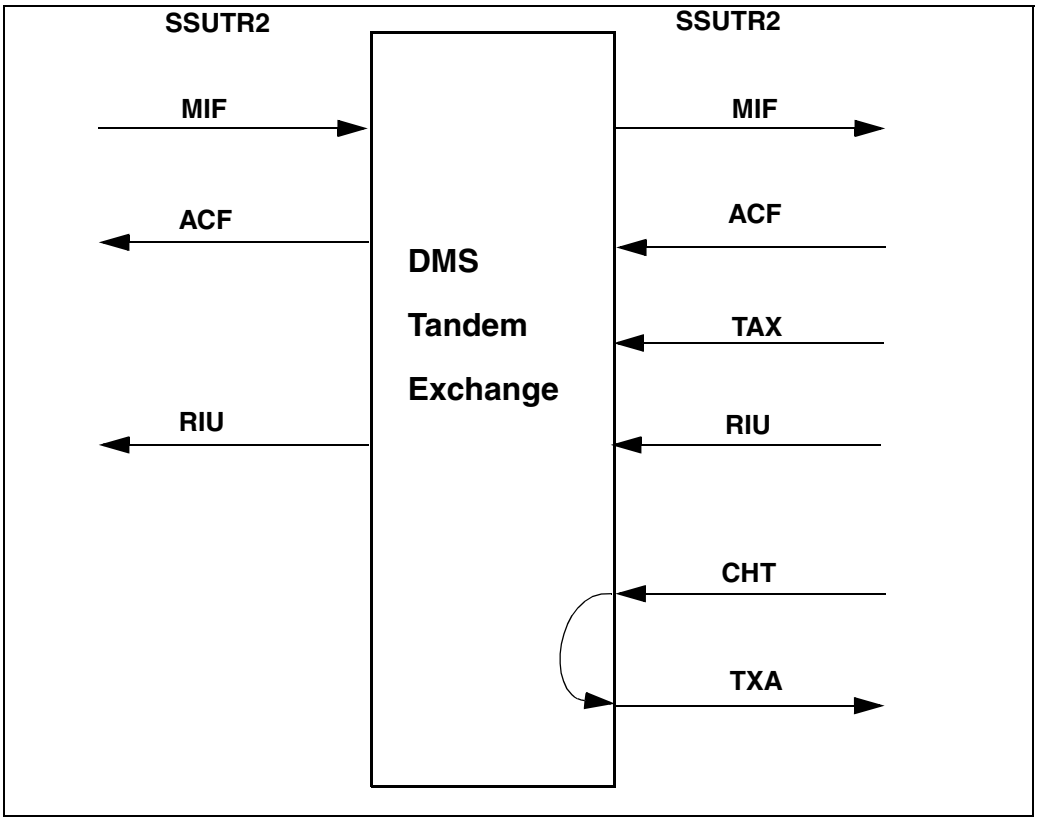
13.2.2.4 TELETAXE_ITX_SIG is datafilled when no NETAOCD datafill exists:

Figure 9 ITX received by tandem with no NETAOCD datafill



The ITX messages received at tandem will be tandemed and will be reported to the CM.

Figure 10 TAX and CHT received by tandem with no NETAOCD datafill



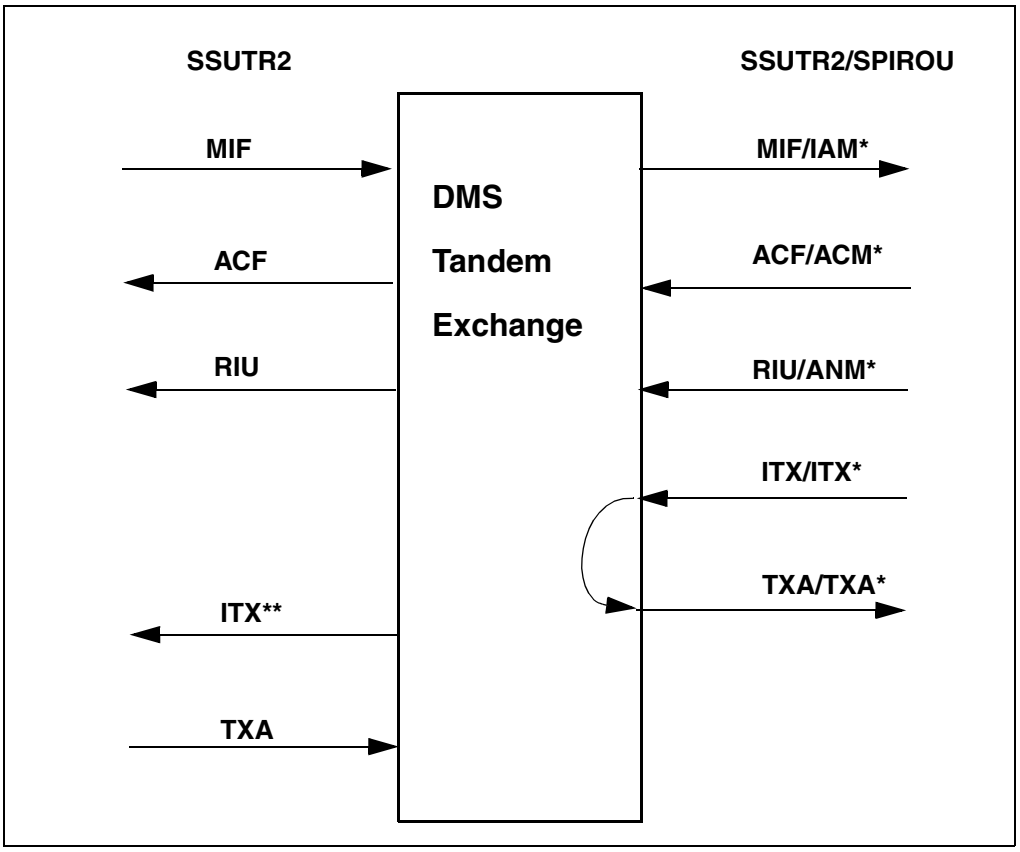
The TAX and CHT messages received at tandem will still not be tandemed and not reported to CM, but CHT messages are acknowledged by TXA.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

13.2.2.5 TELETAXE_ITX_SIG is datafilled when NETAOCD datafill exists:

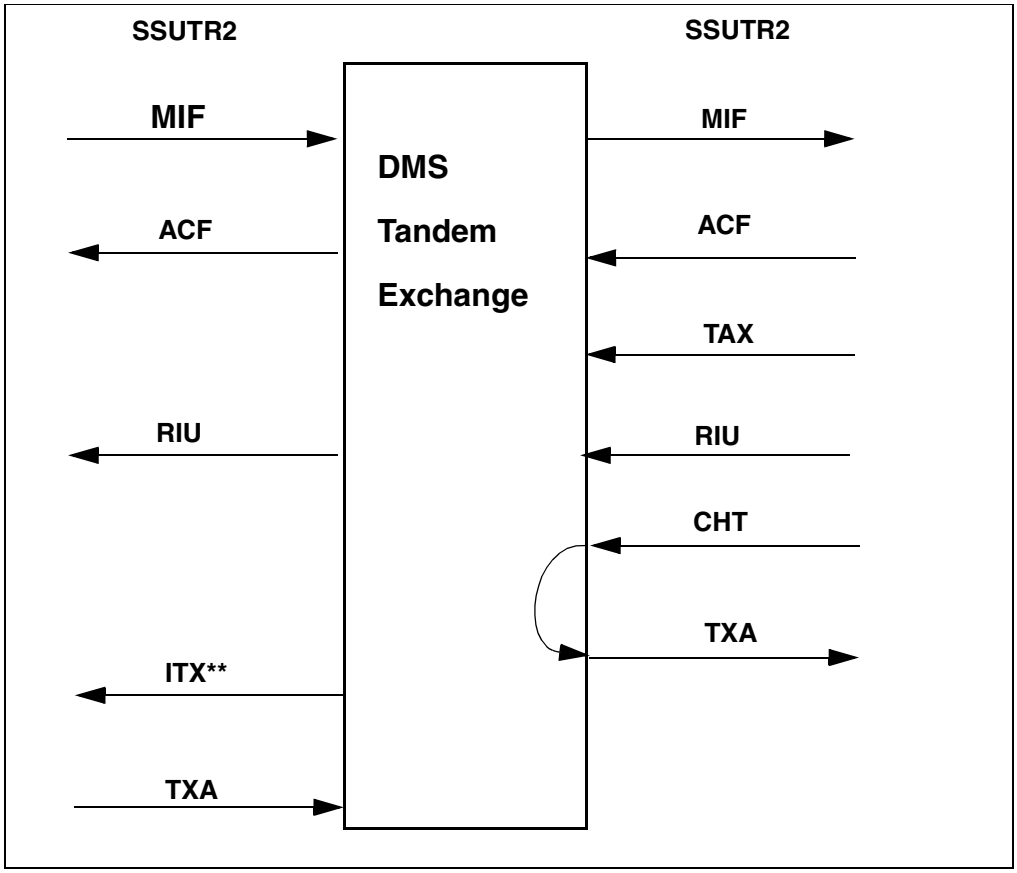
This activity has no impact on existing NETAOCD behaviour.

Figure 11 ITX received by tandem with NETAOCD datafill



The ITX messages received are not tandemed, but reported to CM.

Figure 12 TAX and CHT received by tandem with NETAOCD datafill



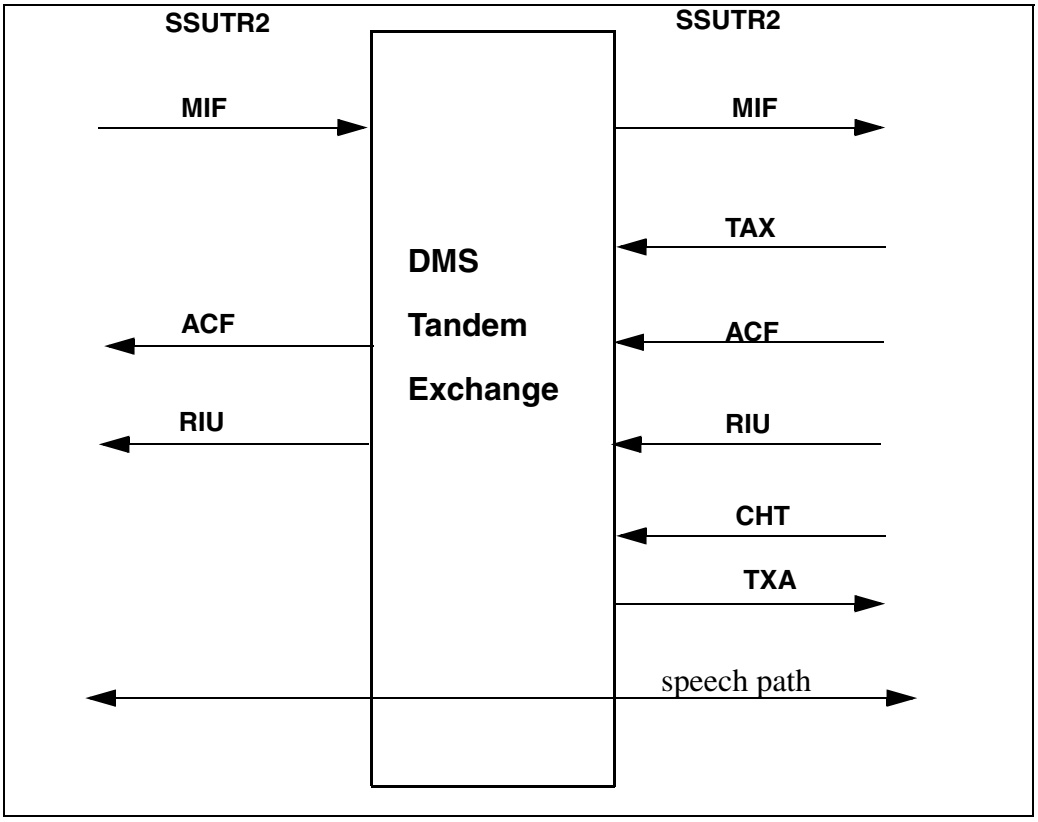
The TAX and CHT messages received are not tandemed, but reported to CM.

*These messages are SPIROU messages sent from/to DMS Tandem Exchange. For SPIROU, TAX and CHT messages are not supported.

**ITX is generated by tandem regarding existing tariff for NETAOCD datafills.

13.2.3 Handling of TAX in pre-ACF condition with Teletax_ITX_SIG Datafilled

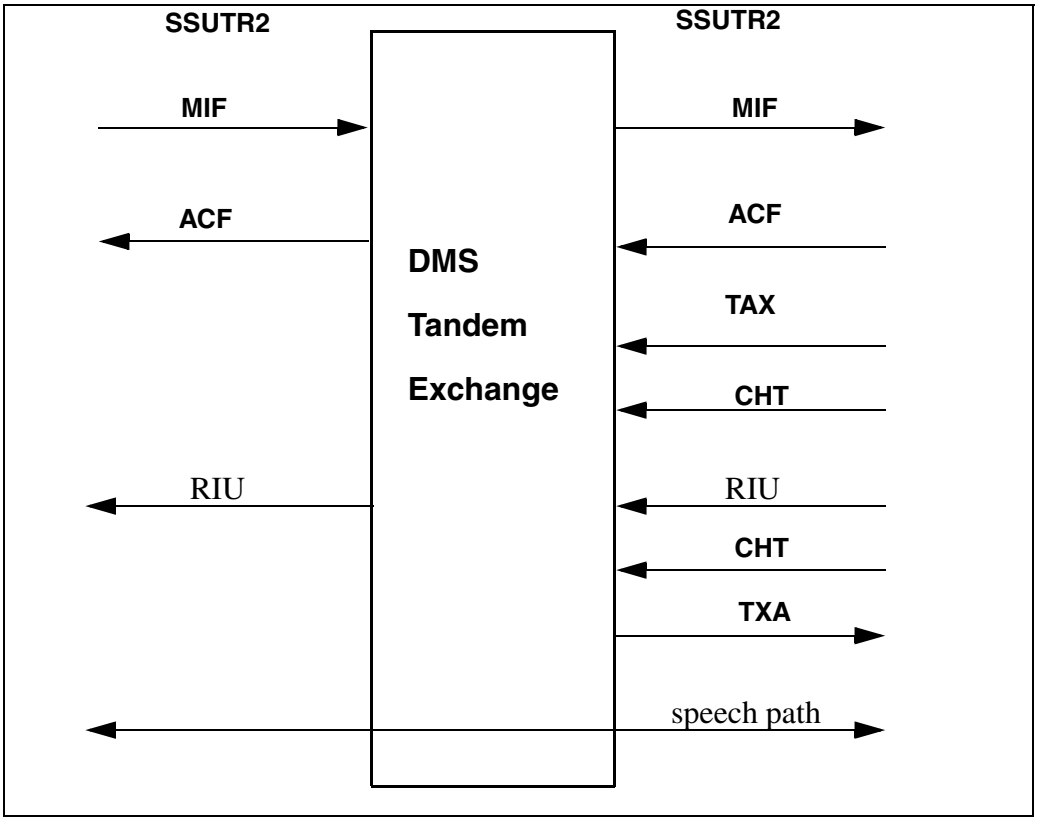
Figure 13 TAX received by tandem in pre-ACF state



The TAX message received at tandem will not be tandemed and not reported to CM.

13.2.4 Handling of CHT in pre-RIU condition with Teletax_ITX_SIG Datafilled

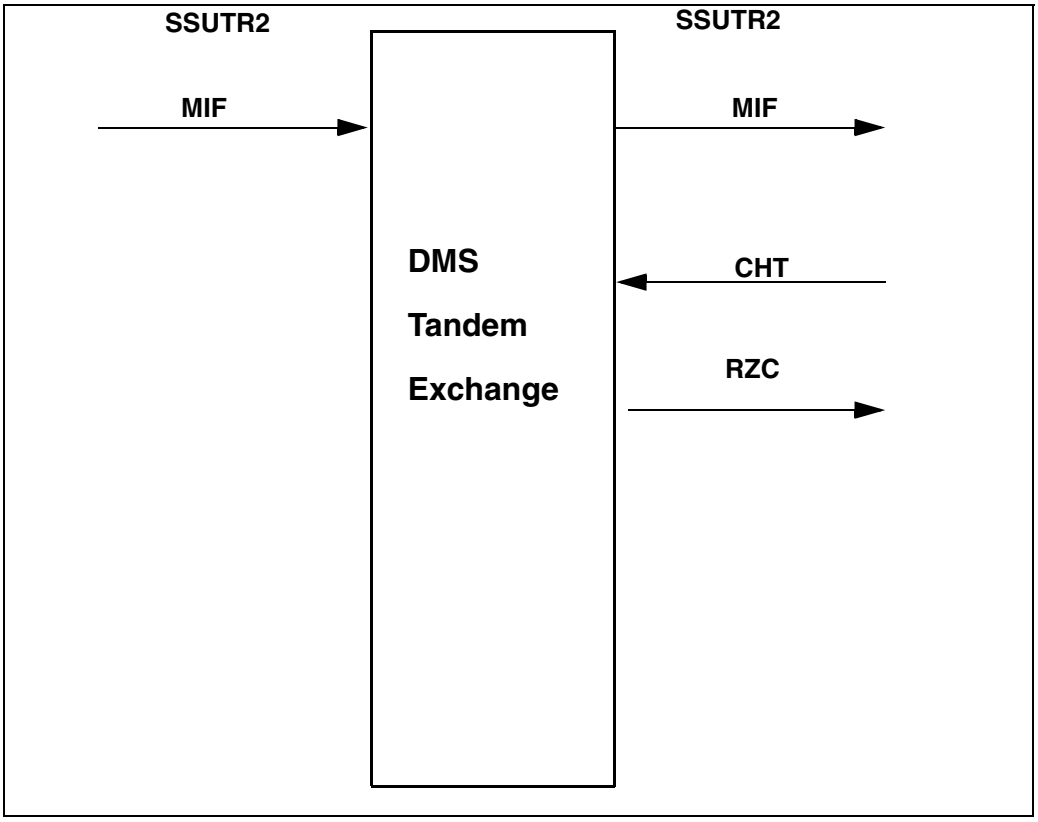
Figure 14 CHT received by tandem with in pre-RIU state with TAX



The CHT messages received at tandem will not be tandemed ,not reported to CM and not acknowledged.

13.2.5 Handling of CHT in pre-ACF condition with TELETAX_ITX_SIG datafilled

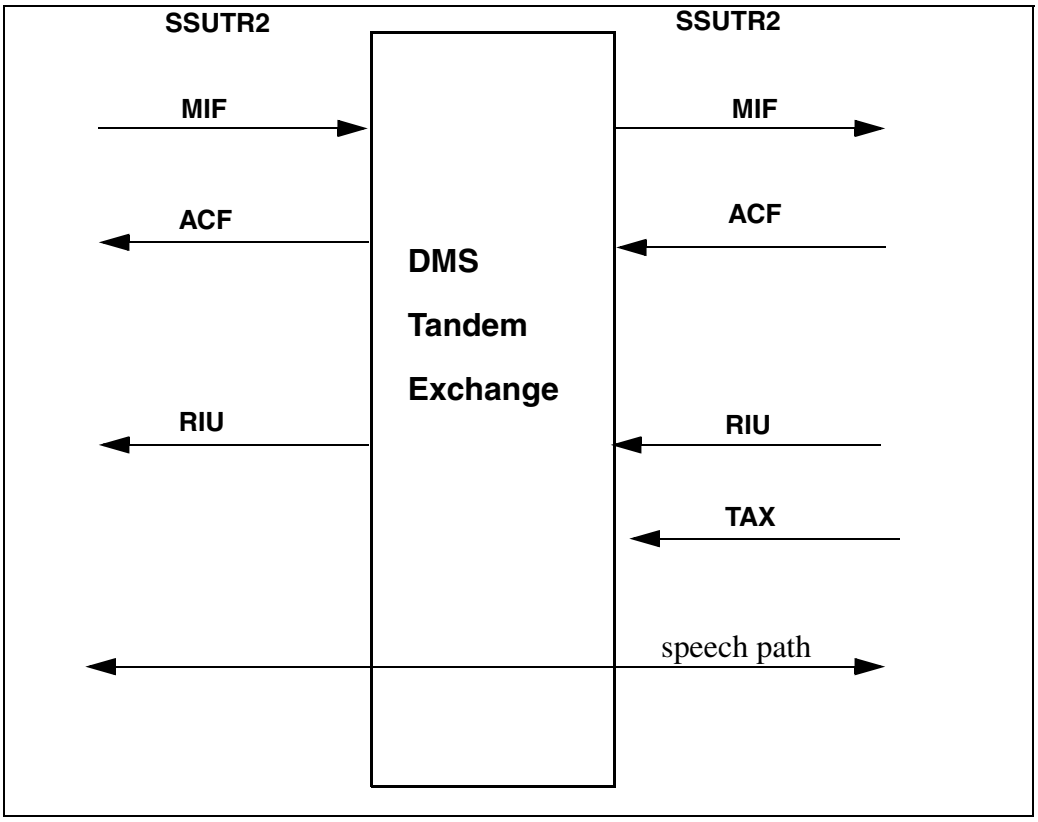
Figure 15 CHT received by tandem in pre-ACF state



The CHT messages received at tandem will not be tandemed ,not reported to CM and not acknowledged, regarding to SSUTR2 specification (Reference-[A]) call will be dropped with RZC message (reset circuit message).

13.2.6 Handling of TAX in post-RIU condition with TELETAX_ITX_SIG datafilled

Figure 16 TAX received by tandem in post-RIU state



The TAX messages received at tandem will not be tandemed and not reported to CM.

13.2.7 Datafill Requirements

13.2.7.1 Table TRKSGRP Datafill

- **SSUTR2 trunk datafill:**

  2WFTUPAB 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMS_NODE N N **FRANCE 100_BLUE** $ FTUP2W CIC

- **SPIROU trunk datafill:**

  SPIROUAB 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMS N N **SPIROU 100_EIV3** $ 2WN7 CIC

13.2.7.2 Table TRKOPTS Datafill

TELETAXE_ITX_SIG option is datafilled for IC/2W trunks as seen in Table-2 below.

If TELETAXE_ITX_SIG option is assigned to an IC/2W SSUTR2 trunk which is datafilled on peripheral not equipped with an SX05, a warning message is generated. Please refer Figure 9 in CN section of this document.

Additionally, just one of the options TELETAXE_NOSIG and TELETAXE_ITX_SIG will be datafillable for the same trunk at a time.

Table 2 Sample Datafill for TELETAXE_ITX_SIG option in Table TRKOPTS

```
TABLE TRKOPTS
- - - - - - - - - - - - - - -
OPTKEY              OPTINFO
- - - - - - - - - - - - - - - - - - - - - - - - -
2WFTUPBA TELETAXE_ITX_SIG TELETAXE_ITX_SIG
```

13.2.7.3 Metering Datafill

The existing DMS “metering” system which is used to drive ISDN Advice of Charge will be used to determine the number of charge units accured for ITX generation on SSUTR2. This system must be activated per PDTC by the METER option in the table LTCINV.

Please refer the Appendix-2.10.1 for metering datafill example.

13.2.7.4 Traver for ITX generating call

Please refer to Appendix-2.10.2 to find an traver example for SSUTR2-SSUTR2 call when NETAOCD datafill exists.

13.3 Hardware Requirements or Dependencies

This feature is supported only on SX05 DTCO/DTCO2 processor.

13.4 Software Requirements or Dependencies

No changes due to this feature. Existing SOC options for backward charging functionality are used.

13.5 Limitations and restrictions

- This feature is supported only on SX05 DTCO/DTCO2 processor.

- All restrictions and limitations in AU3283-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC will be valid for this activity as well.

13.6 Interactions

No changes due to this feature.

13.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

13.8 Glossary

Term	Description
ACF	ISDN address complete message with user to user facilities
ACM	Address Complete Message
AMA	Automatic Message Accounting
ANM	Answer Message
CHT	Change of Charge Rate Message
CM	Computing Module
DMS	Digital Multiplex System

Term	Description
FN	Functional Description
IAM	Initial Address Message
ITX	Charge Unit message
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
MIF	ISDN initial address message with user to user facilities
MMP	Multi-Market Product
RIU	Answer message with user to user information
SPIROU	Signalisation Pour l'Interconnexion des Réseaux Ouverts
SSUTR2	Sous Systeme Utilisateur
TAX	Charging Message
TUP	Telephony User Part
TXA	Charging Acknowledgement message

13.9 References

a.V 11-T 1998 Recommendation, Specification of the SSUTR2 user subsystem on the interface between the France Telecom fixed network and the third party networks at the VN6 functional phase

b.AU3283-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC

c.AU3284-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC

13.10 Appendix

13.10.1 Metering datafill example

TABLE OFCENG

SSUTR2_ITX_RATE 20

TABLE AMAOPTS

BACK_CHARGE ON

TABLE LTCINV

PDTC 1 1 IDTE 1 18 1 C 8 6X02UI ODT17AY (ABTRK DTCEX) $ (2 48) (2 49) (2 50) (2 51) (2 52) (2 53) (2 54) (2 55) (2 56) (2 57) (2 58) (2 59) (2 60) (2 61) (2 62) (2 63) $ (UTR9) (RAM6X69) (NT6X28) $ TURKR1R2 **SX05AA SX05AA** 0 UPFWQM01 (CCS7) (FSTR2) (**METER**) $ 6X40AC N

TABLE MTRLNET

LOC

TABLE MTRTARIF

---

15 SEC N 1 1 1 1 1 1 1 0 0 1 1 1

TABLE MTRTTS

LOC 7 N 15 16 $ $ $ $ $ $ $ $

TABLE MTRMOTS

MOTS_2 LOC 4 7

TABLE MTRMOG

MDI4 MOTS_2 $

TABLE DAYTYPES

NORMAL

SATDAY

SUNDAY

HOLIDAY

TABLE TODHEAD

LOC MTR LOC 0 NORMAL SATDAY SUNDAY $

TABLE DAYOWEEK

LOC MON NORMAL

TABLE AOCBASIC

LOC 4 0 30

TABLE AOCOPT

LOC 30 4 0 $

TABLE CLISERV

METERING 1 SERVSCRN $

TABLE CLISRVPF

----

1 METERING $ $

TABLE DNSCRN

1027835480 NETAOCD 30 CLISERV 1 $

13.10.2 Traver example for SSUTR2-SSUTR2 call when NETAOCD is datafilled:

>traver l 7835480 3953967835479 tariff b
TABLE IBNLINES
HOST 03 0 00 10 0 DT STN IBN 7835480 CUST783 0 0 102 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE NCOS
CUST783 0 0 0 $ (XLAS NETXLA STARCEPT NDGT) (OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783 NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME NETXLA
TUPLE NOT FOUND
Default from table XLANAME:

NETXLA
(NET N Y 0 N NDGT N Y DOD N 1 102_NPRT_1 NLCA_NILLA_1 NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 3953967835479
TABLE PXCODE
NETXLA 395 395 RTE (PF 3) (MM 9 15) (DEST 396) (CLASS NATL) (LNET LOC) (MZONE 4)$
TABLE: PXRTE
KEY: NETXLA 396
. S MFTUPAB
EXIT TABLE PXRTE
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE MTRMOG
TUPLE NOT FOUND
TABLE MTRLNET
LOC
TABLE MTRMOTS
TUPLE NOT FOUND
TABLE MTRNETIF
TUPLE NOT FOUND
TABLE MTRMOTS
TUPLE NOT FOUND
TABLE MTRNAMES
TUPLE NOT FOUND
TABLE TODHEAD
LOC MTR LOC 0 (NORMAL) (SATDAY) (SUNDAY) $
TABLE DAYOYEAR
TUPLE NOT FOUND
TABLE DAYOWEEK
LOC MON NORMAL
TABLE TIMEODAY

TUPLE NOT FOUND
WARNING: TIMEODAY datafill missing
The default TNT in table TODHEAD will be used
TABLE MTRTTS
TUPLE NOT FOUND
TABLE MTRTARIF
4 MIN N 1 1 5 1 1 5 1 0 0 1 1 5

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 MFTUPAB 3967835479 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 MESAJ2
2 OFL
3 LKOUT

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>traver tr mftupba 3967835479 tariff b
TABLE TRKGRP
MFTUPBA IBNT2 0 NPDGP NCRT SERKAN 0 LIDL 0 N ANSDISC 0 Y N N N N N N 0
0 N 0 1 0 1 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP: no subscribed trigger.
TABLE NCOS
SERKAN 0 0 0 $ (XLAS NETXLA1 NETXLA1 NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT,
AND DIGCOL
SERKAN NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP: no subscribed trigger.
TABLE IBNXLA: XLANAME NETXLA1
TUPLE NOT FOUND

Default from table XLANAME:
NETXLA1
(NET N Y 0 N NDGT N Y DOD N 2 102_NPRT_1 NLCA_NILLA_1 NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
2 IBN NONE NT 0 0 NILSFC 4 PX NETXLA1 NIL 00 102_NPRT_1 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA1 DFLT FEATINFO VALIDATE (SUBSCRN (GENERAL N N N N)$) (CLISERV
METERING)$ 0 1 20 PX NETXLA NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 3967835479
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
PLEASE ENTER CLI DIGITS:
>1027835480
TABLE CLISERV
. METERING 1 (SERVSCRN)$
TABLE DNSCRN
. 1027835480 (NETAOCD 30) (CLISERV 1) $
TABLE CLISRVPF
. 1 (METERING $)$
. Matched on METERING
. Service screening succeeded
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 3967835479
TABLE PXCODE
NETXLA 396 396 RTE (PF 3) (MM 9 15) (DEST 394) (CLASS NATL) (LNET LOC) (
MZONE 4)$
TABLE: PXRTE
KEY: NETXLA 394
. S 2WFTUPAB
EXIT TABLE PXRTE
INAP Info Analyzed TDP: no subscribed trigger.
TABLE MTRMOG

```
MDI4 MOTS_2 $
TABLE MTRLNET
LOC
TABLE MTRMOTS
MOTS_2 LOC 4 7
TABLE MTRNETIF
TUPLE NOT FOUND
TABLE MTRMOTS
MOTS_2 LOC 4 7
TABLE MTRNAMES
TUPLE NOT FOUND
TABLE TODHEAD
LOC MTR LOC 0 (NORMAL) (SATDAY) (SUNDAY) $
TABLE DAYOYEAR
TUPLE NOT FOUND
TABLE DAYOWEEK
LOC MON NORMAL
TABLE TIMEODAY
TUPLE NOT FOUND
WARNING: TIMEODAY datafill missing
The default TNT in table TODHEAD will be used
TABLE MTRTTS
LOC 7 N 15 16 $ $ $ $ $ $ $ $
TABLE MTRTARIF
15 SEC N 1 1 1 1 1 1 1 0 0 1 1 1

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WFTUPAB              7835479          ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>traver tr 2wftupba 7835479 tariff b
TABLE TRKGRP
2WFTUPBA IBNT2 0 NPDGP NCRT SERKAN 0 LIDL 0 N ANSDISC 0 Y N N N N N N 0
```

0 N 0 1 0 1 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP: no subscribed trigger.
TABLE NCOS
SERKAN 0 0 0 $ (XLAS NETXLA1 NETXLA1 NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT,
AND DIGCOL
SERKAN NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP: no subscribed trigger.
TABLE IBNXLA: XLANAME NETXLA1
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA1
   (NET N Y 0 N NDGT N Y DOD N 2 102_NPRT_1 NLCA_NILLA_1 NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
2 IBN NONE NT 0 0 NILSFC 4 PX NETXLA1 NIL 00 102_NPRT_1 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA1 DFLT FEATINFO VALIDATE (SUBSCRN (GENERAL N N N N)$) (CLISERV
METERING)$ 0 1 20 PX NETXLA NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 7835479
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
PLEASE ENTER CLI DIGITS:
>1027835480
TABLE CLISERV
. METERING 1 (SERVSCRN)$
TABLE DNSCRN
. 1027835480 (NETAOCD 30) (CLISERV 1) $

TABLE CLISRVPF
. 1 (METERING $)$
. Matched on METERING
. Service screening succeeded
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 7835479
TABLE PXCODE
NETXLA 783 783 CONT (PF 3) (MM 7 7) (CLASS LCL) (XLT OFC OFC783) (LNET LOC) (MZONE 4)$
TABLE OFCHEAD
OFC783 DFLT TRMT (OFC VACT)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 5479
TABLE OFCCODE
OFC783 5 5 RTE (DEST 1)$
TABLE: OFCRTE
KEY: OFC783 1
. T OFRT 783
. . TABLE OFRT
. . 783 DN 102 783 4
. . . TABLE TOFCNAME
. . . 102 783 $
. . . TABLE DNINV
. . . 102 783 5479 L HOST 03 0 00 09
TABLE DNFEAT
TUPLE NOT FOUND
. . . TABLE DNATTRS
. . . TUPLE NOT FOUND
. . . TABLE DNGRPS
. . . TUPLE NOT FOUND
. . EXIT TABLE OFRT
EXIT TABLE OFCRTE
INAP Info Analyzed TDP: no subscribed trigger.
INAP Termination Attempt TDP: no subscribed trigger.
TABLE MTRMOG
MDI4 MOTS_2 $
TABLE MTRLNET
LOC
TABLE MTRMOTS
MOTS_2 LOC 4 7
TABLE MTRNETIF

TUPLE NOT FOUND
TABLE MTRMOTS
MOTS_2 LOC 4 7
TABLE MTRNAMES
TUPLE NOT FOUND
TABLE TODHEAD
LOC MTR LOC 0 (NORMAL) (SATDAY) (SUNDAY) $
TABLE DAYOYEAR
TUPLE NOT FOUND
TABLE DAYOWEEK
LOC MON NORMAL
TABLE TIMEODAY
TUPLE NOT FOUND
WARNING: TIMEODAY datafill missing
The default TNT in table TODHEAD will be used
TABLE MTRTTS
LOC 7 N 15 16 $ $ $ $ $ $ $ $
TABLE MTRTARIF
15 SEC N 1 1 1 1 1 1 1 0 0 1 1 1

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 LINE 1027835479 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

13.10.3 Backward Charging Message Formats

13.10.3.1 ITX-Call Charge Allocation Message

Table 3 ITX message fields

Field	value	no. bits
Message Header Code	#40	8
Call Charge Allocation Domain	*Number of call charges to be allocated to the subscriber's counter when the message is received.*	8
Message Number	*Number of call charge allocation message sent for a given call (the value 0 is not used as a number.)*	8

13.10.3.2 TXA-Call Charge Acknowledgement Message

Table 4 TXA message fields

Field	value	no. bits
Message Header Code	#80	8

13.10.3.3 CHT-Change of Charge Rate Message

Table 5 CHT message fields

Field	value	no. bits
Message Header Code	#30	8

Message Indicators	***bit A**: **Next Charge rate factor indicator*** *0: Next Charge rate factor field missing* *1: Next Charge rate factor field present* ***bits B to D**: For future use (set to '000').*	4
Call Rate Indicators	***bits DCBA:*** *0000: Call charge coefficient 0:Charge rate indepentdent of duration* *0001: Call charge coefficient I(reserved)* *0010: Call charge coefficient II(0.1 second)* *0011: Call charge coefficient III(0.2 seconds)* *0100: Call charge coefficient IV(0.5 seconds)* *0101: Call charge coefficient V(1 second)* *0110: Call charge coefficient VI(2 seconds)* *0111: Call charge coefficient VI(4 seconds)* *1000* *: Call charge coefficients VIII to XV (future use)* *1111*	4
Charge Rate Factor	*Number from 1 to 255 which, when multiplied by the call charge coefficient of the charge rate indicators, gives the call charging period (in seconds) for charging for the call.*	8

Time Indicator	*This indicator gives the time at which the next change of charge rate will take place.* ***bit A**: For future use (set to '0').* ***bits HGFEDCB:*** *0000000: Immediate change of charge rate* *0000001: 00 hours 15* *0000010: 00 hours 30* *0000011: 00 hours 45* *0000100: 01 hours 00* *0000101: 01 hours 15* *0000110: 01 hours 30* *.* *.* *.* *1011111: 23 hours 45* *1100000: 24 hours 00* *1100001* *For future use* *1111111*	8

13.10.3.4 TAX-Call Charge Message

Table 6 TAX message fields

Field	value	no. bits
Message Header Code	#24	8

Message Indicators	***bit A**: **Current Charge Rate Indicator*** *0: Call charge quantum (A) and charge rate indicators (A) fields missing* *1: Call charge quantum (A) and charge rate indicators (A) fields present* ***bit B**: Current Charge Rate Factor Indicator* *0: Charge rate factor (A) field missing* *1: Charge rate factor (A) field present* ***bit C**: **Next Charge Rate Indicator*** *0: Call charge quantum (B) and charge rate indicator (B) fields missing* *1: Call charge quantum (B) and charge rate indicator (B) fields present* ***bit D**: **Next Charge Rate Factor Indicator*** *0: Charge rate factor (B) field missing* *1: Charge rate factor (B) field present* ***bit E to H**: For future use (set to '0000')*	8
Call Charge Quantum	*Number (from 0 to 15) of Telecom units to be recorded when the called subscriber answers.*	4
Charge rate indicators, charge rate factor and time indicator	*The values of these fields are same as for the CHT message in the section 2.2.5.3 ,Table 4.*	

14: Functional Description (FN): A0002173

14.1 Feature name

System of Operative-Searching Measures (SOSM) for Digital Multiplex System (DMS) MMP.

In ISN07 release, SOSM for IBN/V5.2(IBN) lines and ISUP trunks is developed under the following activities:

- A00002172 "SOSM - Provisioning"
- A00002173 “SOSM - X25 Messaging Interface & Speech Connection”
- A00002178 "SOSM - CALLP and Service Interactions"

In ISN08 release, SOSM support for ETSI[1] BRI and ETSI PRI agents is provided under the following activities:

- A00006861 "SOSM PRI Basic Call and Feature Interactions"
- A00006863 "SOSM BRI Basic Call Interactions"
- A00006864 "SOSM BRI FPE Interactions"

14.2 Feature Synopsis

This feature implements supervision of outgoing/incoming calls from/to certain observed subscribers in the Russian telephone network.

This feature provides the ability to monitor calls :

- from/to present exchange subscribers (IBN/V5.2(IBN) and BRI agents).
- to subscribers of other exchanges called over ISUP/ PRI trunks where the originator is a line, and dialed number is supervised by the CP.

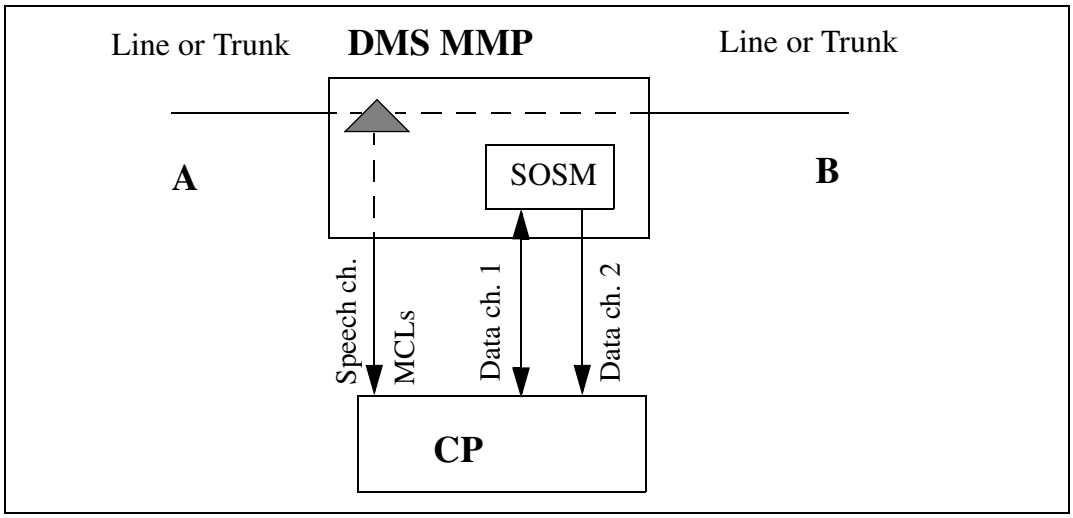
For BRI subscribers monitoring is done DN based, just like IBN subscribers. Thus, in order to monitor all agents on a loop, all of the DNs (MSNs) on the loop must be supervised by CP.

This feature provides SOSM PRI Basic Call and Feature Interactions on ETSI PRI trunks version 1990 on the DMS-100 for the MMP product.

[1]In the rest of the document BRI/PRI will be used instead of ETSI BRI/PRI

14.3 Functional Overview

Figure 1 Control Point (CP) - SOSM & DMS MMP Connection



With this activity, voice information exchange between two parties, A and B in Figure 1, is transmitted to CP over speech channel. Data channel 1 (X.25 protocol) is used for CP to SOSM control commands and SOSM to CP messages. Data channel 2 (X.25 protocol) is used for transmission of information messages from SOSM to CP about the supervised connections.

This feature will be available only for the markets where SOC SOSM0001 is ON. Please refer to Section "2.6 Software Optionality Control (SOC)" on page 149.

14.4 Background Information

This section provides information on other DMS MMP systems used by this feature.

14.4.1 DMS MMP - MPC system

On DMS MMP, X.25 protocol support is implemented in the Multi-Protocol Controller (MPC) system. The system uses either an NT1X89 card on an Input-Output Controller (IOC) shelf or IOM card (NTFX30AA) on an ISME or CISM shelf . MPC system must be installed and configured in the office to allow SOSM system to communicate with the Control Point via X.25 links.

Each MPC card is equipped with three links (1through 3). Each port can be sub-divided into channels. The datafill of the MPC card will determine the configuration of each link. When a link is configured with only one channel, the entire bandwidth of the link is available to that channel.

SOSM system uses links at the minimum 9600 bps . Both channel 1 and 2 of SOSM data interface can be provided on one MPC card, via links 2 and 3.

For datafill instructions of MPC system please refer to section “2.8 Provisioning” on page 150.

Complete information regarding the X.25 and MPC system is available in "297-8991-500 Maintenance and Operations Manual".

14.4.2 SOSM monitoring hardware

SOSM system uses two types of hardware for speech path monitoring. When a call is under "**combined**" surveillance, the speech path information from both parties is transmitted to the CP in a single channel. When “**separate**” monitoring is used, each party’s speech path information is transmitted over its own channel.

Combined monitoring makes use of one Monitoring Connecting Line (MCL) and one Three-way Conference bridge.

Separate monitoring makes use of two Monitoring Connecting Lines, one per party.

> ***Note:*** By design, analog line cards contain a bridge which causes an echo on the backward speech path. If a party in a monitored call is of an analog line card, the party’s MCL will contain a combination of his transmit and receive signals. The transmit signal predominates the other by approximately 20db.

Figure 2 First Variant of connection from DMS to CP via PCM-30

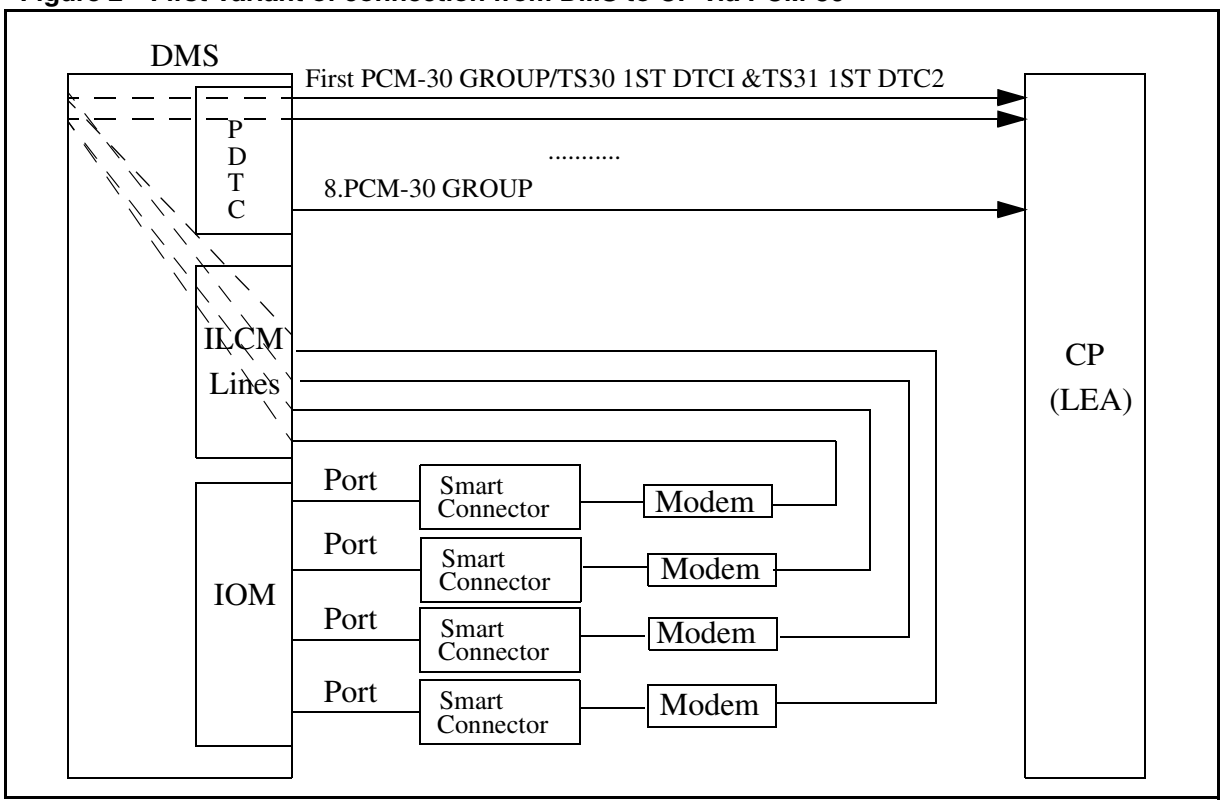
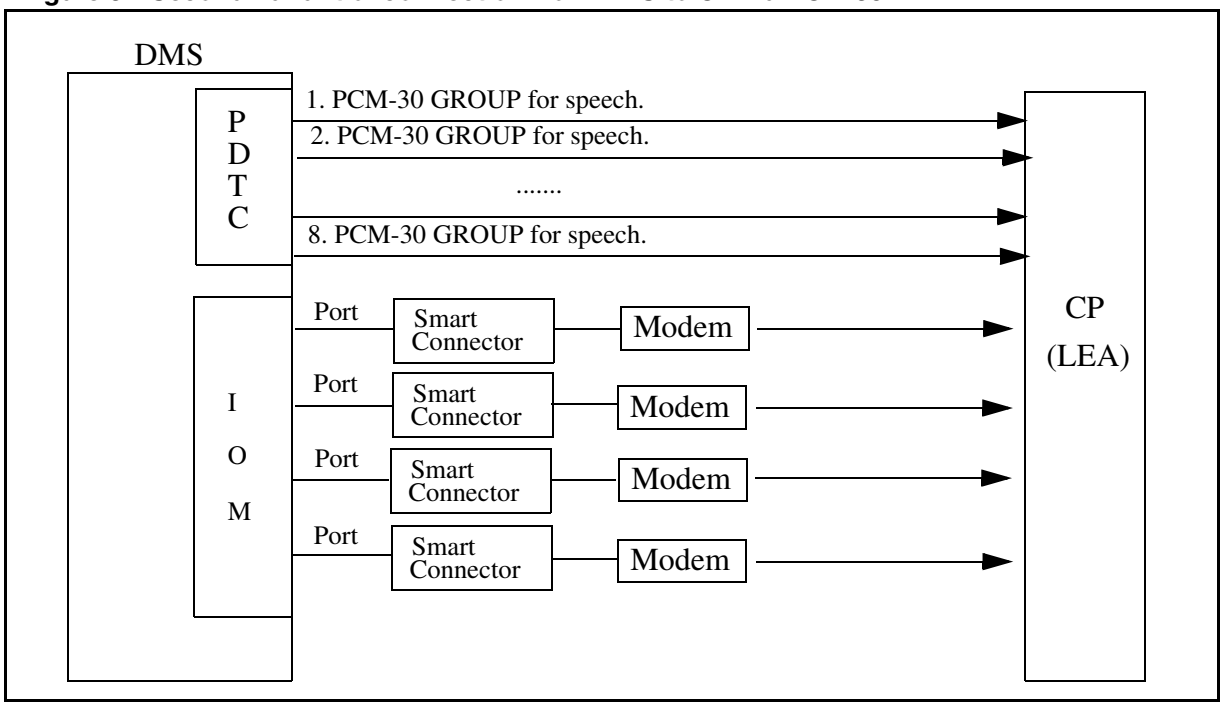


Figure 3 Second Variant of connection from DMS to CP via PCM-30



14.4.2.1 MCL hardware

Monitoring Connecting Lines (MCL) -used by SOSM to transmit speech path information- are implemented by using Pulse Code Modulation 30 (PCM-30) trunks provisioned on a Digital Trunk Controller (DTC).

The system uses 8 trunk groups, and each group contains 28 time slots or channels available for speech path information. Each of these channels constitutes an MCL. Time slots 0, 16, 30 and 31 are not used by the DMS MMP - SOSM.

New trunk groups and members dedicated to the SOSM system must be provisioned in the office to allow the SOSM to transmit information to the CP.

For further information on provisioning SOSM trunks, please refer to section “2.8 Provisioning” on page 150.

For information on Digital Trunk Controllers please refer to "297-1001-592 DMS-100 Family Peripheral Modules Maintenance Guide".

14.4.2.2 Three way conference ports

When party A and B are to be monitored jointly, a three way conference bridge is used to connect A, B and the MCL onto one speech path. Three way conference ports are installed in the office for general use by multi-party calls.

Dedicated three way ports should be allocated for SOSM system to ensure proper operation of the SOSM system, and to minimize the impact of SOSM on the normal operations of the office.

Number of conference ports must be equal to the maximum number of simultaneous monitored calls. For example, 168 conference ports must be installed to be able to transmit call contents of 168 jointly monitored calls.

Caution: The SOSM system uses conference ports from a common pool in the DMS MMP. If **all** ports are used by SOSM, normal 3-way or 6-way calls will be denied. Similarly, if **all** ports are used by 3-way or 6-way calls, SOSM monitored calls will be unable to obtain an MCL connection.

For information on provisioning three way conference ports for SOSM, please refer to section “2.8 Provisioning” on page 150.

Complete information regarding conference port circuits is available in "297-8991-500 Maintenance and Operations Manual".

14.5 Feature Description

14.5.1 General System Description

R-1 Status: C
SOSM system consists of hardware and software used to provide communication with the CP and transmit speech information from observed calls.

R-2 Status: PC[1]
The impact of SOSM system on normal exchange operations and quality of service are kept to a minimum.

R-3 Status: C
SOSM system provides the following capabilities:

a. Supervision of all Outgoing (OG)/ Incoming (IC) calls from/to certain observed subscribers of an exchange, supervision of local, intrazonal, toll and international calls.

b. Supervision of Outgoing (OG) local, intrazonal, toll and international calls to pre-determined numbers of telephone network originating from any subscriber of the exchange.

c. Supervision of calls providing subscriber services; changing call direction or numbering information, and other services such as conference calls.

d. Provide information -about subscriber categories and their subscribed services- to CP when requested.

e. On redirected calls such as Call Forward Do Not Answer (CFD) or Call Forward Busy (CFB), provide supervision of the subscriber that originated the service as well as the subscriber to which calls are forwarded.

14.5.1.1 Interworking between SOSM-DMS MMP and CP

R-4 Status: C
The following items must be provisioned in the exchange to allow interaction between SOSM system and Control Point:

a. Trunks for transmission of speech information to CP, either separately for each party or combined (A & B party on one speech channel).

[1]Specification requires no impact, which is not possible to achieve.

b. Data transmission channel between CP and exchange for control commands via X.25 network protocol

c. Data transmission channel between CP and exchange for transmission of call information via X.25 network protocol

R-5 Status: C
For any monitored call (statistical or complete) the following call phases are reported to the CP:

a. Reception of the called party number

b. Called party answer

c. Call release

d. Service usage

R-6 Status: C
For each call phase of a supervised call, the appropriate message is sent to the CP via data channel 2.

R-7 Status: C
Information about monitored calls is transmitted in real time.

R-8 Status: C
The communication link for transmitting speech path information is setup in parallel with the supervised call.

14.5.1.2 Organization of supervision

R-9 Status: C
The telephone numbers of present exchange and network supervised subscribers are specified by the CP via appropriate commands and stored on the DMS MMP.

R-10 Status: C
The maximum number of supervised subscribers on present exchange is 1024.

R-11 Status: C
The maximum number of network supervised subscribers is 1024.

R-12 Status: C
The number of trunks (MCL's) for call content transmission is provisioned as follows. The values given in Table 1, "SOSM capacity," on page 56 are valid for all DMS MMP exchanges of all sizes.

Table 1 SOSM capacity

Max. Number of supervised subscribers	Max. No. of simultaneous supervised calls	Max. No. of Channels (MCLs)	Number of PCM trunk groups
1024 (present exchange) + 1024 (network)	168	224	8

R-13 Status: C
Supervision category is assigned to a supervised subscriber as follows:

a. Full supervision

b. Statistical supervision

R-14 Status: C
Under full supervision, data about the supervised call and information about call phases is transmitted to the CP in real time, as well as call content. Call content is transmitted to CP either over separate channels, or through a single channel by the use of a conference port..

R-15 Status: C
Under statistical supervision call content is not transmitted to CP. Call data and information regarding call phases are sent to the CP in real-time.

R-16 Status: C
When both parties in a call are monitored subscribers, a unique call number is assigned to each, and call monitoring is done as per each subscriber's information.

R-17 Status: C
The supervision category may be changed during an active call (i.e. statistically monitored call may be turned to complete via command from CP).

R-18 Status: C
Adding or removing subscriber from Supervised Subscribers Database is done via commands from CP.

R-19 Status: C
The time interval between the reception and execution of add/change supervised subscribers' data commands does not exceed 30 seconds.

R-20 Status: C
Access of supervised subscribers to previously assigned features is never restricted.

R-21 Status: C
Assignment of new services does not prevent the supervision of a subscriber.

R-22 Status: C
The response time of the SOSM system, from the time an event is registered to the time action is taken, does not exceed 200 ms.

14.5.1.3 Supervision methods

R-23 Status: C[1]
The calling subscriber number identification should be requested if not present. ANI request should be given before the answer phase.

R-24 Status: NA
The electrical parameters of transmitted and received frequency signal conform to requirements for ANI signalling in the network.

14.5.1.4 Operational testing

R-25 Status: C
SOSM system hardware and software functional testing is carried out by commands from CP without interrupting system operations.

R-26 Status: C
Information about any malfunctions affecting operations of the system is transmitted to the CP.

14.5.1.5 System Security

R-27 Status: C
Unauthorized access to the SOSM system is prevented.

R-28 Status: C
Unauthorized intervention with SOSM operational process and SOSM-CP interworking is prevented.

R-29 Status: C
Any unauthorized attempt to access or intervene with the SOSM system is reported to the CP.

R-30 Status: C
No SOSM operations or activity is recorded into DMS MMP system logs.

[1]SOSM system does not request ANI independently. If ANI is required,
the appropriate office configuration must be performed. (For example in ISUP-line interworkings, proper provisioning should exist in ISUPSVC table for the corresponding ISUP trunk.)

14.5.1.6 System initialization and restarts

R-31 Status: C
In the case of emergency service disruptions and subsequent restart of the exchange, SOSM data is not restored, and the CP is informed of the event.

R-32 Status: C
Upon an exchange restart, SOSM is stopped and the appropriate message is sent to the CP.

R-33 Status: C
SOSM system initialization is included as a part of the exchange restart procedures. SOSM restart can be initiated by command from CP without disruption to exchange operations.

R-34 Status: C
Upon software upgrades from MMP to MMP, SOSM is stopped and an appropriate message is sent to CP. All dynamic data about MCL's and monitoring orders are cleared.

SOSM static data (data in SOSMMPC, SOSMTRK and SOSMPARM) is restored.

R-35 Status: NA
Acceptance of the SOSM functions will be agreed with the customer.

14.5.2 SOSM and CP Interface

14.5.2.1 Speech path information

R-36 Status: C
Call content is transmitted to CP via Monitoring Connecting Lines (MCL). Commands and Information messages are transmitted via X.25 links.

R-37 Status: C
MCLs are digital trunks provisioned for use only by the SOSM system, as shown in "Table 1 SOSM capacity" on page 56.

R-38 Status: C
The number of PCM groups can be from 1 to a maximum value as defined in "Table 1 SOSM capacity" on page 56.

R-39 Status: C
Digital trunks for speech path monitoring are PCM-30 trunks with transmission rate of 2048 Mbits/s as per ITU-T Recommendation G.732 with time slots of 64 kbps.

R-40 Status: C
Time Slots (TS) 1 -15 and 17-29 are used for speech path information. TS 16 is not used by CP equipment.

14.5.2.2 X.25 Communications

R-41 Status: NA
There are two acceptable variants for the X.25 communications interface. DMS MMP SOSM system supports both.

R-42 Status: C
Variant 1: TS 30-31 of the zero PCM-30 group are used for data transmission channels 1 and 2 respectively. For other PCM-30 groups, TS 30-31 are reserved for redundancy in case group zero is out of service for any reason.

R-43 Status: C
TS 30 is used for transmitting command from CP to SOSM, and responses to commands from SOSM to CP (Channel 1).

R-44 Status: C
TS 31 is used for transmission of call phase information of monitored calls.

R-45 Status: C
Variant 2: data transmission channels are formed of physical pairs of telephone cables, 0.7 mm in diameter with distance of up to 16 Km.

R-46 Status: C
Information interchange over data channels is performed via modems with 2 or 4 wire terminations.

R-47 Status: C
Information is transmitted in full duplex mode at a bit rate no less than 9600 bps.

R-48 Status: C
Data Transmission Channel (DTC) provides bit error rate of no more than 10^{-5} and no more than 10^{-3} white noise impact within the frequency band 0.3 to 3.4 KHz and SNR +12dB.

R-49 Status: C
Modem parameters and type should meet ITU-T recommendation for Data Transmission Equipment.

R-50 Status: C
DTCs' working order can be tested by the CP. If a DTC goes out of service during transmission, transmission is stopped and some of the un-transmitted data may be lost. Transmission begins again after the DTC is back in service.

R-51 Status: C
If secondary transmission links are available, when a trouble occurs on the channel in use, SOSM system automatically switches to the next available pair of channels.

14.5.3 Information exchange protocol in data transmission channel

R-52 Status: C
Data interchange protocol between SOSM and CP is done based on ITU-T Recommendation X.25.

R-53 Status: C
X.25 protocol contains the network, channel and physical layers. ITU-T V.24 interface is used for the physical layer.

R-54 Status: C
The communications protocol variable parameters setting for second and third layers is done in the appropriate DMS MMP tables.

R-55 Status: C
Values of the variable parameters will be agreed upon with the customer.

14.5.4 Agent Interactions

SOSM supports line-to-line, trunk-to-line and line-to-trunk calls only. Trunk-to-trunk calls at switches will not be monitored. The following items describe the type of SOSM call triggering when different agents are involved in a call:

- **Line - to - line :**

  Only IBN, BRI, V5.2(IBN) lines can be supervised subscribers. Only calls from/to IBN, BRI, V5.2(IBN) lines are supported by SOSM.

  Calling and called party DNs (Office code + DN Digits, excluding area code) are searched in the SOSM database. If either is found, the call will be monitored by SOSM system.

  The DN of the terminating line (Office code + DN Digits, excluding area code) will be searched into the database instead of dialled digits .

  For BRI subscribers, DN based monitoring is supported, which means only supervised DNs (MSNs) in the same loop are monitored. In order to monitor all agents in the BRI loop, an individual monitoring order should be requested for each DN on the loop.

  Please note that all calls originated from a BRI phone set, where no MSNs are defined on the BRI phone set, uses the primary DN of the loop. Thus it is strongly recommended to send monitoring order for the primary DN, as well as other DNs in the loop.

- **Trunk (ISUP/PRI)-to-line (IBN/V5.2(IBN)/BRI) :**

  Presence of calling party number is NOT checked in SOSM database.

  Called line DN (Office code + DN digits, excluding Area Code) is searched in SOSM Database, and if found, SOSM system monitors the call.

  The DN of the terminating line (Office code + DN Digits, excluding area code) will be searched into the database instead of dialled digits .

- **Line (IBN/V5.2(IBN)/BRI)-to-trunk (ISUP/PRI):**

  Calling party number is searched in SOSM database, and if found, the call is monitored.

  The dialled digits (WITH exit codes) are searched in the database, and if found, the call is monitored. For more information about exit codes, please refer to "2.8.3 Provisioning of SOSM specific parameters" on page 160.

- **Trunk-to-trunk :**

  No database searching is done since SOSM is designed for use at end offices.

- **Trunk(ISUP/PRI)-to-line(IBN/V5.2(IBN)/BRI) with call diversion to either line (IBN/V5.2(IBN)/BRI) or trunk (ISUP/PRI):**

  — Call diversion to trunk : The forwarded digits (taken from CFX table) is searched. If found, SOSM will monitor the call.

  — Call diversion to line : The forwarded subscriber's DN (Office code + DN digits, excluding Area Code) is searched in SOSM database, and if found, SOSM system monitors the call.

- **Line(IBN/V5.2(IBN)/BRI)-to-line with call diversion to either trunk(ISUP/PRI) or line (IBN/V5.2(IBN)/BRI):**

  — Call diversion to trunk : The forwarded digits (taken from CFX table) are searched into the database. If found, SOSM will monitor the call.

  — Call diversion to line : The forwarded subscriber's DN (Office code + DN digits, excluding Area Code) is searched in SOSM database, and if found, SOSM system monitors the call.

- **Huntgroup:**

  — *DNH configuration:* Since each member of huntgroup has its own DN, a member or the pilot can be assigned as target. Calls from the pilot/ member are monitored if assigned as target.

  If call is terminated to the pilot and the DN is busy, and the call is passed to another DN in the huntgroup, the call is monitored. Example scenario:

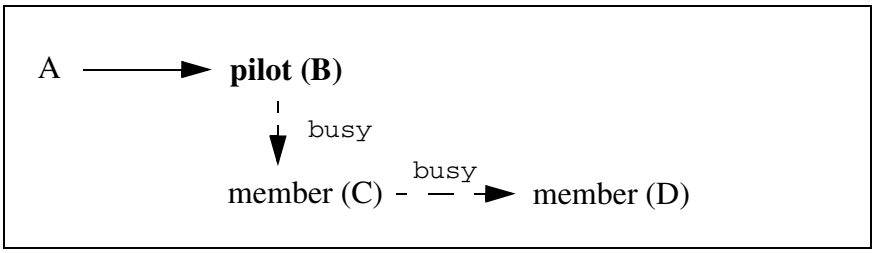


Table 2 Pilot is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	D	D
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

— *DLH/MLH configuration:* Since there is one DN, only the pilot DN can be assigned as target. Calls to/from any member or pilot of the huntgroup are monitored if the pilot DN of the huntgroup is target. Note that the pilot DN is sent to CP whether the call is originated or terminated by pilot/member.

— No usage message is sent to CP while hunting a member within the group.

Supervision of EBS lines are not supported by SOSM software.

SOSM supports inteactions with CEPT and BRI Supplemantary Services .

14.5.5 Format of control commands and messages (Channel 1)

Control commands and messages from CP to SOSM are transmitted using the data transmission link channel 1 (using direct connection or via modem).

The commands and response message (where applicable) are listed in the following table.

Table 3 Summary of Channel 1 commands and messages

Command	Response	Reference
Start of SOSM	- Confirmation (received/executed)	section 2.5.7.2 on page 68
Stop of SOSM	- Confirmation (received/executed)	section 2.5.7.3 on page 70
Password setting	- Confirmation (received/executed)	section 2.5.7.4 on page 71
Assignment of Monitoring Connecting Line (MCL) to group	- Confirmation (received/executed)	section 2.5.7.5 on page 73
Setting of objects for monitoring	- Confirmation (received/executed)	section 2.5.7.6 on page 76
Removal of the object of monitoring data.	- Confirmation (received/executed)	section 2.5.7.7 on page 85
Connection to voice path	- Confirmation (received/executed)	section 2.5.7.8 on page 88
Clearing of Monitoring Connecting Line	- Confirmation (received/executed)	section 2.5.7.9 on page 92
Excluding of Monitoring Connecting Line from group	- Confirmation (received/executed)	section 2.5.7.10 on page 96
Request for transmission of objects of monitoring data.	- Confirmation (received/executed) - Data on objects of monitoring	section 2.5.7.11 on page 98
Request for transmission of information about correspondence between MCLs and groups	- Confirmation (received/executed), - Information about correspondence between MCLs and groups	section 2.5.7.12 on page 102
Request for transmission of the list of Supplementary Services (SS)	- Confirmation (received/executed), - List of subscriber's supplementary services	section 2.5.7.13 on page 105
Interruption of messages sent upon the request for transmission of tables contents	- Confirmation (received/executed)	section 2.5.7.14 on page 107
Testing of data transmission channels	- Answering test message	section 2.5.7.15 on page 108

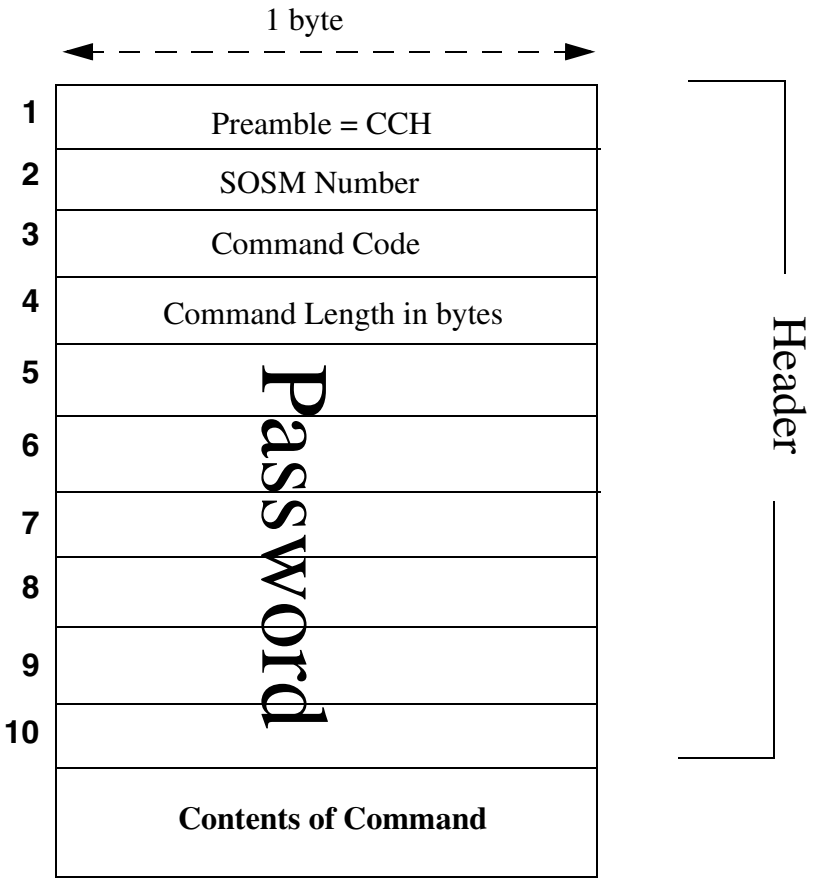
Command	Response	Reference
Objects of monitoring parameters change	- Confirmation (received/executed)	section 2.5.7.16 on page 109
Request for transmission of information about correspondence between exchange incoming group's name and it's conditional number	- Confirmation (received/executed), - Data about correspondence between conditional numbers of incoming groups and their real exchange names	section 2.5.7.17 on page 111
Request for exchange's SW version	- Confirmation (received/executed), Version of exchange's software	section 2.5.7.18 on page 112
	- Unauthorized access to the SOSM software	section 2.5.8.6 on page 121
	- Failure	section 2.5.8.1 on page 114
	- Exchange S/W restart.	section 2.5.8.2 on page 116

14.5.6 Format of CP to SOSM Control Messages

R-56 Status: C

The information field of control commands transmitted from CP to SOSM has the following format:

Figure 4 Format of CP to SOSM control message



First byte is a preamble and has identical value for all commands.

Second byte specifies the SOSM number of the corresponding exchange where the message will be sent.

Third byte defines command code.

Fourth byte defines the length (quantity of bytes) of the command content.

Bytes from fifth to tenth contain SOSM password. The password prevents unauthorized access to the SOSM system. The commands are executed only if the password in the command header is valid.

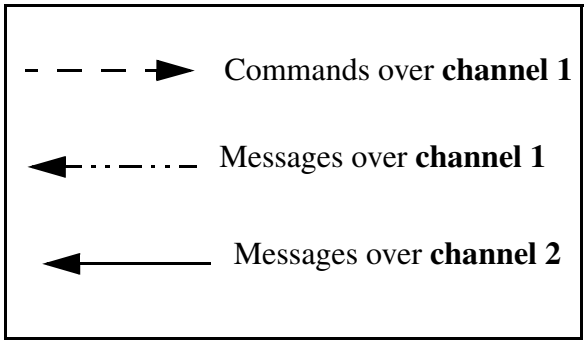
Note: *Initial password is hard-coded by SOSM developers in the SOSM software and reported to the customer.*

Command length and content is different for each command.

14.5.7 CP to SOSM Command Processing

The following sections describe the interactions between the Control Point and the SOSM system. For each command or call phase, the actions taken are described in detail, as well as Message Sequence Charts (MSC). **This activity handles all scenarios within the tests given in section APPENDIX** .

The conventions used in the MSCs are as follows:



14.5.7.1 Generic error handling

When a CP command is received, SOSM system first validates the command and then attempts to execute it.

If the command is properly validated a “confirmation of command reception” message is sent to the CP.

“code of command” field of the confirmation message contains the command code being handled, and the “attribute of command reception” field is set to “**command is received for execution - 00H**".

If the command is properly executed, “confirmation of command execution” message is sent to the CP with “code of command” field including the code of the command being handled. The “attribute of command execution” field is set to “**command executed successfully- 00H**".

14.5.7.1.1 Command reception error handling

Validation of a command includes syntax checking of each and every parameter in the command, as well as combinations of parameters. Syntax

checking is to ensure each parameter received is within the valid range and values. Combination checking ensures that all mandatory parameters within a given command are present.

On any received command, if the password received in command header is not valid, a negative acknowledgment is sent to CP in the form of a “confirmation of command reception” (No:7 NOK). The “Code of command” field is populated with the code of the command that failed. The “attribute of command reception” field is populated with :

— "i**nvalid password character - 15H**" if the password includes unsupported characters.

— "**password mismatch -18H**" if the password does not match system password.

In cases where all characters of the received password are within the supported range, if the password does not match with the system password, “unauthorized access to SOSM”(No:6) message is sent to the CP after sending "confirmation of reception" (No:7 NOK). The “code of access field” in "unauthorized access to SOSM" message includes “**access with wrong password** - **02H**". The message also includes the time at which the access violation occurred in the format **dd:hh:mm:ss** (day, hour, minutes, seconds).

If a command fails validation, a negative acknowledgment is sent to CP in the form of a “confirmation of command reception”(No:7 NOK). The “Code of command” field is populated with the code of the command that failed. The “attribute of command reception” field is populated with an error code.

The following errors and corresponding codes are used for validation failures:

- Incorrect Preamble: When the preamble in the command does not match the preset system preamble (CCH), code **"incorrect preamble’** with value **"01H"** is set.
- Incorrect SOSM Number: When SOSM number in the command header does not match SOSM system number, code **"incorrect sosm number"** with value **"02H"** is set.
- When the command code does not match any of the command codes defined in the specification, code **"invalid message code"** with value**"03H"** is set.
- If the command length (including header) exceeds the maximum message length supported by the system (45 Bytes), code **"message too long"** with value **"04H"** is set.
- If the command length specified in the header does not match the pre-defined command length (as defined in the specification), code **"incorrect message length"** with value **"05H"** is set.

- If the command code is not within the range of supported CP commands as specified in this document, code **"unsupported command"** with value **"06H"** is set.
- If the password specified in the header includes a character which is outside of the printable ASCII range (20H to FFH), code "**"invalid password character"** with value **"15H"** is set.
- If a command (except start SOSM) is received from CP while SOC SOSM0001 is in ON state, and SOSM system is inactive, code **"command out of sequence"** with value **"19H"** is set.
- If command is received during the DS dumping phase of image load of office or during TABXFR and preswact, "**dump restore in progress"** with value "1BH" is set.

Error codes specific to single commands are explained in more detail in the appropriate sections below. A complete list of command reception error codes is provided in "Table 109 Command reception result codes" on page 247 .

If a command fails validation, a rejection message is sent and no further action will be taken by the SOSM system (i.e the command is ignored).

Any command received from CP is ignored while SOC SOSM0001 is IDLE. DMS MMP does not respond to CP messages in this state.

In PRESWACT step of ONP, SOSM is stopped. The commands received are rejected with the reason of **"dump restore in progress"** until SWACT is completed. When SWACT is completed, restart message is sent to CP (Control Point).

14.5.7.1.2 Command execution error handling

If command execution fails, a negative acknowledgment is sent to CP in the form of a "confirmation of command execution". The "code of command" field is populated with the code of the command that failed to execute. The "attribute of command execution" field is populated with an appropriate error code.

For a complete list of error codes please refer to "Table 110 Command execution result codes" on page 248.

14.5.7.2 Start of SOSM (Command N1)

R-57 Status: C
Start of SOSM (command N1) is given by CP to initialize the SOSM system. The SOSM system validates the command, and activates SOSM.

The SOSM number provided in the command header is kept as the current SOSM number and is valid until the next system restart.

This command is expected to contain pre-defined SOSM Initial Password. The initial password begins to be valid again after:

- exchange's failure with loss of data, associated with SOSM operation
- in case of SOSM software restart
- in case of total exchange restart.

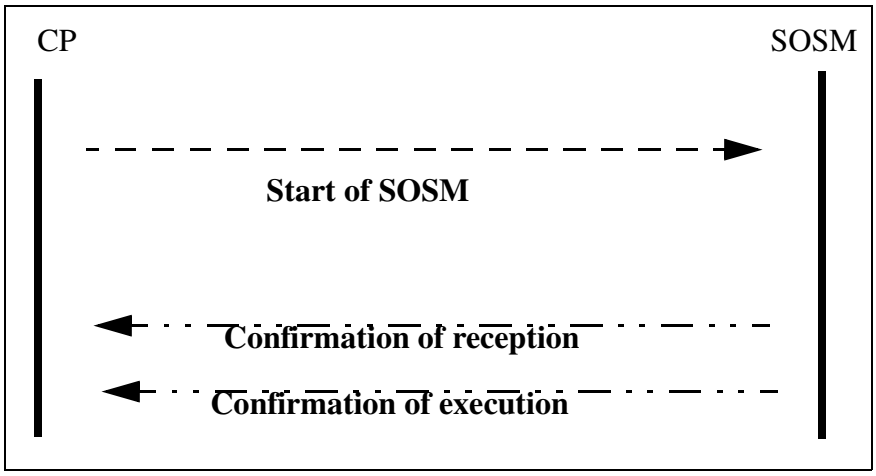
The command format is shown in the following figure.

Figure 5 Start of SOSM command

Code of Command= 01H.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 6 Start of SOSM scenario



Validation error checking:

If "Start of SOSM" command is received when SOSM has already been activated, the command is rejected and "Confirmation of command reception" message is sent to CP. The "attribute of command execution" field is set to code "**command out of sequence**" with value **19H**.

Execution error checking :

If "Start of SOSM" command can not be executed due to technical problems, “Confirmation of command execution” message is sent to CP with the “attribute of command execution” field is set as **"technical_problem - 66H".**

14.5.7.3 Stop of SOSM (Command N2)

R-58 Status: C

"Stop of SOSM" (command N2) is given by CP to stop the SOSM system.

All data related to SOSM operation are deleted and the initial password, set by SOSM developers, is set as the valid password.

Monitoring of all active calls that are under surveillance is stopped, and the MCLs connected to those calls are disconnected, and all data in MCL and monitoring order databases is cleared.

> ***Note:*** *NO INFORMATION IS SENT TO CP about the disconnection of the MCL’s, deactivation of monitoring or any further event in those calls during and after the execution of STOP SOSM command.*

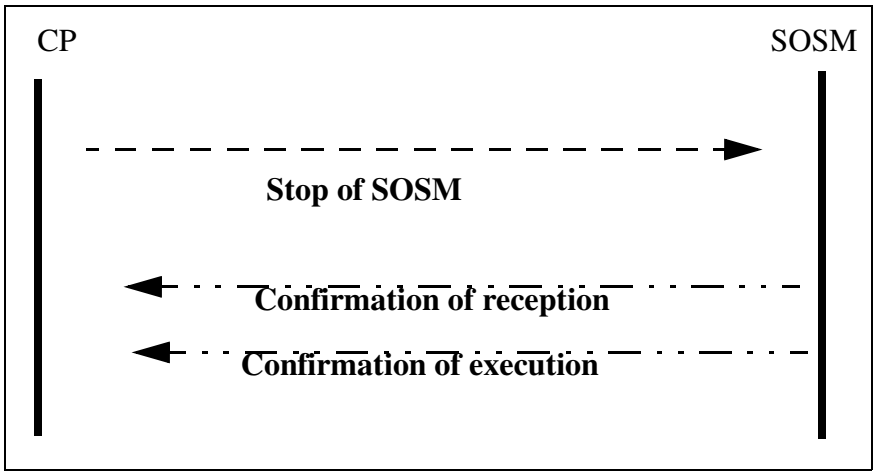
The command format is shown in Figure 7, "Stop of SOSM command".

Figure 7 Stop of SOSM command

Code of *Command* = 02H

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 8 Stop of SOSM



Validation error checking:

If the SOSM system has not been started, the command is rejected and "Confirmation of command execution" message is sent to CP. The "attribute of command execution" field is set to code "**command out of sequence**" with value **19H**.

14.5.7.4 Password setting (Command N3)

R-59 Status: C

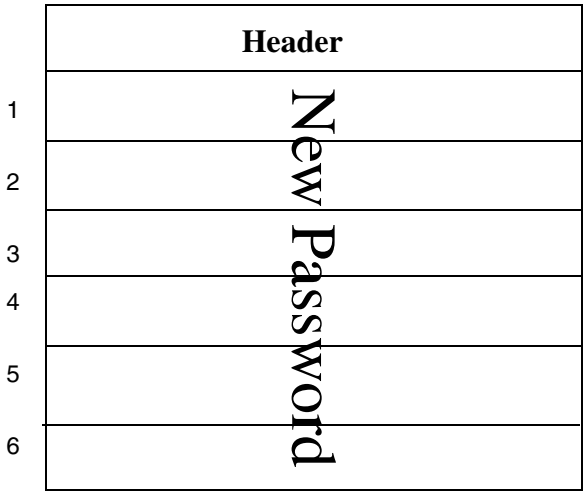
Password Setting (command N3) is sent by CP to set the system password.

This command sets the new password for SOSM operation. The password specified in the "new password" field replaces the current SOSM system password. Any subsequent command must contain the new password.

After a system restart or restart of SOSM, the password is set back to initial system password.

The command format is shown in "Figure 9 Password setting command" on page 72.

Figure 9 Password setting command

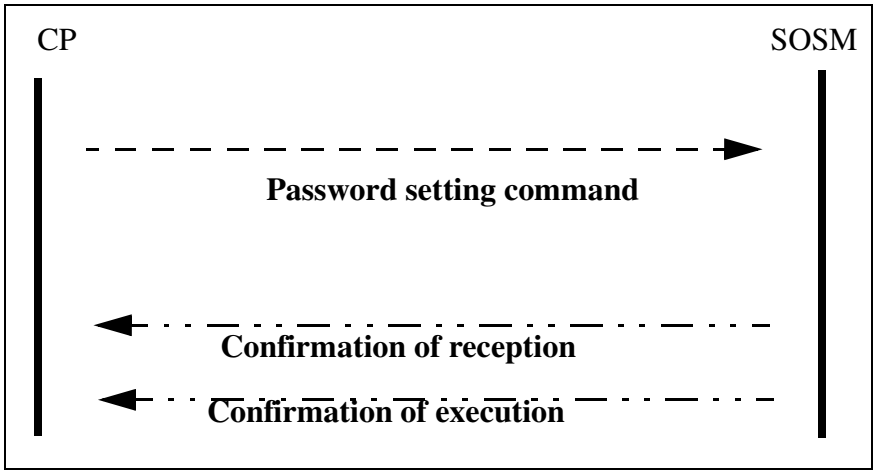


Code of *Command* = 03H

The "new password" parameter must be 6 bytes in length, each with a value within the ASCII printable character range (between **20H** to **FFH**).

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 10 Password setting command



Validation error checking:

If any of the following errors occur the command will be rejected. A "Confirmation of command reception" message is sent to CP. The "attribute of command reception" field is set as follows:

- If any of the new password bytes are outside of the valid PRINTABLE ASCII range of **20H** to **FFH**, code **"invalid password character"** is set with value **"15H"** .
- As in all other commands, password setting command must include a valid “current system password”, which most of the time would be the “initial system password”. Any mismatch will be handled as described in the password checking discussion in “2.5.7.1.1 Command reception error handling” on page 66.

14.5.7.5 Assignment of MCL to group (Command N4)

R-60 Status: C

Assignment of Monitoring Line to Group (command N4) is sent by CP to create and configure MCL groups.

CP defines Monitoring Connecting Lines (MCLs) under a group number. The quantity of MCLs in a group can be from 1 up to the maximum quantity of MCLs between SOSM and CP.

Maximum quantity of MCL groups is also determined by the maximum number of MCLs between SOSM and CP.

The command format is shown in “Figure 11 Assignment of monitoring connecting line to group.” on page 73.

Figure 11 Assignment of monitoring connecting line to group.

	Header
1	MCL group number
2	MCL group type
3	MCL-A number
4	MCL-B number

Code of *Command* = 04H

The most significant three bits (the most significant bit is on the left) of the MCL-A/B number specify the number of the primary PCM-30 group, and the remaining five bits specify the number of the PCM channel (Time Slot) within this primary PCM-30 group.

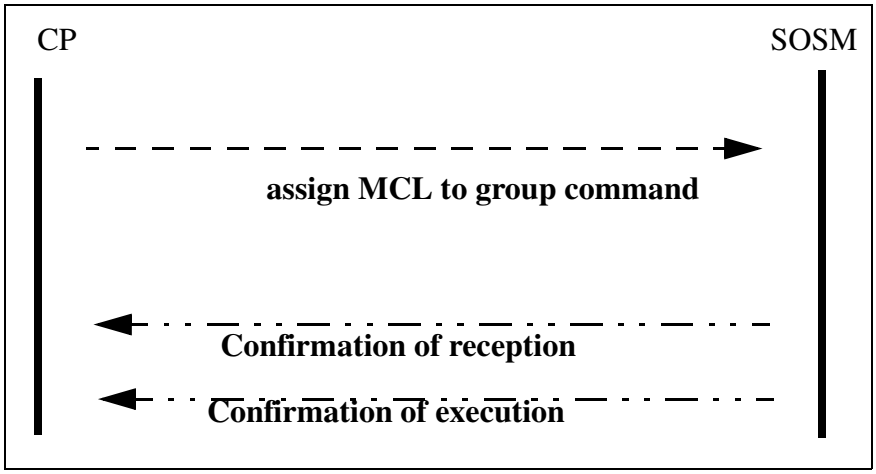
MCL group type:

01H: group for subscribers A and B joint monitoring

11H: group for separate monitoring

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 12 Assign MCL to group command



Requirements:

- Maximum number of MCL groups can not exceed the maximum number of MCLs
- An MCL can not exist in more than one group
- One group may contain MCLs of the same group type, mixed groups (separate and combined) of MCLs are not allowed.
- If Command N4 is received to add MCL's into a group of type "11H - group for separate monitoring", MCLA and MCLB numbers received in the command must correspond to MCL's on the same PCM-30 group.

A new MCL can be added into the MCL database if the following criteria are met.

- MCL group number, MCLA/MCLB number(s) should be within the allowed ranges.
- Number of MCL's and number of MCL groups should remain within the allowed ranges upon execution of the received command.
- If the MCL group received in the message already exists, the group type in the message should match with the existing MCL group's type.

- MCL number(s) should not exist within any of the predefined MCL groups.
- If subject MCL group is for separate monitoring, MCLA and MCLB must be on the same PCM-30.

If the MCL group number does not exist, and the MCLs do not exist in any other group, a new group is created and the new MCLs are stored.

Validation error checking:

If any of the following errors occur, the command will be rejected. A "Confirmation of command reception" message is sent to CP. The "attribute of command reception" field is set as follows:

- If the MCL group number value is less than 1 or exceeds the Maximum Number of MCLs (currently 224), code **"invalid MCL group number"** is set with value **"08H"** .
- If the MCL group type field value is not one of 01H (combined) or 11H (separate), code **"invalid MCL group type"** is set with value **"09H"** .
- If in the MCL number parameter(s), least significant five bits (CL number) do not correspond to a number between 1 and 28, code **"invalid MCL number"** is set with value **"0AH"** .

Execution error checking :

If any of the following errors occur, command execution will fail and the command will be rejected. A "Confirmation of command execution" message is sent to CP. The "attribute of command execution" field is set as follows:

- If MCLA (or MCLB in separate monitoring category) already exists in the database, code "**duplicate MCL number**" is set with value **51H**.
- If in the MCL number parameter(s), most significant three bits do not correspond to a valid trunk group dedicated for SOSM usage, in other words, if the MCL number refers to a PCM-30 group which does not exist in table SOSMTRK, code "**missing PCM-30 group data"** with value "**50H**" is set.
- If the MCL group type is "joint monitoring" and MCL-B field is not either FFH or equal to MCL-A, code **"Invalid MCL B For Group"** is set with value**"5BH"**.
- If the MCL group type is "separate monitoring" and MCL-B is equal to MCL-A, code **"Invalid MCL B For Group"** is set with value **"5BH"**.
- If the MCL group type is "separate monitoring", but MCL-A and MCL-B are not on the same primary PCM-30 group, code **"invalid MCL B for group"** is set with value **5BH**.

- If member_id for MCL does not exist in table TRKMEM, code "**missing trkmem datafill**" with value **53H** is returned and command is rejected.
- If the MCL group to which the MCL is being added, does not match the MCL group type (separate or combined) previously defined for that group, code "**wrong mcl type for group**" with value **52H** is returned and command is rejected.
- If mcl database is being transferred during receiving the command, code **"mcl transfer in progress"** with value **64H** is returned and command is rejected.
- If any other error occurs, code "**invalid parameter"** with value **43H** is returned and command is rejected.

14.5.7.6 Setting an object for monitoring (Command N5)

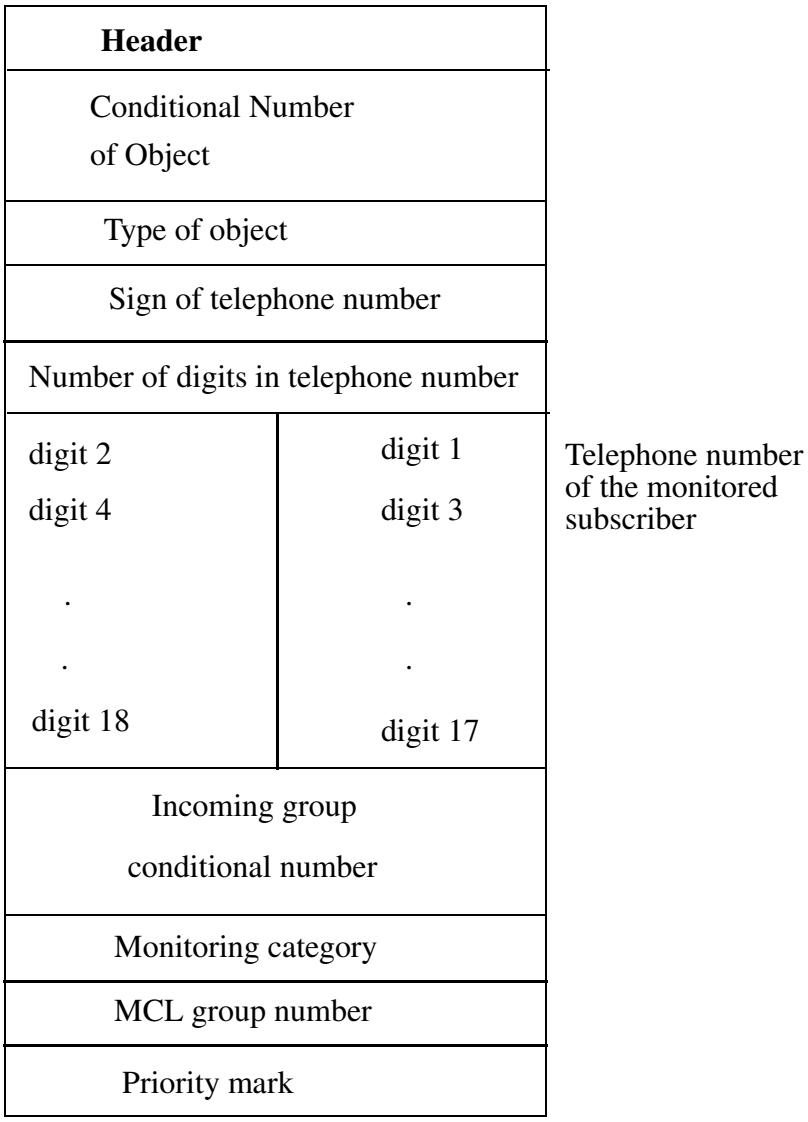
R-61 Status: PC

Setting of Objects for Monitoring (command N5) is sent from the CP to add a monitored subscriber to the database of observed objects.

This command is used to create an object to be supervised with certain properties. The data related to this object is written to the appropriate SOSM database.

The command format is shown in "Figure 13 Setting of objects for monitoring." on page 77.

Figure 13 Setting of objects for monitoring.



Code of *Command* = 05H.

Conditional number of object is unique for each object and is assigned by CP to all objects being monitored. Its value can be within 0000H-FFFEH for "Command N5 - Setting an object for monitoring". The same object may not have several conditional numbers.

"Conditional number of object" parameter might be set as FFFFH in some other CP commands (Please refer to Section “2.5.7.11 Request object data (Command N10)” on page 98.) and Command N8-clearing of MCL (section 2.5.7.9).

FFFFH is not a valid value for "Conditional number of object" in Command N5-setting a monitoring object, Command N6-removal of a monitoring object (section 2.5.7.7), Command N7-connect to voice path (section 2.5.7.8), and Command N15-change a monitoring object (section 2.5.7.16). These commands will be rejected if "Conditional number of object" is received as FFFFH.

Type of object field has following values:

01H:subscriber of present exchange:

This type of object has complete telephone number. Monitoring of IBN and BRI agents are supported by SOSM.

For BRI agents, MSN to be monitored must be given (i.e supervising primary DN or any other DN on the loop is not enough to monitor all calls originating/terminating from/to the loop). In order to provide full monitoring of the BRI loop, all MSNs on the loop must be supervised individually.

02H: telephone network subscriber with complete telephone number;

5-7 digits for local network subscribers

7 digits for present zonal network subscribers

10 digits for other zone subscribers

up to 15 digits for another country’s subscribers

SOSM triggers monitoring for these objects only in line-to-trunk calls where the specified network number is dialled.

12H: telephone network subscriber with incomplete telephone number

Insufficient digits of incomplete numbers are filled by FH

SOSM triggers monitoring for these objects only in line-to-trunk calls where the specified incomplete network number is dialled.

Unsupported:

“03H: group of incoming connecting lines or channels;”

FFH: no value; this value is not accepted as a valid value in Command N5, and the command is rejected if FFH is received within **Type of object**.

FFH value is valid for "Type of Object" parameter only in Command N10. (Please refer to Section “2.5.7.11 Request object data (Command N10)” on page 98.).

> ***Note:*** *In the tables of supervised objects, complete and incomplete telephone numbers coinciding with appropriate first digits can not appear at the same time. After writing this object in the data base if another object with coinciding appropriate first digits (whether more generic or not) is received for recording to the database, it is rejected and this is reported to CP with an appropriate unsuccessful execution code.*
> *This is also valid for network complete numbers.*
> *For example, if the database contains an object of type 12H (or 02H) with digits 216, and subsequently a new object of the type 12H (or 02H) with digits 216329 is wanted to be added, this new object is rejected. If another new object of type 12H (or 02H) and with digits 21 is wanted to be added, this object is also rejected. An object with digits 212 of these types will be accepted.*

Sign of telephone number field has following values:

01H: present exchange subscriber’s telephone number.

02H: local telephone network subscriber’s telephone number (local number).

03H: present zonal telephone network subscriber’s telephone number (zonal number).

04H: another zonal telephone network subscriber’s telephone number (toll number).

05H: another country subscriber’s telephone number (international number).

06H: special services local communication inquiry, informational services telephone numbers or toll and international communication order and inquiry services numeration.

FFH: is used in case of monitoring by connecting lines group number or channels number.

Number of digits in telephone number gives the quantity of the complete digits in the “monitored subscriber’s telephone number” field.

Monitored subscriber telephone number can be complete or incomplete. It can also be local communication special services and inquiry- informational services telephone numbers or toll and international communication order and inquiry services numeration.

> ***Note:*** *According to LONIIS specification, National and international telephone numbers are given with indexes of outlet to urban, toll and international networks and these numbers are corresponding to information dialled by subscriber.*
> *The DMS MMP SOSM expects exit codes in the telephone number. When checking a dialled number in the SOSM subscriber database, the exit codes are NOT removed before searching.*
> *SOSM will not monitor a call FROM a network sosm subscriber, as per specification.*

Unsupported:
Incoming group conditional number DMS MMP does not support this parameter in Command N5, and rejects its all values, but FFFFH.

Category of monitoring defines whether the supervision is performed on a complete or statistical basis. In statistical monitoring a MCL is not connected to speech path where in the complete monitoring case supervised calls are transmitted to CP over the connected MCL.

01H: complete monitoring (joined monitoring).

11H: complete monitoring (separate monitoring).

02H: statistical monitoring.

MCL group number assigns a group of MCLs to a supervised object with complete category of monitoring. It takes the values 01H(1)-E0H (224)and is equal to FFH in case of statistical monitoring.

Priority mark is valid for the complete monitoring category and defines the priority class of the monitored object.

01H: priority object for monitoring.

02H: usual object for monitoring.

FFH: only for statistical monitoring.

“If a call under surveillance -due to a monitoring object with priority class of 01H- can not allocate a free MCL, since all MCLs in the group are busy, another MCL in this group which is used by any monitored call with priority class of 02H is released and connected to that call with 01H priority.” Figure

14, "Clear MCL On Priority" illustrates the messaging between SOSM and CP for this case.

Figure 14 Clear MCL On Priority

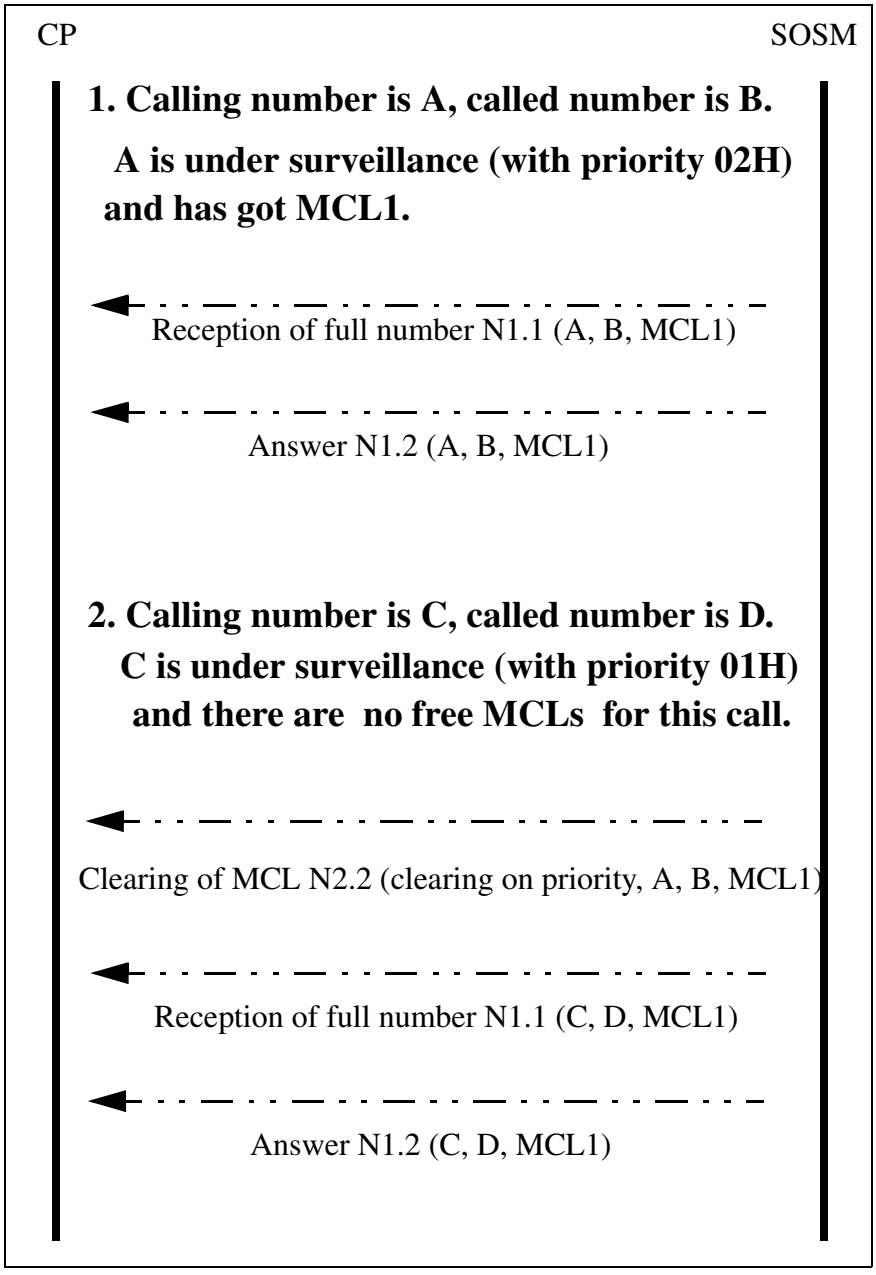
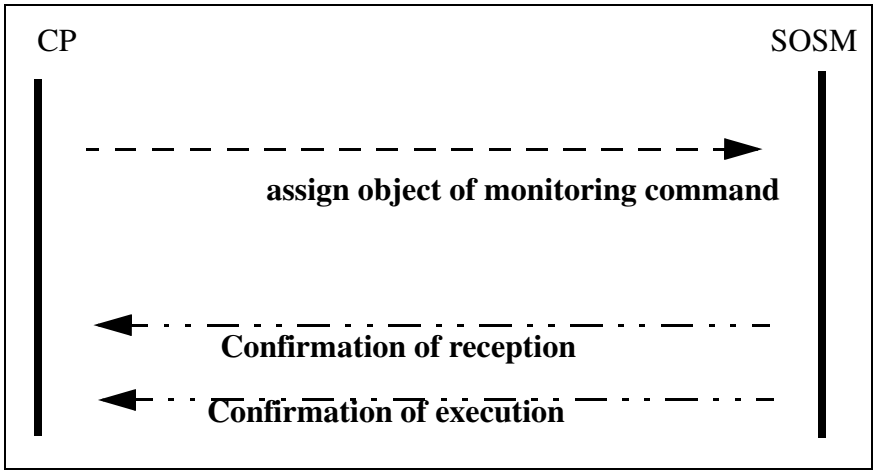


Figure 15, "Assign object of monitoring command" illustrates the messaging between SOSM and CP for handling this command.

Figure 15 Assign object of monitoring command



Those calls, matching criteria within the new monitoring object, and which are active when this command is received by SOSM, are not monitored. Monitoring of the corresponding subscribers takes place in their succeeding calls.

Validation error checking:

If any of the following errors exist, the command will be rejected. A "Confirmation of command reception" message is sent to CP. The "attribute of command reception" field is set as follows:

- if the "conditional number of object" is not within 0H-FFFEH, code "**invalid conditional number**" is set with value "**1AH**"
- if the "type of object" parameter is not one of {01H, 02H, 03H, 12H}, code **"invalid object type"** is set with value **"0BH"** .
- if the "sign of telephone number" parameter is not one of {01H - 06H}, code **"invalid sign of telephone number"** is set with value **"0CH"** .
- if the "number of digits" is less than one or greater than 18, code **"invalid number of digits"** is set with value **"12H"** .
- if the "category of monitoring" is not one of {01H, 02H, 11H}, code **"invalid category of monitoring"** is set with value **"0FH"** .
- if the "MCL group number" is not FFH or not in the range 01H- maximum number of MCLs, code **"invalid MCL group number"** is set with value **"08H"** .

- if the “priority mark” is not one of {01H, 02H, FFH}, code **"invalid priority code"** is set with value **"10H" .**
- if the “dn digits” are not between 0-9, # (0EH) or * (0DH), **"invalid digit"** is set with value **"11H"**

Execution error checking :

If any of the following errors occur, command execution will fail and the command will be rejected. A “Confirmation of command execution” message is sent to CP. The “attribute of command execution” field is set as follows:

- If the “conditional number of object” already exists in the database, code “**duplicate conditional number of object**” is set with value **42H**.
- if the “type of object” parameter is “incoming group of connecting lines” (03H), code "**unsupported parameter**" with value **5EH** is set, not for toll exchange.
- If the MCL group of the object is not found in the MCL database, code “**mcl info not found**” is set with value **4BH**
- If “monitored subscriber telephone number” is non-unique, this implies that an object of this type with this telephone number already exists in the database. The “attribute of command execution” field is set to code “**non-unique object”** with code **44H**.
- If the “type of object” is “subscriber of present exchange”, and the specified telephone number does not exist in the exchange, the “attribute of command execution” field is set to code “**invalid dn for exchange**” with value **58H**
- If the “type of object” is “subscriber of present exchange”, and if the specified telephone number does not correspond to an IBN, V5.2(IBN) or ETSI BRI agent, “attribute of command execution” field is set to code “**unsupported agent type**” with value **5AH**.
- If the maximum number of objects of the specified type is already provisioned in the exchange (i.e. there are 1024 network or 1024 present subscriber objects in the database), code “**maximum number of objects exceeded**” with value **4FH** is set.
- If the “category of monitoring” and the MCL group type do not match, code “**wrong mcl type for group”** with value **52H** is set.
- If the “category of monitoring” and the "priority mark" do not match, code “**priority code mismatch**” with value **5CH** is set.
- If the “number of digits” parameter does not match the actual number of digits in the “telephone number” parameter (actual number is determined by counting digits until an FFH is reached), code **"invalid number of digits"** is set with value **4DH**.

Note: *"01H" and "02H" values of "priority mark" are valid for combined (01H) and separate (11H) monitoring. "FFH" value of "priority mark" is valid only for statistical monitoring (02H).*

- If the “type of object” and “sign of telephone number” do not form a valid combination, code **"type and sign mismatch"** is set with value **5DH**.

  The following table list the valid combinations:

Table 4 Valid object type and sign of telephone number combinations

Object Type	Sign of Telephone Number
Present Exchange (01H)	Present exchange subscriber (01H) Special services number (06H)
Network subscriber with complete number (02H)	All but “present exchange subscriber” (01H) or FFH
Network subscriber with incomplete number (12H)	All but “present exchange subscriber” (01H)
Group of incoming lines (03H)[a]	FFH only, **Unsupported**

a. not supported in DMS MMP

- If “number of digits” is not valid for “type of object” and the “sign of telephone number”, code **"invalid number of digits"** is set with value "**4DH**".

  Valid number of digits for supported "type of object" and "sign of telephone number" combinations are given in Table 5, “Valid number of digits per object type and sign of telephone number,” on page 84

Table 5 Valid number of digits per object type and sign of telephone number[a]

Type of Object	Sign of Telephone Number	Number of digits
Present Exchange (01H)	Present exchange subscriber (01H)	5-7
	special services (06H)	>1

Table 5 Valid number of digits per object type and sign of telephone number[a]

Type of Object	Sign of Telephone Number	Number of digits
Network subscriber with complete number (02H)	Local number (02H)	5-7
	Zonal number (03H)	toll exit code + zonal exit code + 7
	Toll number (04H)	toll exit code + 10
	International number (05H)	toll exit code + international exit code + up to 15
	special services (06H)	>1
Network subscriber with incomplete number (12H)	Not “Present exchange”	>1 or =1
Group of incoming lines (03H)[b]	FFH	0

a. Toll exit code, zonal exit code and international exit codes are provisionable values. Default values are 8 for toll exit code, 2 for zonal exit code and 10 for international exit code. Detailed information about provisioning of these values is given in “2.8.3 Provisioning of SOSM specific parameters” on page 160.
b. not supported

- If "incoming group conditional number" is not "FFFFH", code "**unsupported parm**" is set with value **5EH**.
- If "mcl group number" is specified (other than FFH) for a statistical monitoring, "**invalid mcl group**" is set with value **49H**.
- If "mcl group number" is specified as FFH for non-statistical monitoring, "**invalid mcl group**" is set with value **49H**.
- If object database is being transferred during receiving the command, **"object transfer in progress"** is set with value **63H**.
- If any other failure occurs, code “**command failed**” with value **FFH** is returned.

14.5.7.7 Remove monitored object (Command N6)

R-62 Status: PC[1]

Removal of the Object from Monitoring (command N6) is sent from CP to remove an object of monitoring from the database.

[1]Conditional number of incoming group field is not supported in DMS MMP

Data about the monitored object is removed from the SOSM database by issuing this command. If at the given moment an object with complete monitoring category is under monitoring, MCL connected to this object is cleared.

Figure 16 Removal of the object from monitoring

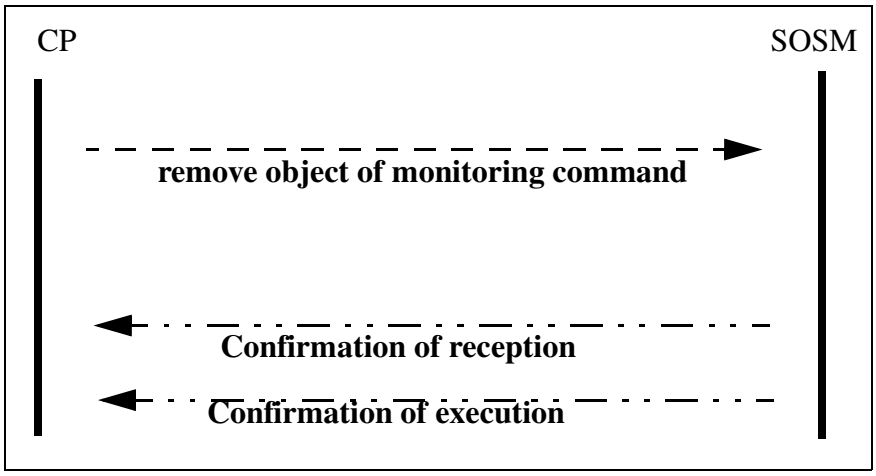
Header		
Conditional Number of Object		
Type of Object		
Sign of telephone number		
Number of digits in telephone number		
digit 2 digit 4 . digit 18	digit 1 digit 3 . digit 17	Telephone number of the monitored subscriber
Conditional number of incoming groups (unsupported)		

Code of *Command* = 06H.

Descriptions of the fields in this command are the same as in “Figure 13 Setting of objects for monitoring.” on page 77.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 17 Remove object of monitoring command



Validation error checking:

Please refer to the validation error checking of the relevant parameters in section “2.5.7.6 Setting an object for monitoring (Command N5)” on page 76 for validation of the parameters in this command.

Execution error checking :

For errors related to the combinations of parameters, digit numbers etc. please refer to section “2.5.7.6 Setting an object for monitoring (Command N5)” on page 76.

- If the object specified in the command is not found in the monitored subscribers database, the command is rejected. The “attribute of command execution” field is set to code “**object not found**” with code **45H**.
- if the “sign of telephone number” parameter does not match the same parameter for the object in the database, code “**sign of dn mismatch”** with value **56H is set,** and the command is rejected.
- if the “telephone number” parameter does not match the same parameter in the object database, code “**digits mismatch”** with value **55H** is set and command is rejected.
- if the “type of object” parameter does not match the same parameter in the object database, code “**object type mismatch”** with value **54H** is set and the command is rejected.
- amount of digits in the “telephone number” parameter does not match the the “Number of digits in telephone number” parameter in the message, “**digits mismatch”** with value **55H** is set and command is rejected.
- If the "conditional number of incoming group" is received with a value but FFFFH, command is rejected with the "**unsupported parm-5EH**" code.

- If object database is being transferred during receiving the command, command is rejected with the **"object transfer in progress-63H".**

14.5.7.8 Connect to voice path (Command N7)

R-63 Status: C

Connection to Voice Path (command N7) is sent from CP to request an explicit connection of MCL to a statistically monitored call.

This command connects an MCL to the speech path defined by the “Number of call” field.

This command can be executed before answer (during ring).

Execution of this command is performed for supervised subscribers with:

- Statistical monitoring category: In this case MCL connection is performed using the MCL group’s number given in the command. Monitoring category of the **call** is set to complete. Priority of MCL connection -in the **call-** is set as 01H.
- Complete monitoring category: For this category ‘Connection to voice path” command is used:
  - — If earlier connected MCL had been released due to “Clearing of MCL” command or its MCL had been connected to a high priority call.
  - — If no MCL had been found during connection of subscribers.

If free MCL cannot be found during the execution of this command, an MCL in the group -which is used for a low priority call- is disconnected, and it is used for the call identified in this command.

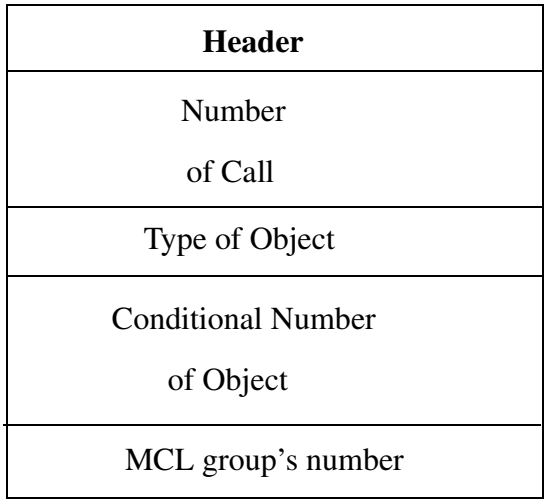
For the complete monitoring category case “MCL group’s number” field is ignored and connection is performed using MCL group defined in “Setting of objects for monitoring” command.

"Command N7-Connect to voice path" does not change the category of monitoring object which is defined by “Command N5-Setting of objects for monitoring". For subscribers supervised with statistical monitoring category, this command connects voice path only for the current active call.

Number of MCL (MCL-A in joint monitoring) to be connected is transmitted to CP in message “MCL’s connection” (N2.1).

The format of this command is shown in “Figure 18 Connection to voice path” on page 89.

Figure 18 Connection to voice path



Code of Command = 07H

Number of call is assigned by DMS MMP exchange for every monitored connection (either incoming or outgoing call). This number is unique for each monitored call, and varies from 0000H up to FFFFH. When it reaches FFFFH it returns again to 0000H.

Other fields correspond to the definitions given for "Setting of objects for monitoring" command.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

This command related call scenarios and call messages are:

1. A is under surveilance as statistical. A calls B. B answers. MCL of joint group is connected to this call with the command No.7 and then call is completed. The messages are:

Table 6 A is under surveilance as statistical.

	1.1	**1.2**	**2.1**	**1.3**
Calling DN	A	A	A	A
Called DN	B	B	B	B
SOSM Call #	1	1	1	1
Attribute of choice	02	02	02	02

	1.1	1.2	2.1	1.3
Parameters of connection	1C	1C	1C	1C
MCL #	#FF	#FF	**1**	1
Code of operation	#FF	#FF	**00**	**05**
Priority	#FF	#FF	#FF	#FF

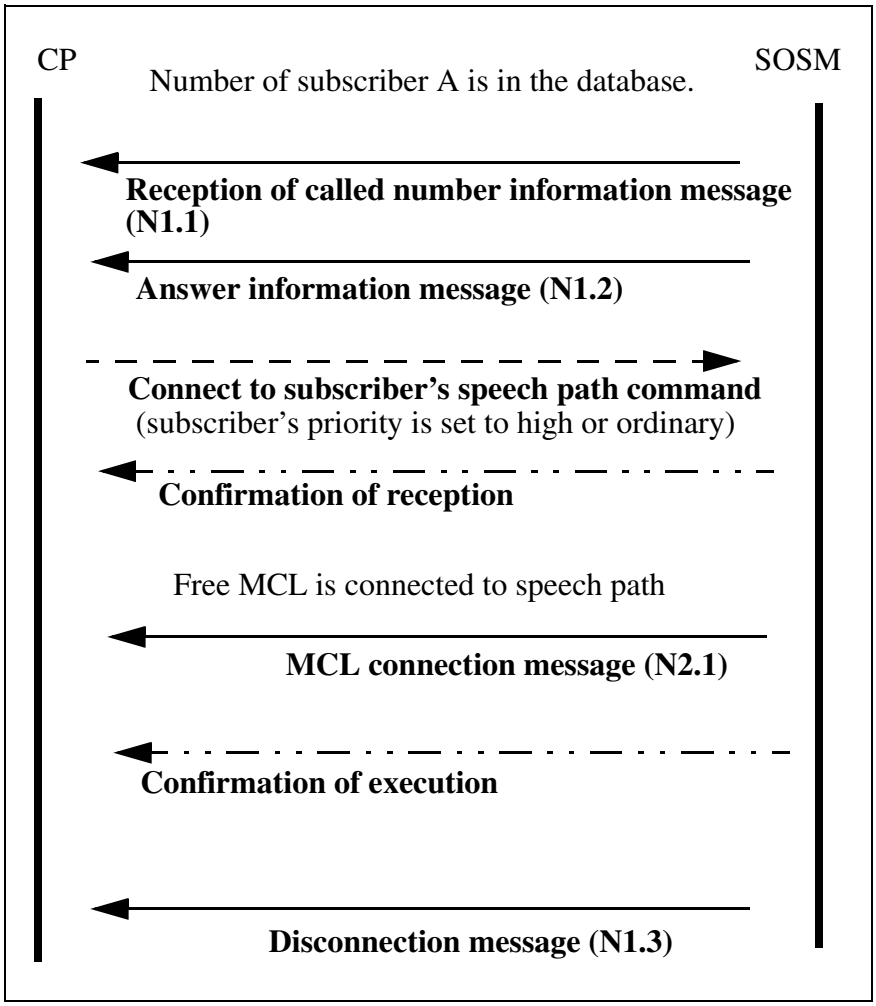
2. A is under surveilance as joint. A calls B. B answers. The MCL connection in the call is disconnected due to priority and then new MCL is connected to this call with the command No.7 *(new MCL is taken from MCL group in database of A line. The MCL information in the command No.7 is ignored)* and then call is completed. The SOSM callp messages for this call are:

Table 7 A is under surveilance as joint

	1.1	1.2	2.2	2.1	1.3
Calling DN	A	A	A	A	A
Called DN	B	B	B	B	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C
MCL #	1	1	1	**2 (new MCL)**	**2**
Code of operation	00	00	**02**	**00**	**05**
Priority	2	2	2	2	2

As you seen in tables above, MCL and Code of operation informations are only updated in the message 2.1 (MCL connection).

Figure 19 Connect to voice path command



Validation error checking:

Please refer to the validation error checking of the relevant parameters in section "2.5.7.5 Assignment of MCL to group (Command N4)" on page 73 and section "2.5.7.6 Setting an object for monitoring (Command N5)" on page 76 for validation of the parameters in this command.

Execution error checking :

If any of the following error conditions occur, the command is rejected and the specified error code is set in the confirmation message:

- if the "call number" field corresponds to a call which no longer exists (i.e. disconnection occurred), the "attribute of command execution" field is set to "**invalid call number**" code, with value **46H**.

- if the “conditional number of object” field does not match the object monitored in the specified call, the “attribute of command execution” field is set to “**invalid object number**” code with value **47H**.
- if the “type of object” field does not match the type of monitored object involved in the specified call, the “attribute of command execution” field is set to “**invalid object type**” code with value **48H**.
- If the category of monitoring is statistical and MCL group number is greater than 224 then code **"invalid MCL group"** with value **"49H"** is set.
- if the “MCL group number” field specifies an MCL group which does not exist, and if the value of "**category of monitoring**" parameter of the object in database is "**02H- statistical**", the “attribute of command execution” field is set to “**invalid MCL group number**” code with value **49H**.

  Note: If category of the monitoring is complete (either combined or seperate), MCLs of the group specified in the object are used. *MCL group received in the command is ignored even if it is invalid (i.e MCL group greater than 224 or inexisting MCL group).*
- if the call specified in “call number” is already connected to an MCL, code “**call already monitored**” is set with value **4EH**.
- if the MCL is not present in the given group, code “**mcl info not found**” with value **4BH** is set.
- if the connect command is given while a call is ON HOLD, code “**command out of sequence**” with value **4CH** is set.
- If MCL connection cannot be done because of the technical problem in PDTC, code **"sosm command failed"** with value **"FFH"** is set.

14.5.7.9 Clearing of MCL (Command N8)

R-64 Status: C

Clearing of Monitoring Connecting Line (command N8) is sent from CP to request disconnection of an MCL from a call.

This command clears a selected connection between SOSM and CP by force. If parameters in the bytes from 1 up to 5 are given then MCL occupied by present connection is cleared. If only MCL-A (MCL-B number is equal to FFH for joint monitoring) is given (bytes from 1 up to 5 are filled with FFH) then this MCL is cleared.

Format of this command is given in “Figure 20 Clearing of monitoring connecting line” on page 93.

Messages about further phases of monitored call should be transmitted to CP after command Clearing of MCL is sent to SOSM, as in a statistically monitored call.

Figure 20 Clearing of monitoring connecting line

Header
Number of Call
Type of Object
Conditional Number of Object
MCL-A number
MCL-B number

Code of *Command* = 08H

Number of call is the number of a call among incoming and outgoing calls.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

This command related call scenarios and call messages are:

1. A is under surveilance as joint. A calls B. B answers. MCL connection in the call is disconnected with the command No.8 and then call is completed. The messages are:

Table 8 A is under surveilance as joint.

	1.1	1.2	2.2	1.3
Calling DN	A	A	A	A
Called DN	B	B	B	B
SOSM Call #	1	1	1	1
Attribute of choice	01	01	01	01

	1.1	1.2	2.2	1.3
Parameters of connection	1C	1C	1C	1C
MCL #	1	1	1	**#FF**
Code of operation	00	00	**01**	**05**
Priority	2	2	2	2

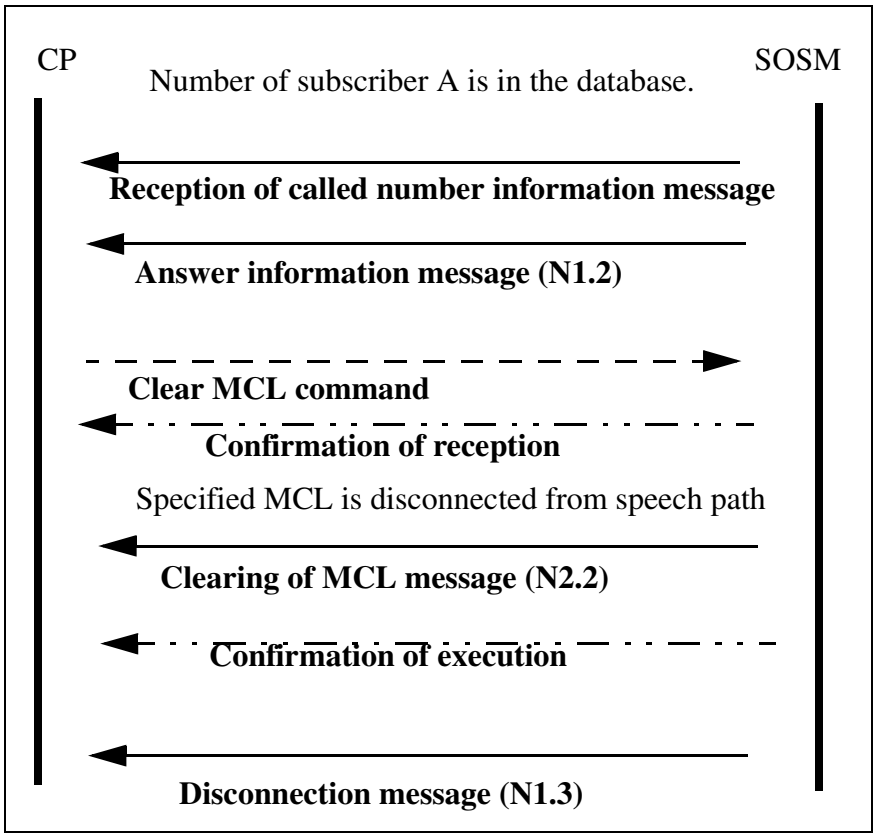
2. A is under surveilance as statistical. A calls B. B answers. The MCL connection is connected to the call with the command No.7 and then MCL connection is disconnected from this call with the command No.8 and then call is completed. The SOSM callp messages for this call are:

Table 9 A is under surveilance as statistical

	1.1	1.2	2.1	2.2	1.3
Calling DN	A	A	A	A	A
Called DN	B	B	B	B	B
SOSM Call #	1	1	1	1	1
Attribute of choice	02	02	02	02	02
Parameters of connection	1C	1C	1C	1C	1C
MCL #	#FF	#FF	**1**	**1**	**#FF**
Code of operation	#FF	#FF	**00**	**01**	**05**
Priority	#FF	#FF	#FF	#FF	#FF

As you seen in tables above, Code of operation information is only updated in the message 2.2 (Clearing of MCL message).

Figure 21 Clearing of MCL command



Validation error checking:

Please refer to the validation error checking of the relevant parameters in section “2.5.7.5 Assignment of MCL to group (Command N4)” on page 73 and section “2.5.7.6 Setting an object for monitoring (Command N5)” on page 76 for validation of the parameters in this command.

Execution error checking :

If any of the following error conditions occur, the command is rejected and the specified error code is set in the confirmation message:

- if the “call number” field is specified and corresponds to a call which no longer exists (i.e. disconnection occurred), the “attribute of command execution” field is set to “**invalid call number**” code, with value **46H**.
- if the “conditional number of object” field is specified and does not match the object monitored in the specified call, the “attribute of command execution” field is set to “**invalid object number**” code with value **47H**.

- if the "type of object" field is specified and does not match the type of monitored object involved in the specified call, the "attribute of command execution" field is set to "**object type mismatch**" code with value **54H**.
- if the MCL number(s) specified are not currently connected to a call, code "**invalid mcl number**" is set with value **4AH**.
- if at the time the command is given the specified call is not connected to an MCL, code "**command out of sequence**" with value **4CH** is set.

14.5.7.10 Exclude MCL command (Command N9)

R-65 Status: C

Excluding of MCL out of Group (command N9) is sent from CP to request the removal of an MCL from an MCL group.

Parameters of this command are the same as for command "Assignment of MCL to group". In case of joint monitoring one MCL (MCL-A) is excluded out of group. MCL-B has the value equal to MCL-A or FFH. In the case of Separate monitoring, two MCLs are deleted from the specified group.

MCL A (and B if not combined) are removed from specified group. If there are no MCLs left in the group, the MCL group is removed as well.

Note: *The MCL numbers in the exclude mcl command* ***MUST*** *match the numbers that were given in the Add MCL command.*
For example, if in the Add MCL command MCL-A was given as #22 and MCL-B was equal to MCL-A, the exclude command must specify MCL-A and MCL-B as #22 #22 respectively. However, if MCL-A was #22 and B was #FF in the add command, the exclude command MUST specify MCL-A as #22 and B as #FF. Failure to do so will result in MCL information not found error.

The format of this command is shown in the following figure.

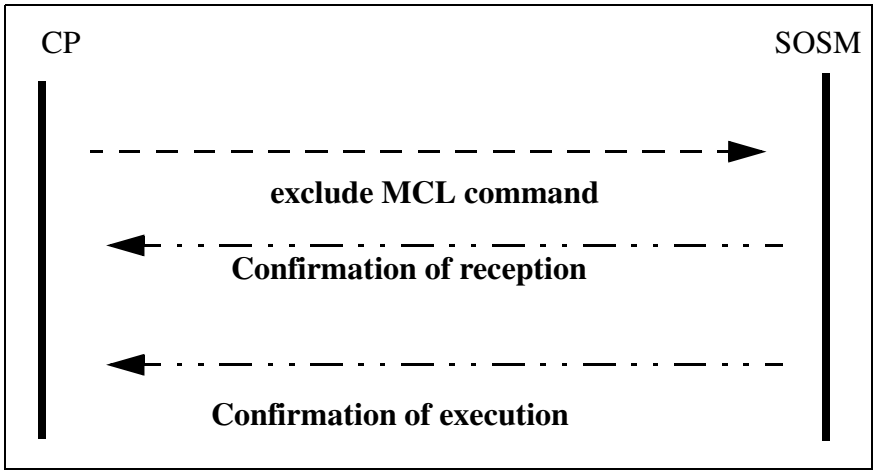
Figure 22 Excluding of MCL out of group

Header
MCL group number
MCL-A number
MCL-B number

Code of Command = 09H

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 23 Exclude MCL from group command



Validation error checking:

When any of the parameters in this command are specified (i.e. are not FFH), validation rules as specified in section “2.5.7.9 Clearing of MCL (Command N8)” on page 92 apply.

Execution error checking :

- If the specified “mcl group” does not exist in the database, the “attribute of command execution” field is set to “**mcl information not found**” code with value **4BH**.
- If MCLA number, received in the command, is not defined in MCL database, the “attribute of command execution" field is set to “**mcl information not found**” code with value **4BH**.
- If the MCL group type is “separate monitoring”, and MCL-B number received in the command is not defined in MCL database, the “attribute of command execution" field is set to “**mcl information not found**” code with value **4BH**.
- If the MCL group type is “separate monitoring”, and MCLB is defined, but not engaged with MCLA, the “attribute of command execution" field is set to “**mcl information not found**” code with value **4BH**.
- If at the time the command is given the MCL(s) specified is in use, the “attribute of command execution” field is set to “**mcl in use**” code with value **41H**.
- If the MCL group type is “separate monitoring” and MCL-B is equal to MCL-A, code **"Invalid MCL B For Group"** is set with value **"5BH"** .

- If mcl database is being transferred during receiving the command, code **"MCL data transfer in progress"** is set with value **"64H"**.

  The behavior in this scenario is changed for this command. For this scenario, the command “Assignment of MCL to group” fails in the validation error checking, That is No:7 (NOK) is only sent to CP but the messages No:7 (OK) and No:8 (NOK) is sent to CP in this command.

14.5.7.11 Request object data (Command N10)

R-66 Status: PC[1]

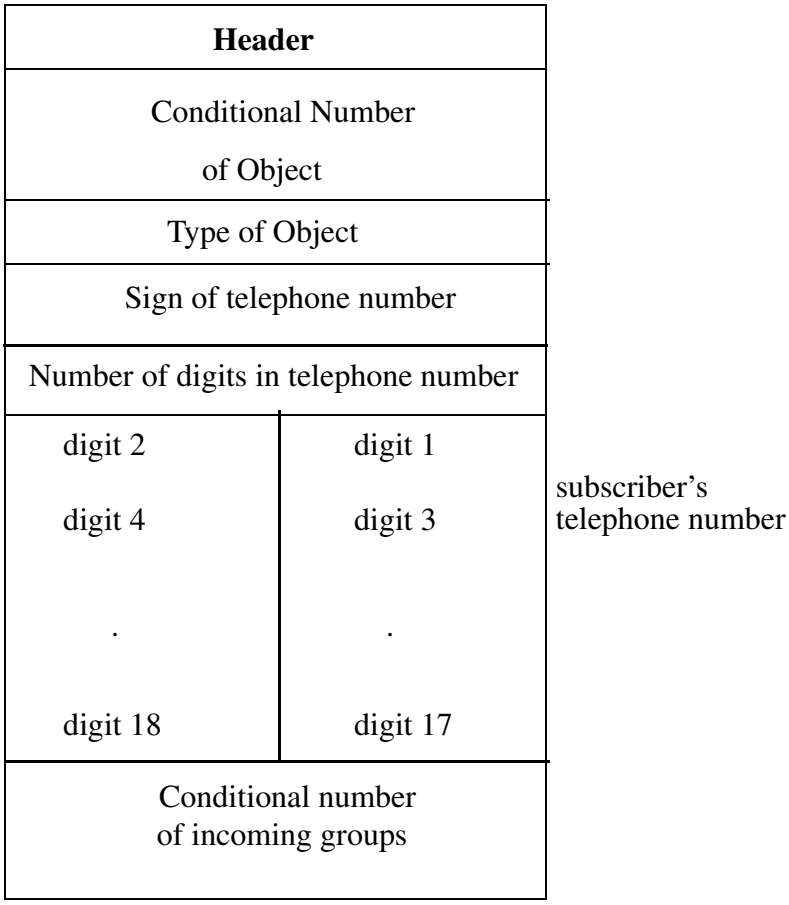
Request for Objects of Monitoring Data Transmission (command N10) is sent from CP to request information about one or more monitored objects.

This command sends a request for information transmission about the monitored object or objects.

The format of this command is shown in “Figure 24 Request for objects of monitoring data transmission” on page 99.

[1]Conditional number of incoming group is not supported in DMS MMP.

Figure 24 Request for objects of monitoring data transmission



Code of *Command* = 0AH

Parameters of this command have the same meanings as for command "Setting of objects for monitoring".

Conditional number of object: If it is set then this object's data are sent to CP.

Type of object: If it is set all this type objects are reported to CP.

Sign of telephone number, number of digits in telephone number, monitored subscriber telephone number: If they are set then this object's data are transmitted to CP.

Not supported in DMS MMP: "Conditional number of incoming group: If this is set this object's data is reported to CP."

If none of the above mentioned parameters is set then all objects of monitoring data are transmitted to CP.

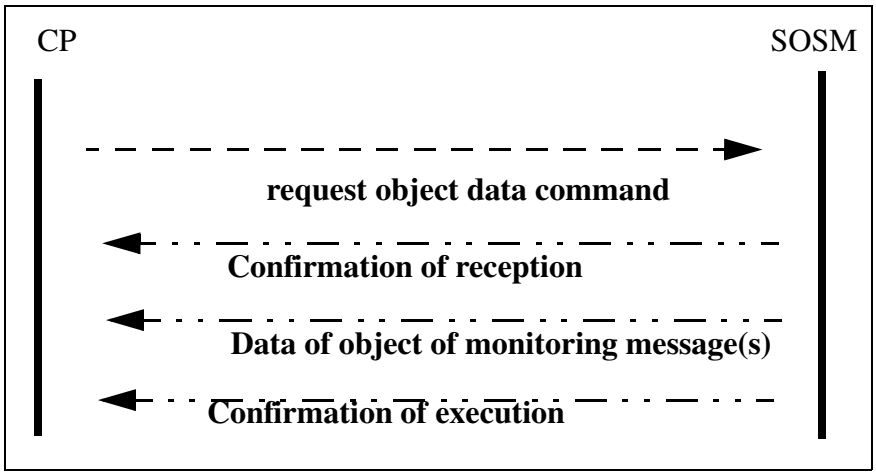
Table 10 Valid parameter combinations for No10, and SOSM actions for each

Conditional Number	Type of Object	DN	Actions
Corresponds to an existing object	FFH	all digits are FF	Transmit object's data (No7:OK - No3 -No8:OK)
Corresponds to an existing object	{01H, 02H, 12H }	all digits are FF	Ensure that the type_of_ objects -in the message and in the database- are same. Otherwise, reject command (No7:OK - No3 - No8:NOK) Transmit object's data. (No7:OK - No3 -No8:OK)
Corresponds to an existing object	{01H, 02H, 12H }	Valid digits and digit count	Ensure that the type_of_ object and digits -in the message and in the database- are same. Otherwise, reject command (No7:OK - No3 - No8:NOK) Transmit object's data. (No7:OK - No3 -No8:OK)
FFFFH	{01H, 02H, 12H }	all digits are FF	Transmit all objects of the type received in the message. (No7:OK -(n* No3) -No8:OK)
FFFFH	{01H, 02H, 12H }	Valid digits and digit count	Find the object with the type_of_ object and digits received in the message. If not found, , reject command (No7:OK - No3 - No8:NOK) Ensure that the type_of_ objects - in the command and in the database- are same. Otherwise, reject command (No7:OK - No3 -No8:NOK) Transmit object's data. (No7:OK - No3 -No8:OK)
FFFFH	FFH	Valid digits and digit count	Find the object with the digits received in the message. If not found, , reject command (No7:OK - No3 - No8:NOK) Transmit object's data. (No7:OK - No3 -No8:OK)
FFFFH	FFH	all digits are FF	Transmit all objects. (No7:OK -(n* No3) -No8:OK)

If more than one object's data is retrieved, several response message will be sent as described in "2.5.8 SOSM to CP Ch.1 messages" on page 113.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 25 Request object data command



Validation error checking:

Please refer to Section “2.5.7.1.1 Command reception error handling” on page 66.

Execution error checking :

For any of the execution errors specified below, data in the request message is copied into the response message Msg.N3 and sent to CP before Msg.N8- "confirmation of command execution" message. (Please refer to Section “2.5.8.3 Data of objects of monitoring (Msg. N3)” on page 116.)

- If the "conditional number of incoming group" is received with a value but FFFFH, command is rejected with the "**unsupported parm-5EH**" code.
- If the conditional number is not FFFFH, but it does not exist in the database, command is rejected with the "**object not found-45H**" code.
- If a telephone number is specified in the command, but it does not exist in the database, command is rejected with the "**object not found-45H**" code.
- If the conditional number corresponds to an object in the database, and if a telephone number is specified in the command, the specified telephone number must comply with the object’s telephone number in the database. Otherwise,command is rejected with "**object not found-45H**" code.
- If the conditional number and telephone number is specified in the command and the conditional number corresponds to an object in the database but phone number does not exist in the database then command is rejected with thethe **"object not found-45H"** code.

- If telephone number is specified within command, and amount of digits in "subscriber's telephone number" does not comply with the value in "number of digits in telephone number" parameter, command is rejected with the "**invalid number of digits-4DH**" code.
- if "type of object" parameter is not one of {01H, 02H, 03H, 12H} or FFH, code **"invalid object type"** is set with value **"48H"**.
- if an object which exists in the database is specified with "sign of telephone number" and/or "conditional number of object", "type of object" received in the command must comply with the object's type in the database. Otherwise, command is rejected with "**object type mismatch-54H**" code.
- if the "sign of telephone number" parameter is not one of {01H - 06H}or FFH, code **"invalid sign of telephone number"** is set with value **"5FH"**.
- If sign of dn in the command does not matches with the sign of dn in database, command is rejected with **"sign of dn mismatch-56H".**
- If all parameters are set in the command but this object does not exits in the database, command is rejected with the **"object not found-45H"**
- If object database is empty, command is rejected with **"no data exists in database-60H"**

14.5.7.12 Request MCL group information (Command N11)

R-67 Status: C

Request for Transmission of Information about MCL and Group Correspondence (command N11) is sent from CP to obtain MCL group configuration.

Any field of the command can be set or empty. Empty fields are filled with value FFH.

- If all fields have value FFH then complete table of correspondence is sent to CP.
- If number of group is given then list of MCLs belonging to this group is reported.
- If MCL group's type is given then correspondence table of MCLs and groups for this type is transmitted to CP.
- If MCL number is given then group corresponding to it is reported to CP.

The format of this command is shown in the following figure.

Figure 26 The request for transmission of the information about MCL and group correspondence

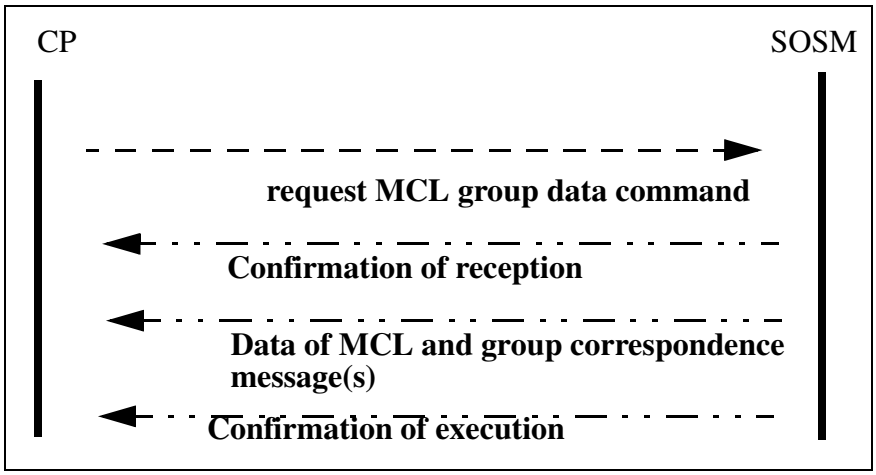
Header
MCL group number
MCL group type
MCL-A number
MCL-B number

Code of *Command* = 0BH

If more than one message is required to transmit the information, several response message will be sent as described in “2.5.8 SOSM to CP Ch.1 messages” on page 113.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 27 Request MCL group information command



Validation error checking:

Please refer to Section “2.5.7.1.1 Command reception error handling” on page 66.

Execution error checking :

- If the MCL group number is not within allowed range (greater than 224 or less than 1), command is rejected with "**invalid MCL group-49H**" code.

- If the value of MCL group type field is not one of 01H (combined) or 11H (separate), code **"invalid MCL group type"** is set with value **"61H".**
- If MCLA and/or MCLB are specified (not FFH), but the specified value is not within allowed range (number of PCM channel in MCLA and MCLB is one of values (0, 16, 30, 31)), command is rejected with "**invalid MCL number-4AH**" code.
- If both MCL group and MCL group type are specified in the command, the group type in the command must comply with the type previously defined in the database. Otherwise, the command will be rejected with "**wrong MCL type for group-52H**".
- If only a valid MCL group number is received in the command, but if it does not correspond to an existing MCL group, command is rejected with "**MCL information not found**" code with value "**4BH**".
- If only MCL group type parameter is set in the received command, but if there is no MCL group of the specified type in the database, command is rejected with "**MCL information not found**" code with value "**4BH**".
- If MCLA and/or MCLB numbers are set in the command, but if the specified MCL(s) does not exist in the database, command is rejected with "**MCL information not found**" code with value "**4BH**".
- If MCL group number, and MCLA and/or MCLB are received in this command, it is checked in the database if the specified MCL(s) are assigned to the given MCL group. If MCL(s) belong to other MCL groups, command is rejected with "**invalid MCL number-4AH**" code.
- If MCL group type and MCLA/MCLB number parameters are set, the value of MCL group type parameter within the command and the type of the MCL group in the database (which includes MCLA/MCLB specified in the command) must be identical. Otherwise, command is rejected with code "**invalid MCL group type-61H**" code.
- If MCL group type and MCLB number parameters are set, and if value of MCL group type is not "separate monitoring",code **"invalid MCL group type"** is set with value **"61H".**
- If MCLA number and MCLB number are specified within the command, MCLA and MCLB numbers must be equal or MCLB must be FF where MCL group type is combined. (Note that MCLA and MCLB number must match with the values in database). Otherwise, command is rejected with "**invalid MCLB for group-5BH**" code.
- If MCLA number and MCLB number are specified within the command, MCLA and MCLB numbers must be different where MCL group type is separate (Note that MCLA and MCLB number must match with the values in database). Otherwise, command is rejected with "**invalid MCLB for group-5BH**" code.

- If MCL database is empty, command is rejected with **"no data exists in database-60H"**.

14.5.7.13 Request subscriber's SS list (Command N12)

R-68 Status: C
Request for Transmission of Supplementary Services List (command N12)

Upon issuing this command SOSM gives the list of supplementary services (SS) that are available to **supported subscribers (IBN/V5.2(IBN)/ETSI BRI)** of present exchange. Digits without value in telephone number field are filled with FFH. Format of this command is given in the following Figure.

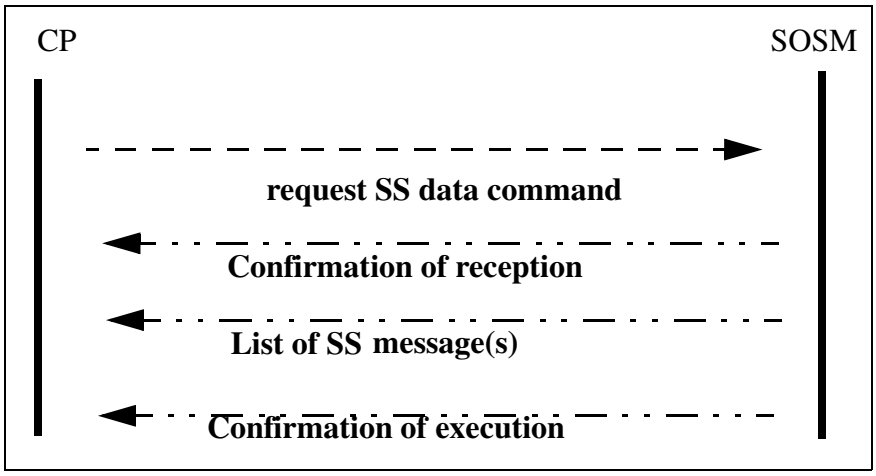
Figure 28 The request for transmission of supplementary services list

Header	
Sign of telephone number: 01H	
Number of digits in telephone number	
digit 2	digit 1
digit 4	digit 3
.	.
.	.
digit 18	digit 17

Code of *Command* = 0CH.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 29 Request SS list command



While executing this command, all features in the customer group and CEPT casual features in table CUSTSTN are sent sent to CP, as well.

This command is not supported for EBS lines. For unsupported line types, the message 8-NOK is sent.

Validation error checking:

Please refer to the validation error checking of the relevant parameters in section “2.5.7.6 Setting an object for monitoring (Command N5)” on page 76 for validation of the parameters in this command.

- If the number of digits specified is greater than 7 (local exchange subscriber), code **"number of digits mismatch"** is set with value **"13H" .**

Execution error checking :

- If the requested subscriber’s telephone number does not exist in the exchange, command execution will fail and the command will be rejected. A “Confirmation of command execution” message is sent to CP and the “attribute of command execution” field is set to code “**invalid dn for exchange**” code with value **58H**.
- If the specified subscriber does not have any assigned supplementary services, A “Confirmation of command execution” message is sent to CP and the “attribute of command execution” field is set to code “**no services found**” code with value **57H**.
- If the requested subscriber’s “sign of telephone number” is not “subscriber of present exchange”, code **"invalid sign of telephone number"** is set with value **"5FH"** .

- If the subscriber is of the unsupported line type, code **"unsupported agent type"** is set with value **"5AH"**.
- If amount of digits in phone No does not comply with the mentioned in byte 2, code **"invalid number of digits"** is set with value **"4DH"**.

14.5.7.14 Interrupt transmission command (Command N13)

R-69 Status: C

Interruption of Messages Output on the Request for Transmission of the Tables Contents (command N13) is sent from CP to stop data transmission.

Current output of information about the query to a SOSM table is stopped upon this command. Un-transmitted portion of the data is lost.

The format of this command is given in the following Figure.

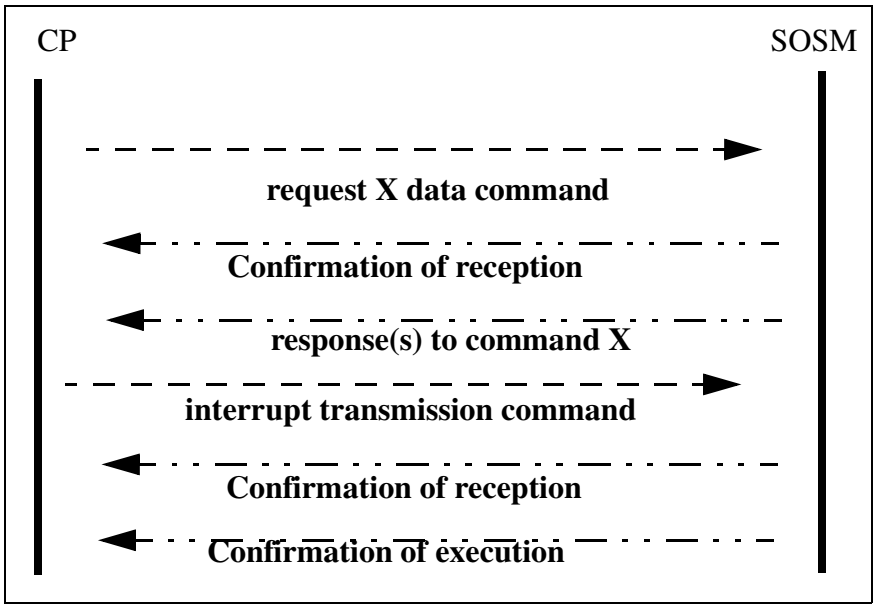
Figure 30 Interruption of messages output on the request for the transmission of the tables contents

Code of *Command* = 0DH

Note: When this command is executed, the message 8-NOK is sent to CP for the command requesting the data transmission.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 31 transmission of information interrupt



Execution error checking :

- If at the time the interrupt request is received no transmission is taking place, command execution will fail and the command will be rejected. A "Confirmation of command execution" message is sent to CP and the "attribute of command execution" field is set to code "**command out of sequence**" code with value **4CH**.

14.5.7.15 Testing DTC command (Command N14)

R-70 Status: C

Testing of Data Transfer Channels (command N14) is sent from CP to validate operational state of the Data Links.

Testing of data transfer channels (DTC) 1 and 2 between SOSM and CP is started upon this command.

If SOSM does not receive a new N14 command during 10 minutes after the last N14 command is received, SOSM tries to switch to the next link datafilled in table SOSMMPC. If the actual link is the last link, then the next link is the first link. If there are no other reserved links, then R-48 is applied. Test answer will only be sent over current channels 1 and 2.

The format of this command is given in the following figure.

Figure 32 Testing of data transfer channels

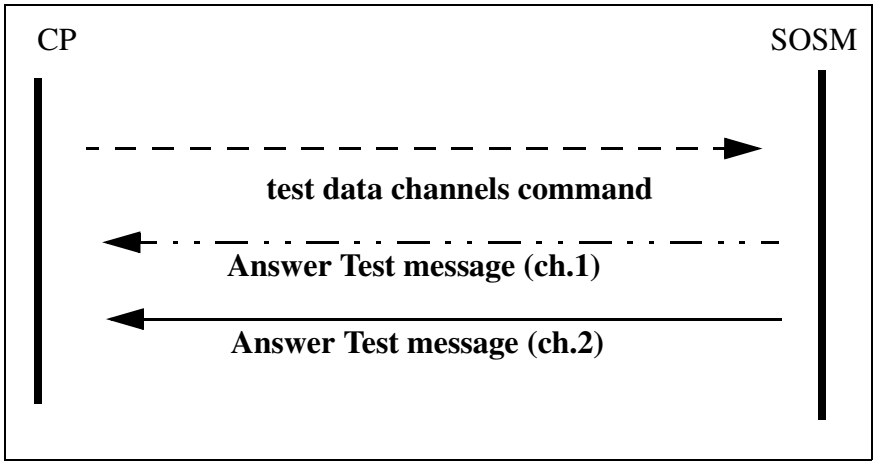
Header
Number of test message

Code of Command = 0EH

Number of test message: It changes cyclically from 00H to FFH.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 33 Test data channel command



14.5.7.16 Change object of monitoring (Command N15)

R-71 Status: Object of Monitoring Parameters Change (command N15) is sent from CP to modify the parameters of an existing object.

Following parameters assigned by the command “Setting of object for monitoring” are changed:

— Category of monitoring

— MCL group number

— Priority mark

If at the moment of this command’s reception, the object is in conversation state then new parameters set by this command takes place from the next call of the object.

The format of the command is given in the following figure.

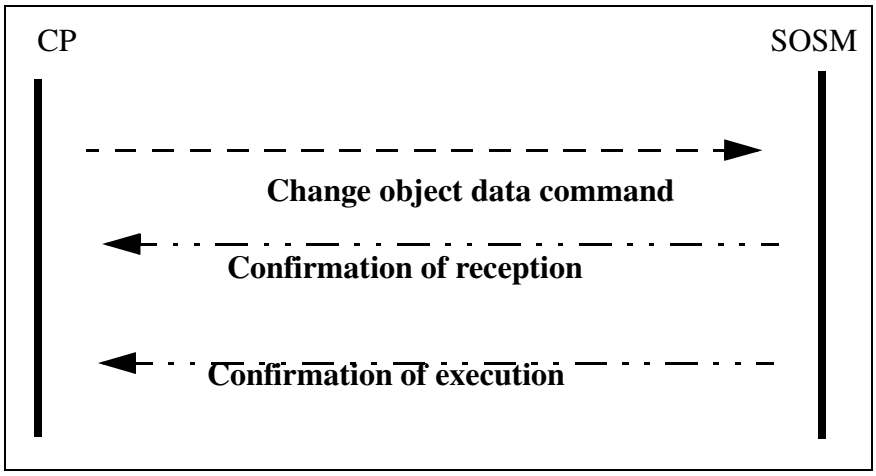
Figure 34 Object of monitoring parameters change

Header
Conditional Number of Object
Category of monitoring
MCL group number
Priority mark

Code of Command = 0FH

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 35 Change object of monitoring command



Validation error checking:

Please refer to the validation error checking of the relevant parameters in section “2.5.7.6 Setting an object for monitoring (Command N5)” on page 76 for validation of the parameters in this command.

Execution error checking :

- If the requested object does not exist in the database, command execution will fail and the command will be rejected. A “Confirmation of command execution” message is sent to CP and the “attribute of command execution” field is set to code “**object not found**” with value **45H**.
- If the MCL group number is not found in the database, code “**mcl info not found**” with value **4BH** is returned and command rejected
- If the type of MCL group specified does not correspond to the Category of monitoring, code “**wrong mcl type for group**” with value **52H** is returned and command is rejected.
- If the "category of monitoring" and the "priority mark" do not match, code **"priority code mismatch"** with value **5CH** is returned and command is rejected.
- If MCL group number is specified for statistical monitoring change order, code "**invalid mcl group**" with value **49H** is returned and command rejected.
- If MCL group number is specified as for non-statistical monitoring change order, code "**invalid mcl group**" with value **49H** is returned and command rejected.
- If me database is being transfferred during receiving the command, code **"me transfer in progress"** with value **63H** is returned and command is rejected.

14.5.7.17 Request incoming group information (Command N16)

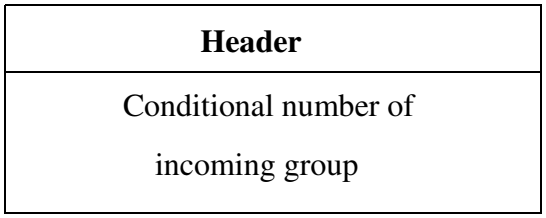
R-72 Status: C

Request for Transmission of Information about Correspondence between Exchange Incoming Group’s Name and It’s Conditional Number (command N16).

Upon receiving this command SOSM should give information about incoming groups’ lines (channels) symbolic exchange’s names correspondence to conditional number of incoming groups.

The format of the command is given in the following figure.

Figure 36 Request for transmission of information about correspondence between exchange incoming group’s name and it’s conditional number

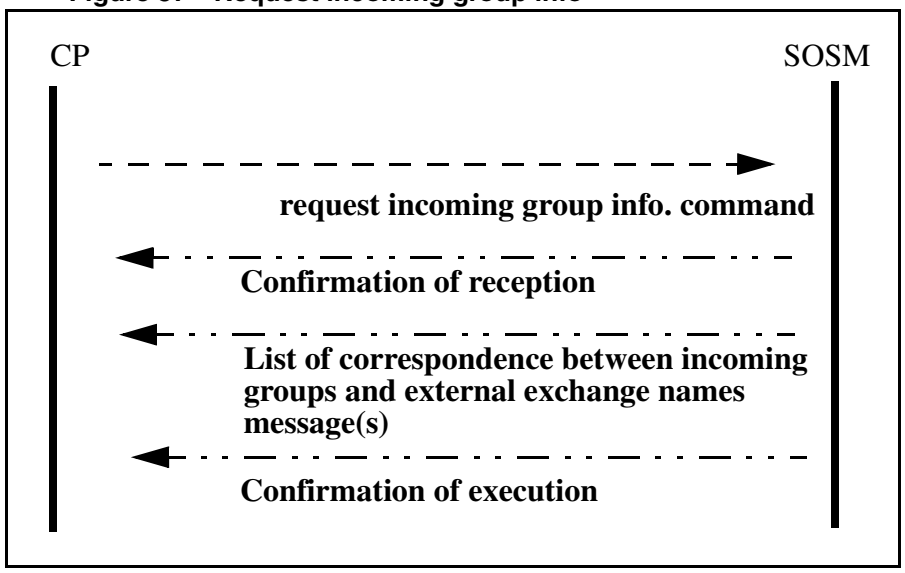


Code of Command = 10H

If the "conditional number of incoming group" value is FFFFH, a complete list of incoming groups on the exchange is sent to the CP.

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 37 Request incoming group info



Execution error checking :

- If the Incoming Group number is specified (i.e. not FFFFH) and that group is not found on the exchange, command execution will fail and the command will be rejected. A "Confirmation of command execution" message is sent to CP and the "attribute of command execution" field is set to code "**object not found**" with value **45H**.

14.5.7.18 Request SW version command (Command N17)

R-73 Status: C

Request of Exchange's SW Version (command N17) is sent by CP to request information about the exchange's software.

SOSM gives the version and edition of exchange's software upon this command.

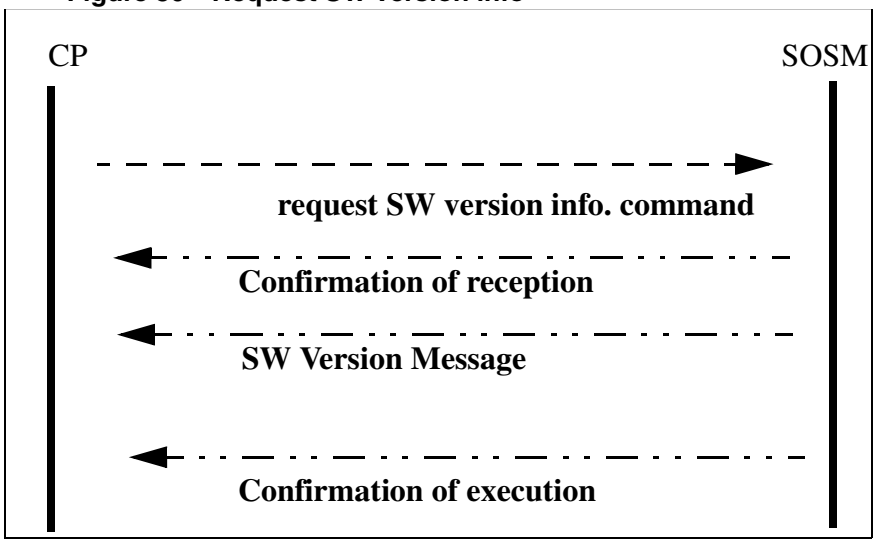
The format of the command is given in the following figure.

Figure 38 Request of exchange's SW version

Code of Command = 11H

The following message sequence illustrates the messaging between SOSM and CP for handling this command.

Figure 39 Request SW version info

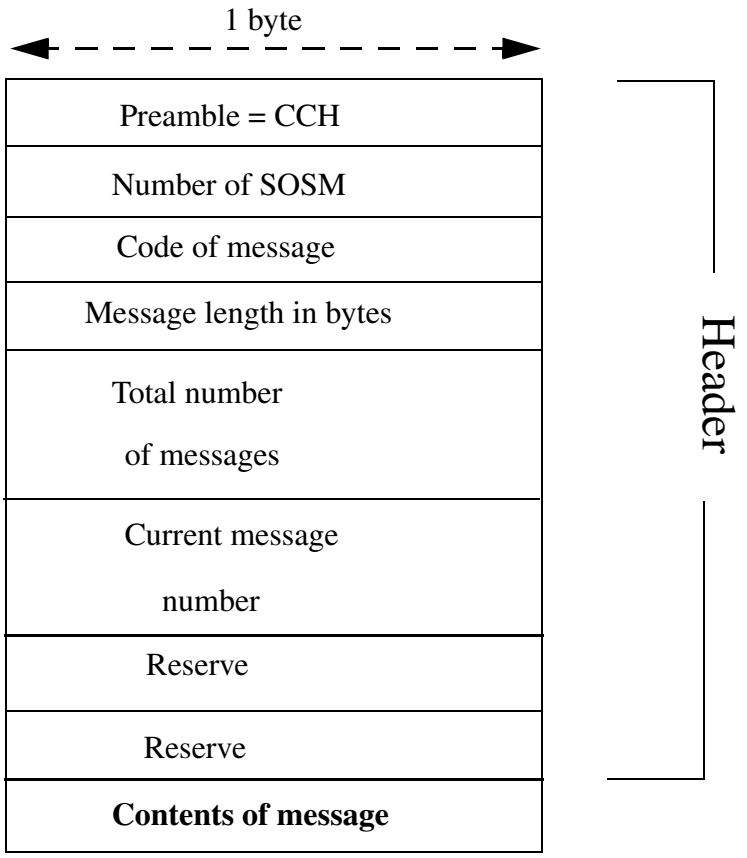


14.5.8 SOSM to CP Ch.1 messages

Channel 1 messages are messages in response to commands from CP or messages informing the CP of system events. For those messages that are sent in response to a command, information regarding the command can be found in section "2.5.7 CP to SOSM Command Processing" on page 66.

R-74 Status: C
The information field of messages from SOSM to CP has the following format:

Figure 40 Format of SOSM to CP Control Message



Total number of messages field is used if the length of a message is insufficient for information transmission to CP. In this case additional messages are formed to transmit the whole information and sequence number of the message is indicated in **Current message number** field. If no additional messages are needed then **Total number of messages** field is equal to 1 in binary code.

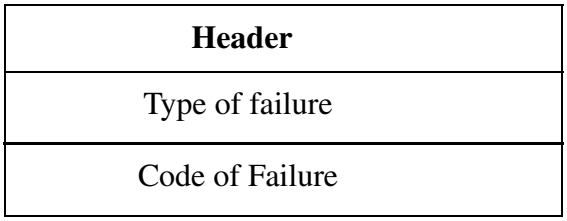
14.5.8.1 Failure Message (Msg.N1)

R-75 Status: C
Failure (message N1) is sent to alert the CP of a system failure.

This message is transmitted in case of exchange's hardware or software failure, influencing SOSM operation or upon monitored objects maintenance.

The format of this message is given in the following figure.

Figure 41 Failure message format



Code of Message = 21H

Type of failure can take the following values:

01H: Causes loss of exchange's SOSM database and requires retransmission of SOSM tables from CP side.

02H: Does not cause SOSM's database loss, but it requires CP operator intervention.

03H: Does not cause SOSM's database loss and does not require SOSM tables retransmission or CP operator intervention.

When a problem occurs during the processing of a SOSM operation, an appropriate code will be reported in the failure message. Since the SOSM software is not to generate any reports or logs on the exchange, when software errors or resource problem occur, the CP will be informed with a failure message. **The CP operator should report these failures to the vendor**.

The following "code of failure" values are defined:

Table 11 Expanded codes of failure

Name	Value	Action
system outage	01H	Inform operating company
subscriber circuit failure	02H	Inform operating company
PCM30 link fault	03H	Inform operating company if problem persists
conference circuit fault	04H	Inform operating company if problem persists[a]
Maximum calls exceeded	06H	None, this may occur if many observed subscribers originate or receive calls at the same time
Resource Problem	10H - 19H	None, this may occur periodically under heavy traffic. report to vendor if this problem persists
software error	20H - FEH	Report to vendor (NETAS)

a. NOTE: under heavy SOSM traffic, it is possible that the conference circuits may fail. This is a limitation of the 3X67 conference circuit card on the MTM or CTM shelf. In those rare cases, failure message will be sent to the CP, the MCL using that conference port card will be release, and message 52 (MCL cleared) will be reported to CP. In addition, NET102 logs (not SOSM specific) may be generated in the office, reporting the card problem.

14.5.8.2 Restart message (Msg.N2)

R-76 Status: C
Exchange S/W Restart (message N2) is sent to inform CP of a system restart.

This message is sent if exchange or SOSM are ready for service after the following events:

— Initial start of exchange

— Failure of exchange

— Restart of exchange's SW

— Upon software upgrade (ONP) from MMP to MMP

— Restart of SOSM system due to system failure

After this message, CP should:

— Send "Start of SOSM" command for initialization of SOSM

— Retransmit SOSM tables

The format of this message is given in the following figure.

Figure 42 Exchange S/W restart

Code of Message= 22H

14.5.8.3 Data of objects of monitoring (Msg. N3)

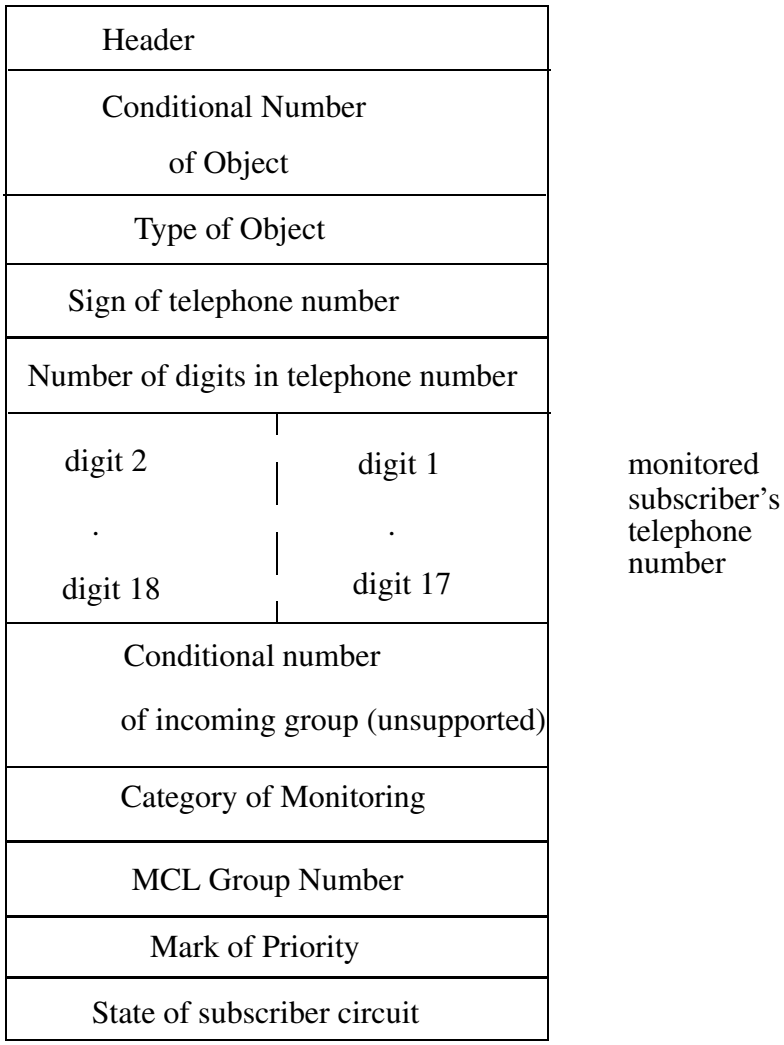
R-77 Status: C
Data of Objects of Monitoring (message N3) is sent to CP as a response to a previous query.

This message is transmitted as an answer upon the command "**Request for objects of monitoring data transmission**". When appropriate fields in this command are filled with FFH then "**Data on objects of monitoring**" message about every monitored object is transmitted to CP.

For information about message sequence and processing please refer to “2.5.7.11 Request object data (Command N10)” on page 98.

Format of the message is given in “Figure 43 Data of objects of monitoring” on page 117.

Figure 43 Data of objects of monitoring



Code of Message = 23H

Unsupported:
Conditional number of connecting lines incoming group is present if type of object = 03H, otherwise is equal to FFFEH.

State of subscriber circuit can take the following values:

00H: Subscriber circuit is in good working order (subscriber can use incoming/ outgoing communication)

01H: Subscriber circuit is out of order (subscriber can not use incoming/ outgoing communication).

If more than one message is required to transmit all the requested data, then **Total number of messages** and **Number of current message** fields in the message header are set.

If no supervised objects with required parameters in command "**Request for objects of monitoring data transmission**" are found in the database then these parameters are repeated in "**Data on objects of monitoring**" message and remaining fields are filled with FFH.

14.5.8.4 Information about MCL groups message (Msg.N4)

R-78 Status: C

The Information about Correspondence between MCLs and Groups (message N4) is sent to CP in response to a previous request.

This message is sent as the answer to the command "Request for Transmission of Information about Correspondence between MCLs and Groups". Message contents length should be 45 bytes. If the message length is less than 45 bytes then the unused bytes are filled with FFH. If more than 45 bytes are needed for information transmission (that means there are more than 11 MCLs in the group) then additional messages are formed. In this case appropriate values should be put in the fields, "**Total number of messages**" and "**Current message number**", of header.

For information about message sequence and processing, please refer to "2.5.7.12 Request MCL group information (Command N11)" on page 102.

Format of the message is given in "Figure 44 Information about correspondence between MCLs and groups" on page 119.

Figure 44 Information about correspondence between MCLs and groups

Header
MCL group number
MCL group type
MCL-A1 number
MCL-B1 number
MCL group number
MCL group type
MCL-A2 number
MCL-B2 number
. . .
MCL group number
MCL group type
MCL-AN number
MCL-BN number
FFH

Code of Message = 24H

14.5.8.5 List of Supplementary Services message (Msg.N5)

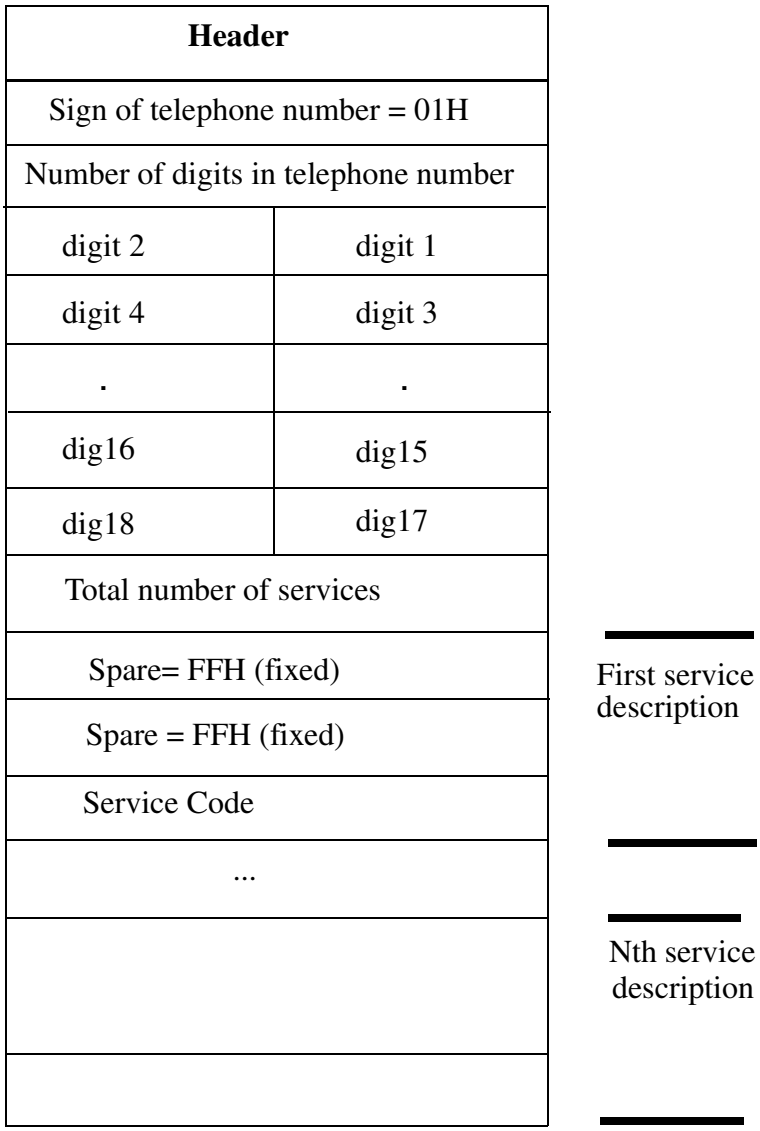
R-79 Status: C
The List of Subscriber's Supplementary Services (message N5)

This message is sent as an answer to the command "Request for Transmission of Supplementary Services List" for every subscriber of the exchange.

For information about message sequence and processing, please refer to "2.5.7.13 Request subscriber's SS list (Command N12)" on page 105.

Format of the command is given in the following figure.

Figure 45 List of Subscriber's Supplementary Services



Code of Message= 25H

The service description parameter is a three byte parameter as follows:

- Byte 1 and Byte 2 are both set to FFH
- Byte 3 represents the Service Code.

The service codes correspond to service names as defined in "Table 108 Subscriber Services Codes" on page 243.

Message length can not exceed 55 bytes including the header. The maximum number of services codes in one message is 11.

14.5.8.6 Unauthorized access message (Msg.N6)

R-80 Status: C

Unauthorized Access to SOSM's Software (message N6) is transmitted to report an unauthorized access to the software and data of SOSM.

The format of this message is given in the following figure.

Figure 46 Unauthorized Access to SOSM's software

Header
Code of access
Date of current month (2 Digits)
Hour (2 Digits)
Minutes (2 Digits)
Seconds (2 Digits)

Code of Message= 26H

Code of access field can take following values;

01H: access trial from forbidden port

02H: access trial with wrong password

03H: trial of SOSM data tables reading/record

04H: trial to refix port of SOSM communication with CP

05H: attempt to access SOSM configuration tables directly (not via SOSMCONF interface[1]

06H: attempt to access SOSMCONF interface with wrong password

[1]Please refer to "2.8.4 Access to SOSM configuration tables and parameters : SOSMCONF" on page 161.

Bytes from 2 up to 45 are used for additional information about unauthorized access as follows:

- Byte 2 to 5 present the time the access violation was detected as:

2	Date of current month (two DIGITS)
3	Hours (Two DIGITS)
4	Minutes (Two DIGITS)
5	Seconds (Two DIgits)

The date and time information is stored in BCD digits from 0 to 9.

14.5.8.7 Confirmation of command reception (Msg.N7)

R-81 Status: C

Confirmation of Command out of CP Reception (message N7) is sent to confirm receipt of a command, or to indicate an error in a command.

This message is transmitted for any received command from CP over data channel 1 after correctness of the command parameters are checked. This check should be done within **400 milliseconds** since the command entered exchange's port.

This message is not transmitted for the command "**Testing of data transfer channels**".

Format of the message is given in the following figure.

Figure 47 Confirmation of command out of CP reception

Header
Code of command
Attribute of command's reception

Code of Message = 27H

Code of command stands for the command for which the confirmation is given.

Attribute of command's reception can take the following values:

00H: command is accepted for execution

Any value other than 0H indicates an error as described in “Table 109 Command reception result codes” on page 247 .

14.5.8.8 Confirmation of command execution (Msg.N8)

R-82 Status: C
Confirmation Command out of CP Execution (message N8) is sent to confirm execution of a command, or to indicate an error in the processing of a command.

This message is sent after execution or non-execution of the command received over channel 1.

This message is not transmitted for the command “**Testing of data transfer channels**”.

The format of the message is given in the following figure.

Figure 48 Confirmation command out of CP execution

Header
Code of command
Attribute of command’s execution

Code of Message = 27H

Code of command stands for the command for which the confirmation is given.

Attribute of command’s execution can take the following values:

00H: command is executed successfully

Any value other than 0H indicates an error as described in “Table 110 Command execution result codes” on page 248.

14.5.8.9 Answer test message (Msg.N9)

R-83 Status: C
Answer Test Message Sent over DTC1 (message N9) for data channel diagnostics.

This message is sent over **all** existing data transfer channel 1s (DTC 1) as an answer to the command “Testing of data transfer channels” which is received over an available DTC1. After the command entered exchange’s port answer message should be sent within 200 milliseconds.

The format of the message is given in the following figure.

Answer test message sent over DTC 1

Header								
Number of test message								
X	X	X	X	X	X	X	X	**State DTC 1**
X	X	X	X	X	X	X	X	**State DTC 2**
PCM group 7	PCM group 6		...				PCM group 0	

Code of Message = 29H

Number of test message should coincide with the value of the “**Number of test message**” field in “**Testing of data transfer channels**” command.

State of DTC 1 and state of DTC 2 can take following values:

1: if the DTC is in working condition

0: in case of DTC failure or absence

Bits of fields “State of DTC 1 and DTC 2” belong to PCM-30 primary groups from 0 up to 7.

14.5.8.10 Incoming group data message (Msg.10)

R-84 Status: PC
Data about Correspondence between Conditional Numbers of Incoming Groups and Their Real Exchange Names (message 10).

This message is issued ONLY upon command from CP. Format of the message is given in Figure 37, "Request incoming group info"..

For information about message sequence and processing, please refer to “2.5.7.17 Request incoming group information (Command N16)” on page 111.

Figure 49 Data about correspondence between conditional numbers of incoming groups and their real exchange names

Header
Conditional number
of incoming group
Incoming group’s symbolic exchange’s name

Code of Message = 2AH

Conditional number of incoming group can take values from 0000H up to FFFEH.

If the field “**Conditional number of incoming group**” in the command “**Request for transmission of information about correspondence between exchange incoming group’s name and it’s conditional number**” (command N16) has the value FFFFH then SOSM should give the whole correspondence table for incoming groups.

If the length of the message exceeds **45** bytes then additional messages are formed with appropriate “**Number of current message**” and “**Total number of messages**” values in the header.

The Incoming group exchange name parameter has the following structure:

- Byte 1 to 2: Common Language Name Identifier: identifies the numeric value of the Incoming Trunk group number
- Bytes 3 and 4: Name length, the length of the actual string representation in bytes
- Bytes 5 to 20: Incoming group’s name in ASCII characters

All remaining bytes in the message are set to FFH.

14.5.8.11 Exchange SW version message (Msg.11)

R-85 Status: C
Version of Exchange's SW is sent as a response to a previous request from CP.

This message is transmitted as an answer to the command "**Request of exchange's SW version**" (command N17).

For information about message sequence and processing, please refer to "2.5.7.18 Request SW version command (Command N17)" on page 112.

The format of the message is given in the following figure.

Version of exchange's SW

Header
Version and edition of exchange's SW

Code of Message = 2BH

Values in bytes from 1 up to 7 define exchange's SW version and edition in ASCII code as follows:

1	B (42H)
2	C (43H)
3	S (53H)
4	5 (35H)
5	5 (35H)
6	. (2E)
7	0 (30H)

- Bytes 1-3 are hard coded to the string 'BCS' in ASCII code
- Bytes 4-5 represent the release number in ASCII code
- Bytes 7-8 represent the sub-release number in ASCII code
- All remaining bytes in the message are set to FFH

14.5.9 Information Messages Transmitted over Data Channel 2

The following messages are sent from SOSM to CP over data channel 2:

- Reception of called subscriber complete telephone number.
- Called subscriber answer.
- Disconnection.
- Supplementary services (SS) using.
- Monitoring Connecting Line's (MCL) connection.
- Clearing of MCL.
- Answering test message.

14.5.9.1 Format of SOSM to CP Information Messages

R-86 Status: C

Information field of the messages about monitored connections have the following format:

Figure 50 Format of Header in Information Messages from SOSM to CP

Byte No.	Parameter
1	Preamble =CCH
2	Number of SOSM
3	Message Code
4	Message length
5	Number of call
6	
7	type of object
8	conditional number of object
9	
10	attribute of object's selection
11	parameter of communications
12	code of SS phase

Byte 1 is the SOSM Preamble, a constant with value CC Hex.

Byte 2 is the SOSM number as assigned by software.

Byte 3 is the message code, values are defined in the following sections.

Byte 4 is the message content length in bytes.

Bytes 5-6 identify the Call Number as previously defined.

Byte 7 identify object type as previously defined

Byte 8-9 identify Conditional Number of Object.

Byte 10 identify the object selection as follows:

Figure 51 Attribute of object selection

Bit No.	Parameter
D1 D0	**Selection according to calling subscriber**
0 1	Complete monitoring, combined
1 1	Complete monitoring, separate
1 0	Statistical monitoring
D3 D2	**Selection according to called subscriber**
0 1	Complete monitoring, combined
1 1	Complete monitoring, separate
1 0	Statistical monitoring
D5 D4	**Selection according to Conditional Number of incoming group (UNSUPPORTED)**
0 1	Complete monitoring, combined
1 1	Complete monitoring, separate
1 0	Statistical monitoring
D7 D6	**Selection according to Conditional Number of Object**
0 1	Complete monitoring, combined
1 1	Complete monitoring, separate
1 0	Statistical monitoring

Byte eleven identifies communications parameters and is defined as follows:

Figure 52 Parameters of communication

Bit No.	Parameter
D3 D2 D1 D0	**Type of communications**

Bit No.	Parameter
0 0 0 1	Outgoing call
0 0 1 0	incoming call
0 1 0 0	international transit
1 0 0 0	toll transit
11 0 0	cross-office call
D5 D4	**Call setup method[a]**
0 1	Direct Dialled(Automatic)
1 0	Operator Assisted (Semi-automatic)
D7 D6	**reserved**
0 0	Reserved = 0

a. Note: The 'type of communications' byte is assigned as 'Semi-automatic' for all operator originating calls.

Byte 12 defines code of supplementary services phase and has the following values:

- 00H - Normal call
- 01H - order of SS service
- 02H - test of SS service
- 03H - abolition of SS service
- 04H - SS activation

Contents of Message field of the information message has the following format:

Figure 53 Format of the Contents field of Information Message

Byte No.	Parameter
1	Attribute of Telephone number
2	Number of digits in telephone number

Byte No.	Parameter
3	Calling DN
4	
5	
6	
7	
8	
9	
10	
11	
12	attribute of telephone number
13	Number of digits in telephone number
14	Called DN
15	
16	
17	
18	
19	
20	
21	
22	
23	Conditional number of incoming group
24	
25	MCL-A number
26	MCL-B number
27	Date of current month (two DIGITS)
28	Hours (Two DIGITS)
29	Minutes (Two DIGITS)
30	Seconds (Two DIgits)

Byte No.	Parameter
31	Priority
32	Operation Code
33	Description of Service
34	
35	
36	Additional Code

Bytes 1 to 11 define the Calling subscriber. Bytes 12 to 22 define the Called subscriber.

Attribute of telephone number is defined as follows:

- 01H - present exchange subscriber
- 02H - local network subscriber
- 03H - local ZONE subscriber
- 04H - OTHER ZONE subscriber
- 05H - Other country subscriber
- 06H - local or international emergency or inquiry services
- FFH - combination without value

Note: *Attribute of telephone number for Called DN will always be present correctly. For calling DN, if the originator is a line in the present exchange, that attribute will be present, otherwise, combination without value (FFH) is set.*

The content of the calling DN field depends on the originator of the call as follows :

— If the call is a line originated call, the DN (Office code + DN Digits, excluding area code) is provided in the calling DN field.

— If the call is a trunk originated call, the incoming ANI digits are provided in the calling DN field. SOSM is not able to determine the sign of the incoming ANI digits, therefore the attribute of the calling DN parameter will be set as #FF in these scenarios.

— If the call is a trunk originated call, and ANI digits are not received, calling DN field are filled with #F.

The content of the called digits depends on the terminating agent as follows :

— If the call terminates to an exchange subscriber, the called DN field will include the DN of the terminating line (Office code + DN Digits, excluding area code) instead of dialled digits.

— If the call terminates to a trunk, called DN field will include all available dialed digits.

Note: *The available digits depend on the dial plan in the given office and changes between Local Offices and Toll/Tandem offices.*

Bytes 23-24 is used when the number of the incoming call to the supervised subscriber can not be determined,otherwise it is set to FFFFH. It may take values from 0000H to FFFFH and corresponds to group's symbolic name."

Bytes 25-26 define the MCL numbers used for monitoring.

Bytes 27-30 define the current month's day and time stamp.

Byte 31 defines the priority of the object.

Byte 32 defines the operation code as:

- Code of connection completion for Disconnection message
- Code of MCL connection for messages Connection of MCL, Reception of called number, Answer and Using of SS services. Please refer to "Table 110 Command execution result codes" on page 248 for an expanded list of mcl connection codes
- Code of MCL clearing for message Clearing of MCL
- Code FFH otherwise

Bytes 33-36 are used for service codes in Use of SS message, otherwise, FFH is used.

If in a call, both Calling and Called parties are monitored objects, then for each party, a separate information message is sent to the CP reporting the call phases, with a unique call number. If MCL connection is required, each "SOSM call" is connected as defined in the subscriber object definition.

The SOSM system can support any monitoring type (statistical, combined or separate) for both agents involved in a call -where both called and calling parties are under surveillance- , if adequate resources are available for MCL connections.

14.5.9.2 Reception of called party number (Msg. No.1.1)

R-87 Status: PC
Reception of the called subscriber telephone number message (N1.1) is sent to CP to report reception of called number in a monitored call.

This message is transmitted after receiving called subscriber's number information and if any of the numbers is found in the SOSM database for supervised objects. If calling number can not be determined, and the originator is a trunk, the number of incoming trunk group is reported instead.

In line-to-trunk overlapped calls, it can be determined if the call should be monitored prior to reception of the full called number. In these calls, reception of called_party number message (MSG.1.1) is sent just after enough digits are received to determine the monitoring object.

The "description of service" fields are set to FFH.

The format of the message is given in "Figure 53 Format of the Contents field of Information Message" on page 129.

Code of Message = 41H.

For links, selected on "complete monitoring" category, this message should be transmitted to CP immediately after free MCL had been fastened to the selected call, or after decision about the absence of free MCL for this call.

The result of MCL allocation is set in the Operation's code "code of MCL unconnection" as follows:

- 00H - Normal connection
- 01H- no free MCL in group
- FFH - for statistical monitoring
- other connection code (Please refer to "Table 110 Command execution result codes" on page 248 for an expanded list of mcl connection codes)

14.5.9.3 Answer message (Msg. No 1.2)

R-88 Status: C
Answer of the Subscriber message (N1.2) is sent to CP to report Answer event in a monitored call.

This message is transmitted after the called subscriber answers the call. Format of the message is given in "Figure 53 Format of the Contents field of Information Message" on page 129.

Code of Message = 42H.

The result of MCL connection is set in the Operation's code "code of MCL unconnection" as follows:

- 00H - Normal connection
- 01H- no free MCL in group
- FFH - for statistical monitoring

other connection code (Please refer to "Table 110 Command execution result codes" on page 248.).

14.5.9.4 Disconnection message (Msg. No 1.3)

R-89 Status: C
Disconnection message (N1.3) is sent to the CP to report call completion.

This message is transmitted when the call is complete and taken down. If applicable, data transmission over MCL is stopped and MCL resources allocated to this conversation are deallocated.

The format of the message is given in "Figure 53 Format of the Contents field of Information Message" on page 129.

The "operation code" field of the message is set to have "code of connection completion" parameter as follows:

- 01H - disconnection because of technical reason
- 02H - disconnection after incomplete dialling
- 03H - disconnection in case of busy called party
- 04H - disconnection if subscriber B does not answer
- 05H - disconnection after normal conversation ends

Code of Message = 43H.

> ***Note:*** **(01H)** Technical reason will be used for any cause values which are not defined above.

14.5.9.5 Service usage message (Msg. No 1.4)

R-90 Status: C
SS services usage message (N1.4) is transmitted when a Supplementary Service (SS) is activated, deactivated, or interrogated by a monitored subscriber.

The format of the message is given in “Figure 53 Format of the Contents field of Information Message” on page 129.

The “description of service” field of the message is populated the service code being used as defined for message “List of Subscriber’s Supplementary Services” on page 120.

The “Additional code” field is populated with FFH.

The “additional code” field is populated with codes of services not defined by international standards. Values of these services should be communicated to the customer**.**

> ***Note:*** *DMS specific service codes are put in the Service Code field as opposed to the Additional Code byte as requested by LONIIS. Refer to “List of Subscriber’s Supplementary Services” on page 120 for complete information.*

Code of Message = 44H.

The value of MCLA, MCLB, category, priority and Operation code fields of this message are determined as follows :

- **Service activation / interrogation / deactivation:**

  IBN subscribers can activate/interrogate/deactivate CEPT services even within a separate call, or during an answered call.

  BRI subscribers can activate/deactivate/interrogate ISDN BRI supplementary services via using CEPT dialing sequences, or via using BRI phone set facilities. Subscriber action using phone set facilities can be done when phone is on-hook. Subscriber action using CEPT dialing sequence can be done in the first call originated from the BRI phone set, or in a new call initiated after holding the active call.

  ISDN PRI Supplementary services are provisioned in related tables for PRI trunks.

  If a subscriber only makes a service activation/deactivation/interrogation at origination, and does not connect to another agent, SOSM does not connect MCLs for this call in order to optimize resource usage. MCLA and MCLB indexes of the messages (service usage (Msg.1.4) and call clearing (Msg.1.3) messages) in these calls are set as FFH.

  The category of the call is filled with monitoring order category.

  The priority of the call is filled with monitoring order priority.

  The parameter of communications field is set to "cross-office call".

  The operation code field of service usage message (Msg.1.4) is set to FFH.

Upon unsuccessful service activation/interrogation/deactivation attempts, SOSM does not send service notification message. Instead, only call clearing message (Msg.1.3) is sent with "*disconnection after incomplete dialling* - 02" operation code. However, if the service is inactive for the monitored subscriber, the call clearing message (Msg.1.3) is sent with "*disconnection because of technical reason* - 01" operation code upon interrogation of the service.

SOSM sends service notification message (Msg.1.4) for the monitored agent's activation/interrogation/deactivation attempts during the call.

If an IBN/V5.2 (IBN) subscriber flashes, and activates/deactivates/ interrogates a CEPT service during an active call, SOSM reports this event with the same call number as in the call data messages of the original call. Additionally, category and priority fields of the message is the same with the call data messages of the original call. However, Parameter of Comm. is set as "cross-office call", the MCL# and Operation Code fields are set to FFH even though it is not FFH in the call data message.

If a BRI subscriber activates/deactivates/interrogates an ISDN BRI supplementary service, after holding the active call, subscriber actions performed in the new call is reported to CP with a new call number. And all other data in the message is filled according to properties of the new call.

Service usage:

In some scenarios, SOSM reports the subscriber services -which are used within a monitored call- to the control point. MCLA and MCLB fields within service usage messages depend on the call state at which SOSM sends the message.

In a monitored call, SOSM allocates MCLs after the dialled digits are successfully translated (just before sending reception of full number message). MCLs are connected as the originating subscriber receives ring-back tone.

If the service usage message is sent before MCL allocation (as in CCBS), MCLA and MCLB fields of the service usage message are filled with FFH. In such scenarios, the operation code of this message will also be populated with FFH.

If the service usage message is sent after MCL allocation, MCLA and MCLB fields of the message are populated with the MCL indexes which are used for the call. The operation code field icludes information about the state of the MCLs (i.e normal connection-00H, -01H- no free MCL in group, etc...)

The below tables shows the list of CEPT and ISDN BRI supplementary services services supported by SOSM:

Table 12 CEPT features supported by SOSM

Feature	Activation	Deactivation	Interrogation	Usage
ACRJ	+	+	+	-
AR	+	+	+	-
AUL	N/A	N/A	N/A	-
CCBS	+	+	+	+
CEPTPW	+	N/A	+	N/A
CEPTRA	N/A	N/A	N/A	+
CDND	+	+	+	-
CDTA	+	+	+	+
CDTO	+	+	+	+
CFB	+	+	+	+
CFD	+	+	+	+
CFF	+	+	+	+
CFRA	N/A	N/A	N/A	+
CFU	+	+	+	+
CLF	N/A	N/A	N/A	+
CND (CLIP)	+	+	+	-
CNDB (CLIP)	N/A	N/A	N/A	-
CNDBO (CLIRO)	N/A	N/A	N/A	-
CPU	N/A	N/A	N/A	+
I3WC	N/A	N/A	N/A	+
I6WC	N/A	N/A	N/A	+
ICT	N/A	N/A	N/A	+
ICWT	+	+	+	+
ILR	+	+	+	+
IWUC	+	+	+	+
LNR	N/A	N/A	N/A	-
SCL / SCS	+	+	+	-
SCR	N/A	N/A	N/A	-

Table 12 CEPT features supported by SOSM

Feature	Activation	Deactivation	Interrogation	Usage
SUPPRESS	+	+	+	-
WML	+	+	+	-

Table 13 ISDN BRI Services supported by SOSM

Feature	Activation	Deactivation	Interrogation	Usage
CFU, CFB, CFD	+	+	+	+
CW	N/A	N/A	N/A	+
3PTY	N/A	N/A	N/A	+
HOLD	N/A	N/A	N/A	+
ECT	N/A	N/A	N/A	+
CONF	N/A	N/A	N/A	+
MCID	N/A	N/A	N/A	+
CD	N/A	N/A	N/A	+
TP	N/A	N/A	N/A	+
CLIR - Temporary Mode	N/A	N/A	N/A	+
COLR- Temporary Mode	N/A	N/A	N/A	+
UUS1	N/A	N/A	N/A	+
CCBS	+	+	+	+
CCNR	NOT SUPPORTED			
REV-C	N/A	N/A	N/A	-
AOC-D, AOC-E	N/A	N/A	N/A	-
MSN	N/A	N/A	N/A	-
CLIP	N/A	N/A	N/A	-
COLP	N/A	N/A	N/A	-
CLIR - Permanent Mode	N/A	N/A	N/A	-
COLR - Permanent Mode	N/A	N/A	N/A	-
CUG	N/A	N/A	N/A	-
SUB	N/A	N/A	N/A	-
AUL	N/A	N/A	N/A	-
WML	+	+	+	-

Feature	Activation	Deactivation	Interrogation	Usage
WUCR	+	+	+	+
OCB	+	+	+	+
ISDN BRI Cept Call Forwarding	+	+	+	+
DCF	N/A	N/A	N/A	-
Huntgroups (DNH / DLH / MLH)	N/A	N/A	N/A	-

Table 14 ISDN PRI Supplementary Services supported by SOSM

Feature	Activation	Deactivation	Interrogation	Usage
DCF	N/A	N/A	N/A	-
3PTY	N/A	N/A	N/A	N/A
ECT	N/A	N/A	N/A	+
MCID	N/A	N/A	N/A	-
ETSIDIV	N/A	N/A	N/A	+
TP	N/A	N/A	N/A	N/A
CLIR - Temporary Mode	N/A	N/A	N/A	-
COLR- Temporary Mode	N/A	N/A	N/A	-
UUS1	N/A	N/A	N/A	-
CCBS	Not supported			
CCNR	Not supported			
DDI	N/A	N/A	N/A	-
AOC-D, AOC-E	N/A	N/A	N/A	-
MSN	N/A	N/A	N/A	-
CLIP	N/A	N/A	N/A	-
COLP	N/A	N/A	N/A	-
CLIR - Permanent Mode	N/A	N/A	N/A	-
COLR - Permanent Mode	N/A	N/A	N/A	-
CUG	N/A	N/A	N/A	-
SUB	N/A	N/A	N/A	-

For the above table,

(**+**) denotes that SOSM sends Msg.1.4. For detailed usage notification of above features, see appropriate section (2.11.x) of this document.

(-) denotes that SOSM does not send Msg.1.4.

(**N/A**) denotes that Msg.1.4 cannot be sent.

14.5.9.6 MCL connection message (Msg No 2.1)

R-91 Status: C
Connection of MCL message (N2.1) is transmitted after MCL connection as a result of command N7.

The format of the message is given in “Figure 53 Format of the Contents field of Information Message” on page 129.

The “operation code” field is populated with “code of MCL unconnection” as follows:

- 00H - normal connection
- 01H- no free MCL in group
- other connection code (Please refer to “Table 110 Command execution result codes” on page 248 for an expanded list of mcl connection codes)

Code of Message = 51H

14.5.9.7 Clearing of MCL message (Msg No.2.2)

R-92 Status: C
Clearing of Monitoring Connecting Line message (N2.2) is transmitted if clearing of MCL has happened for **any reason**.

The format of the message is given in “Figure 53 Format of the Contents field of Information Message” on page 129.

The “operation code” field is populated with “code of MCL clearing” code as follows:

- 01H - on command N8 “clearing of MCL”
- 02H - on monitored object priority
- 03H - on priority as a result of command N7: “connection to voice path”
- 04H - equipment failure

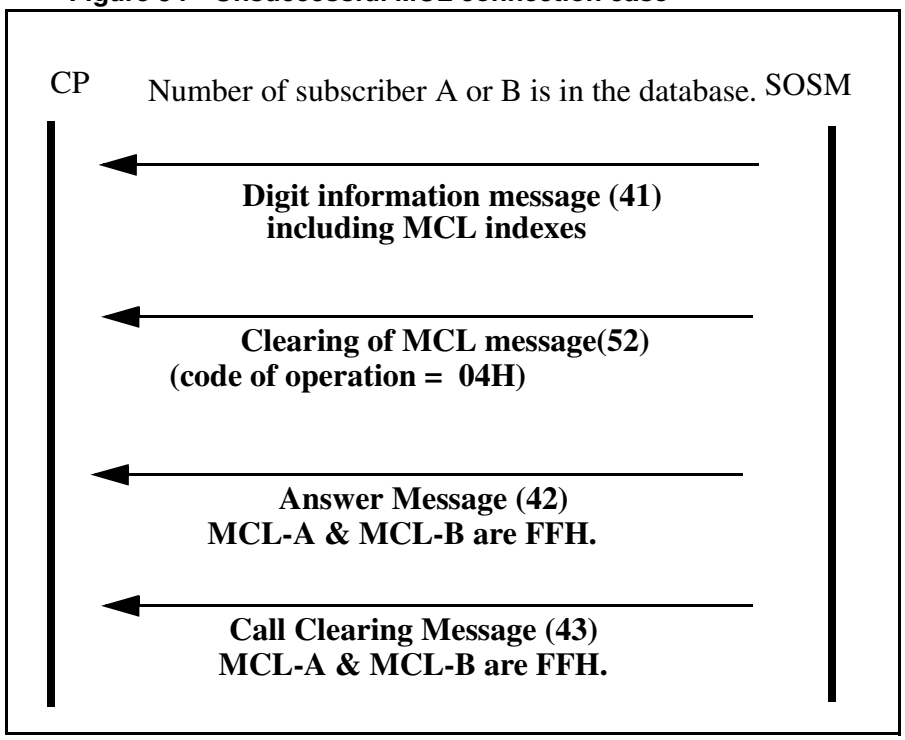
- 05H - on command N6 “removal of object of monitoring”

  Note: *On command “stop sosm” if there is an active monitored call, the MCL is cleared but* ***no message in sent to CP.***

Code of Message = 52H

SOSM only reserves MCLs those will be used within a call while sending reception of full number message (Msg.1.1). Call content delivery is started when the speech path is established between the connected parties. Therefore, SOSM notifies control point about the connection failures (i.e. resource problem, MCL outage,...) using this message with the operation code set to "equipment failure - 04H".

Figure 54 Unsuccessful MCL connection case



14.5.9.8 Answer test message (Msg. No 2.3)

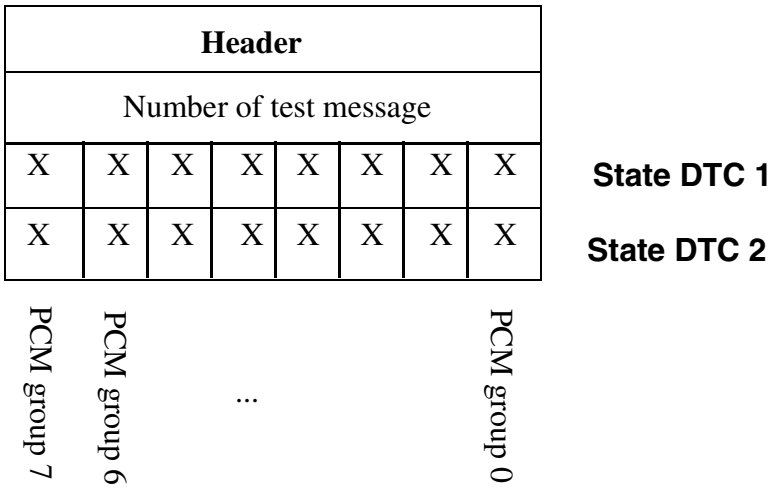
R-93 **Status:** C

Answering test message (N2.3) is sent for diagnostics of data channel 2.

This message is sent over **all** existing data transfer channel 2 (DTC 2) as an answer to the command “Testing of data transfer channels” which is received over an available DTC1. After the command entered exchange’s port answer message should be sent within 200 milliseconds.

The format of the message is given in the following figure.

Figure 55 Answer test message sent over DTC 2



Code of Message = 53H

Number of test message should coincide with the value of the “**Number of test message**” field in “**Testing of data transfer channels**” command.

State of DTC 1 and state of DTC 2 can take following values:

1:if the DTC is in working condition

0:in case of DTC failure or absence

Bits of fields “State of DTC 1 and DTC 2” belong to PCM-30 primary groups from 0 up to 7.

The Channel 2 header fields “number of call”, “type of object”, “conditional number of object”, “sign of object’s selection”, “link’s parameters” and “code of SS phase” are all set to FFH.

14.5.10 Failure Cases message scenarios

14.5.10.1 Failure of Exchange

Figure 56 Failure of exchange causing SOSM tables to be deleted

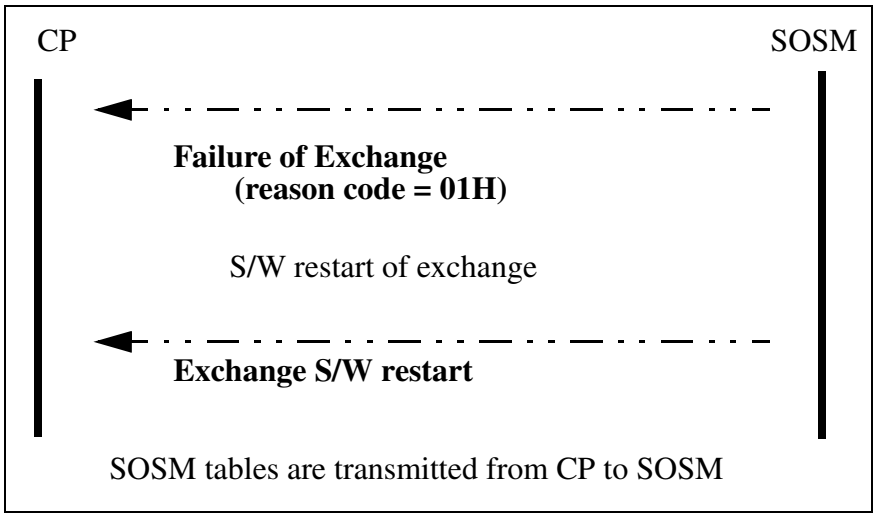


Figure 57 Failure of exchange that does not need CP intervention

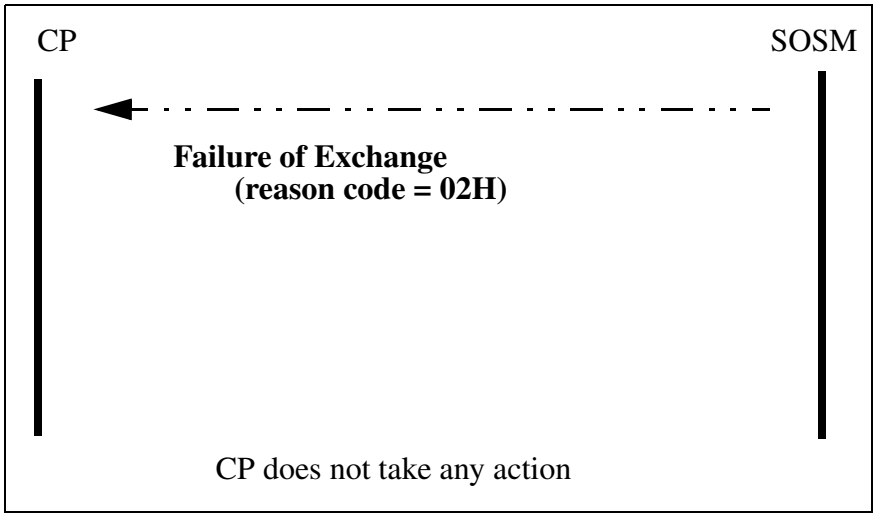
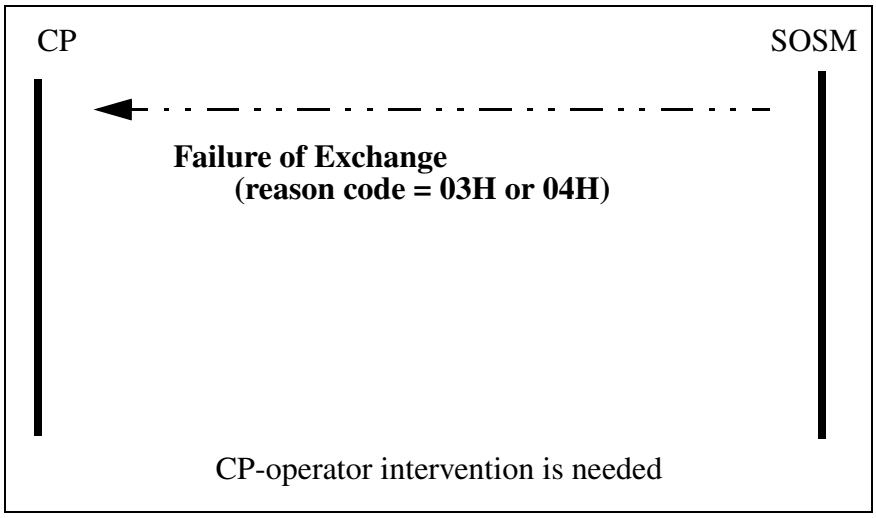


Figure 58 Failure of exchange that needs CP intervention



14.5.11 Monitored Call Scenarios

The process of selecting an object of monitoring is as follows:

a. In line originated calls, the DN of the originating line (office code + DN digits, excluding area code) is obtained, and searched in the monitored objects database.

   For BRI subscribers the MSN, which originates the call, is searched in the database. Please note that this is not necessarily the primary DN of the loop.

b. If the call is originated from an incoming trunk, SOSM does not search the originating number in monitoring order database.

   If the call is monitored due to called party, ANI information received from the incoming trunk is reported in the call information messages. If ANI is not received, incoming group number is reported in the Call information message.

c. Called party number is obtained and searched in the monitored object database.

   If the called party is a network subscriber, the dialled digits are searched within the database.

   If called party is a present exchange subscriber, the DN of the terminating subscriber (office code + DN digits, excluding area code) is searced in the database instead of the dialled digits. This way, SOSM monitores all accesses to the present exchange subscribers, and is not impacted by the retranslation scenarios.

If called party is a BRI subscriber, the MSN of the terminating subscriber (not the primary DN on the loop) is searched in the database.

d. If no objects are found, the call continues normally.

e. If one object is found, the call becomes a monitored call, the object's data is retrieved, and the call continues. All subsequent required call events will be reported to the CP. If the object has complete monitoring category, MCL connection is made when ringback tone is received(before answer phase). Please refer to the following figures.

f. If both calling and called objects are found in the database, then two sosm call numbers are assigned for each subscriber's call. The properties of the each subscriber are used for making MCL connection (if required). A separate message for each object is sent to the CP for each required call event.

g. SUSpended agents are not monitored by SOSM, although they exist in monitoring order database.

The following sections describe the messaging that takes place for each call scenario.

14.5.11.1 Supervised Subscriber with Complete Monitoring

Figure 59 Successful MCL connection

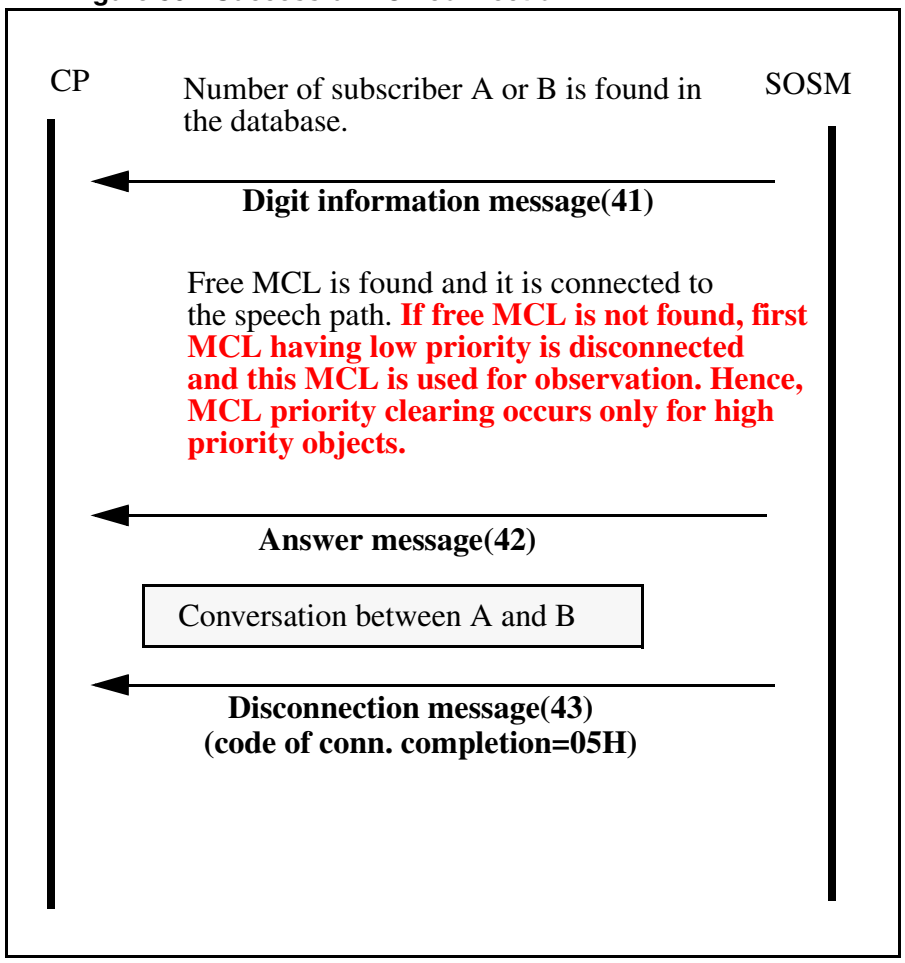


Figure 60 Unsuccessful MCL connection if no free MCL is found

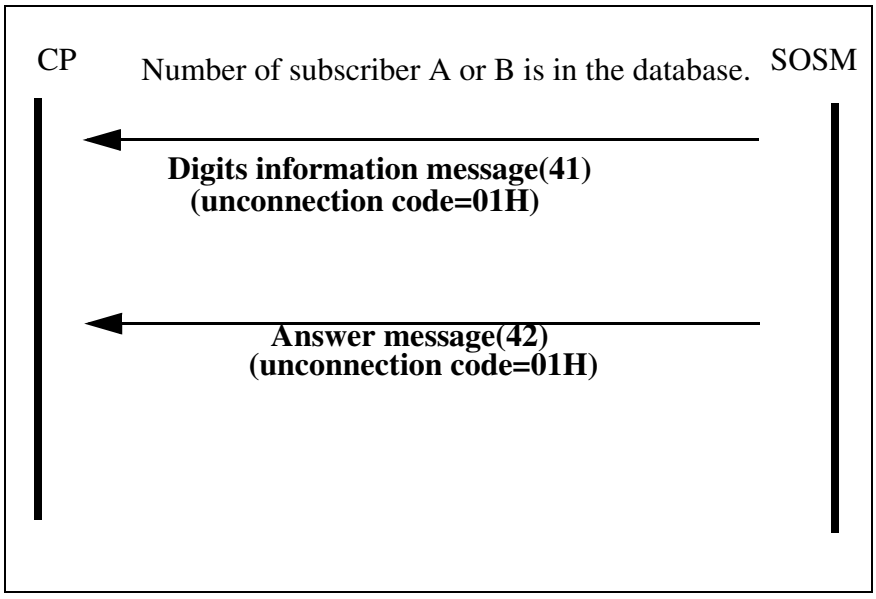


Figure 61 Unsuccessful call setup case (busy/route failure)

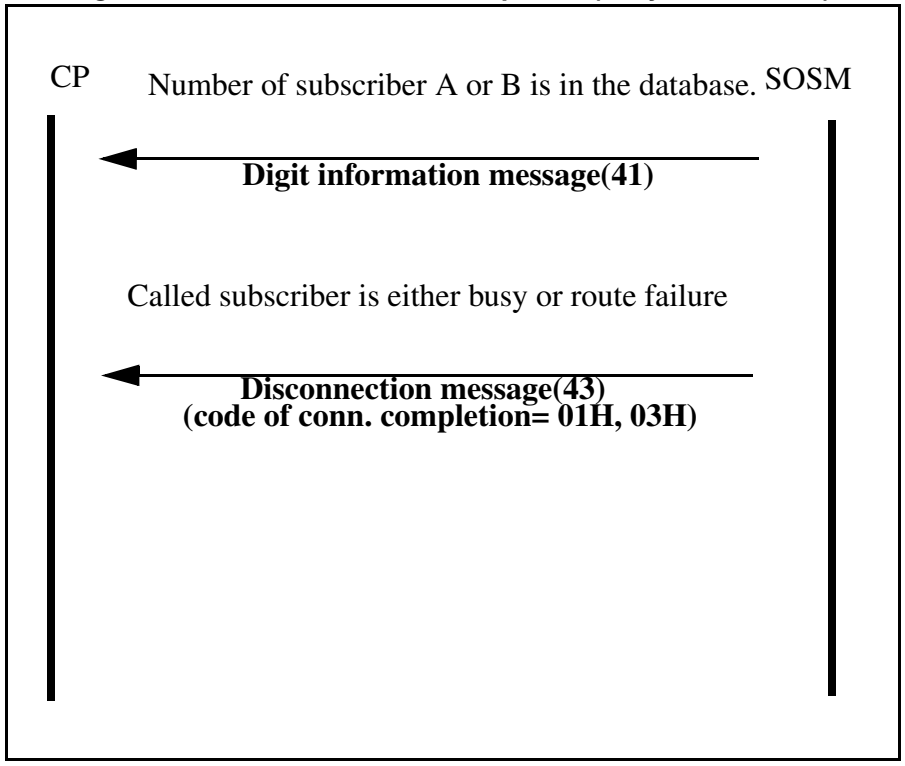


Figure 62 Messaging when the translation fails (partial/no dial)

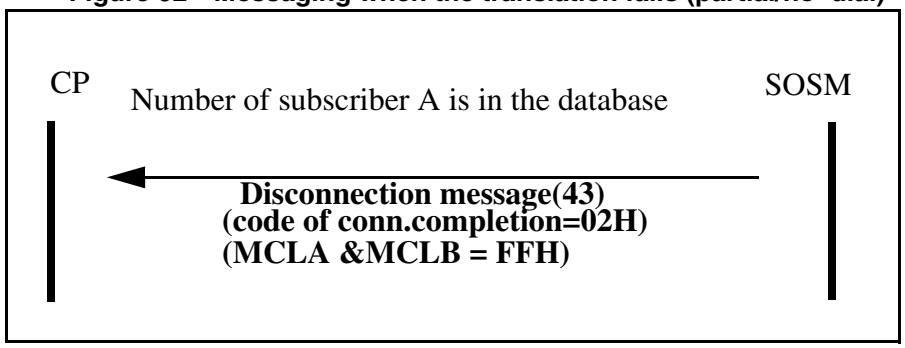
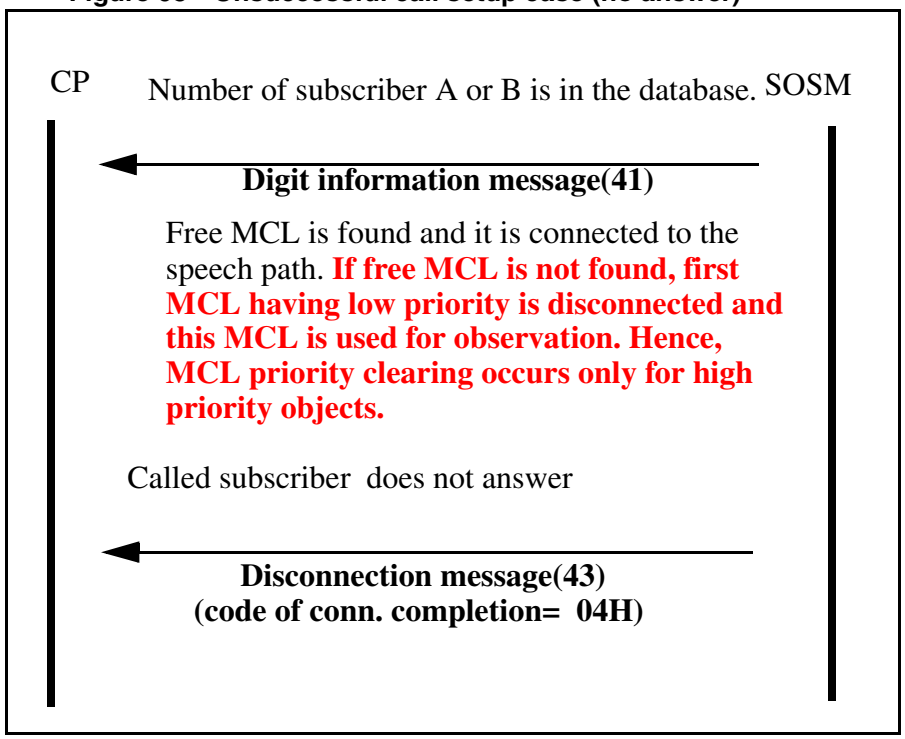
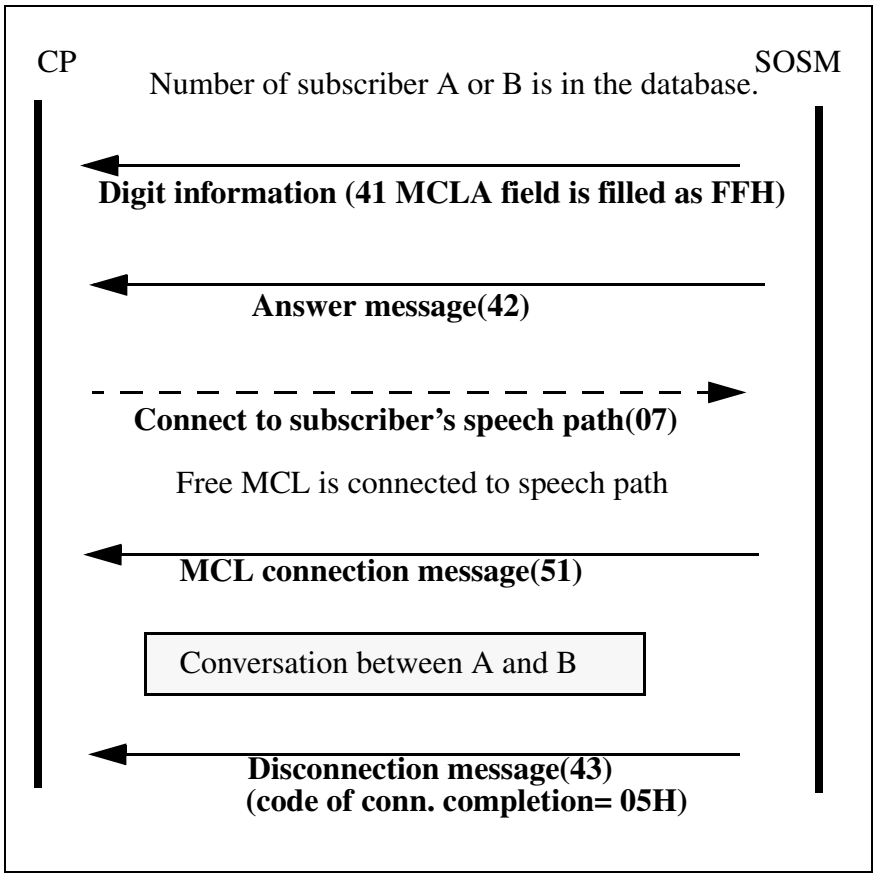


Figure 63 Unsuccessful call setup case (no answer)



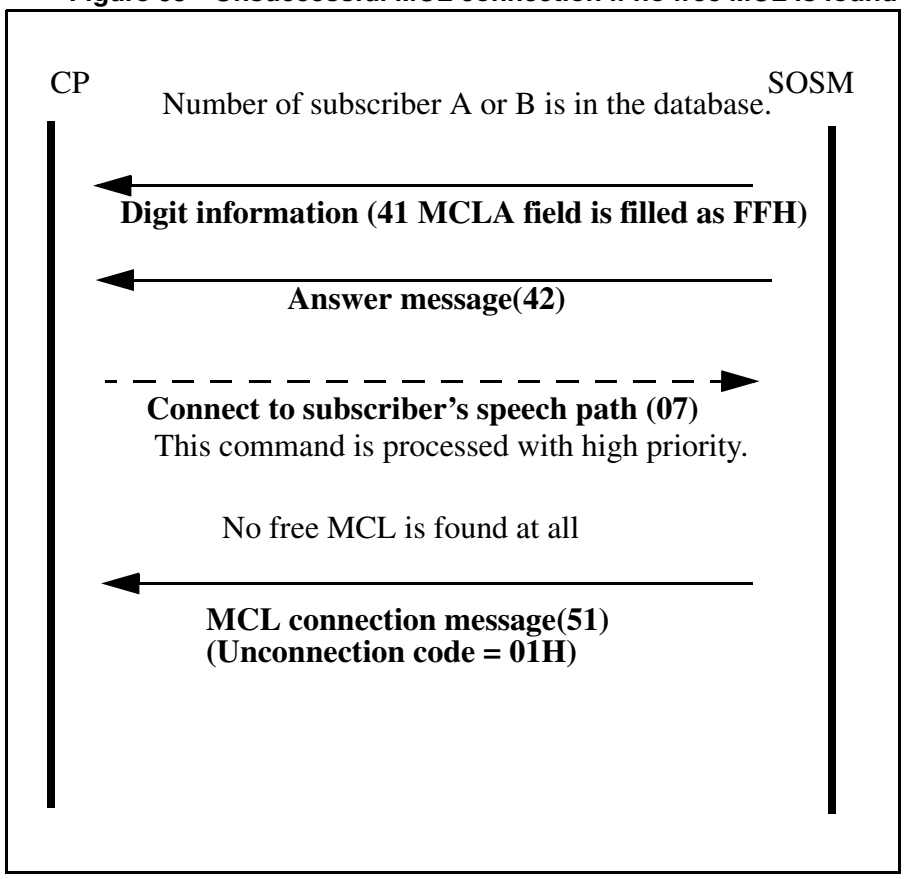
14.5.11.2 Supervised Subscriber with Statistical Monitoring

Figure 64 Successful MCL connection



After receiving "Connect to subscriber's speech path" command, category of monitoring is switched from statistical to complete ONLY for the specified call.

Figure 65 Unsuccessful MCL connection if no free MCL is found



14.6 Software Optionality Control (SOC)

Software Optionality Control is provided for this feature. SOC order code is SOSM0001.

While SOSM0001 is OFF:

- Any message received from CP are ignored. (DMS MMP neither executes the message nor sends response.)
- Access to SOSM configuration CI level is not permitted even if the valid password is entered.
- SOSM configuration tables SOSMMPC, SOSMTRK and SOSMPARM can be reached only within SOSMCONF CI level. Since access to SOSMCONF CI level is not permitted at this state, access to SOSM configuration tables is not possible while SOSM0001 is OFF.

Activation of SOSM0001:

- It is not allowed to turn SOSM0001 to ON state, while there is any other active NBD flavor (DNBD, etc...) on the switch.

While SOSM0001 is ON:

- Activation of any other Network Broadcast Delivery (NBD) application is prevented after turning SOSM0001 to ON state.
- Access to SOSM configuration tables via SOSMCONF CI level is possible.
- Commands received from CP are processed as described in the previous sections.

Deactivation of SOSM0001:

- Turning SOSM0001 OFF deactivates all SOSM applications on the exchange. SOSM is stopped, and all dynamic data within MCL and monitoring order databases are cleared.
- SOSM system password is reset with the initial password.
- Data in SOSMMPC, SOSMTRK and SOSMPARM tables remains unchanged. However, access to these tables are prevented as indicated above.

14.7 Password Management

The SOSM system has 3 different passwords:

- SOSM initial password
- SOSM current password
- SOSM CI access password

A Password is defined as a character string of no more and no less than SIX (6) bytes. Characters are represented as per the ASCII printable character set in the range (20H to FFH).

14.7.1 SOSM initial password

14.7.2 SOSM current password

14.7.3 SOSMCONF CI access password

14.8 Provisioning

The SOSM system makes use of several DMS MMP tables and commands for static data which is used in the operation of SOSM. The following sub-sections describe those tables and commands.

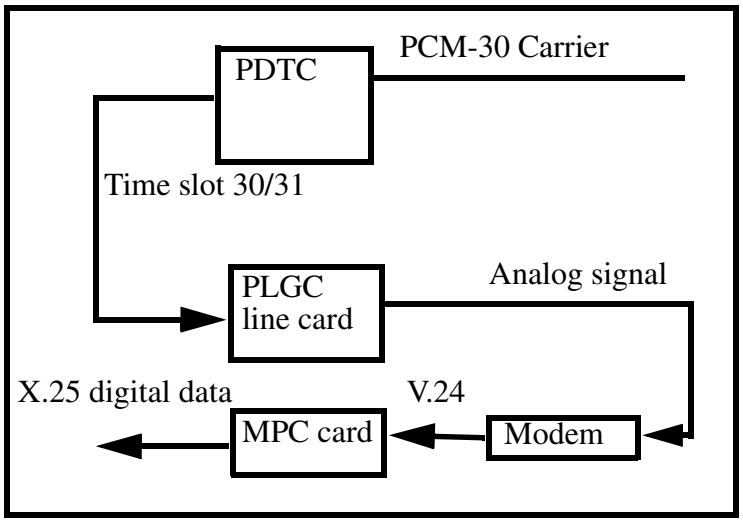
14.8.1 X.25 related tables

SOSM X.25 system uses the MPC card and associated tables to provide X.25 DTC 1 and 2. When X.25 data is transmitted via PCM-30 carriers, additional datafill is required to transfer that data from the PCM-30 carrier into the appropriate MPC card.

The following figure depicts the general configuration required for supporting X.25 on PCM-30. A connection is made between the MCL timeslot 30/31 on the carrier and a line card, via table SPCCON. The analog line is connected to a modem, which is then connected to the V.24 (RS232) port of the MPC card.

For each X.25 channel, a dedicated connection must be made. Semi-Permanent Connection trunks are used for this purpose.

Figure 66 X.25 on PCM-30 hardware configuration



The following sections describe the datafill requirement for MPC operations as well as additional datafill for X.25 on PCM-30 variant.

14.8.1.1 Table IOC

The datafill of this table is needed for IOM. Example datafill is shown in the following:

```
IOCNO FRTYPE FRNO SHPOS FLOOR ROW FRPOS MSCARD
MSPORT PECINFO

-----------------------------------------------

2   ISME 0    33     0   B     0     21    3  FX30AA
MTM 10 3   IOMRAS01 D010PMLD
```

```
3   ISME 0    47     0   B     0     20    3  FX30AA
MTM 11 3  IOMRAS01 D010PMLD
```

14.8.1.2 Table MPC

Table MPC must be datafilled with all the MPC card(s) used by the DMS-MMP. The SOSM system will use some of those cards for it's communications with the CP.

For each pair of data channels between the DMS MMP and the CP, one MPC card must be installed. Link 2 on the card will be used for Data Channel 1, and Link 3 for Data Channel 2.

At a minimum, one card must be installed and dedicated for SOSM. If multiple redundant cards are installed, each card will provide a redundant pair of Channels. When the card currently being used is experiencing trouble, the new card will automatically be selected.

An example datafill of table MPC is shown in the following table.

Table 15 Table MPC datafill example

MPCNO	MPCIOC	IOCCCT	EQ	DLDFILE
0	0	24	1X89BB	MPC403AC
1	1	24	1X89BB	MPC403AC
2	2	4	FX30AA	IOM$LOAD
3	3	4	FX30AA	IOM$LOAD

14.8.1.3 Table MPCLINK

Table MPCLINK is used to specify the protocol parameters of the X.25 link. For each MPC card and port (link), one entry must be datafilled in this table.

An example assumes clocking is provided by the Control Point X.25 card. An example datafill of table MPCLINK is shown in the following table. The example assumes clocking is provided by the Control Point X.25 card.

Table 16 Table MPCLINK datafill example for Modem Connection

LINKKEY	LINKALM	PRTCLDAT
1 1	Y	X2584 0 0 (NODETYPE DTE) (CLKSRCE EXTERNAL) (THRUPUT T9600) (NUMPVCS 1) (PVCDBIT DON)$ $
1 2	Y	X2584 0 0 (NODETYPE DTE) (CLKSRCE EXTERNAL) (THRUPUT T9600) (NUMPVCS 1) (PVCDBIT DON)$ $

Table 17 Table MPCLINK datafill example for Direct Cable Connection[a]

LINKKEY	LINKALM	PRTCLDAT
1 1	Y	X2584 0 0 (NODETYPE DTE) (CLKSRCE EXTERNAL) (THRUPUT T9600) (NUMPVCS 1) (PVCDBIT DON)$ $
1 2	Y	X2584 0 0 (NODETYPE DTE) (CLKSRCE EXTERNAL) (THRUPUT T9600) (NUMPVCS 1) (PVCDBIT DON)$ $

a. Note that datafill in this table may change depending on Control Point configuration.

Each entry corresponds to one link on the card.

The LINKKEY (Link Key) field identifies which MPC is used (i.e. MPC 3 Link 2 will appear as 3 2).

The LINKALM (Link Alarm) field controls the generation of system alarms in case when the link goes in to trouble state (SBSY).

The PRTCLDAT (Protocol Data) field specifies the protocol parameters.

There are several other X.25 L2 and L3 parameters that may be added, depending on the configuration of the control point X.25 system.

14.8.1.4 Table SOSMMPC (new)

Table SOSMMPC is used to map existing MPC cards and links in the office to pairs of SOSM channel 1 and 2. For each SOSM pair of channel, one entry is required.

This table can ONLY be accessed via SOSMCONF CI. Direct access attempt will result in “unauthorized access” message sent to CP, and any table commands thereafter is rejected. For information regarding SOSMCONF please refer to “2.7.3 SOSMCONF CI access password” on page 150.

An example datafill is shown in the following table.

Table 18 Table SOSMMPC example datafill

SOSMLINK	CHNL1	CHNL2
0	0 2	0 3
1	1 2	1 3
2	2 2	3 3

The SOSMLINK field indicates the SOSM Link number. Each new number can be used for redundancy. At least one entry must be present for SOSM to operate.

The CHNL1 and CHNL2 fields specify the MPC number and Link number to be used. MPC number must be a valid MPC datafilled in table MPC. The link number must can be {2 or 3} and must be a valid link datafilled in table MPCLINK.

CHNL1 and CHNL2 do not have to reside on the same MPC card.

Note: *The deletion of the active link in this table is denied while SOSM is active. Other tuples (non-active links) can be deleted or added when sosm is active.*

14.8.1.5 Table LINEATTR

This table is used to define the Line Attribute Index of a line. The SOSM application uses it to define the dedicated lines used for connection between the MCL carrier (TS 30 or 31) and the modem. This line must be have a Line Class Code (LCC) of type **SPC.** An example datafill is shown below:

```
15 SPC NONE NT 15  15 NILSFC 0  PX  NETXLA NTRS02 00
102_NPRT_1 NLCA_NILLA_1 $
```

14.8.1.6 Table LCCOPT

To define SPC line in MMP, the following tuple must be in table LCCOPT.

```
SPC (DGT) $
```

14.8.1.7 Table LENLINES

Example SPC line datafill is shown below:

> Servord

> new $ 7835479 spc 15 HOST 01 0 00 09 DGT $

table LENLINES:

```
HOST 01 0 00 09 S 0 102 7835479 DT 27 102_NPRT_1
NLCA_NILLA_1 $
```

14.8.1.8 TABLE SPCCON

This table is used for making Leased line (Semi-permanent) connections on DMS MMP. The SOSM system uses it to make a connection between an MCL trunk and a line card. The analog output of the line is then connected to the Modem. Trunks and lines datafilled in table SPCCON MUST be of type SPC.

An example datafill is shown below:

Table 19 SPCCON Datafill

SPCKEY	AGENT1	AGENT2	CONNECT
0	SOSMGRP0	LINE HOST 01 0 00 09	Y

Agent 1 identifies the trunk member to use. This trunk must be previously datafilled in table TRKMEM and put into service (please refer to "2.8.2 MCL trunk related datafill" on page 155 for complete information on creation of SOSM MCL trunks).

Agent 2 identifies a line dedicated for the SOSM X.25 connection. This line must be properly created and put in service prior to datafill of table SPCCON.

The CONNECT field indicates if a connection should be established when the datafill is complete.

14.8.2 MCL trunk related datafill

The SOSM MCL trunks are implemented using SPC (Semi-Permanent Connection) trunks with no signalling.

These MCLs are used to transmit speech information to CP, as well as to provide X.25 channels for commands and data (if variant 1 is required).

Note that there is no correspondence between MCL groups and PCM-30 trunk groups. An MCL group can contain members from different PCM-30 trunk groups. However, for each group of PCM-30 carriers, there must be a UNIQUE CLLI assigned as shown in the sections to follow.

To provide MCL trunks the following datafill order is required: CLLI, TRKGRP, TRKSGRP, TRKMEM, SOSMTRK (via SOSMCONF CI).

When a PCM-30 trunk group is datafilled in table SOSMTRK, that trunk group can not be deleted from TRKGRP table.

The sections to follow describe each table and provide a datafill example. For complete information regarding these tables, please refer to the appropriate NTP.

14.8.2.1 Table CLLI

Table CLLI is used to define Common Language Names for every piece of equipment on the DMS MMP. The SOSM system uses it to define MCL trunk groups. An example datafill for SOSM MCL trunk groups in table CLLI is shown in the following table.

Table 20 Table CLLI datafill

CLLI	ADNUM	TRKGRSIZ	ADMININF
SOSMGRP0	218	30	SOSM_MCL_GROUP_0
SOSMGRP1	219	30	SOSM_MCL_GROUP_1
SOSMGRP2	220	30	SOSM_MCL_GROUP_2
SOSMGRP3	221	30	SOSM_MCL_GROUP_3
SOSMGRP4	222	30	SOSM_MCL_GROUP_4
SOSMGRP5	223	30	SOSM_MCL_GROUP_5
SOSMGRP6	224	30	SOSM_MCL_GROUP_6
SOSMGRP7	225	30	SOSM_MCL_GROUP_7

For each PCM-30 group of MCLs, a separate CLLI is required. The number of members specified in TRKGRSZ corresponds to the number of PCM-30 time slots in an MCL group.

14.8.2.2 Table TRKGRP

This table is used to define the characteristics of a trunk in DMS MMP. For each trunk group, a tuple must be datafilled.

The SOSM system uses this table to define MCL trunk groups. An example datafill of this table is shown in the following table. The example shows eight MCL groups for up to 224 MCLs.

Table 21 Table TRKGRP datafill

GRPKEY	GRPTYP	TRAFSNO	PADGRP	NCCLS	GRPINFO
SOSMGRP0	SPC	0	NPDGP	NCRT	OG
SOSMGRP1	SPC	0	NPDGP	NCRT	OG
SOSMGRP2	SPC	0	NPDGP	NCRT	OG
SOSMGRP3	SPC	0	NPDGP	NCRT	OG
SOSMGRP4	SPC	0	NPDGP	NCRT	OG

Table 21 Table TRKGRP datafill

GRPKEY	GRPTYP	TRAFSNO	PADGRP	NCCLS	GRPINFO
SOSMGRP5	SPC	0	NPDGP	NCRT	OG
SOSMGRP6	SPC	0	NPDGP	NCRT	OG
SOSMGRP7	SPC	0	NPDGP	NCRT	OG

For each PCM-30 group a separate trunk group must be defined.

The GRPTYP field MUST be SPC, and the direction field must indicate OG (outgoing).

14.8.2.3 Table TRKSGRP

This table is used to provide more specific information about a trunk group. An example datafill is shown in the following table.

Table 22 Table TRKSGRP datafill

SGRPKEY	CARD-CODE	SGRPVAR
SOSMGRP0	DS1SIG	NOSIG

The card-code filed MUST specify P30CAS, and SGRPVAR must be NOSIG.

14.8.2.4 Table TRKMEM

This table defines the peripheral and carrier parameter of each PCM-30 carrier in a trunk group. The SOSM system uses a PDTC with QDT load for MCL trunks. For each MCL in a PCM-30 group, a tuple must be added to this table. The following table provides an example datafill.

Table 23 Table TRKMEM datafill

CLLI	EXTRKNM	SGRP	MEMVAR	
SOSMGRP0	1	0	PDTC	7 2 21

The CLLI field corresponds to the PCM-30 group name created in table CLLI and further defined in tables TRKGRP and TRKSGRP. The EXTRKNM field identifies the trunk member number. The member information field identifies the PDTC on which the trunk is installed (e.g. PDTC 7) and the carrier number (e.g. 2) and timeslot number (e.g. 21) on that carrier.

For a PCM-30 group of MCLs with all members defined, there must be one tuple per MCL member (i.e. members 1 through 28). If X.25 channels 1 and 2 are transmitted over PCM-30, two additional members are required (30 and 31).

There is a one-to-one correspondence between the member number in field EXTRKNM and MCL number. Mapping of MCL number to Timeslot number is done via the MEMVAR field.

> ***Note:*** *MCL numbers 1 through 15 map to Timeslot 1 through 15. Timeslot 16 IS NOT USED! MCL 16 must be mapped to Timeslot* ***17****, MCL 17 to Timeslot* ***18****, and so on up to MCL 28- timeslot 29. The following table shows an example of this mapping.*

Suppose PDTC 7 carrier 0 is used, and the PCM-30 group number is 0 (i.e. table SOSMTRK contains a tuple: 0 SOSMGRP0). The following table gives the correct mapping between TRKMEM datafill and MCL numbers.

Table 24 Mapping of Time Slot to MCL numbers

Trunk Member Number (EXTRKNM in table TRKMEM)	MEMVAR field	Timeslot	PCM-30 Group number in CP commands and messages	MCL member number (in CP commands and messages)
0	PDTC 7 0	0	N/A	N/A
1	PDTC 7 0 1	1	0	1
2	PDTC 7 0 2	2	0	2
3	PDTC 7 0 3	3	0	3
4	PDTC 7 0 4	4	0	4
5	PDTC 7 0 5	5	0	5
6	PDTC 7 0 6	7	0	6
7	PDTC 7 0 7	7	0	7
8	PDTC 7 0 8	8	0	8
9	PDTC 7 0 9	9	0	9
10	PDTC 7 0 10	10	0	10
11	PDTC 7 0 11	11	0	11
12	PDTC 7 0 12	12	0	12
13	PDTC 7 0 13	13	0	13

Table 24 Mapping of Time Slot to MCL numbers

Trunk Member Number (EXTRKNM in table TRKMEM)	MEMVAR field	Timeslot	PCM-30 Group number in CP commands and messages	MCL member number (in CP commands and messages)
14	PDTC 7 0 14	14	0	14
15	PDTC 7 0 15	15	0	15
16	PDTC 7 0 17	17	0	16
17	PDTC 7 0 18	18	0	17
18	PDTC 7 0 19	19	0	18
19	PDTC 7 0 20	20	0	19
20	PDTC 7 0 21	21	0	20
21	PDTC 7 0 22	22	0	21
22	PDTC 7 0 23	23	0	22
23	PDTC 7 0 24	24	0	23
24	PDTC 7 0 25	25	0	24
25	PDTC 7 0 26	26	0	25
26	PDTC 7 0 27	27	0	26
27	PDTC 7 0 28	28	0	27
28	PDTC 7 0 29	29	0	28
29	PDTC 7 0		N/A	N/A

14.8.2.5 Table SOSMTRK (new)

This table is used by the SOSM system for mapping generic trunk groups into dedicated SOSM trunks. Each entry identifies a trunk group to be used for the PCM-30 group of MCLs.

This table can ONLY be accessed via SOSMCONF CI, while SOC SOSM0001 is ON.

While SOSM0001 is ON,direct access attempt to this table will result in “unauthorized access” message sent to CP, and any table commands thereafter is rejected. For information regarding SOSMCONF please refer to “2.7.3 SOSMCONF CI access password” on page 150.

An example datafill is shown in the following table.

Table 25 Table SOSMTRK example datafill

SOSMGRP	CLLI
0	SOSMGRP0
1	SOSMGRP1

The SOSMGRP field identifies the PCM-30 group number (0 through 7).

The CLLI field identifies the trunk group to be used. The CLLI entered here must correspond to a valid trunk datafilled in tables CLLI, TRKGRP, TRKSGRP and TRKMEM.

When a trunk is datafilled in this table, it can not be deleted from tables TRKGRP and TRKMEM.

Note: *Changing data in this table will result in an "Unauthorized access to SOSM" message if the SOSM system is active, and the change will be rejected. SOSM must be switched OFF with a "STOP SOSM" command from CP before data is removed or changed.*

14.8.3 Provisioning of SOSM specific parameters

Table SOSMPARM is used by SOSM for saving SOSM specific parameters.

This table can ONLY be accessed via SOSMCONF CI while SOC SOSM0001 is ON.

While SOSM0001 is ON, direct access attempt to SOSMPARM will result in "unauthorized access" message sent to CP, and any table commands thereafter is rejected. For information regarding SOSMCONF please refer to "3.6.3 SOSMCONF CI access password" on page 133.

SOSMPARM table has 2 fields ; PARMNAME, and PARMVAL.

PARMNAME is the name of the parameter. Currently, TOLL_EXIT_ CODE, INTRAZONAL_CODE, and INTERNTNL_CODE parameters exist within this table.

The second field is PARMVAL. This field is a refinable area. Each parameter refines this area to hold its required data.

The selector field in PARMVAL area is PARMSEL. It identifies the appropriate subfields within PARMVAL area for the corresponding SOSM parameter.

Table 26 Default SOSMPARM tuples

PARMNAME	PARMVAL	
	PARMSEL	EXCODE
TOLL_EXIT_CODE	TOLL	8 (1 digit is allowed for this parameter)
INTRAZONAL_CODE	INTRAZONAL	2 (1 digit is allowed for this parameter)
INTERNTNL_CODE	INTERNTNL	10 (1-2 digit(s) are allowed for this parameter)

Data in SOSMPARM table can not be deleted. Furthermore, addition of new tuples with table editing commands is prevented by SOSM software. Default values for parameters which are provisionable via SOSMPARM are given in Figure 25, "Default SOSMPARM tuples".

It is not permitted to change PARMSEL for TOLL_EXIT_CODE, INTRAZONAL_CODE and INTERNTNL_CODE by table editing commands.

Note: *Changing data in this table will result in an "Unauthorized access to SOSM" message if the SOSM system is active, and the change will be rejected. SOSM must be switched OFF with a "stop sosm" command from CP before data is changed.*

14.8.4 Access to SOSM configuration tables and parameters : SOSMCONF

Access to SOSM configuration tables, namely, SOSMMPC, SOSMTRK and SOSMPARM is restricted. The only way to reach these tables is with a new CI level called SOSMCONF (SOSM CONFiguration). In order to reach this CI level, the correct SOSM CI access password must be entered.

SOSMCONF provides the access to tables SOSMMPC, SOSMTRK, and SOSMPARM through normal table control, only after a valid password is entered. If password checking fails three consecutive times, the SOSMCONF CI is exited and an unauthorized access message will be sent to CP.

If access to either tables SOSMMPC, SOSMTRK, or SOSMPARM is attempted outside of SOSMCONF level, the corresponding unauthorized access message will be sent to CP.

Access to SOSMCONF CI level is not permitted while SOC SOSM0001 is OFF state.

The following example shows editing of table SOSMTRK via SOSMCONF.

```
>SOSMCONF
THIS IS THE SOSM CONFIGURATION TABLES
          ACCESS INCREMENT
SOSMCONF:
ENTER PASSWORD:
>******
INVALID PASSWORD
ENTER PASSWORD:
>******
 ************************************
 *          ACCESS CONFIRMED *
 *     SOSM CONFIGURATION TABLES *
 *           ACCESS LEVEL *
 ************************************
>table SOSMTRK
TABLE: SOSMTRK
>QUIT
SOSMCONF
>QUIT
CI:
```

In this example, a wrong password was entered, followed by a valid password. Once access is granted, all normal editing can resume using TABLE command.

In the next example, attempt to access table SOSMTRK directly is blocked:

```
>table SOSMTRK
EMPTY TABLE
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SOSMMPC
>
>ADD 1 SOSMGRP1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
YOU ARE NOT AUTHORIZED TO REACH TO THIS TOOL
TUPLE TO BE ADDED:
  2     2 2     2 3
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>N
DMO REJECTED
WARNING:  CURRENTLY NOT POSITIONED
>QUIT
CI:
>
```

In the above example, the craftsperson attempts to access the table directly rather than through SOSMCONF. An attempt to ADD a tuple to the table results in unauthorized access message with code **05H**, and the add command is refused.

14.9 Hardware Requirements

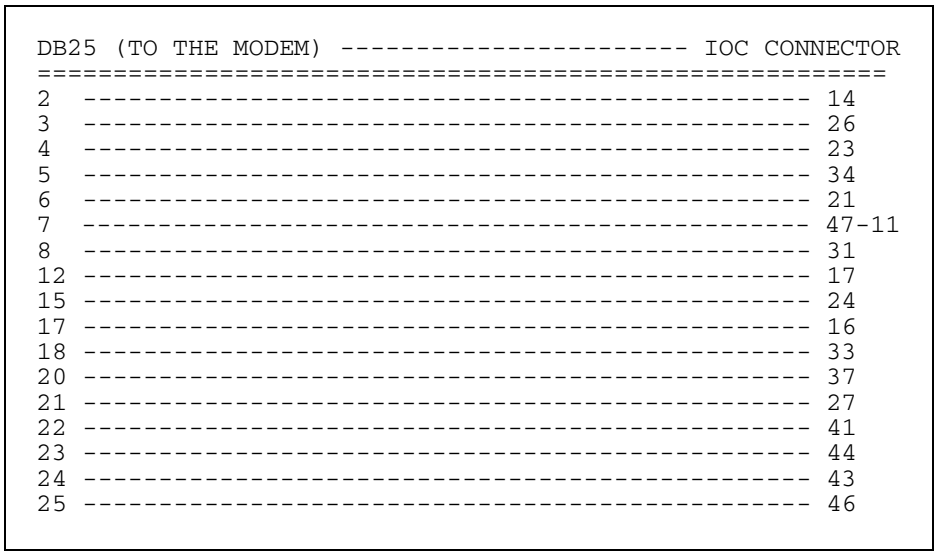
The exchange must be provisioned with additional conference circuits to support SOSM combined monitoring. For each MCL there must be one conference port (i.e. if 112 simultaneous calls with combined monitoring are allowed, 112 conference circuits are required.

Either MPC cards (NT1X89) or IOM must be installed to provide X.25 connection to the control point. For each pair of X.25 channels, one MPC card is needed.

If X.25 data is carried over PCM-30 channels, one dedicated line card per X.25 channel is required on an PLGC.

For each X.25 channel one **synchronous power-up leased line modem** is required to be connected between the serial port of the MPC card, and the data source (either line card for PCM-30 X.25 variant) or directly to the other (CP) modem. The serial port of the modem is connected to the MPC card via IOC to DB25 cable, NT part ID: **PEC NT0X26LY**. Pinout mappings are as follows:

Figure 67 Pinout mappings for DB25-IOC connector



MCL trunks must be provisioned on an existing or new DTC and datafilled as described in “2.8.2 MCL trunk related datafill” on page 155.

Configuring an IOM

The Input Output Module (IOM) replaces the functionality of the DMS IOC. The IOM minimally consists of an IOM motherboard, NTFX30AA, and an IOM paddleboard, NTFX31AA. The NTFX30AA inserts into a universal slot, slot 3 or 4, of an ISME or CISM shelf. The NTFX31AA attaches to thebackplane behind the NTFX30AA. The NTFX30AA paddleboard has twenty 2x4 connector sockets. Two of the twenty are spares, two are Message Switch links (for planes 0 and 1), and the remaining sixteen, numbered 0 through 15, are connected via 26 gauge two-pair twisted-pair cabling to what are called smart-connectors. The cable that connects the paddleboard 2x4 connectors directly to a smart- connector is an NT0X96LU; it has a 2x4 connector on one side, and has a six position modular plug on the smart-connector side. In the case of a CISM shelf, the paddleboard’s connectors are brought out to the bulkhead using cable harnesses (one DB37 per 8 ports and

MS link), and each port appears on the outside of the frame as a separate 1x4 connector; the cable between these 1x4 connectors and the smart-connectors is an NTRX26GA. As viewed by a user of the bulkhead connectors, the IOM in slot 3 is on the right, and the IOM in slot 4 is on theleft. The bottom 1x4 in each column of nine connectors is for a Message Switch link; the upper eight correspond to the eight positions of the 2x4 sockets on the IOM's paddleboard.

**** The following description is restricted to synchronous data links only. ****

For EIA/TIA-232-F, the NTFX34AA smart-connector is used. For ITU_T V.35, either the NTFX35AA or the NTFX35BA smart- connectors are used; the NTFX35AA is used for speeds up to and including 64 KBPS, and the NTFX35BA is used for speeds up to and including 512 KBPS. When the NTFX35BA is used, only two of the sixteen IOM ports, ports 0 and port 8, can be used, and the IOM firmware name is of the form IOMHaann, where a is an alphabetic and n is a numeric. Normally, the regular IOM firmware is used; its name is of the form IOMRaann. Under the regular IOM firmware, any combination of NTFX34AAs or NTFX35AAs can be connected to any of the sixteen ports, observing IOM engineering guidelines to prevent overloading.

Neither a disk nor a DAT can be configured on an IOM that is running IOMHaann (high speed) firmware, but either or both may be on an IOM used for lower speed serial interfaces.

IOM smart-connectors ARE ALWAYS HARDWARE DTEs. They can provide ITU_T circuit 113 (ANSI/EIA/TIA circuit DA) clock. The DTE clock rate is controlled by DMS datafill.

The NTFX35BA smart-connectors' DTE clock is always 512 KBPS.

Smart-connectors, unlike MPC and EMPC cards, provide signal ground isolation, and can therefore be directly connected to DCEs that may or may not provide ground isolation. Modems or modem-eliminators are no longer necessary for National Electric Code compliance.

Smart-connectors may be connected to their IOM paddleboard with up to 750 feet of cabling.

The housing of the smart-connector can and should be bonded to the DCE's ground. This will not cause a ground loop.

The DCE's timing provided to the smart-connector's receive and transmit clocks must be at the same rate and must be in-phase. The easiest way of accomplishing this is to set the DCE to derive its transmit clock from receive data, or by setting both receive and transmit clocks to synchronize with the digital network serving the DCE (the DS1/E1 transmit side should always be traceable to the receive side). In other words, the modem physically connected to a smart-connector should always be set to "slave" timing, and the other modem should be set to either "internal" or "external" timing.

Other than the clocking restriction, both V.35 smart-connectors are perfect implementations of CCITT Red BookAppendix II, and are in the range for maximum compatibility with ITU_T V.11 or EIAConfiguring an IOM-422-B balanced interchange circuit drivers.

The NTFX34AA has a male DB25 connector complying with ISO 2110-1991(E) pin definitions for EIA/TIA-232-F.

The NTFX35AA has a male DB25 connector. The V.35 pin definitions match the DMS EMPC DB25, and are listed on a data sheet provided with every smart-connector. The NTFX35AA can be adapted to an ISO 2593 DTE (male) connector by using an NTFX3505, B0250556. (Standard V.35.)

The NTFX35BA has a male DB25 connector. The V.35 pin definitions match the MVME 709-1 DB25, and are listed on a data sheet provided with every smart-connector. The NTFX35BA can be adapted to an ISO 2593 DTE (male) connector by using an NTFX3506, B0250557. (High speed V.35.)

One of the two twisted-pairs between a smart-connector and the IOM paddleboard transmits data from the smart- connector to the IOM. This pair is biased with 48 vdc which is used to power the smart-connector. If the smart-connector suffers an internal failure or this twisted-pair becomes shorted, the IOM will discontinue powering that line until the short/overload is removed; it will then automatically restore power to that line.

Smart-connectors will illuminate a green LED when they are properly configured and in service.

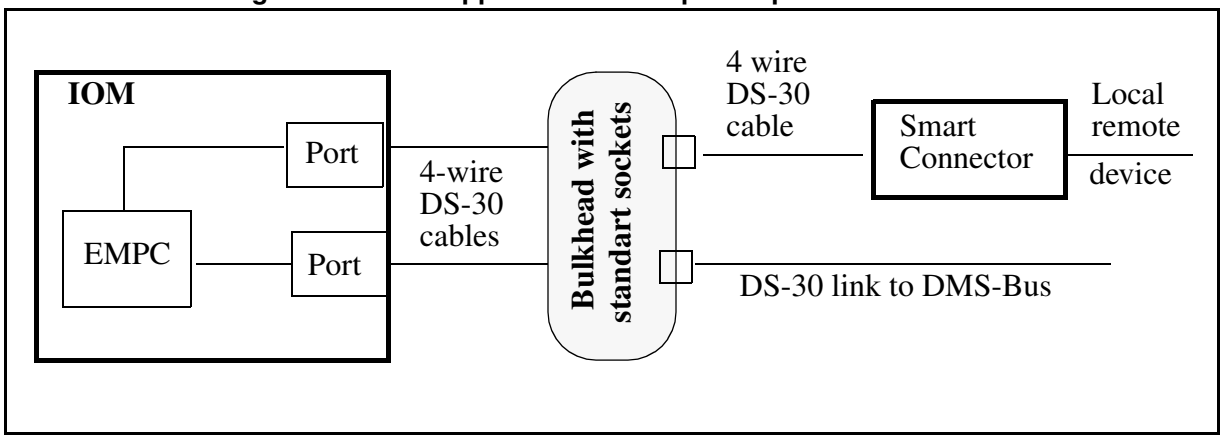
DMS datafill of the IOM is similar to IOC/EMPC datafill; three tables are involved: IOC, MPC, and MPCLINK. The IOM is first datafilled in table IOC and given a unique IOC number; associated with that IOC number are the MS ports, location, and the firmware to be downloaded to the IOM. Then a unique MPC number is arbitrarily chosen and used as an index in table MPC; the MPC number is associated with the IOC number just datafilled in table IOC, and with a port on the IOM, 0 through 15. Unlike EMPCs, the firmware file, already specified in table IOC, is always datafilled in table MPC as IOM$LOAD. In table MPCLINK, the IOM port is indexed with an MPC number, just assigned in table MPC, and a link number which is always 3 for

IOM ports; the MPCLINK entry contains the same configuration parameters that would be used for an EMPC port - with two exceptions for an NTFX35BA. When an NTFX35BA port is entered in table MPCLINK, its Electrospec is 512KV35, and parameter RITMAX should be set to 0. Again, a smart-connector is always a hardware DTE, so only the NODETYPE, DTE or DCE, needs to be set for appropriate LAPB addressing; the hardware type (DCE/DTE/DXE) should not be datafilled.

MAPCI commands allow the IOM firmware version to be queried. There are also commands to ask the IOM if it sees the correct smart-connector on a port, and commands to test data connectivity with the smart-connector via loopback testing. The DMS NTPs cover downloading, programming, and testing of the IOM and its smart-connectors.

At the device end of the cable is a smart connector that performs the necessary mapping between the standart 4-wire interface and the external interface, as summarised in figure 67.

Figure 68 IOM support for serial input/output



14.10 Software Requirements

N/A.

14.11 Feature Interactions

This section describes the feature interactions of SOSM and other subscriber services. For each feature, message sequence is shown identifying some basic information reported to CP.

For IBN agents, SOSM supports usage/activation/deactivation and interrogation of only CEPT features. For BRI agents ISDN BRI Supplementary services are supported.

SOSM sends service usage notification message(s) only if both the subscriber using the service and the monitored subscriber are in the same exchange.

For PRI agents ISDN PRI Supplementary services are supported. But SOSM sends service usage notification message(s) only for ETSIDIV, ECT and CUG supplementary services.

14.11.1 IBN CEPT Services

Usage, activation, deactivation, and interrogation of IBN CEPT services are reported to CP.

SOSM behavior for CEPT service interactions are determined regarding to Annex 2 of "Typical Program and Methods for Certification Tests of Communications Interface and Information Interexchange Protocol in Data Transfer Channels Between SOSM and CP on Electronic Telephone Exchanges" document.

In this document, reporting of service usage messages is mentioned as optional in several scenarios. SOSM reports optional service usage messages to CP if data regarding to usage of the service is available.

Any subscriber can put the connected subscriber on HOLD by FLASH.

In any of the scenarios described, when a party is put on HOLD, its MCL connection (if any) is also held.

The activation, deactivation and interrogation of CEPT IBN features (ILR, IWUC, CFU, CFB, CFD, ICWT, SCL, LNR, WML, CCBS, CND, SUPPRESS, CEPTPW) will be reported to CP. Message 1.4 indicating the code of service to be rendered to the subscriber will be sent. If these CEPT features are not assigned to the line, but exists in table CUSTSTN as default features, message 1.4 will be again send

A subscriber can activate/deactivate/interrogate CEPT features also within answered calls. In such scenarios, SOSM reports service activation/ deactivation/interrogation of CEPT services only for the observed subscribers.

The following shown scenarios through this section are for "complete combined" monitoring. The attribute of object's selection for other monitoring types are shown in "Table 26 Attribute of object's selection values" on page 168.

Table 27 Attribute of object's selection values

	Calling DN is SOSM subscriber	Called DN is SOSM subscriber	No one is SOSM subscriber in message
complete combined	01H	04H	40H
complete separate	03H	0CH	C0H
statistical	02H	08H	80H

If MCL connection cannot be established, only MCL-A and MCL-B fields of call messages are set to FFH, and any other information (i.e. Attribute of Objects Selection) is not affected by the failure.

14.11.1.1 Hold Functionality

Enquiry is responsible to setup multi-party calls as well as a base for Call Waiting, Call Transfer, Three Way Calling and Six Way Calling features.

When a party is added to a call via Enquiry, SOSM criteria check is performed on the added leg. If the controller is a SOSM subscriber, a new SOSM call number is allocated and the new call leg will be monitored as if it was a normal SOSM call. The original connection is also put on hold. When the controller returns to the original first call, the MCL connection is reactivated.

The following sections describe the messaging and behavior in each Enquiry scenario.

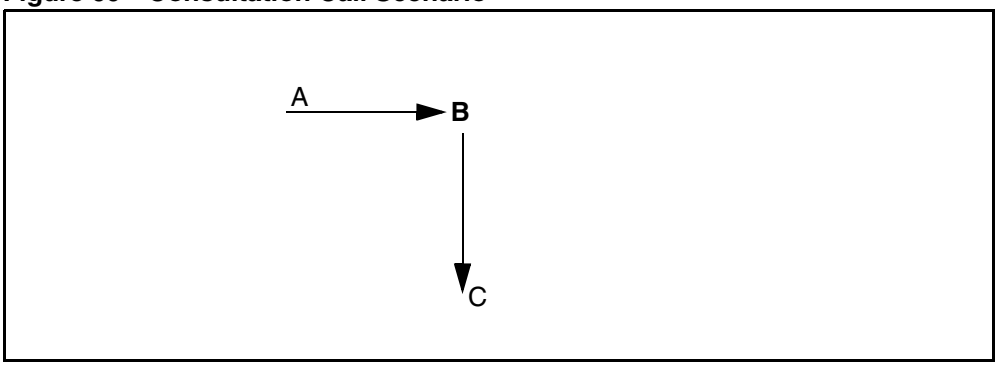
14.11.1.1.1 Consultation Call

In this scenario, B is the controller which has one of the Enquiry feature options. A calls B, B answers. B flashes (holds party A) and calls C. C answers. While A and C are talking, C hangs-up. B flashes and dials R-code for toggle to return to A. Sometime later, conversation ends.

For IBN lines, I3WC, I6WC, ICT, ICWT line options provide this functionality.

If controller exists during consultation call, held party will rering the controller. The existing MCL connection will be active. The same messages will be sent.

Figure 69 Consultation Call Scenario



The message sequence is shown in the following tables

Table 28 A is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 29 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	B	A
Called DN	B	B	A	C	C	C	A	B
SOSM Call #	1	1	1	2	2	2	1	1
Attribute of choice	04	04	01	01	01	01	01	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.1	1.2	1.3	1.4	1.3
Code of supp. service phase	00	00	04	00	00	00	04	00
MCL #	1	1	1	2	2	2	1	1
Code of operation	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HOLD	FF	FF	FF	HOLE	FF

Table 30 C is under surveillance

	1.1	1.2	1.3
Calling DN	B	B	B
Called DN	C	C	C
SOSM Call #	2	2	2
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

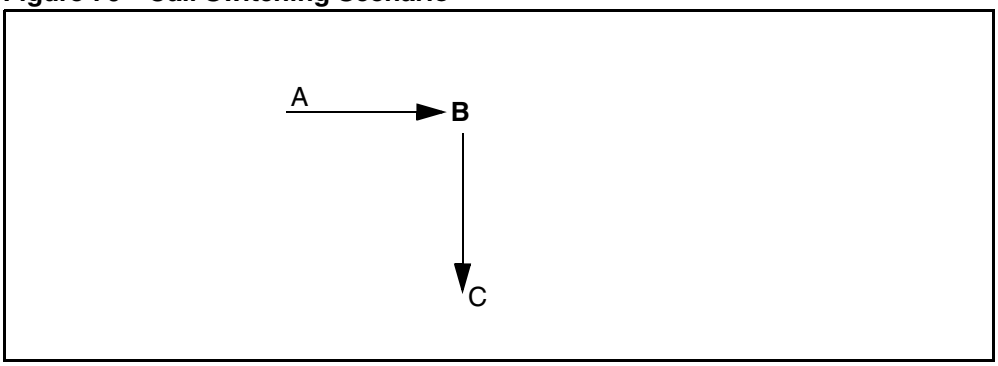
14.11.1.2 Call Switching

In this scenario A calls B, B flashes (holds party A) and calls C. During conversation with C, B flashes (holds subscriber C), then dials R-code for toggle and re-connect to A. B switches to C, and then switches to A again. A to B call disconnects. The other call disconnects.

For IBN lines, I3WC, I6WC, ICT, ICWT line options provide this functionality.

In this scenario, MCL connection suspends after flashes, and resumes when speech is re-established.

Figure 70 Call Switching Scenario



The message sequence is shown in the following tables.

Table 31 A is under surveillance

	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	A	A	B	B	B	B	A
Called DN	B	B	A	A	A	A	B
SOSM Call #	1	1	1	1	1	1	1
Attribute of choice	01	01	04	04	04	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

Table 32 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.4	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	B	B	B	B	B	A	B	B
Called DN	B	B	A	C	C	C	A	A	C	C	A	B	C	C
SOSM Call #	1	1	1	2	2	2	1	1	2	2	1	1	2	2
Attribute of choice	04	04	01	01	01	01	01	01	01	01	01	04	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.4	1.3	1.4	1.3
Code of supp. service phase	00	00	04	00	00	04	04	04	04	04	04	00	04	00
MCL #	1	1	1	2	2	2	1	1	2	2	1	1	2	2
Code of operation	00	00	00	00	00	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	HO LE	HO LD	HO LE	HO LD	HO LE	FF	HO LE	FF

Table 33 C is under surveillance

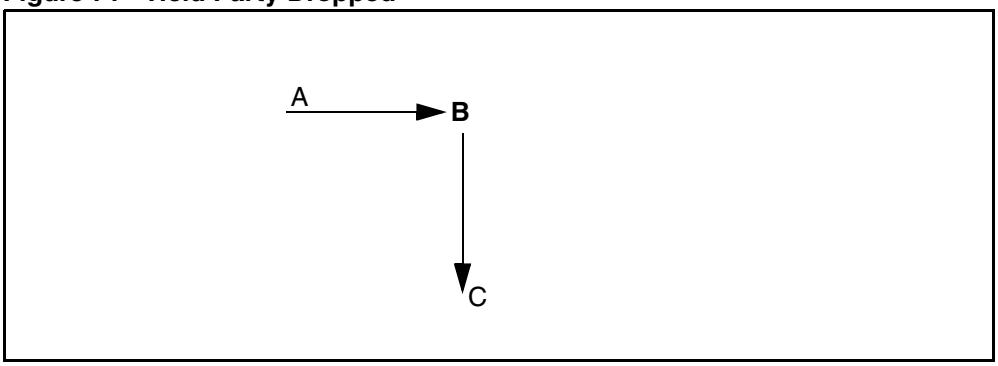
	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B	B
Called DN	C	C	C	C	C	C	C
SOSM Call #	1	1	1	1	1	1	1
Attribute of choice	04	04	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

14.11.1.2.1 Drop Held Party during Enquiry

In this scenario B is the controller which has one of the enquiry feature options. A calls B, B flashes and calls C. During conversation with C, B flashes (holds C) and dials R-code for disconnect first held party (A) and reconnects to C. Then B-C call is disconnected.

In this scenario, MCL connection suspends after flashes, and resumes when speech is established.

Figure 71 Held Party Dropped



The message sequence is shown in the following tables.

Table 34 A is under surveillance

	1.1	1.2	1.4	1.3
Calling DN	A	A	B	A
Called DN	B	B	A	B
SOSM Call #	1	1	1	1
Attribute of choice	01	01	04	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	HO LD	FF

Table 35 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	A	B	B
Called DN	B	B	A	C	C	C	B	C	C
SOSM Call #	1	1	1	2	2	2	1	2	2
Attribute of choice	04	04	01	01	01	01	04	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.4	1.3
Code of supp. service phase	00	00	04	00	00	04	00	04	00
MCL #	1	1	1	2	2	2	1	2	2
Code of operation	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	FF	HO LE	FF

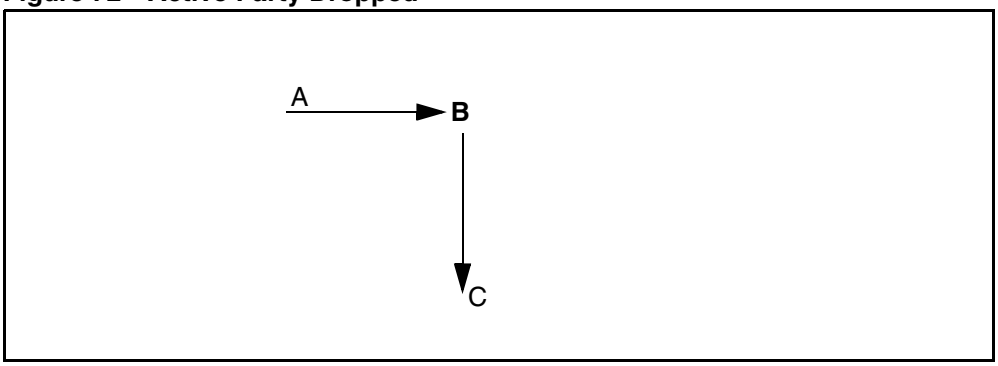
Table 36 C is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	B
Called DN	C	C	C	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

14.11.1.2.2 Drop Active Party during Enquiry In this scenario B is the controller which has one of the enquiry feature options. A calls B, B flashes (holds A) and calls C. During conversation with C, B flashes (holds C) and dials R-code to disconnect the last active party (C) and then toggles to re-connect to A. Then A-B call is disconnected.

In this scenario, MCL connection suspends after flashes, and resumes when speech is established.

Figure 72 Active Party Dropped



The message sequence is shown in the following tables.

Table 37 A is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 38 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	B	B	A
Called DN	B	B	A	C	C	C	C	A	B
SOSM Call #	1	1	1	2	2	2	2	1	1
Attribute of choice	04	04	01	01	01	01	01	01	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.4	1.3
Code of supp. service phase	00	00	04	00	00	04	00	04	00
MCL #	1	1	1	2	2	2	2	1	1
Code of operation	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HOLD	FF	FF	HOLD	FF	HOLE	FF

Table 39 C is under surveillance

	1.1	1.2	1.4	1.3
Calling DN	B	B	B	B
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	HOLD	FF

14.11.1.3 Call Waiting

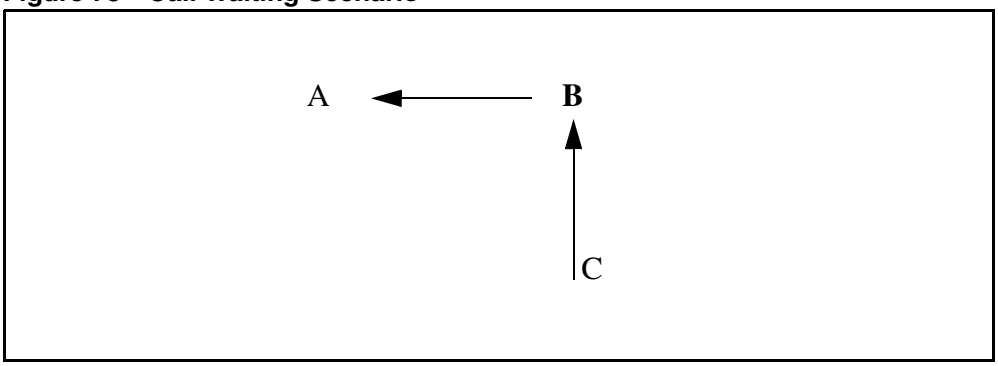
Call Waiting allows a subscriber (controller) to receive a call while active in another call.

In this scenario, B has the Call Waiting feature. B calls A, A answers and they are talking. C calls B. B hears Call Waiting tone. Then party B holds A with flash and answers C by dialing R-code(toggle). While B and C are talking, C exits. Sometime later, A or B exit.

In this scenario, MCL connection suspends after flashes, and resumes when speech is established.

For IBN lines, ICWT line option provide this functionality.

Figure 73 Call Waiting Scenario



The message sequence is shown in the following tables.

Table 40 A is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	B
Called DN	A	A	A	A	A
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 41 B is under surveillance

	1.1	1.2	1.1	1.4	1.4	1.2	1.3	1.4	1.3
Calling DN	B	B	C	B	B	C	C	B	B
Called DN	A	A	B	A	A	B	B	A	A
SOSM Call #	1	1	2	1	1	2	2	1	1
Attribute of choice	01	01	04	01	01	04	04	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.1	1.4	1.4	1.2	1.3	1.4	1.3
Code of supp. service phase	00	00	00	04	04	00	00	04	00
MCL #	1	1	2	1	1	2	2	1	1
Code of operation	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	FF	CW T	HO LD	FF	FF	HO LE	FF

Table 42 C is under surveillance

	1.1	1.2	1.3
Calling DN	C	C	C
Called DN	B	B	B
SOSM Call #	2	2	2
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

14.11.1.4 Three Way Calling

Three Way Calling feature allows a subscriber to establish a three way conference.

In this scenario, A calls B. B has the Three Way Call feature. B puts A on HOLD, and calls C. Later B flashes (holds C) and conferences A and C into a three way conference by dialing corresponding R-code. The A-B conversation is completed, in due to realization of supplementary service. Then the conference ends.

In this scenario, MCL connection suspends after flashes, and resumes when Conference/speech is established. When all parties are in conference, MCL speech path contains voice from ALL parties.

For IBN lines, I3WC line option provide this functionality.

Figure 74 Three Way Calling Scenario

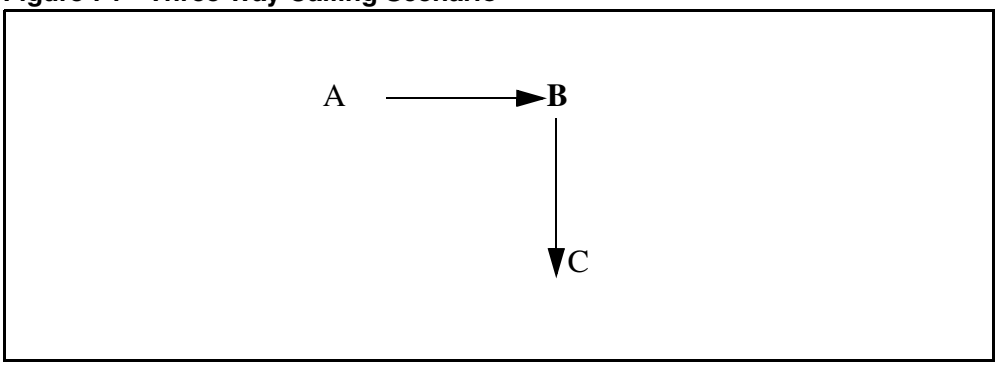


Table 43 A is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	C	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HOLD	3PTY	FF

Table 44 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.3	1.3
Calling DN	A	A	B	B	B	B	B	A	B
Called DN	B	B	A	C	C	C	A	B	C
SOSM Call #	1	1	1	2	2	2	2	1	2
Attribute of choice	04	04	01	01	01	01	01	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.3	1.3
Code of supp. service phase	00	00	04	00	00	04	04	00	00
MCL #	1	1	1	2	2	2	2	1	2
Code of operation	00	00	00	00	00	00	00	05	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	3PT Y	FF	FF

Table 45 C is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	B
Called DN	C	C	C	A	C
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	40	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	3PT Y	FF

14.11.1.5 Six Way Calling

The Six Way Calling feature allows a subscriber to establish a six way conference. I6WC option provides this functionality.

In this scenario the controller of a six way call (B) calls A. A answers. B puts A on HOLD and calls C. C answers. B flashes (puts C on hold) and dials R-code for 6WC to CONFerence A and C. The B-A conversation is completed, in due to realization of supplementary service. Then B puts the conference on HOLD and calls D. D answers. B flashes (puts D on hold) and dials 6 to conference all parties. Again due to realization of supplementary service, B-C conversation is disconnected. Then the conference is disconnected.

In this scenario, MCL connection suspends after flashes, and resumes when Conference/speech is established. When all parties are in conference, MCL speech path contains voice from ALL parties.

Figure 75 Six Way Calling Scenario

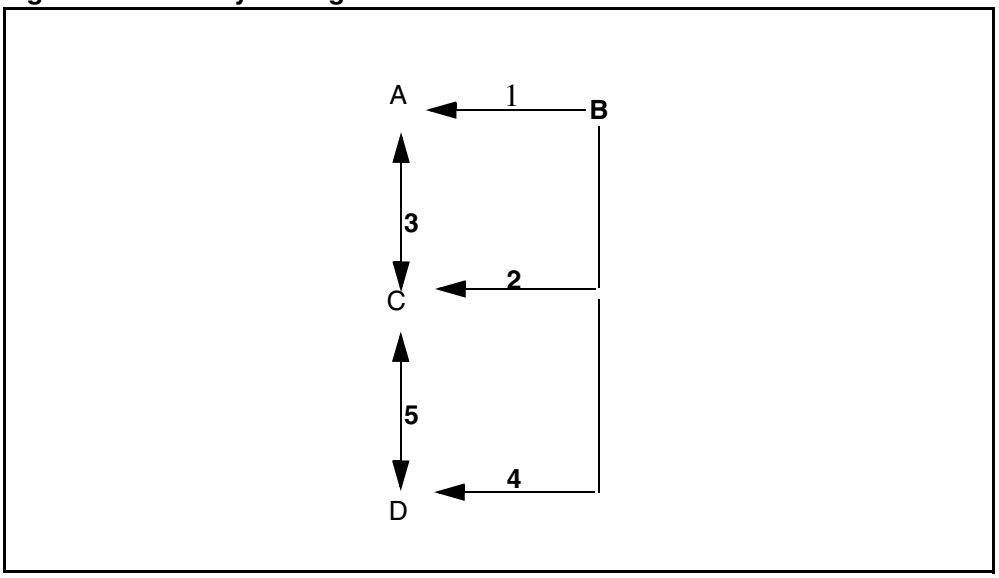


Table 46 A is under surveillance

	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B
Called DN	A	A	A	C	D	A
SOSM Call #	1	1	1	1	1	1
Attribute of choice	04	04	04	40	40	04
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	00
MCL #	1	1	1	1	1	1
Code of operation	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	CO NF	CO NF	FF

Table 47 B(IBN) is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.3	1.4	1.1	1.2	1.4	1.4	1.3	1.3
Calling DN	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B
Called DN	A	A	A	C	C	C	A	A	C	D	D	D	C	C	D
SOSM Call #	1	1	1	2	2	2	2	1	2	3	3	3	3	2	3
Attribute of choice	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	04	00	04	00	00	04	04	00	00
MCL #	1	1	1	2	2	2	2	1	2	3	3	3	3	2	3
Code of operation	00	00	00	00	00	00	00	05	00	00	00	00	00	05	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	CO NF	FF	HO LD	FF	FF	HO LD	CO NF	FF	FF

Table 48 C is under surveillance

	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B
Called DN	C	C	C	A	D	C
SOSM Call #	1	1	1	1	1	1
Attribute of choice	04	04	04	40	40	04
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	00
MCL #	1	1	1	1	1	1
Code of operation	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	CO NF	CO NF	FF

Table 49 D is under surveillance

	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B
Called DN	D	D	D	C	A	D
SOSM Call #	1	1	1	1	1	1
Attribute of choice	04	04	04	40	40	04
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	00
MCL #	1	1	1	1	1	1
Code of operation	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	CO NF	CO NF	FF

14.11.1.6 Call Transfer

Call Transfer feature allows to hold the current party, calling a new party (C), and transferring the Held party to the new party. After the transfer, the controller is no longer involved in the call.

If the controller in a Call Transfer is a SOSM agent, the SOSM call ends when the call is transferred. If the party being transferred is the SOSM agent, monitoring continues until the call completes.

The following scenarios provide more details regarding call transfer.

In this scenario, B has the Call Transfer feature. A calls B. B puts party A on HOLD, and dials C. B flashes (puts C on hold) and dials R-code to transfer A to C. A-B and B-C conversations are completed, in due to realization of supplementary service. Then the transferred call ends. ICT line option provides this functionality.

Figure 76 Call Transfer Scenario

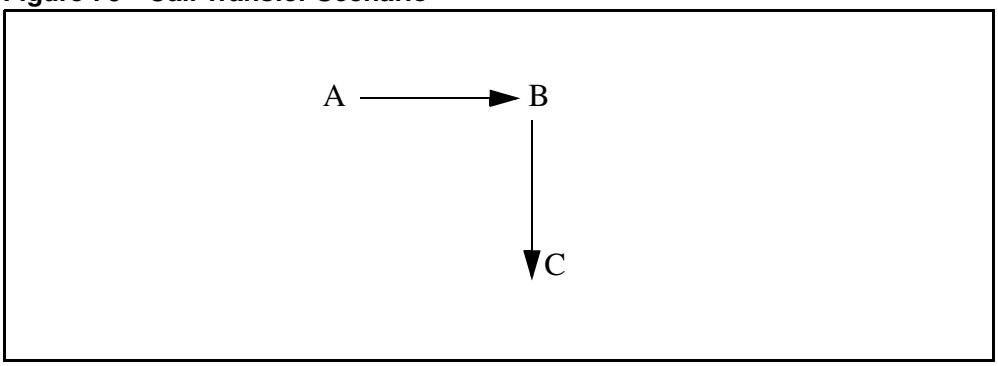


Table 50 A is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	ICT	FF

Table 51 B is under surveillance

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.3	1.3
Calling DN	A	A	B	B	B	B	B	A	B
Called DN	B	B	A	C	C	C	A	B	C
SOSM Call #	1	1	1	2	2	2	2	1	2
Attribute of choice	04	04	01	01	01	01	01	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	04	00	00

	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.3	1.3
MCL #	1	1	1	2	2	2	2	1	2
Code of operation	00	00	00	00	00	00	00	05	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	ICT	FF	FF

Table 52 C is under surveillance

	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	A
Called DN	C	C	C	A	C
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	40	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	ICT	FF

14.11.1.7 Call Forward (Busy, Unconditional, Do Not Answer)

Call Forward allows a subscriber to divert a call to another agent. If one of the parties is SOSM agent in a diverted call, monitoring continues in the new call formed after diversion. If the forwarded agent is a SOSM agent, the call is also monitored.

In this scenario, subscriber A calls B. B has Call Diversion Feature programmed to divert the call to C. CFU, CFB and CFD line options are used for IBN lines.

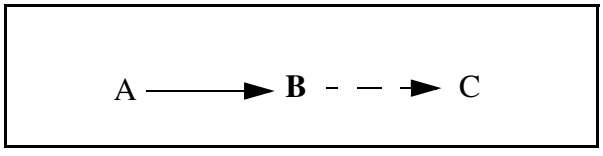


Table 53 A is under surveillance

	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	01	40	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

Table 54 B is under surveillance

	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

Table 55 C is under surveillance

	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

Note1: The message sequence for CDTO (Call Diversion To Operator) feature is as same as CFU, and feature code field in Msg.1.4 is sent as "**CFU - 21H**" to control point.

Note2: The message sequence for CFF (Call Diversion Fixed) feature is as same as CFU, and feature code field in Msg.1.4 is sent as "**CFU - 21H**" to control point.

Note3: No service usage notification is sent to CP if the call is diverted to a vacant (blank) DN for CFX scenarios.

14.11.1.7.1 Call Forward Chaining

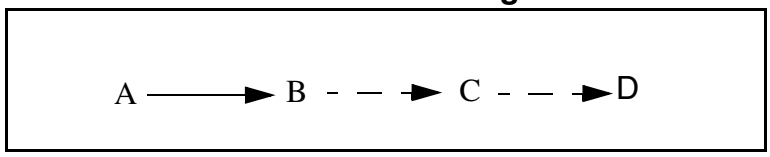


Table 56 A is under surveillance

	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	B	C	D	D	D
SOSM Call #	1	1	1	1	1

	1.1	1.4	1.4	1.2	1.3
Attribute of choice	01	40	40	01	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	Cfu Cfb Cfd	FF	FF

Table 57 B is under surveillance

	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	B	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	01	40	40	40
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	Cfu Cfb Cfd	FF	FF

Table 58 C is under surveillance

	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	C	C	D	D	D
SOSM Call #	1	1	1	1	1

	1.1	1.4	1.4	1.2	1.3
Attribute of choice	04	04	01	40	40
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	Cfu Cfb Cfd	FF	FF

Table 59 D is under surveillance

	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	D	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	40	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	Cfu Cfb Cfd	FF	FF

14.11.1.7.2 Trunk Implementation

In local exchange, if the monitored call is routed over trunk then service usage notification messages (Msg.1.4) are not generated when call diversion (including call forward chain) takes place in other exchange.

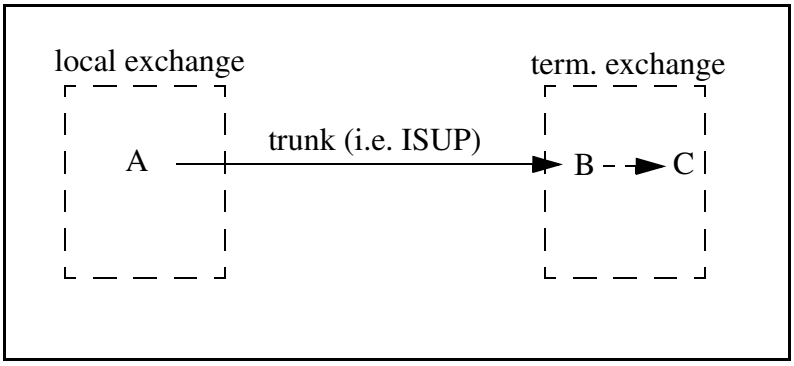


Table 60 A is under surveillance (Local Exchange)

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	11	11	11
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 61 B is under surveillance (Terminating Exchange)

	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	12	1C	12	12
Code of supp. service phase	00	04	00	00

	1.1	1.4	1.2	1.3
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

Table 62 C is under surveillance (Terminating Exchange)

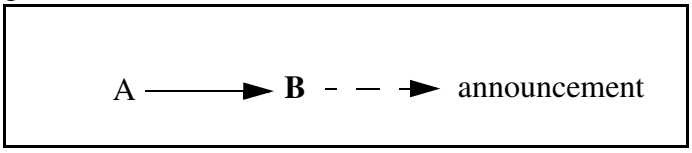
	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	12	1C	12	12
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

14.11.1.8 Call Forward to Announcement

This feature allows a subscriber to divert a call to the announcement. This feature can be activated either before or during a call.

If one of the parties is SOSM agent in a diverted call, monitoring continues in the new call formed after diversion.

In this scenario, subscriber A calls B. B has Call Diversion Feature programmed to divert the call to announcement.



For IBN lines, CDTA line option provide this functionality.

Table 63 A is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	0	0
Code of operation	00	05
Feature Code	FF	FF

Table 64 B is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	0	0
Code of operation	00	05
Feature Code	FF	FF

In line-to-line calls, SOSM stops monitoring the call when the originating subscriber starts to receive the announcement.

However, if the call is established via trunk, call content (annoucement) is sent to control point via MCL channel(s).

14.11.1.9 Speed Call

Speed Call allows a subscriber to make calls dialing abbreviated codes which were programmed before by the subscriber. This feature can be programmed either before or during a call.

Party A dials the abbreviated digits to call B.

For IBN lines, SCL line option provides this functionality.

Table 65 A is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 66 B is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C

	1.1	1.2	1.3
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

14.11.1.10 Call Completion to Busy Subscriber

This feature allows the subscriber to activate himself against the called party that is busy at the moment. A dials B which is busy. A activates CCBS against B. When B on-hooks, A rings. When A off-hooks, the call is setup automatically established between A and B. SOSM interaction for network CCBS will be supported only over ISUP V2 trunks.

In this scenario, A is SOSM agent. A calls B which is busy at that time. A activates CCBS against B. Then A goes on-hook.

Note that a SOSM call arises due to the activation of CCBS feature; because A is a SOSM agent. After a while, B finishes his conversation and goes on-hook. After B on-hooks, A rings and call is setup between A and B automatically. This is a normal SOSM call between A and B. CCBS line option provides this functionality.

Table 67 A is under surveillance

	1.1	1.3	1.4	1.3	1.4	1.1	1.2	1.3
Calling DN	A	A	A	A	A	A	A	A
Called DN	B	B	B	B	B	B	B	B
SOSM Call #	1	1	2	2	3	3	3	3
Attribute of choice	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C*	1C	1C	1C
Code of supp. service phase	00	00	01	00	04	00	00	00
MCL #	1	1	FF	FF	FF**	2	2	2
Code of operation	00	03	FF	05	FF	00	00	05
Feature Code	FF	FF	CC BS	FF	CC BS	FF	FF	FF

Note 1: * Parameter of connection is always set as 1C in CCBS service usage message, since at this call step, SOSM is unable to determine whether B is a present exchange subscriber or not.

Note 2: ** In CCBS service usage message, MCL number is always set as FF.

14.11.1.11 Malicious Call Trace

This feature allows a subscriber to detect a continuously disturbing number by using double FLASH during the call. If a subscriber activates feature against a calling agent, that agent stays held and a log is produced for the operator to detect the number.

In this scenario, A calls B. B activates feature against A.

For IBN lines, CLF line option provide this functionality.

Table 68 A is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 69 B is under surveillance

	1.1	1.2	1.4	1.3
Calling DN	A	A	B	A
Called DN	B	B	A	B
SOSM Call #	1	1	1	1

	1.1	1.2	1.4	1.3
Attribute of choice	04	04	01	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	CLF	FF

Note: If terminating line is monitored and has MCT option (CEPT and CLF) then call clearing (Msg.1.3) message is not sent as the originator on-hooks unless MCT is activated.

14.11.1.11.1 Post Disconnection

Definition: If calling party on hooks before called party has activated MCT, and if called party activates MCT by double flash within post diconnection timer then MCT logs will be printed like a normal activation in case of terminating office has calling DN information.

If the terminating line is monitored and has MCT option (CEPT and CLF) then service usage notification (Msg.1.4) and call clearing (Msg.1.3) messages are sent after terminator activates MCT.

14.11.1.12 International Line Restriction

International Line Restriction allows subscribers to restrict some of their own calls.

14.11.1.12.1 Activation from translations

In this scenario, A has ILR option. A activates ILR feature directly from the translations. The message sequence is shown in the following table.

For IBN lines, ILR line option provides this functionality.

Table 70 A is under surveillance

	1.4	1.3
Calling DN	A	A

	1.4	1.3
Called DN	Dilaed Digits	Dilaed Digits
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	ILR[a]	FF

a. * Same feature code is used for OCB.

14.11.1.12.2 Activation during a call

In this scenario, A calls B. During the call, A activates ILR feature.The message sequence is shown in the following table.

Table 71 A is under surveillance

	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	A	A	A	A	A	A
Called DN	B	B	B	ILR activation digits	B	B
SOSM Call #	1	1	1	1	1	1
Attribute of choice	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	01	04	00
MCL #	1	1	1	FF	1	1
Code of operation	00	00	00	FF	00	05
Feature Code	FF	FF	HOLD	ILR	HOLE	FF

14.11.1.12.3 ILR Usage

In this scenario, A calls a restricted number. The message sequence is shown in the following table.

Table 72 A is under surveillance

	1.1	1.4	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	04	00
MCL #	1	1	1
Code of operation	00	00	01
Feature Code	FF	ILR	FF

14.11.1.13 Last Number Re-dial

Last Number Re-dial allows the subscriber to repeat the last dialled number by using a defined code. There is no interaction with SOSM.

In this scenario, A calls B using LNR service. The message sequence is shown in the following table. No usage message is reported to control point for LNR service.

Table 73 A is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C

	1.1	1.2	1.3
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

If B is under surveillance, the message sequence is the same with the basic call where called party is under surveillance.

14.11.1.14 Automatic Line

Automatic line allows a subscriber to have a direct connection to a DN which was programmed before by the office personnel as soon as the subscriber goes off-hook. The subscriber does not have effect in activating or deactivating this feature.

If a SOSM agent has this feature and uses it, a SOSM call arises. The message sequence is shown in the following table. AUL line option provide this functionality.

Table 74 A is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

If B is under surveillance, the message sequence is the same with the basic call where called party is under surveillance.

14.11.1.15 Warm-Line

WML (Warm Line) feature is similar to HTL except for CEPT_WML_DEFAULT_TMO parameter in table OFCVAR. If the subscriber does not make a call within this time interval, a direct connection to a determined DN is made. This feature can be activated by the subscriber.

SOSM interacts with this feature when a direct feature access is made to activate the feature. The message sequence for activation is shown in the following table. WML line option provide this functionality.

Table 75 A is under surveillance

	1.4	1.3
Calling DN	A	A
Called DN	Dialled digits	Dialled digits
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	WML	FF

When the call is being placed automatically, WML has the same behavior as AUL feature.

If B is under surveillance, the message sequence is the same with the basic call where called party is under surveillance.

14.11.1.16 CEPT Do Not Disturb

While CDND is active for IBN lines, no calls will be routed to this subscriber.

SOSM only interacts with this feature when direct feature access is made to activate or deactivate the feature. The message sequence for activation is shown in the following table.

Table 76 A is under surveillance

	1.4	1.3
Calling DN	A	A
Called DN	Dialled digits	Dialled digis
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	CDND	FF

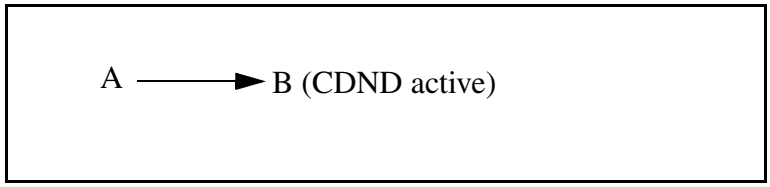


Table 77 A is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	FF	03

	1.1	1.3
Feature Code	FF	FF

Table 78 B is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	03
Feature Code	FF	FF

14.11.1.17 Wake-up Call

This feature allows the subscriber to ring his/her telephone set at a specified time which can be programmed by the subscriber himself/herself.

SOSM only interacts with this feature when direct feature access is made. The message sequence for IWUC activation is shown in the following table.

For IBN lines, IWUC line option provide this functionality.

Table 79 A is under surveillance

	1.4	1.3
Calling DN	A	A
Called DN	Dialled digis	Dialled digits
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C

	1.4	1.3
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	IWUC[a]	FF

a. Same feature code is used by WUCR.

If wakeup call arises through party A, message 1.4 should be sent for IWUC usage.

Table 80 A is under surveillance

	1.4	1.3
Calling DN	A	A
Called DN		
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	04	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	IWUC	FF

14.11.1.18 Call Pickup

This feature allows the subscriber to answer an incoming call at any station in call pickup group.

SOSM only interacts with this feature when direct feature access is made.The message sequence for CPU activation is shown in the following table.

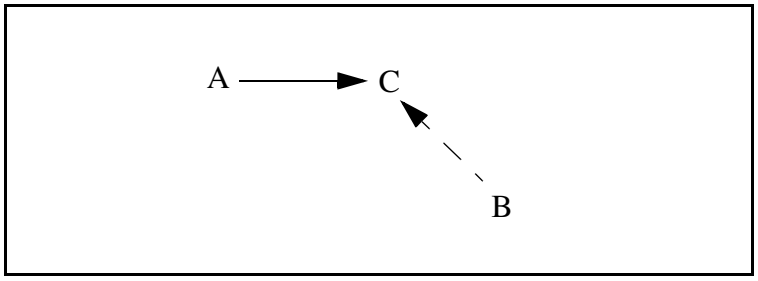


Table 81 A is under surveillance

	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	C	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 82 B is under surveillance

	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	B	B
SOSM Call #	1	1	1	1
Attribute of choice	04	01	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1

	1.1	1.4	1.2	1.3
Code of operation	00	00	00	05
Feature Code	FF	CPU	FF	FF

Table 83 C is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	C	C
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	04
Feature Code	FF	FF

14.11.1.19 Call Forward Remote Access (CFRA)

CFRA allows user to (de)activate Call Forward and enter the forward-to number by remotely dialling a DISA number and entering a PIN. This feature is implemented by activity A59019083 (MMP14).

Figure 77 CF Remote Access successfull call scenario

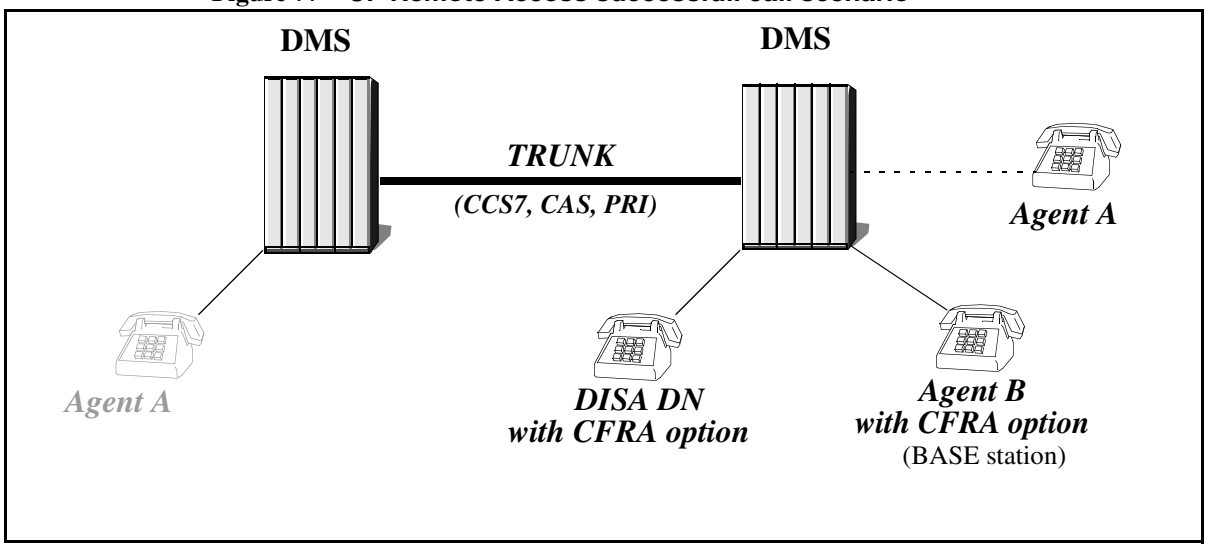


Table 84 A is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	DISA	DISA
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	05
Feature Code	FF	FF

Note: For Line (A) to DISA calls where call is established over trunk, the parameter of connection is set as "**outgoing call - 11H**", and code of operation is set as "**no answer - 04H**" in Msg.1.3.

Table 85 B is under surveillance

	1.4	1.4
Calling DN	A	A
Called DN	B	B

	1.4	1.4
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	04	01/ 02/03
MCL #	FF	FF
Code of operation	FF	FF
Feature Code	CFRA	CFU/ CFB/ CFD

Note: Since no MCL(s) are assigned during act/deact/inter via CFRA, MCL# field is always set to FFH within Msg.1.4s.

14.11.1.20 CEPT Remote Access (CEPTRA)

CEPTRA (CEPT Features Remote Access) feature allows subscribers to control some CEPT feature functionalities of IBN lines from remote agents. CEPTRA allows activation/programming, deactivation or interrogation of CEPT features on end user's phone from a remote location.

The below figure show the functionality of CEPTRA in MMP.

Figure 78 CEPT Features Remote Access successfull call scenario

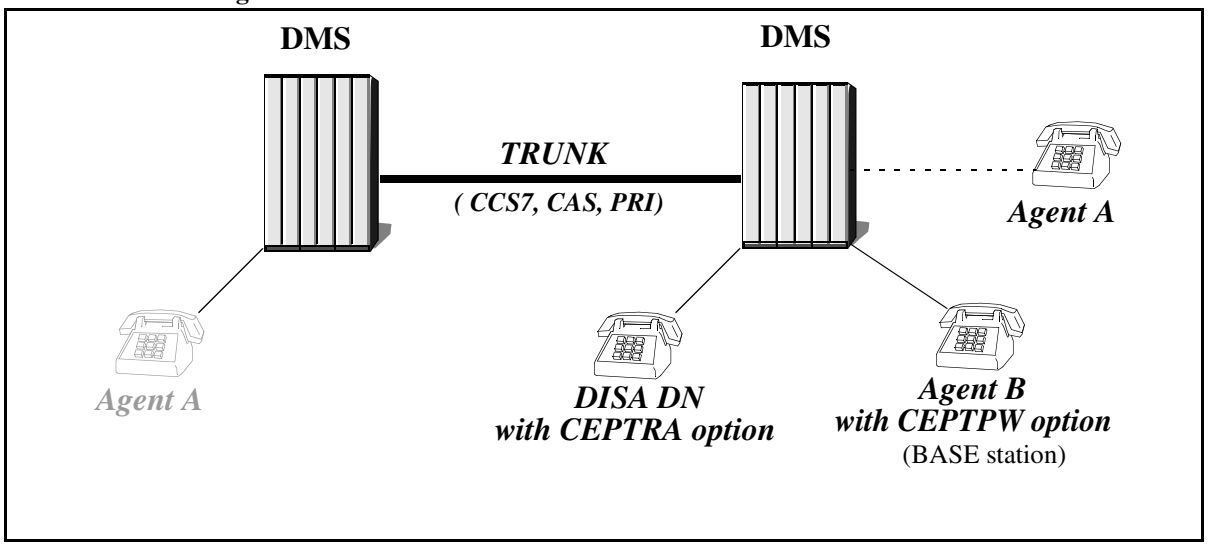


Table 86 A is under surveillance

	1.1	1.3
Calling DN	A	A
Called DN	DISA	DISA
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	05
Feature Code	FF	FF

Note: For Line (A) to DISA calls where call is established over trunk, the parameter of connection is set as "**outgoing call - 11H**", and code of operation is set as "**no answer - 04H**" in Msg.1.3.

Table 87 B is under surveillance

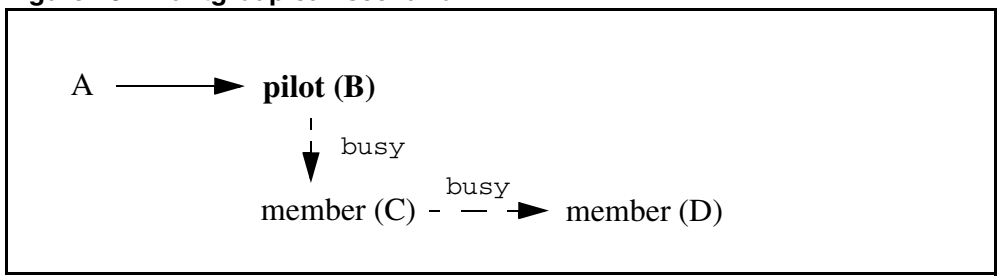
	1.4	1.4
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	04	01/ 02/ 03
MCL #	FF	FF
Code of operation	FF	FF
Feature Code	CEP TRA	Feat.

Note1: Since no MCL(s) are assigned during act/deact/inter via CFRA, MCL# field is always set to FFH within Msg.1.4s.

14.11.1.21 Huntgroups (DNH, DLH, MLH)

DNH configuration: Since each member of huntgroup has its own DN, any member or the pilot can be assigned as target. Calls from the pilot/member(s) are monitored if the subscriber is assigned as target.

Figure 79 Huntgroup call scenario



If call is terminated to the busy pilot, and the call is passed to another DN in the huntgroup, the call steps in this scenario are as follows:

1- A calls B while B is busy; **2-** The call is rerouted to C (Realization of hunt group), and C is busy; **3-** The call is rerouted to D (Realization of hunt group); **4-** D answers; **5-** Disconnection of A-D call.

Table 88 A is under surveillance

No of step	**1**	**4**	**5**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	D	D
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 89 Pilot (B) is under surveillance

No of step	**1**	**4**	**5**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	D	D
SOSM Call #	1	1	1
Attribute of choice	04	40	40
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 90 C is under surveillance

No of step	**3**	**4**	**5**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	04	40	40
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 91 D is under surveillance

No of step	3	4	5
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

DLH/MLH configuration: Since there is one DN, only the pilot DN can be assigned as target. Calls to/from any member or pilot of the huntgroup are monitored if the pilot DN of the huntgroup is target. Note that the pilot DN is sent to CP whether the call is originated or terminated by pilot/member.

SOSM does not send Hunt Group service usage message to CP while hunting a member within the group.

14.11.2 ISDN BRI Supplementary Services

Usage, activation, deactivation, and interrogation of BRI supplementary services are reported to CP.

"SOSM Message Sequences for ISDN Supplementary Services" (SOSMISDN in FMDOC library) document describes the SOSM behavior for BRI/PRI supplementary services.

In this document, reporting of service usage messages is mentioned as optional in several scenarios. SOSM reports optional service usage messages to CP if data regarding to usage of the service is available.

During activation, deactivation and interrogation of ISDN BRI Supplementary Services, message 1.4 indicating the code of service to be rendered to the subscriber is sent. BRI service act/deact/interrogation can be done in two different ways:

- via using CEPT dialing sequence (CFx, WML, WUCR, OCB)
- via using BRI phone set facilities (CFx and CCBS)

If BRI phone set facilities are used during subscriber action (CFx and CCBS act/deact/int), 1.3 - Disconnect message is not reported to CP, since no off-hook/on-hook takes place.

If CEPT dialing sequence is used during subscriber action, behavior of 1.3 - Disconnect Message varies depending on how dialed digits are sent:

- If digits are sent **inside the origination message,** 1.3 - Disconnect message is reported to CP, as soon as 1.4 - Suppl. Service Usage message is sent (before subscriber goes on-hook).
- If digits are sent **in digits message(s),** 1.3 - Disconect message is sent after subscriber on-hooks.

If BRI supplementary service act/deact/interrogation (using CEPT dialing sequence) takes place after taking active call on HOLD, 1.4 - Suppl. Service Usage and 1.3 - Disconnect messages are sent with a new call number, since subscriber action takes place in a new call. See the following example message sequence.

Consider agent A is under surviellance, and performs the followings in turn:

1. A calls B.

2. B answers.

3. While A and B are talking, A takes A-B call on hold.

4. A activates xx Suppl. Service via using Cept dialing sequence.

5. Activation is successful, and A retrieves A-B call.

6. A goes on hook after a while.

Table 92 A is under surveillance

	1.1	1.2	1.4	1.4	1.3	1.4	1.3
STEP	**1**	**2**	**3**	**4**	**4**	**5**	**6**
Calling DN	A	A	A	A	A	A	A
Called DN	B	B	B	Dialed Digits	Dialed Digits	B	B
SOSM Call #	1	1	1	**2**	2	1	1
Attribute of choice	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C

	1.1	1.2	1.4	1.4	1.3	1.4	1.3
Code of supp. service phase	00	00	04	01	00	04	00
MCL #	1	1	1	FF	FF	1	1
Code of operation	00	00	00	FF	05	00	05
Feature Code	FF	FF	HOLD	xx	FF	HOLE	FF

14.11.2.1 Consultation Call (by using ISDN BRI HOLD service)

ISDN BRI HOLD service allows a user to interrupt an active call, and subsequently to re-establish that call or establish other calls.

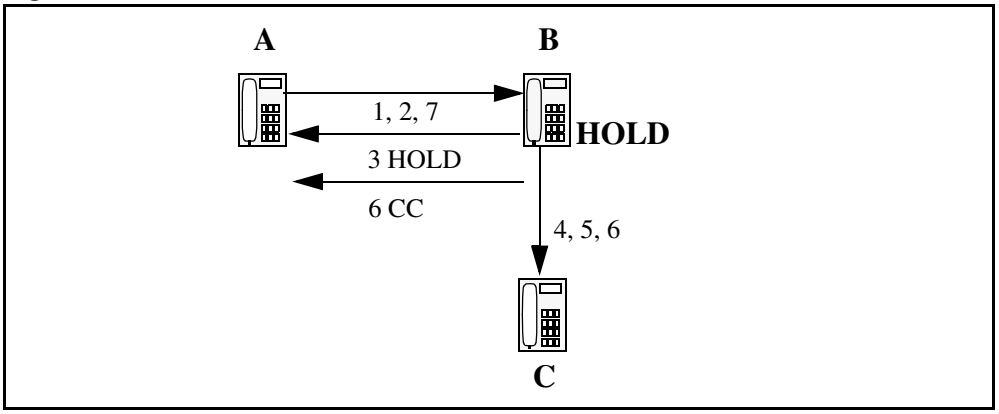
The required SOSM message sequences in Section5 of Annex2 of SOSM Conformance Test document are also valid for ISDN BRI HOLD service.

The following call steps are reported to CP according to SOSM Conformance Test document.

Scenario 1: Controller with a single MSN

1- A dials B; **2-** B answers; **3-** B puts A on hold; **4-** B dials C; **5-** C answers; **6-** B ends the consultation call with C and returns to conversation with A; **7-** disconnection of conversation A-B.

Figure 80 Consultation Call with ISDN BRI HOLD service



The required SOSM message sequences for Consultation Call are listed in Table 93 , Table 94 and Table 94 .

Table 93 A is under surveillance

No of step	1	2	3	6	7
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 94 B is under surveillance

No of step	1	2	3	4	5	6	6	7
Messages	1.1	1.2	1.4	1.1	1.2	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	B	A
Called DN	B	B	A	C	C	C	A	B
SOSM Call #	1	1	1	2	2	2	1	1
Attribute of choice	04	04	01	01	01	01	01	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	00	04	00
MCL #	1	1	1	2	2	2	1	1
Code of operation	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	FF	HO LE	FF

Table 95 C is under surveillance

No of step	4	5	6
Messages	1.1	1.2	1.3
Calling DN	B	B	B
Called DN	C	C	C
SOSM Call #	2	2	2
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates an HOLD service usage scenario where B(controller) has different MSN numbers.

Note: B1 and B2 represents the MSN1 and MSN2 DNs on the same BRI phone set.

Scenario 2: Controller with different MSN's

1- A dials B1; **2-** B1 answers; **3-** B1 puts A on hold; **4-** B2 dials C; **5-** C answers; **6-** B2 ends the consultation call with C and returns to conversation with A; **7-** disconnection of conversation A-B1.

Figure 81 Consultation Call with ISDN BRI HOLD service

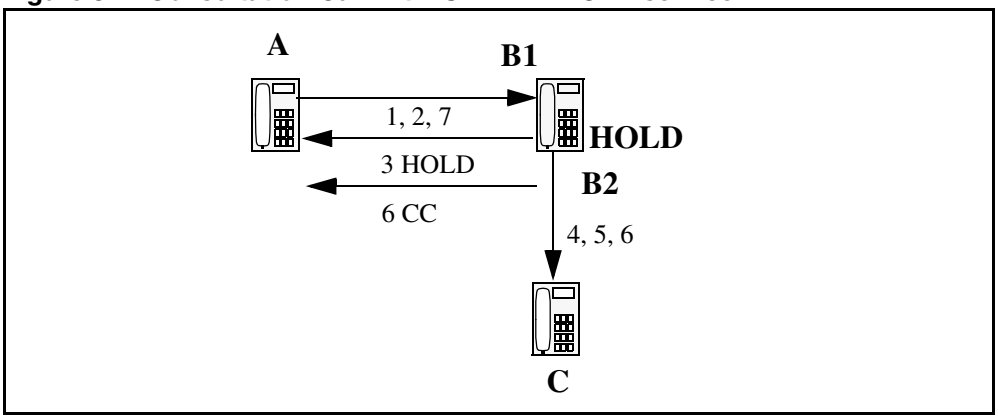


Table 96 B1 is under surveillance

No of step	1	2	3	6	7
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B1	B1	A
Called DN	B1	B1	A	A	B1
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 97 B1 and B2 are under surveillance

No of step	1	2	3	4	5	6	6	7
Messages	1.1	1.2	1.4	1.1	1.2	1.3	1.4	1.3
Calling DN	A	A	B1	B2	B2	B2	B1	A
Called DN	B1	B1	A	C	C	C	A	B1
SOSM Call #	1	1	1	2	2	2	1	1
Attribute of choice	04	04	01	01	01	01	01	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	00	04	00
MCL #	1	1	1	2	2	2	1	1
Code of operation	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	FF	HO LE	FF

Table 98 B2 is under surveillance

No of step	4	5	6
Messages	1.1	1.2	1.3
Calling DN	B2	B2	B2
Called DN	C	C	C
SOSM Call #	2	2	2
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

14.11.2.2 Call Switching (by using ISDN BRI HOLD service)

Required SOSM message sequences in Section6 of Annex2 of SOSM Conformance Test document are also valid for ISDN BRI HOLD service.

Following call steps are reported to CP according to SOSM Conformance Test document:

Scenario 1: Controller with a single MSN

1- A dials B; **2-** B answers; **3-** B puts A on hold; **4-** B dials C; **5-** C answers; **6-** call switching; **7-** call switching; **8-** call switching; **9-** disconnection of conversation A-B and return to conversation with C; **10-** disconnection of conversation B-C.

Figure 82 Call Switching with ISDN BRI HOLD service

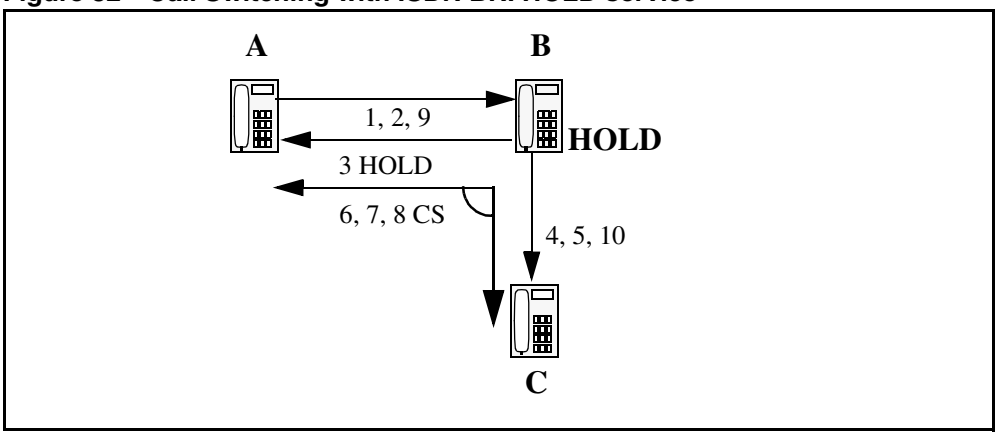


Table 99 A is under surveillance

No of step	1	2	3	6	7	8	9
Messages	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	A	A	B	B	B	B	A
Called DN	B	B	A	A	A	A	B
SOSM Call #	1	1	1	1	1	1	1
Attribute of choice	01	01	04	04	04	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

Table 100 B is under surveillance

No of step	1	2	3	4	5	6	6	7	7	8	8	9	9	10
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.4	1.3	1.4	1.3
Calling DN	A	A	B	B	B	B	B	B	B	B	B	A	B	B
Called DN	B	B	A	C	C	C	A	A	C	C	A	B	C	C
SOSM Call #	1	1	1	2	2	2	1	1	2	2	1	1	2	2

No of step	1	2	3	4	5	6	6	7	7	8	8	9	9	10
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.4	1.3	1.4	1.3
Attribute of choice	04	04	01	01	01	01	01	01	01	01	01	04	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	04	04	04	04	04	00	04	00
MCL #	1	1	1	2	2	2	1	1	2	2	1	1	2	2
Code of operation	00	00	00	00	00	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	HO LE	HO LD	HO LE	HO LD	HO LE	FF	HO LE	FF

Table 101 C is under surveillance

No of step	4	5	6	7	8	9	10
Messages	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B	B
Called DN	C	C	C	C	C	C	C
SOSM Call #	2	2	2	2	2	2	2
Attribute of choice	04	04	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

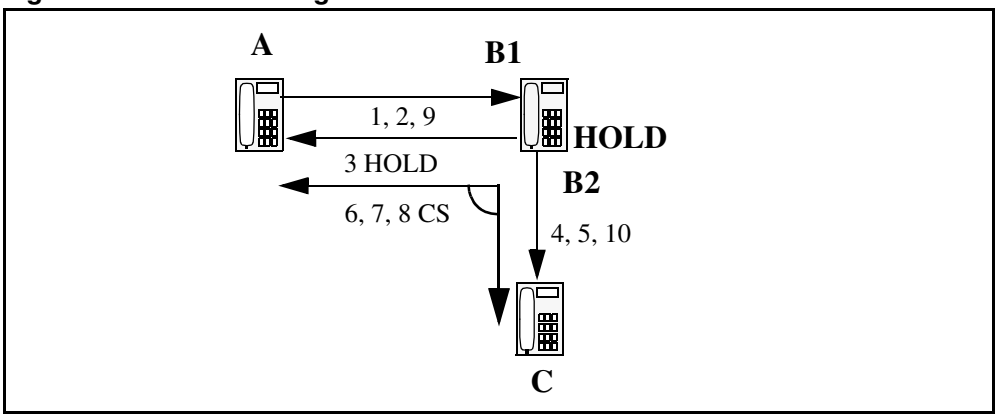
A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates a Call Switching scenario where B(controller) has different MSN numbers.

Note: B1 and B2 represents the MSN1 and MSN2 DNs in the same BRI phone set.

Scenario 2: Controller with different MSN's

1- A dials B1; **2-** B1 answers; **3-** B1 puts A on hold; **4-** B2 dials C; **5-** C answers; **6-** call switching; **7-** call switching; **8-** call switching; **9-** disconnection of conversation A-B1 and return to conversation with C; **10-** disconnection of conversation B2-C.

Figure 83 Call Switching with ISDN BRI HOLD service



.

Table 102 B1 is under surveillance

No of step	1	2	3	6	7	8	9
Messages	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	A	A	B1	B1	B1	B1	A
Called DN	B1	B1	A	A	A	A	B1
SOSM Call #	1	1	1	1	1	1	1
Attribute of choice	01	01	04	04	04	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

Table 103 B1 and B2 both are under surveillance

No of step	1	2	3	4	5	6	6	7	7	8	8	9	9	10
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.4	1.3	1.4	1.3
Calling DN	A	A	B1	B2	B2	B2	B1	B1	B2	B2	B1	A	B2	B2
Called DN	B1	B1	A	C	C	C	A	A	C	C	A	B1	C	C
SOSM Call #	1	1	1	2	2	2	1	1	2	2	1	1	2	2
Attribute of choice	04	04	01	01	01	01	01	01	01	01	01	04	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	04	04	04	04	04	00	04	00
MCL #	1	1	1	2	2	2	1	1	2	2	1	1	2	2
Code of operation	00	00	00	00	00	00	00	00	00	00	00	05	00	05
Feature Code	FF	FF	HO LD	FF	FF	HO LD	HO LE	HO LD	HO LE	HO LD	HO LE	FF	HO LE	FF

Table 104 B2 is under surveillance

No of step	4	5	6	7	8	9	10
Messages	1.1	1.2	1.4	1.4	1.4	1.4	1.3
Calling DN	B2	B2	B2	B2	B2	B2	B2
Called DN	C	C	C	C	C	C	C
SOSM Call #	2	2	2	2	2	2	2
Attribute of choice	04	04	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	00
MCL #	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	HO LD	HO LE	FF

14.11.2.3 Call Waiting (CW)

ISDN BRI Call Waiting (CW) service allows a user to be notified that there is a new incoming call while there is no available B-channel. The user then has the choice of accepting, rejecting or ignoring the new call.

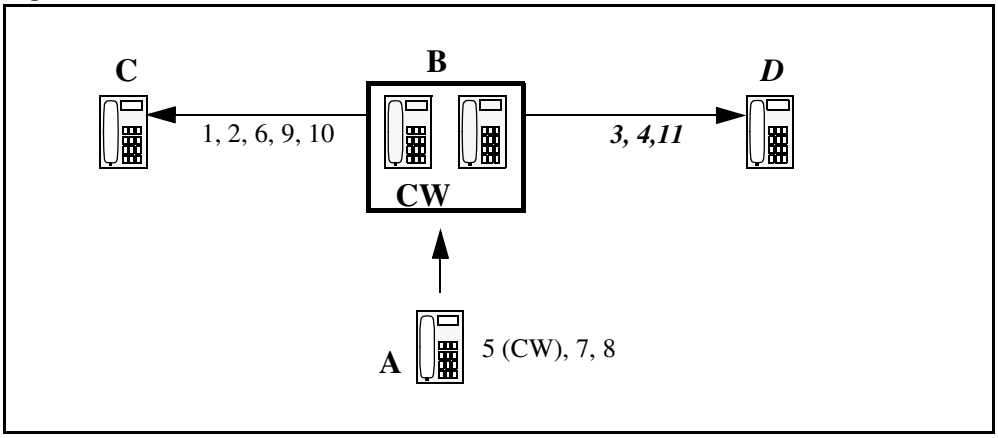
Required SOSM message sequences in Section3 of Annex2 of SOSM Conformance Test document are not valid entirely for ISDN BRI CW service. The difference is that ISDN BRI CW service is invoked when a third call arrives after two calls were made to subscriber B (both B-channels are busy). Therefore, required SOSM message sequences for CW are updated below regarding this difference.

Scenario 1: Controller with a single MSN
(ISDN CW differences from SOSM Conformance Test document are in bold&italic).

1- B dials C; **2-** C answers; **3- B dials D**; **4- D answers**; **5-** A dials B and B is notified about the incoming call; **6-** B puts C on hold and switches to conversation A-B; **7-** B answers; **8-** Disconnection of conversation A-B; **9-** Retrieve conversation B-C; **10-** Disconnection of conversation B-C; **11- Disconnection of conversation B-D**.

Please note that CW service is activated only if both B-channels of BRI access is busy. For this purpose, A-B and A-C calls in the given example are considered to be on different terminals. Therefore, A does not need to put A-B call on hold in order to establish A-C call.

Figure 84 CW Service



The SOSM message sequence is shown in the following tables.

Table 105 A is under surveillance

No of Step	**5**	**7**	**8**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 106 B is under surveillance

No of Step	**1**	**2**	**3**	**4**	**5**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Messages	**1.1**	**1.2**	**1.1**	**1.2**	**1.1**	**1.4**	**1.4**	**1.2**	**1.3**	**1.4**	**1.3**	**1.3**
Calling DN	B	B	B	B	A	B	B	A	A	B	B	B
Called DN	C	C	D	D	B	A	C	B	B	C	C	D
SOSM Call #	1	1	2	2	3	3	1	3	3	1	1	2
Attribute of choice	01	01	01	01	04	01	01	04	04	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	00	00	00	04	04	00	00	04	00	00
MCL #	1	1	2	2	3	3	1	3	3	1	1	2
Code of operation	00	00	00	00	00	00	00	00	05	00	00	05
Feature Code	FF	FF	FF	FF	FF	CW	HOLD	FF	FF	HOLE	FF	FF

Table 107 C is under surveillance

No of Step	1	2	6	9	10
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	B	B	B	B	B
Called DN	C	C	C	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 108 D is under surveillance

No of Step	3	4	11
Messages	**1.1**	**1.2**	**1.3**
Calling DN	B	B	B
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates a CW service usage where A has different MSN numbers.

In below scenario, B1, B2 and B3 represent the MSN1, MSN2 and MSN3 DNs on the same BRI access. In order to realize the scenario below, B1 and B3 must be on the same BRI set, and B2 must be on a different BRI set.

Scenario 2: Controller with different MSN's

(ISDN CW differences from SOSM Conformance Test document are in bold&italic).

1- B1 dials C; **2-** C answers; **3- B2 dials D; 4- D answers**; **5-** A dials B3, B1 and B2 are notified about the incoming call; **6-** B1 puts C on hold and switches to conversation A-B3; **7-** B3 answers; **8-** Disconnection of conversation A-B3; **9-** Retrieve conversation B1-C; **10-** Disconnection of conversation B1-C; **11- Disconnection of conversation B2-D**.

The SOSM message sequence is shown in the following tables.

Table 109 A is under surveillance

No of steps	**5**	**7**	**8**
messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B3	B3	B3
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 110 B1 is under surveillance

No of step	1	2	6	9	10
messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	B1	B1	B1	B1	B1
Called DN	C	C	C	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 111 B2 is under surveillance

No of step	3	4	11
messages	**1.1**	**1.2**	**1.3**
Calling DN	B2	B2	B2
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 112 B3 is under surveillance

No of step	5	5	7	8
messages	**1.1**	**1.4**	**1.2**	**1.3**
Calling DN	A	B3	A	A
Called DN	B3	A	B3	B3
SOSM Call #	1	1	1	1
Attribute of choice	04	01	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CW	FF	FF

Table 113 B1, B2, B3 all are under surveillance

No of Step	**1**	**2**	**3**	**4**	**5**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Messages	**1.1**	**1.2**	**1.1**	**1.2**	**1.1**	**1.4**	**1.4**	**1.2**	**1.3**	**1.4**	**1.3**	**1.3**
Calling DN	B1	B1	B2	B2	A	B3	B1	A	A	B1	B1	B2
Called DN	C	C	D	D	B3	A	C	B3	B3	C	C	D
SOSM Call #	1	1	2	2	3	3	2	3	3	1	1	2
Attribute of choice	01	01	01	01	04	01	01	04	04	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	00	00	00	04	04	00	00	04	00	00
MCL #	1	1	2	2	3	3	2	3	3	1	1	2
Code of operation	00	00	00	00	00	00	00	00	05	00	00	05
Feature Code	FF	FF	FF	FF	FF	CW	HOLD	FF	FF	HOLE	FF	FF

Table 114 C is under surveillance

No of steps	**1**	**2**	**6**	**9**	**10**
messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	B1	B1	B1	B1	B1
Called DN	C	C	C	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	HO LE	FF

Table 115 D is under surveillance

No of step	**3**	**4**	**11**
messages	**1.1**	**1.2**	**1.3**
Calling DN	B2	B2	B2
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

14.11.2.4 Three Party (3PTY)

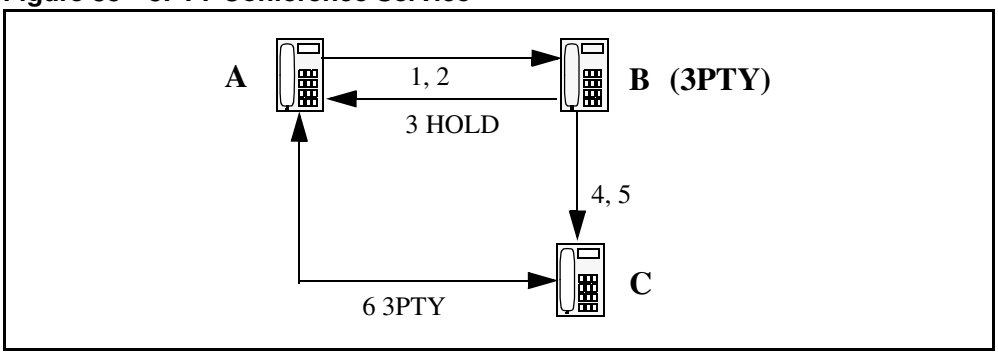
With the ISDN BRI 3PTY service, the served user, which has only one Active-Idle connection, and one Active-Held connection can join the Active-Idle connection with the Active-Held connections, to form a three-way conversation.

For a basic three-way conversation, the following call steps are reported to CP.

Scenario 1: Controller with a single MSN

1- A dials B; **2-** B answers; **3-** B puts A on hold; **4-** B dials C; **5-** C answers; **6-** B put A&C into three-party conference; **7-** disconnection after the end of conversation A-B; **8-** disconnection after the end of conversation B-C.

Figure 85 3PTY Conference Service



The SOSM message sequence is shown in the following tables.

Table 116 A is under surveillance

No of step	1	2	3	6	7
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	C	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HOLD	3PTY	FF

Table 117 B is under surveillance

No of step	1	2	3	4	5	6	7	8
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.3
Calling DN	A	A	B	B	B	B	A	B
Called DN	B	B	A	C	C	A	B	C
SOSM Call #	1	1	1	2	2	2	1	2
Attribute of choice	04	04	01	01	01	01	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	00	00
MCL #	1	1	1	2	2	2	1	2
Code of operation	00	00	00	00	00	00	05	05
Feature Code	FF	FF	HOLD	FF	FF	3PTY	FF	FF

Table 118 C is under surveillance

No of step	4	5	6	8
Messages	1.1	1.2	1.4	1.3
Calling DN	B	B	B	B
Called DN	C	C	A	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	40	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	3PTY	FF

A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates a CW service usage where A has different MSN numbers.

In below scenario, B1 and B2 represent the MSN1 and MSN2 DNs on the same BRI phone set.

Scenario 2: Controller with different MSN's

1- A dials B1; **2-** B1 answers; **3-** B1 puts A on hold; **4-** B2 dials C; **5-** C answers; **6-** B2 put A&C into three-party conference; **7-** disconnection after the end of conversation A-B1; **8-** disconnection after the end of conversation B2-C.

The SOSM message sequence is shown in the following tables.

Table 119 A is under surveillance

No of step	1	2	3	6	7
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B1	B2*	A
Called DN	B1	B1	A	C	B1
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HOLD	3PTY	FF

Note: * During activation of 3PTY service, B2 is sent as the calling DN within 3PTY service usage message, since B2 is the subscriber which activates the service..

Table 120 B1 is under surveillance

No of step	1	2	3	7
Messages	1.1	1.2	1.4	1.3
Calling DN	A	A	B1	A

Called DN	B1	B1	A	B1
SOSM Call #	1	1	1	1
Attribute of choice	04	04	01	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	HOLD	FF

Table 121 B2 is under surveillance

No of step	**4**	**5**	**6**	**8**
Messages	1.1	1.2	1.4	1.3
Calling DN	B2	B2	B2	B2
Called DN	C	C	A	C
SOSM Call #	2	2	2	2
Attribute of choice	01	01	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	2	2	2	2
Code of operation	00	00	00	05
Feature Code	FF	FF	3PTY	FF

Table 122 B1 and B2 both are under surveillance

No of step	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.3
Calling DN	A	A	B1	B2	B2	B2	A	B2
Called DN	B1	B1	A	C	C	A	B1	C
SOSM Call #	1	1	1	2	2	2	1	2

Attribute of choice	04	04	01	01	01	01	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	00	00
MCL #	1	1	1	2	2	2	1	2
Code of operation	00	00	00	00	00	00	05	05
Feature Code	FF	FF	HOLD	FF	FF	3PTY	FF	FF

Table 123 C is under surveillance

No of step	**4**	**5**	**6**	**8**
Messages	1.1	1.2	1.4	1.3
Calling DN	B2	B2	B2	B2
Called DN	C	C	A	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	40	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	3PTY	FF

During the three-way conversation the served user can request that the network:

— explicitly disconnect one of the remote users and the connection to that remote user,

— terminate the three-way conversation,

— create a private communication with one of the remote users.

Additionally, during three-way conference, one of the remote users can disconnect from the conference. This results in the termination of the

conference (three way bridge is released). After this action, the conversation of the controller with the remaining remote party continues.

Please note that, upon termination of three party conference due to any reason, initial connections are re-established. For example, in Scenario 2 given above (where different MSN's of the controller is used), A is connected to B1, and C is connected to B2 after conference terminates.

In addition to Annex2 of SOSM Conformance Test document, below scenarios are investigated for 3PTY service.

14.11.2.4.1 Disconnection of one remote user, and retention of the other

Scenario1: Disconnection of Held leg A-B

B disconnects subscriber A (Active-Held connection), three-way bridge is released and the call B-C continues.

- When A is under surveillance; the disconnection message of conversation A-B (No.1.3 in step7) is reported to CP.
- When B is under surveillance; the disconnection message of conversation A-B (No.1.3 in step7) is reported to CP.
- When C is under surveillance; no message is reported.

Scenario 2: Disconnection of Active leg B -C

B disconnects subscriber C (Active-Idle connection), three-way bridge is released and the call A-B continues.

- When A is under surveillance; the"No.1.4- SS Usage - HOLE" message is reported when subscriber B retrieves the conversation A-B.
- When B is under surveillance; the disconnection message of conversation B-C (No.1.3 in step8) is reported to CP and the"No.1.4- SS Usage - HOLE" message is reported when subscriber B retrieves the conversation A-B.
- When C is under surveillance; the disconnection message of conversation B-C (No.1.3 in step8) is reported to CP.

14.11.2.4.2 Creation of a private communication with remote user

Scenario 1: Controller returns to the initial held call.

Subscriber B ends the 3PTY call and creates a private communication with subscriber A (Active-Held connection). The three-party bridge is released and there are still two calls (A-B idle and B-C held).

- When A is under surveillance; the“No.1.4- SS Usage - HOLE” message is reported when subscriber B retrieves the conversation A-B.
- When B is under surveillance; the“No.1.4- SS Usage - HOLE” message is reported when subscriber B retrieves the conversation A-B.
- When C is under surveillance; no message is reported to CP.

Scenario 2: Controller returns to initial active call

Subscriber B ends the 3PTY call and creates a private communication with subscriber C(Active-Idle connection). The three-party bridge is released and there are still two calls (B-C idle and A-B held).

- When A is under surveillance; no message is reported to CP.
- When B is under surveillance; no message is reported to CP.
- When C is under surveillance; no message is reported to CP.

14.11.2.4.3 Remote user terminates the call

Scenario 1: A (held party) terminates

Subscriber A disconnects from 3PTY call, three-way bridge is released and the call B-C continues.

- When A is under surveillance; the disconnection message of conversation A-B (No.1.3 in step7) is reported to CP.
- When B is under surveillance; the disconnection message of conversation A-B (No.1.3 in step7) is reported to CP.
- When C is under surveillance; no new message is reported to CP.

Scenario 2: C (active party) terminates

Subscriber B disconnects from 3PTY call, three-way bridge is released and the call A-B continues.

- When A is under surveillance; the“No.1.4- SS Usage - HOLE” message is reported when subscriber B retrieves the conversation A-B.
- When B is under surveillance; the disconnection message of conversation B-C (No.1.3 in step8) is reported to CP and the“No.1.4- SS Usage - HOLE” message is reported when subscriber B retrieves the conversation A-B.
- When C is under surveillance; the disconnection message of conversation B-C (No.1.3 in step8) is reported to CP.

14.11.2.5 Conference Call (ECONF)

The ECONF supplementary service enables a user who is connected to the network via a point to multipoint ISDN ETSI BRI to establish/participate in and control a simultaneous communication involving a number of users up to 6.

Required SOSM message sequences in Section9 of Annex2 of SOSM Conformance Test document are used as a reference for a basic ISDN BRI Conference call.

The following call steps are reported to CP.

Scenario 1: Controller with a single MSN

1- B dials C; **2-** C answers; **3-** B puts C into conference call; **4-** B puts conference call on hold; **5-** B dials A; **6-** A answers; **7-** B adds A into conference call; **8-** completion of one conversation in due to realization of supplementary service; **9-** B dials D; **10-** D answers; **11-** B adds D into conference call; **12-** completion of one conversation in due to realization of supplementary service; **13-** B retrieves the conference call; **14-** disconnection of conference call.

Figure 86 ISDN BRI ECONF service

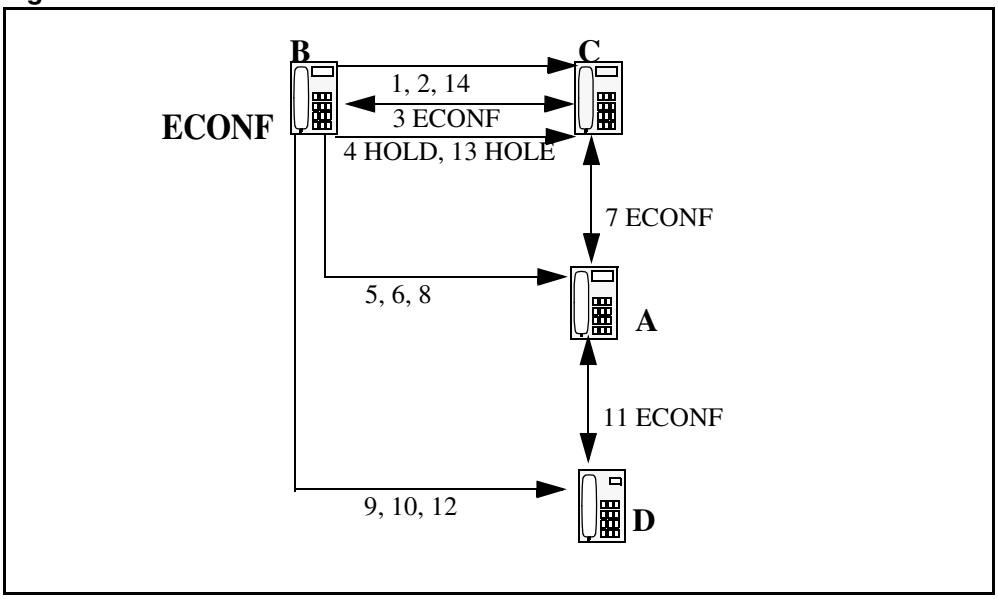


Table 124 Controller A is under surveillance

No of step	5	6	7	11	14
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	B
Called DN	A	A	C	D	A
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	**40**	40	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	FF

Table 125 B is under surveillance

No of step	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Messages	1.1	1.2	1.4	1.4	1.1	1.2	1.4	1.3	1.1	1.2	1.4	1.3	1.4	1.3
Calling DN	B	B	B	B	B	B	B	B	B	B	B	B	B	B
Called DN	C	C	C	C	A	A	A	A	D	D	D	D	C	C
SOSM Call #	1	1	1	1	2	2	1	2	3	3	1	3	1	1
Attribute of choice	01	01	01	01	01	01	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00	00	04	00	00	00	04	00	04	00
MCL #	1	1	1	1	2	2	1	2	3	3	1	3	1	1
Code of operation	00	00	00	00	00	00	00	05	00	00	00	05	00	05
Feature Code	FF	FF	ECO NF	HO LD	FF	FF	ECO NF	FF	FF	FF	ECO NF	FF	HO LE	FF

Table 126 C is under surveillance

No of step	1	2	3	7	11	14
Messages	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	B	B	B	B	B	B
Called DN	C	C	C	A	D	C
SOSM Call #	1	1	1	1	1	1
Attribute of choice	04	04	04	**40**	40	04
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	00
MCL #	1	1	1	1	1	1
Code of operation	00	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	ECO NF	FF

Table 127 D is under surveillance

No of step	9	10	11	11	14
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	B	B	B	B	B
Called DN	D	D	C	A	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	40	**40**	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	FF

A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates an ECONF usage where A(controller) has different MSN numbers.

In below scenario, B1, B2 and B3 represent the MSN1, MSN2 and MSN3 DNs on the same BRI phone set.

Scenario 2: Controller with different MSN's

1- B1 dials C; **2-** C answers; **3-** B1 puts C into conference call; **4-** B1 puts conference call on hold; **5-** B2 dials A; **6-** A answers; **7-** A is added into conference call with B1; **8-** completion of B2-A conversation in due to realization of ECONF service; **9-** B3 dials D; **10-** D answers; **11-** D is added into conference call with B1; **12-** completion of B3-D conversation in due to realization of ECONF service; **13-** B1 retrieves the conference call; **14-** disconnection of conference call.

Table 128 A is under surveillance

No of step	5	6	7	11	14
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	B2	B2	B1*	B1*	B1*
Called DN	A	A	C	D	A
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	**40**	40	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	FF

Note: * While adding A into the conference, SOSM replaces B2 with the DN of the controller (B1). This is due to ECONF service behavior. By the activation of ECONF, A is involved into a conference with the controller (B1), and B2 is disconnected from the call.

Table 129 B1 is under surveillance

No of step	1	2	3	4	7	11	13	14
Messages	1.1	1.2	1.4	1.4	1.4	1.4	1.4	1.3
Calling DN	B1	B1	B1	B1	B1	B1	B1	B1
Called DN	C	C	C	C	A	D	C	C
SOSM Call #	1	1	1	1	1	1	1	1
Attribute of choice	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	04	04	00
MCL #	1	1	1	1	1	1	1	1
Code of operation	00	00	00	00	00	00	00	05
Feature Code	FF	FF	ECO NF	HO LD	ECO NF	ECO NF	HO LE	FF

Table 130 B2 is under surveillance

No of step	5	6	8
Messages	1.1	1.2	1.3
Calling DN	B2	B2	B2
Called DN	A	A	A
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 131 B3 is under surveillance

No of step	9	10	12
Messages	1.1	1.2	1.3
Calling DN	B3	B3	B3
Called DN	D	D	D
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 132 B1, B2, B3 all are under surveillance

No of step	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Messages	1.1	1.2	1.4	1.4	1.1	1.2	1.4	1.3	1.1	1.2	1.4	1.3	1.4	1.3
Calling DN	B1	B1	B1	B1	B2	B2	B1	B2	B3	B3	B1	B3	B1	B1
Called DN	C	C	C	C	A	A	A	A	D	D	D	D	C	C
SOSM Call #	1	1	1	1	2	2	1	2	3	3	1	3	1	1
Attribute of choice	01	01	01	01	01	01	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00	00	04	00	00	00	04	00	04	00
MCL #	1	1	1	1	2	2	1	2	3	3	1	3	1	1
Code of operation	00	00	00	00	00	00	00	05	00	00	00	05	00	05
Feature Code	FF	FF	ECO NF	HO LD	FF	FF	ECO NF	FF	FF	FF	ECO NF	FF	HO LE	FF

Table 133 C is under surveillance

No of step	1	2	3	7	11	14
Messages	1.1	1.2	1.4	1.4	1.4	1.3
Calling DN	B1	B1	B1	B1	B1	B1
Called DN	C	C	C	A	D	C
SOSM Call #	1	1	1	1	1	1
Attribute of choice	04	04	04	**40**	40	04
Parameters of connection	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	04	00
MCL #	1	1	1	1	1	1
Code of operation	00	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	ECO NF	FF

Table 134 D is under surveillance

No of step	9	10	11	11	14
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	B3	B3	B1*	B1*	B1*
Called DN	D	D	C	A	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	40	**40**	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	ECO NF	ECO NF	FF

Note: * While adding D into the conference, SOSM replaces B3 with the DN of the controller (B1). This is due to ECONF service behavior. By the activation of ECONF, D is involved into a conference with the controller (B1), and B3 is disconnected from the call.

In addition to Annex2 of SOSM Conformance Test document, below scenarios are investigated for ECONF service.

14.11.2.5.1 Controller isolates and reattaches a conferee

Scenario 1: B isolates A from the conference call.

- When A is under surveillance; a “No.1.4-SS Usage:HOLD” message is reported to CP for the isolation from the conference call.
- When B is under surveillance; no message is reported to CP.
- When C is under surveillance; no action is taken.
- When D is under surveillance; no action is taken.

Scenario 2: B reattaches A to the conference call.

- When A is under surveillance; a “No.1.4-SS Usage:HOLE” message is reported to CP for the reattaching to the conference call.
- When B is under surveillance; no message is reported to CP.
- When C is under surveillance; no action is taken.
- When D is under surveillance; no action is taken.

14.11.2.5.2 Controller drops a conferee from the conference

B disconnects A from the conference :

- When A is under surveillance; the disconnection of conference call (No.1.3 in step14) is reported to CP.
- When B is under surveillance; no message is reported to CP since the disconnection of call A-B (step 8) was already reported.
- When C is under surveillance; no action is taken.
- When D is under surveillance; no action is taken.

14.11.2.5.3 Disconnection of a conferee from the conference

A disconnects from the conference call:

- When A is under surveillance; the disconnection of conference call (No.1.3 in step14) is reported to CP.
- When B is under surveillance; no message is reported to CP since the disconnection of call A-B (step 8) was already reported.

- When C is under surveillance; no action is taken.
- When D is under surveillance; no action is taken.

14.11.2.6 Call Transfer (ECT) for BRI

Explicit Call Transfer is an ISDN supplementary service which enables a user who has two calls, each of which can be an incoming or an outgoing call, to connect the other parties and get out from the call. ECT has two invocation types: implicit invocation and explicit invocation.

The required SOSM message sequences in Section7 of Annex2 of SOSM Conformance Test document are valid for a basic ISDN BRI ECT service.

The following call steps are reported to CP according to SOSM Conformance Test document:

Scenario 1: Controller with a single MSN

1- A dials B; **2-** B answers; **3-** B puts A on hold; **4-** B dials C; **5-** C answers; **6-** B makes call transfer; **7-** disconnection of conversation A-B; **8-** disconnection of conversation B-C; **9-** disconnection of transferred call A-C.

Figure 87 ECT activation - Controller with a single MSN

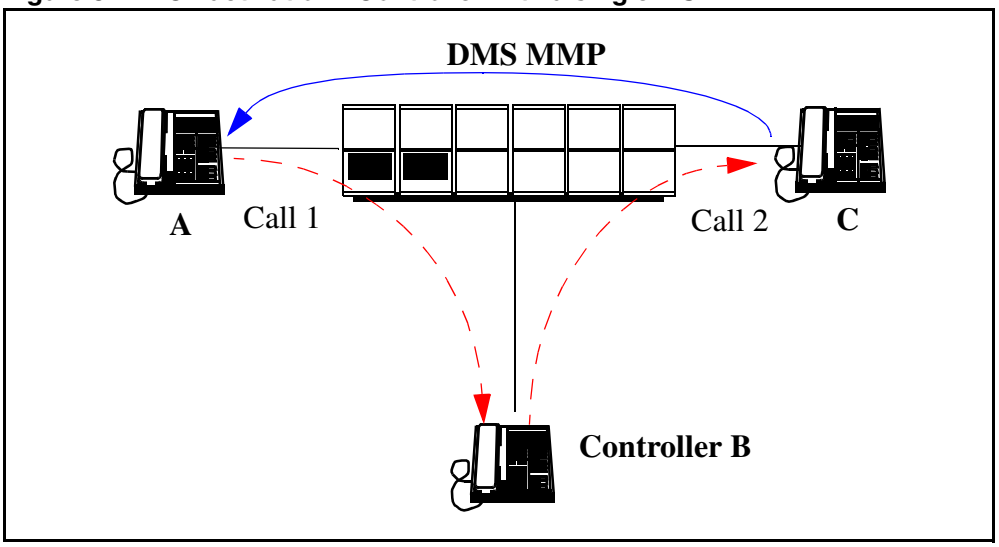


Table 135 A is under surveillance

No of step	1	2	3	6	9
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B	B	A
Called DN	B	B	A	C	C
SOSM Call #	1	1	1	1	1

No of step	1	2	3	6	9
Messages	1.1	1.2	1.4	1.4	1.3
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	ECT	FF

Table 136 B is under surveillance

No of step	1	2	3	4	5	6	7	8		-*	-*	6*	7*	8*
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.3		1.4	1.4	1.4	1.3	1.3
Calling DN	A	A	B	B	B	B	A	B		B	B	B	**B**	**A**
Called DN	B	B	A	C	C	A	B	C		C	A	**C**	**C**	**B**
SOSM Call #	1	1	1	2	2	2	1	2		2	1	**1**	**2**	**1**
Attribute of choice	04	04	01	01	01	01	04	01		01	01	01	01	**04**
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C		1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	00	00		04	04	04	00	00
MCL #	1	1	1	2	2	2	1	2		2	1	**1**	**2**	**1**
Code of operation	00	00	00	00	00	00	05	05		00	00	00	05	05
Feature Code	FF	FF	HO LD	FF	FF	ECT	FF	FF		HO LD	HO LE	ECT	FF	FF

Note: * If the subscriber A returns to the first conversation (A-B) and then makes call transfer, these messages are expected according to SOSM Conformance Test document.

Table 137 C is under surveillance

No of step	4	5	6	9
Messages	1.1	1.2	1.4	1.3
Calling DN	B	B	B	A
Called DN	C	C	A	C
SOSM Call #	2	2	2	2
Attribute of choice	04	04	40	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	ECT	FF

A BRI phone set can have multiple DN's by the use of MSN supplementary service. Below scenario illustrates an ECT activation scenario where A(controller) has different MSN numbers, and both MSN's are under observation

In below tables, B1 and B2 represent MSN1 and MSN2 DNs on the same BRI phone set.

Scenario 2: Controller with different MSN's

1- A dials B1; **2-** B1 answers; **3-** B1 puts A on hold; **4-** B2 dials C; **5-** C answers; **6-** B2 makes call transfer; **7-** disconnection of conversation A-B1; **8-** disconnection of conversation B2-C; **9-** disconnection of transferred call A-C.

Figure 88 Result of successfully invoking ECT in Scenario 2

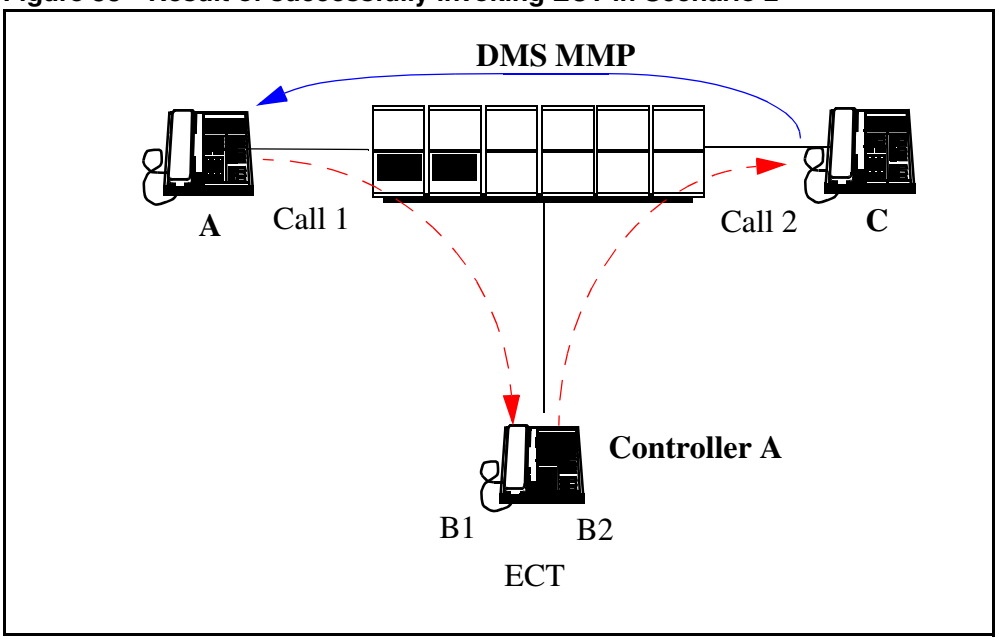


Table 138 A is under surveillance

No of step	1	2	3	6	9
Messages	1.1	1.2	1.4	1.4	1.3
Calling DN	A	A	B1	B2	A
Called DN	B1	B1	A	C	C
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	40	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	HO LD	ECT	FF

Table 139 B1 is under surveillance

No of step	1	2	3	7
Messages	1.1	1.2	1.4	1.3
Calling DN	A	A	B1	A
Called DN	B1	B1	A	B1
SOSM Call #	1	1	1	1
Attribute of choice	04	04	01	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	HO LD	FF

Table 140 B2 is under surveillance

No of step	4	5	6	8
Messages	1.1	1.2	1.4	1.3
Calling DN	B2	B2	B2	B2
Called DN	C	C	A	C
SOSM Call #	2	2	2	2
Attribute of choice	01	01	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	ECT	FF

Table 141 B1 and B2 is under surveillance

No of step	1	2	3	4	5	6	7	8
Messages	1.1	1.2	1.4	1.1	1.2	1.4	1.3	1.3
Calling DN	A	A	B1	B2	B2	B2	A	B2
Called DN	B1	B1	A	C	C	A	B1	C
SOSM Call #	1	1	1	2	2	2	1	2
Attribute of choice	04	04	01	01	01	01	04	01
Parameters of connection	1C	1C	1C	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00	00	04	00	00
MCL #	1	1	1	2	2	2	1	2
Code of operation	00	00	00	00	00	00	05	05
Feature Code	FF	FF	HO LD	FF	FF	ECT	FF	FF

Table 142 C is under surveillance

No of step	4	5	6	9
Messages	1.1	1.2	1.4	1.3
Calling DN	B2	B2	B2	A
Called DN	C	C	A	C
SOSM Call #	2	2	2	2
Attribute of choice	04	04	40	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	ECT	FF

14.11.2.7 Call Forward (Busy, Unconditional, Do Not Answer)

Call Forward allows a subscriber to divert a call to another agent. If one of the parties is SOSM agent in a diverted call after diversion.

In BRI lines call forwarding is provisioned with CFU, CFD, CFB and CFK (Call Forward per Key) line options.

CFK feature can be assigned to any vacant key on the loop. Those DN keys, which are to receive the CFK functionality are specified in a KEYLIST. For CFK, user can provide a different DN for each key specified in the KEYLIST. CFU and CFK provides the same functionality in terms of call forwarding. Therefore, **CFK usage/act/deact/int is reported with "CFU" feature code in 1.4 - Suppl. Service Usage message.**

CFB and CFD features might be assigned per DN in the existing system, and there are 4 types of CFB and CFD which are N (Normal), F (Fixed), P (Programmable), and K (Programmable per Key). Following table shows the overall picture of CFx. Please refer to activity "A59028702 - Support of CFx for Multiple DNs on ETSI BRI" for further information.

Table 143 Overall Picture of CFx

Cfx	Possible Activation
CFU	Per Access
CFK	Per DN
CFB N, F, P	Per Access
CFB K	Per DN
CFD N, F, P	Per Access
CFD K	Per DN

14.11.2.7.1 CFx Act/Deact/Interrogation

BRI Subscriber can act/deact/interrogate CFx flavors either by using CEPT dialing sequences, or via using call forward programming facilities of BRI phone set. **SOSM sends different message sequences to CP for those two kinds of CFx act/deact/interrogation.**

Subscriber actions for Act/Deact/Interrogation of CFx flavors is reported to CP only for the DN initiating the CFx act/deact/interrogation (i.e. Other DNs affected by CFx Act/Deact/Int are not reported), if DN was supervised for monitoring.

a. CFx Act/Deact/Interrogation Using Cept Dialing Sequence

BRI subscriber can act/deact/interrogate CFx flavors using CEPT dialing sequences. Please refer to activity "A59034125 - ISDN BRI CEPT Call Forwarding" for detailed information.

SOSM sends 1.4 - Suppl. Service Usage and 1.3 - Disconnect messages consequently (only for the DN subscriber action is initiated from), when subscriber CFx act/deact/interrogation is completed successfully.

Behavior of 1.3 - Disconnect Message varies depending on how dialed digits are sent. If dialed digits are sent

— inside origination message, 1.3 Message is sent just after 1.4 Message, before subscriber on-hook.

— in digits message(s), 1.3 Message is sent just after subscriber on-hook.

See SOSM message sequences for the example below.

Figure 89 BRI CFx Example

```
>qlt isdn1 1
------------------------------------------------------------------------
LTID:  ISDN1       1
SNPA: 102
DIRECTORY NUMBER:     7831002
LT GROUP NO: 1
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  24 0 00 02    TEI: UNATEI
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 5
OPTIONS:
AFC
CFB P $ I 1 SFC HOLD

   KEY       DN
   ---       --
     1       DN          1027831002 (A1)
     5       DN          1027831003 (A2)
     6       DN          1027831004 (A3)

   KEY     FEATURE
   ---     -------
     1       HOLD
     1        CFB P                              $         I  1
     2        AFC
     3        AFC
     4        AFC
------------------------------------------------------------------------
>
```

There are three DNs defined on this loop, and "$" on the KEYLIST of CFB option states that any DN on the loop will be affected by CFB act/deact/int. Consider that 7831002(A1) and 7831003(A2) are being monitored.

SOSM message sequence reported to CP as a result of CFB programming initiated from A1 is as follows:

Table 144 A1 is under surveillance, CFB programming initiated by A1

Messages	1.4	1.3
Calling DN	**A1**	**A1**
Called DN	Dialled Digits	Dialled Digits
SOSM Call #	**1**	**1**
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	CFB	FF

SOSM message sequence reported to CP as a result of CFB programming initiated from A2 is as follows:

Table 145 A2 is under surveillance, CFB programming initiated by A2

Messages	1.4	1.3
Calling DN	**A2**	**A2**
Called DN	Dialled Digits	Dialled Digits
SOSM Call #	**1**	**1**
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF

Messages	1.4	1.3
Code of operation	FF	05
Feature Code	CFB	FF

If CFB programming is initiated by A3 (not being monitored) no SOSM messages will be reported to CP as a result of CFB programming, although programming affects other DNs.

b. CFx Act/Deact/Interrogation Using Phone Set (when on-hook)

BRI subscriber can act/deact/interrogate CFx flavors using BRI phone set menu, when on-hook. In this kind of subscriber actions, phone set sends facility messages, and act/deact/interrogate action is performed according to the information received in the facility message. However, number of facility messages, and information sent inside the message strictly depends on the BRI phoneset which subscriber action is initiated from.

For example, activating a CFx flavor with an ASCOM Eurit 30 phone set causes deactivation of other CFx flavors active on the set, while this does not happen with TELES.FON sets.

The ASCOM phone sets send three facility messages since the basic service can not be chosen from the phone menu. So the phone set sends the same facility messages for all basic services. Moreover TELES.FON set sends 9 facility messages because even call forward type (CFU, CFB, CFD) can not be chosen from its menu.

Since all facility messages are processed by DMS, SOSM is responsible to report each facility message, which causes successful subscriber action. So a seperate 1.4 - Suppl. Service Usage message is sent for each facility message causing successful act/deact/interrogation.

Please note that 1.3 - Disconnect message is not reported to CP, since no off-hook/on-hook occurs during this kind of CFx act/deact/ interrogation.

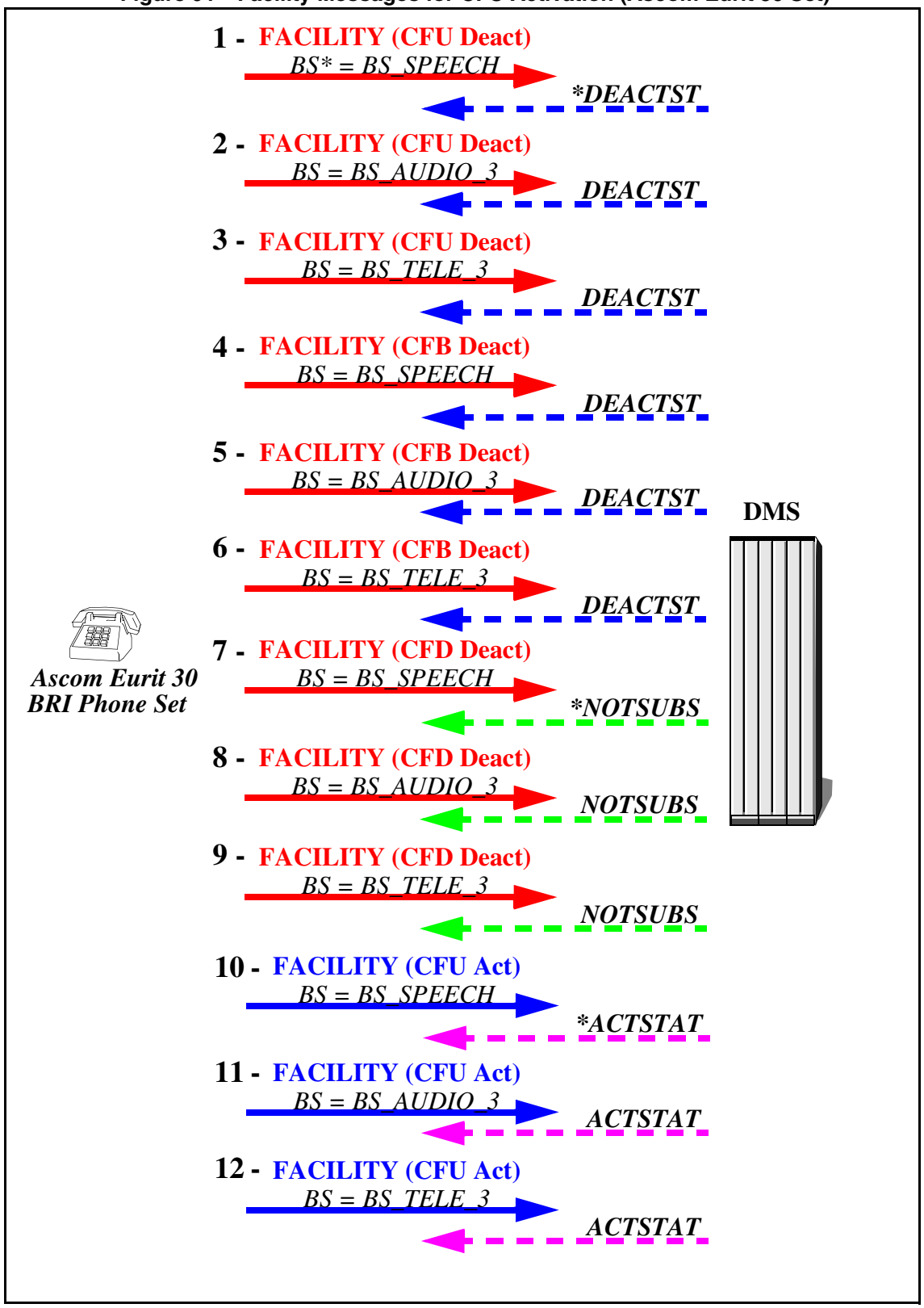
In the exaple below, CFB is active for both DNs on the loop, while CFU is also assigned but not active. Consider A1 is being monitored and CFU programming is initiated from A1.

Figure 90 BRI CFx Example

```
>qlt isdn1 1
------------------------------------------------------------------------
LTID:  ISDN1       1
SNPA: 102
DIRECTORY NUMBER:     7831002
LT GROUP NO: 1
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  24 0 00 02    TEI: UNATEI
CUSTGRP:        CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 5
OPTIONS:
CFU Y 7835340 I $ CFB F 7835340 A $ SFC HOLD

   KEY       DN
   ---       --
     1       DN          1027831002 (A1)
     5       DN          1027831003 (A2)

   KEY     FEATURE
   ---     -------
     1       HOLD
     1        CFU Y                        7835340 I $
     1        CFB F                        7835340         A $
------------------------------------------------------------------------
```

When subscriber(A1) initiates CFU activation from ASCOM Eurit 30 phone set, where three facility messages(one per basic service) are sent for CFU activation, and also three facility messages are sent for deactivation of per CFx flavor assigned, facility messages processed by DMS and SOSM message sequence reported to CP would be as follows.

Figure 91 Facility Messages for CFU Activation (Ascom Eurit 30 Set)



** BS- Basic Service*

** ACTST - Activation Status Notification Diversion*

** DEACTST - Deactivation Status Notification Diversion*

** NOTSUBS - Not Subscribed*

Table 146 A1 is under surveillance

STEP	1	2	3	4	5	6	7-8-9	10	11	12
	1.4	1.4	1.4	1.4	1.4	1.4		1.4	1.4	1.4
Calling DN	A1	A1	A1	A1	A1	A1		A1	A1	A1
Called DN	B1*	B1	B1	C*	C	C		B2*	B2	B2
SOSM Call #	1	2	3	4	5	6		7	8	9
Attribute of choice	01	01	01	01	01	01		01	01	01
Parameters of connection	1C	1C	1C	1C	1C	1C		1C	1C	1C
Code of supp. service phase	03	03	03	03	03	03		01	01	01
MCL #	FF	FF	FF	FF	FF	FF		FF	FF	FF
Code of operation	FF	FF	FF	FF	FF	FF		FF	FF	FF
Feature Code	CFU	CFU	CFU	CFB	CFB	CFB		CFU	CFU	CFU

* B1 - Previous Forwarded DN (CFU)

* B2 - Forwarded DN (CFU)

* C - Previous Forwarded DN (CFB)

NOTE : B1 and C might be NIL in case related CFx flavor was not activated before.

14.11.2.7.2 CFx Usage

The Call Forwarding Unconditional (CFU) service causes all incoming calls to a BRI line to be forwarded immediately to an alternative number. The called party's ability to originate calls is unaffected.

The Call Forwarding Busy (CFB) service causes an incoming call to a BRI line to be forwarded immediately to an alternative number if it encounters a busy subscriber. The called party's ability to originate calls is unaffected. The DMS implementation does not support the User Determined User Busy procedures. The DMS uses the Network Determined User Busy procedures.

The Call Forwarding No Reply (CFNR) service causes an incoming call to a BRI line to be forwarded to an alternative number if it is not answered within a specified time. The called party's ability to originate calls is unaffected.

In the scenario given below, subscriber A calls B. B has Call Diversion Feature programmed to divert the call to C. CFU, CFB and CFD line options are used for BRI lines.

SOSM message sequences provided in Section1 of Annex2 of SOSM Conformance Test document are also valid for ISDN BRI Call Forwarding services. The SOSM message sequences of ISDN BRI CF services should be same with CEPT CF ones.

The following call steps are reported to CP:

1- A dials B; 2- call forwarding; 3- C answers; 4- disconnection.

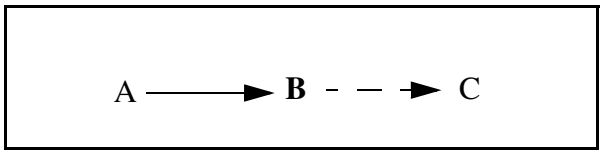


Table 147 A is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	01	40	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1

Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	FF	FF

Table 148 B is under surveillance

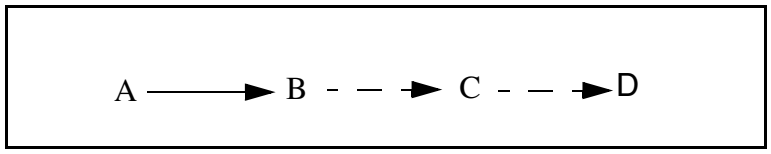
No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	FF	FF

Table 149 C is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	FF	FF

Chain CF Services



The following call steps are reported to CP:

1- A dials B; 2- B diverts the call to C; 3- C diverts the call to D; 4- C answers; 5- disconnection.

Table 150 A is under surveillance

No of step	1	2	3	4	5
Messages	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	B	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	01	40	40	01	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	Cfu Cfb Cfnr	FF	FF

Table 151 B is under surveillance

No of step	1	2	3	4	5
Messages	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	B	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	01	40	40	40
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	Cfu Cfb Cfnr	FF	FF

Table 152 C is under surveillance

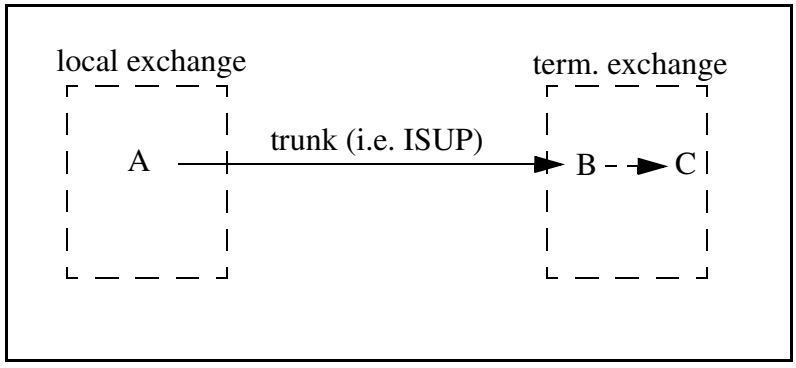
No of step	1	2	3	4	5
Messages	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	C	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	01	40	40
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	Cfu Cfb Cfnr	FF	FF

Table 153 D is under surveillance

No of step	1	2	3	4	5
Messages	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	C	A	A
Called DN	D	C	D	D	D
SOSM Call #	1	1	1	1	1
Attribute of choice	04	40	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	Cfu Cfb Cfnr	Cfu Cfb Cfnr	FF	FF

Trunk Implementation

In local exchange, if the monitored call is routed over trunk then service usage notification messages (Msg.1.4) are not generated when call diversion (including call forward chain) takes place in other exchange.



In the scenario given above, the following call steps are reported to CP from the local exchange if the originator is a monitored subscriber or if B's number is observed as a network number at local exchange.

1- A dials B; 2- A receives answer over trunk; 3- disconnection.

Table 154 A is under surveillance (Local Exchange)

No of Steps	**1**	**2**	**3**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	11	11	11
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 155 B is under surveillance as a network number (Local Exchange)

No of Steps	**1**	**2**	**3**
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	11	11	11
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

In this scenario, the following call steps are reported to CP from the terminating exchange if the forwarding (B) or terminating agent (C) is target..

1- B receives the incoming call from trunk; 2- B forwards the call to C; 3-C answers; 4- disconnection.

Table 156 B is under surveillance (Terminating Exchange)

No of Steps	**1**	**2**	**3**	**4**
Messages	**1.1**	**1.4**	**1.2**	**1.3**
Calling DN	A	B	A	A
Called DN	B	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	12	1C	12	12
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

Table 157 C is under surveillance (Terminating Exchange)

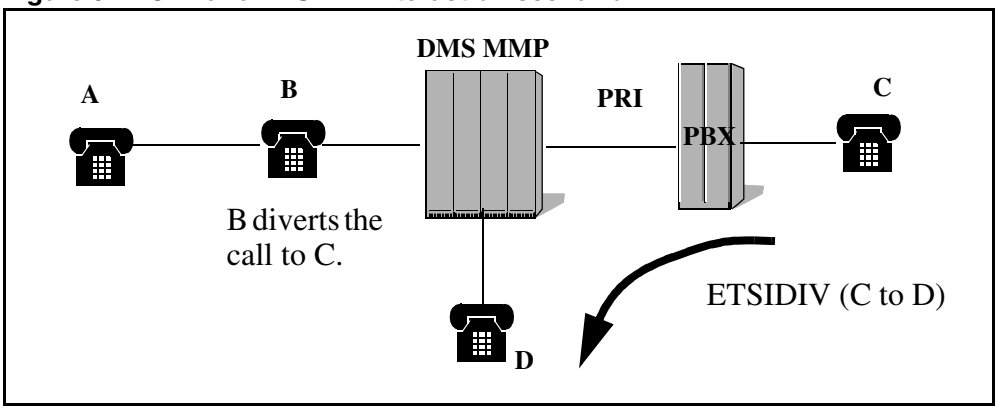
No of Steps	**1**	**2**	**3**	**4**
Messages	**1.1**	**1.4**	**1.2**	**1.3**
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	12	1C	12	12
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	Cfu Cfb Cfd	FF	FF

CFx interaction with ISDN PRI ETSIDIV service

ETSIDIV is an ISDN PRI service which allows a private network user to reroute an incoming call from a PRI agent to another network number. CFx service has interaction with ETSIDIV.

As it is described in detail in section "14.11.3.2 ETSIDIV - ETSI PRI Diversion", SOSM is unable to find previous diversion information after the call is rerouted by ETSIDIV service.

Figure 92 CFx and ETSIDIV interaction scenario



Above figure illustrates a scenario where the call is diverted twice with CFx and ETSIDIV services.

In this scenario, SOSM is unable to collect diversion information for ETSIDIV service when D is monitored.

Additionally, if subscriber C uses ETSIDIV Late Release, also B-to-C forwarding data is lost upon activation of ETSIDIV.

Therefore, SOSM does not send ETSIDIV usage message if monitoring starts after ETSIDIV activation (i.e. while monitoring D). Additionally, SOSM sends CFx notification message -only if ETSIDIV Early Release activated-with the available called party information which can be determined after monitoring starts.

In the above scenario, the call steps are as follows.

1- A dials B; **2-** B forwards the call to C over PRI; **3-** C diverts the call to D by using ETSIDIV; **4-** D answers; **5-** disconnection.

Table 158 D is under surveillance in CFx and ETSIDIV interaction

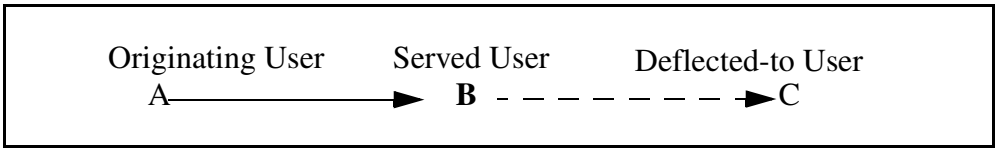
No of step	3	3*	4	5
Messages	1.1	1.4	1.2	1.3

Calling DN	A	B	A	A
Called DN	D	D	D	D
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CFU/ CFB/ CFNR	FF	FF

Note: *This column is reported only if ETSIDIV Early Release is invoked.

14.11.2.8 Call Deflection (CD)

The ISDN BRI Call Deflection (CD) service allows a user to respond to an incoming call by requesting redirection of that call to another user.



Call deflection service can be invoked in two different ways:

- **Call Deflection Immediate (CDI):** CD is invoked in response to the offered call
- **Call Deflection on Alerting (CDA):** during the period that the served user is being informed of the call

DMS MMP supports two different modes of CD functionality according to the CD subscription option per subscriber: clearcall or retain call. DMS MMP behavior on these subscription options can be summarized as follows:

- **Call Deflection with Early Release (Clear Call on Invocation):** Upon activation of CD service, the served user is immediately disconnected via sending a DISCONNECT message, and the call is rerouted to the deflected-to-user.

- **Call Deflection with Late release (Retain Call Until Alerting):** Upon activation of CD service, DMS MMP establishes a new call between originating user (A) and deflected-to user (C). Initial call between the originating user (A) and served user (B) is not cleared until an alerting indication is received from the deflected-to user (C).

SOSM has different functionalities for CD early release and CD late release.

14.11.2.8.1 Call Deflection with Early Release

The following call steps are reported to CP:

1- A dials B; **2-** B deflects the call to C; **3-** C answers; **4-** disconnection.

Table 159 A is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C*	C	C
SOSM Call #	1	1	1	1
Attribute of choice	01	40	01	01
Parameters of connection	1C	1C**	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CDI/ CDA	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step-2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 160 B is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A

Called DN	B	C*	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	1C	1C**	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CDI/ CDA	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step-2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 161 C is under surveillance

No of step	**1**	**2**	**3**	**4**
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CDI/ CDA	FF	FF

14.11.2.8.2 Call Deflection with Late Release

In this scenario, A-B call is retained until deflected-to user (C) begins to alert.

Please note that when the late release of Call Deflection occurs, the deflected call is reported as a new call with a new SOSM call number since there are two calls until reception of alert notification from deflected-to user (C).

Scenario 1: Call is deflected to C (C is idle and alerting)

If the deflected-to user is idle, then CD service clears the initial call between the originator (A) and served user (B).

The following call steps are reported to CP:

1- A dials B; **2-** B requests call deflection to C; **3-** C alerts (call is deflected); **4-** C answers; **5-** Call disconnection (A-C).

Table 162 A is under surveillance

No of step	**1**	**2**	**2**	**3**	**4**	**5**
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	B	C	C
SOSM Call #	1	**2**	**2**	1	**2**	**2**
Attribute of choice	01	40	01	01	01	01
Parameters of connection	1C	1C**	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	1	**2**	**2**
Code of operation	00	00	00	**04**	00	05
Feature Code	FF	CDI/ CDA	FF	FF	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step-2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 163 B is under surveillance

No of step	**1**	**2**	**2**	**3**	**4**	**5**
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A

Called DN	B	C*	C	B	C	C
SOSM Call #	1	**2**	**2**	1	**2**	**2**
Attribute of choice	04	01	40	04	40	40
Parameters of connection	1C	1C**	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	1	**2**	**2**
Code of operation	00	00	00	**04**	00	05
Feature Code	FF	CDI/ CDA	FF	FF	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step 2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 164 C is under surveillance

No of step	**1**	**2**	**4**	**5**
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	C	C	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CDI/ CDA	FF	FF

Scenario 1: Call Deflection fails (i.e. C is busy)

If the deflected-to user (C) is busy, then CD service clears the second call established between the originator (A) and deflected-to user (C).

The following call steps are reported to CP:

1- A dials B; **2-** B requests call deflection to C; **3-** Call deflection fails (i.e. C is busy); **4-** B answers; **5-** Call disconnection (A-B).

Table 165 A is under surveillance

No of step	1	2	2	3	4	5
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	C	B	B
SOSM Call #	1	**2**	**2**	**2**	1	1
Attribute of choice	01	40	01	01	01	01
Parameters of connection	1C	1C**	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	**2**	1	1
Code of operation	00	00	00	**01/ 03**	00	05
Feature Code	FF	CDI/ CDA	FF	FF	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step-2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 166 B is under surveillance

No of step	1	2	2	3	4	5
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	C	B	B
SOSM Call #	1	**2**	**2**	**2**	1	1
Attribute of choice	04	01	40	40	04	04
Parameters of connection	1C	1C**	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	**2**	1	1

Code of operation	00	00	00	**01/ 03**	00	05
Feature Code	FF	CDI/ CDA	FF	FF	FF	FF

Note 1: * C in 1.4 service usage message in step 2 is the deflected-to number sent by the served user (B).

Note 2: ** In step-2, SOSM always sets parameter of connection as 1C, since at this point of call, SOSM can not determine whether C is a present exchange subscriber or a network subscriber.

Table 167 C is under surveillance

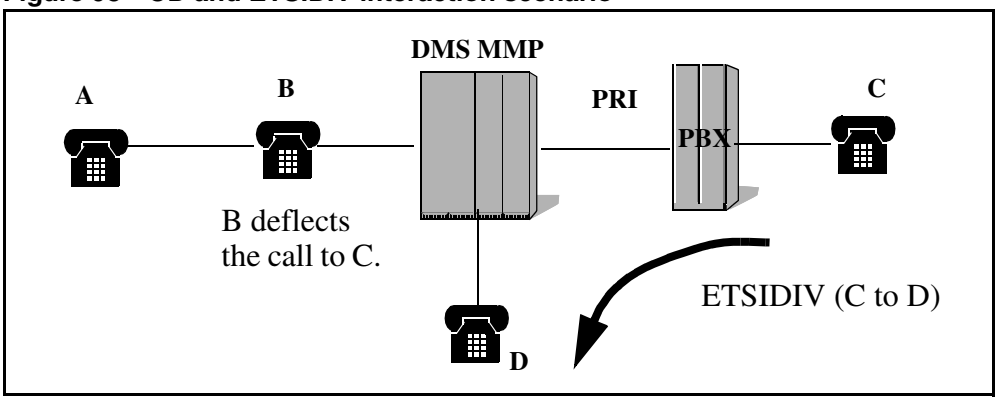
No of step	**1**	**3**
Messages	1.1	1.3
Calling DN	A	A
Called DN	C	C
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	**01/ 03**
Feature Code	FF	FF

14.11.2.8.3 CD interaction with ISDN PRI ETSIDIV service

ETSIDIV is an ISDN PRI service which allows a private network user to reroute an incoming call from a PRI agent to another network number. CD service has interaction with ETSIDIV.

As it is described in detail in section “14.11.3.2 ETSIDIV - ETSI PRI Diversion”, SOSM is unable to find correct information about diverting and diverted-to subscribers after the call is rerouted by ETSIDIV service.

Figure 93 CD and ETSIDIV interaction scenario



Above figure illustrates a scenario where the call is rerouted twice with CD and ETSIDIV services.

In this scenario, SOSM is unable to collect diversion information for ETSIDIV service when D is monitored.

Additionally, if subscriber C uses ETSIDIV Late Release, also B-to-C deflection data is lost upon activation of ETSIDIV.

Therefore, SOSM does not send ETSIDIV usage message if monitoring starts after ETSIDIV activation (i.e. while monitoring D). Additionally, SOSM sends CD notification message -only if ETSIDIV Early Release activated-with the available called party information which can be determined after monitoring starts.

In the above scenario, the call stepsare as follows.

1- A dials B; **2-** B deflects the call to C over PRI; **3-** C diverts the call to D; **4-** D answers; **5-** disconnection.

Table 168 D is under surveillance in CD and ETSIDIV interaction

No of step	3	3*	4	5
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	D	D	D	D
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C

Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CD-I/ CD-A	FF	FF

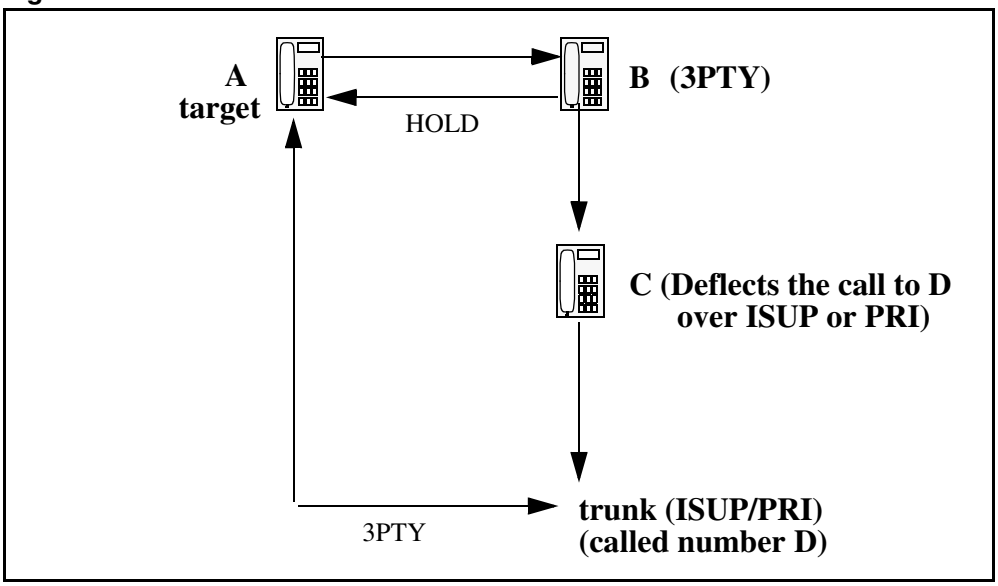
Note: *This column is reported only if ETSIDIV Early Release is invoked.

14.11.2.8.4 CD interaction with multi-party services

When a subscriber deflects a call over an ISUP or PRI trunk, original deflected-to number can not be determined after deflected-to subscriber alerts.

In multi-party services such as conference calls or call transfer, SOSM informs CP about all subscribers involved in the call, even if they are not monitored subscribers.

Figure 94 3PTY Conference Service



Above scenario illustrates a scenario where CD and 3PTY service interacts. In this scenario, SOSM is expected to notify CP about the conference and the conferees (A, B and D), when B establishes conference between A, B and the trunk agent.

However, due to the existing Call Deflection service functionality, SOSM is unable to determine original deflected-to number during activation of three

party conference, if D is not a present exchange subscriber. Therefore, in 3PTY service notification message, C is sent to CP as the called number instead of C.

14.11.2.9 Terminal Portability (TP)

The Terminal Portability (TP) supplementary service allows a user to move one terminal from one socket to another within one given basic access during the active state of a call.

TP service also allows a user to move a call from one terminal to another terminal within one given basic access during the active phase of call.

SOSM messages for the above scenarios are as follows.

Scenario 1 : Call is resumed from the same terminal

1. A dials B; **2.** B answers; **3.** B parked the call; **4.** B resumed the call; **5.** The call completed.

This call scneario is shown in the Figure 95 .

Figure 95 TP call scenario 1.

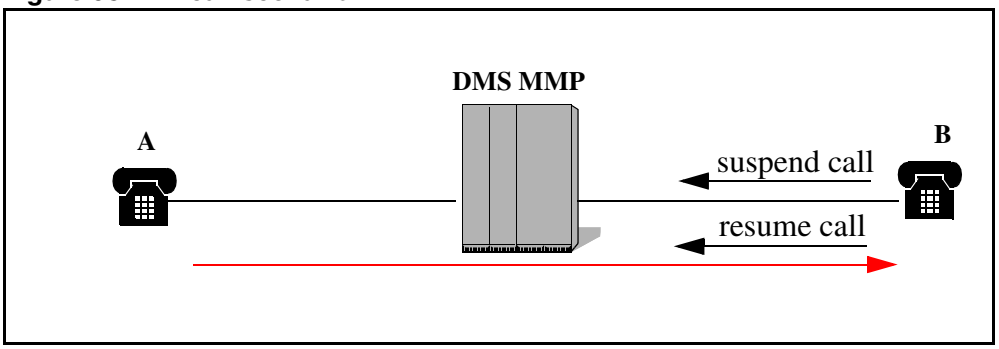


Table 169 A is target for TP call scenario 1.

No of step	1	2	3	4	5
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	A	A	B	B	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00

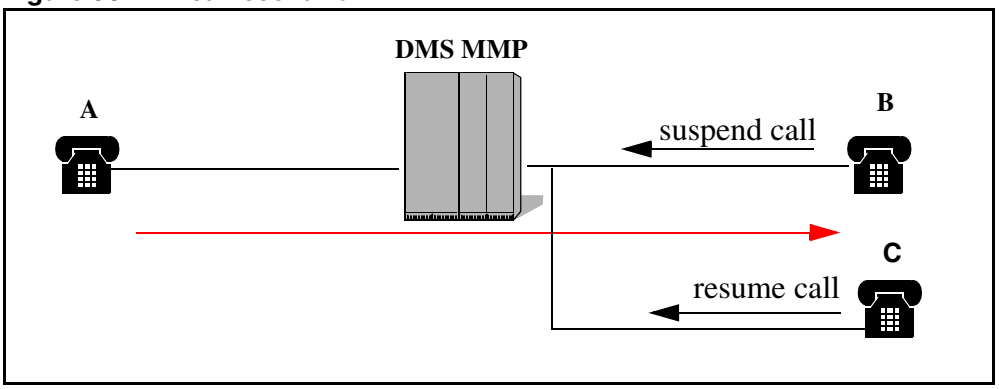
No of step	1	2	3	4	5
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	TP Suspend	TP Resumed	FF

Table 170 B is target for TP call scenario 1.

No of step	1	2	3	4	5
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	A	A	B	B	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	01	01	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	TP Suspend	TP Resumed	FF

Scenario 2: Call is resumed from another terminal (C).

Figure 96 TP call scenario 2.



1. A dials B; **2.** B answers; **3.** B parked the call.; **4.** C resumed the call; **5.** The call completed.

Table 171 A is target for TP call scenario 2

No of step	**1**	**2**	**3**	**4**	**5**
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	A	A	B	C	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	01	01	04	04	01
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	FF	TP Suspend	TP Resumed	FF

Table 172 B is target for TP call scenario 2

No of step	**1**	**2**	**3**	**4**	**5**
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Calling DN	A	A	B	C	A
Called DN	B	B	A	A	B
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	01	01	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	04	04	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05

No of step	1	2	3	4	5
Messages	**1.1**	**1.2**	**1.4**	**1.4**	**1.3**
Feature Code	FF	FF	TP Suspend	TP Resumed	FF

14.11.2.10 Malicious Call Identification (MCID)

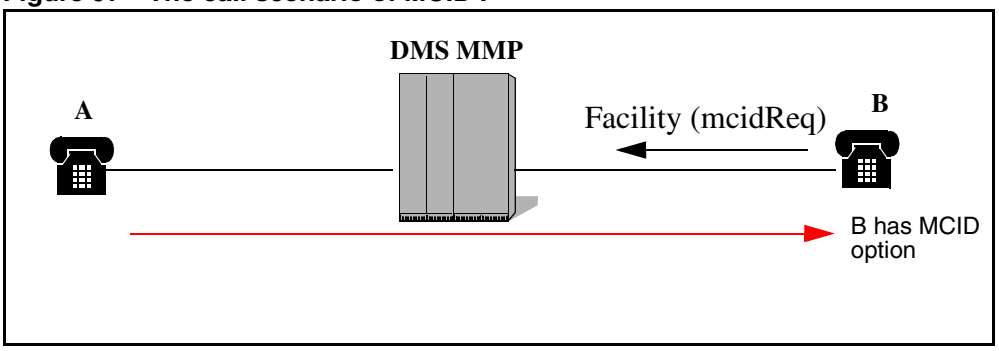
ISDN BRI MCID service enables the network to identify an incoming call. MCID can be invoked either manually by the subscriber or automatically by the network for all unanswered calls. It can be requested during the active phase of call or in the call clearing phase after receipt of DISCONNECT.

The following call steps are reported to CP.

1- A dials B; **2-**B answers; **3-**B invokes MCID service against A; **4-**disconnection of conversation A-B

This call scenario is shown in the Figure 97 .

Figure 97 The call scenario of MCID .



The SOSM message squences of ISDN BRI MCID service is same with CEPT MCT (CLF option). Please refer to Section “14.11.1.11 Malicious Call Trace” on page 405.

SOSM message sequences for MCID are listed in the tables below .

Table 173 A is under surveillance

No of step	1	2	4
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1

No of step	1	2	4
Messages	**1.1**	**1.2**	**1.3**
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Table 174 B is under surveillance

No of step	1	2	3	5
Messages	**1.1**	**1.2**	**1.4**	**1.3**
Calling DN	A	A	B	A
Called DN	B	B	A	B
SOSM Call #	1	1	1	1
Attribute of choice	04	04	01	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	MCID	FF

Note 1: When B attempts to activate MCID multiple times within a call, only the first MCID activation attempt is reported to CP as MCID usage message (1.4) .

Note 2: DMS generates an MCID log for unanswered calls automatically. However, SOSM does not send MCID usage notification for this MCID log, since there is no user action in this scenario.

Note 3: After originator (A) goes onhook, terminator (B) can request MCID within the next 30 secs. This functionality is provided by delaying the release of the call. In this scenario, SOSM behavior will be the same with the behavior in the MCID request during talking.

14.11.2.11 Calling Line Identification Restriction (CLIR)-Temp Mode

The ETSI BRI CLIR service restricts presentation of the calling user's ISDN number and subaddress to the called user. BRI CLIR service can be assigned to subscribers as permanent mode or temporary mode. If the calling user has subscribed to CLIR with permanent mode, then the presentation indicator forwarded thru the network indicates' presentation restricted' for all calls.

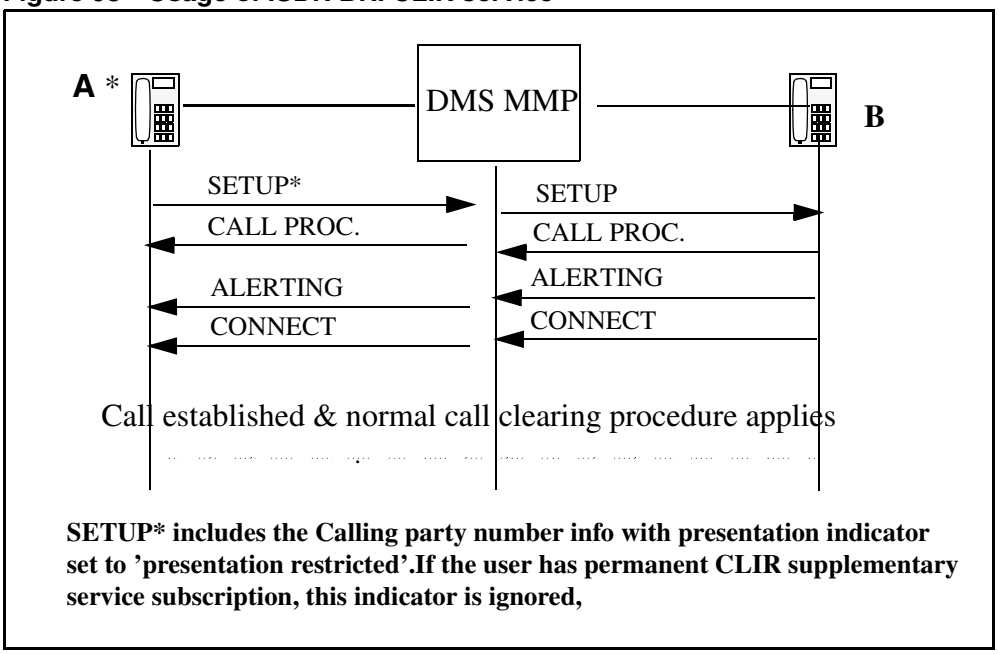
Since there is no user interaction in permanent mode, no SOSM service usage message is reported to CP when the subscriber has CLIR with permanent mode.

If the calling user has subscribed to the CLIR service with temporary mode and CLIR is requested by the user on a per call basis, the calling party number information element containing a presentation indicator is included in the SETUP message, then the originating network shall set the presentation indicator according to that in the received Calling party number information element.

SOSM reports service usage notification message for CLIR (temporary mode) to Control Point, if a SETUP message with presentation indicator set to 'presentation restricted' is received from a monitored subscriber.

CLIR usage notification is sent only for the user of the service - i.e. only when originator is target.

Figure 98 Usage of ISDN BRI CLIR service



The following call steps are reported to CP:

1- A dials B by using CLIR service per call basis; **2-** B answers; **3-** disconnection of conversation A-B.

Table 175 A is under surveillance

No of Steps	**1**	**1**	**2**	**3**
Messages	**1.1**	**1.4**	**1.2**	**1.3**
Calling DN	A	A	A	A
Called DN	B	B	B	B
SOSM Call #	1	1	1	1
Attribute of choice	01	01	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	CLIR	FF	FF

Table 176 B is under surveillance

No of Steps	1	2	3
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

14.11.2.12 Connected Line Identification Restriction (COLR)-Temp mode

The ETSI BRI COLR service is a service offered to connected party. It restricts presentation of connected party's ISDN number and subaddress to calling party.It can be assigned to subscribers as permanent mode or temporary mode.

If the called user has subscribed to COLR with permanent mode, the presentation indicator forwarded through the network indicates 'presentation restricted' for all calls.

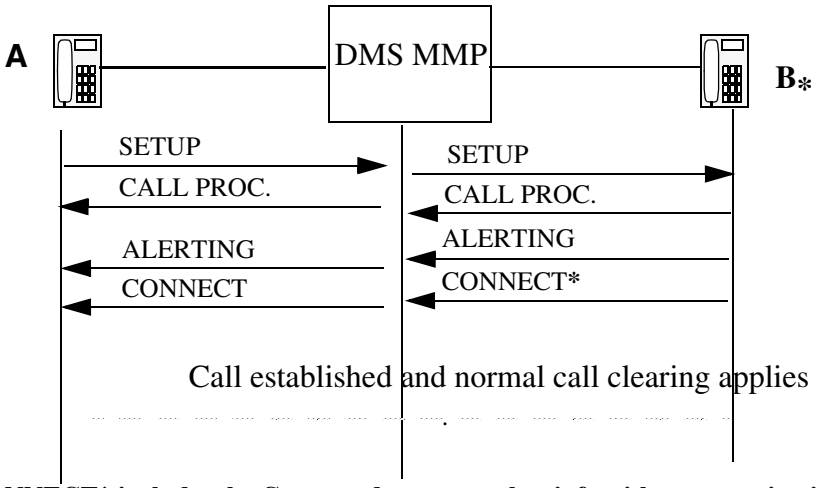
Since there is no user interaction in permanent mode, SOSM does not send service usage message for COLR (permanent mode) to CP.

If the calling user has subscribed to the COLR with temporary mode and if COLR is requested by the user on a per call basis, the Connected Number information element containing a presentation indicator is included in the CONNECT message. Destination network sets the presentation indicator according to presentation indicator in the received Connected Number information element.

SOSM sends service usage notification message for COLR (temporary mode) to CP, upon reception of presentation indicator with 'presentation restricted' value within CONNECT message.

COLR usage notification is expected only for the user of the service - i.e. only if terminating agent is target.

Figure 99 Usage of ISDN BRI COLR service



CONNECT* includes the Connected party number info with presentation indicator set to 'presentation restricted'. If the user has permanent COLR supplementary service subscription, this indicator is ignored,

The following call steps are reported to CP:

1- A dials B; **2-** B answers by using COLR service per call basis; **3-** disconnection of conversation A-B.

Table 177 A is under surveillance

No of Steps	1	2	3
Messages	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05

No of Steps	1	2	3
Messages	**1.1**	**1.2**	**1.3**
Feature Code	FF	FF	FF

Table 178 B is under surveillance

No of Steps	1	2	2	3
Messages	**1.1**	**1.2**	**1.4**	**1.3**
Calling DN	A	A	B	A
Called DN	B	B	A	B
SOSM Call #	1	1	1	1
Attribute of choice	04	04	01	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	CO LR	FF

14.11.2.13 User to User Signalling (UUS)

ISND BRI UUS service allows either party in a call to provide up to 128 octets of free-format information to the other party. UUS1 Service supports the exchange of information via UUI parameters in the standart call setup and clearing messages such as SETUP.

There are two types of UUS1 request: Implicit and explicit request.

An implicit request is preferred as default. This "preferred" means the call has not to be ended if UUI element can not be passed.

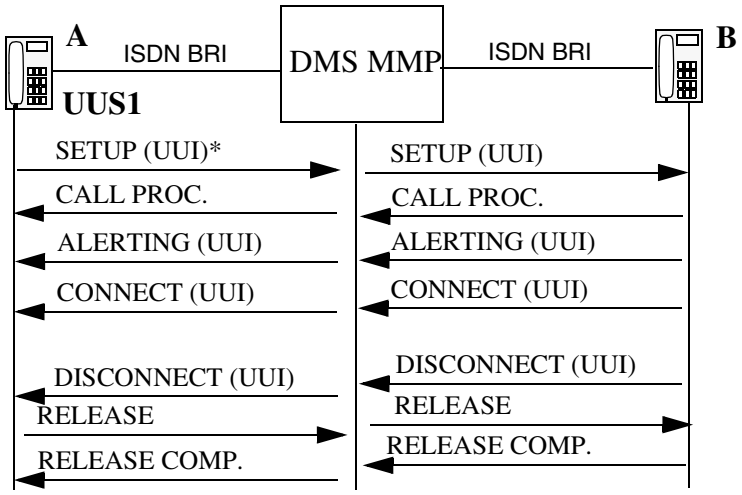
Explicit request has two types as required and preferred. The calling user may be able to specify whether the request for service is required or preferred for the call (whether the call should be completed or not if User to User information can not be passed).

The following call steps are reported to CP if UUS1 service is successfully invoked:

1- A dials B; **2-** UUS1 service successfully invoked; **3-** B answers; **4-** disconnection of conversation A-B.

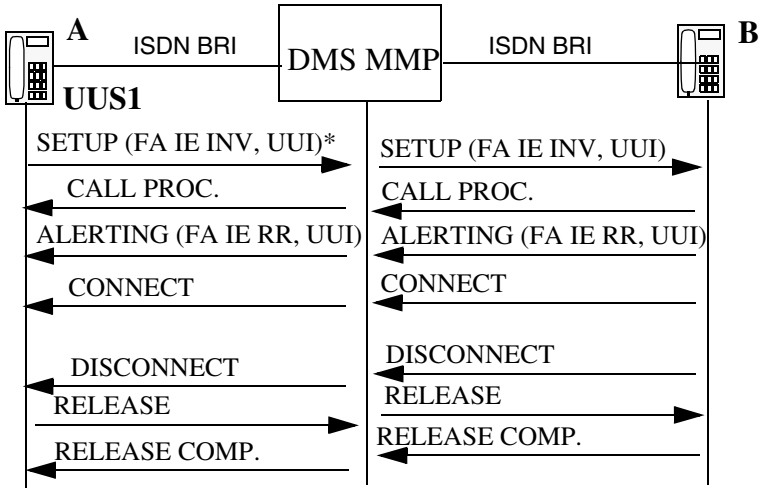
SOSM assumes that the UUS1 service is invoked successfully by the followings: with a valid UUI in SETUP message for UUS1 implicit mode, or with a valid FA IE INV component in SETUP message for UUS1 explicit mode.

Figure 100 Usage of ISDN BRI UUS1 implicit service



*** UUS1 implicit service successful invocation:** If the DMS office receives a valid "User-to-User Information (UUI)" in SETUP message from the calling party, it is assumed that the UUS1 implicit service is invoked successfully and the message "No.1.4- SS Usage" is reported to CP.

Figure 101 Usage of ISDN BRI UUS1 explicit (required or preferred) service



*** UUS1 explicit service successful invocation:** If the DMS office receives a valid "FA IE INV" component in SETUP message from the calling party, it is assumed that the UUS1 explicit service is invoked successfully and the message "No.1.4- SS Usage" is reported to CP.

Table 179 A is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	A	A	A
Called DN	B	B	B	B
SOSM Call #	1	1	1	1
Attribute of choice	01	01	01	01
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	UUS1	FF	FF

Table 180 B is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	A	A	A
Called DN	B	B	B	B
SOSM Call #	1	1	1	1
Attribute of choice	04	04	04	04
Parameters of connection	1C	1C	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	UUS1	FF	FF

Note: In unsuccessfull calls (called agent is busy, etc..), UUS service is not realized. Therefore, SOSM does not send "No.1.4-SS usage" message for UUS in such calls.

14.11.2.14 Closed User Group (CUG) for BRI

CUG provides a mechanism for forming groups to and from which access is restricted. A specific user may be member of one or more Closed User Groups. Members of a specific CUG can communicate among each other but not, in general, with users outside of the group.

CUG service does not have subscriber interactions Therefore, "No.1.4-SS usage" message is not reported for CUG service. SOSM message sequence for successful calls to/from Closed User Group members is the same with the basic calls.

If a call to a Closed User Group member fails, and if the call is monitored, operation code in the message 1.3 "Call Clearing" can vary according to the treatment set by the CUG service. SOSM does not send service usage notification for CUG in such scenarios.

If the treatment is set to busy treatment by CUG service , the operation code in 1.3 "Call Clearing" message is set to 3 (busy call) otherwise it is set to 2 (partial dialling).

Figure 102 Unsuccessful call from a remote subscriber to CUG

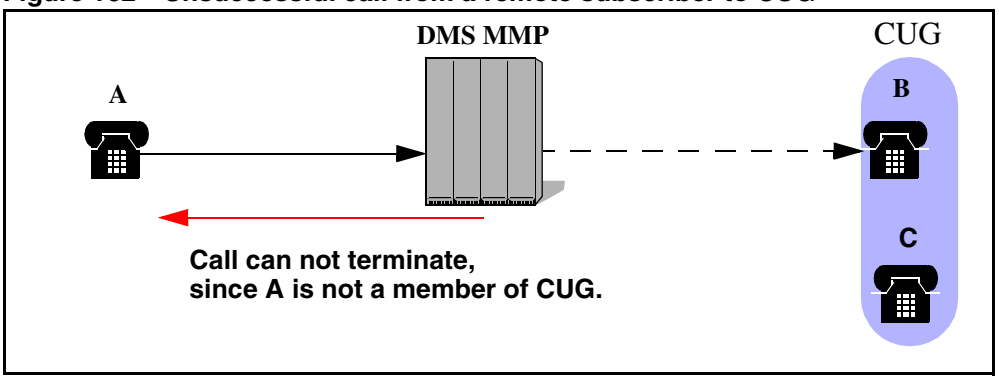


Table 181 CUG - A (originator) is under surveillance for unsuccessful call

Messages	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	02 / 03
Feature Code	FF	FF

Table 182 CUG - B(terminator) is under surveillance for unsuccessful call

Messages	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00

Messages	1.1	1.3
MCL #	1	1
Code of operation	00	02/ 03
Feature Code	FF	FF

If a monitored member of a Closed User Group attempts to make a call to a restricted number, the call fails, and the operation code within 1.3 " Call Clearing" message depends on the treatment value set by the CUG service.

Figure 103 Unsuccessful call from CUG to a restricted subscriber

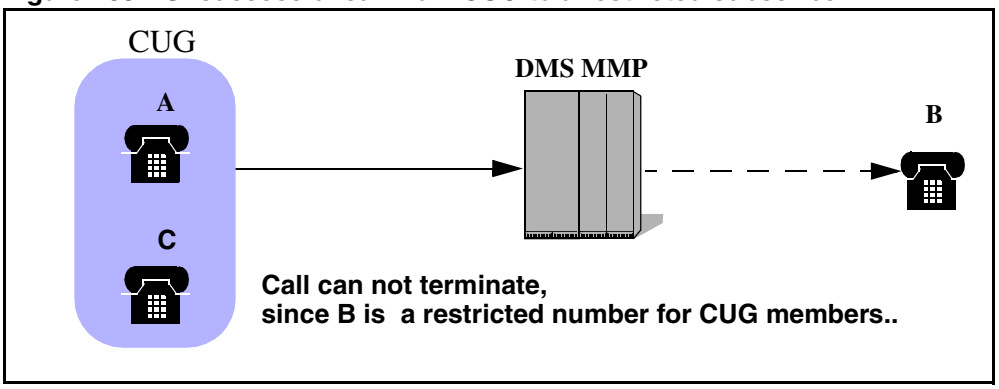


Table 183 CUG - A (originator) is under surveillance in unsuccessfull call.

Messages	1.1	1.3
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	02/ 03
Feature Code	FF	FF

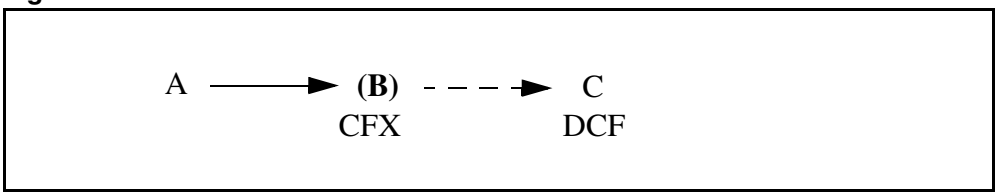
14.11.2.15 Huntgroups (DNH, DLH, MLH)

SOSM behavior for Hunt Group service realization is the same in BRI and IBN agents. For detailed information about SOSM interaction with hunt groups, please refer to Section “14.11.1.21 Huntgroups (DNH, DLH, MLH)” on page 419.

14.11.2.16 Deny Call Forward (DCF)

This feature allows the subscriber the ability to prevent incoming forwarded calls from terminating.

Figure 104 DCF call scenario



The following call steps will be reported to CP:

1. A calls B; **2.** B has any of CFX option and call forwarded to C; **3.** A-C call is disconnected due to DCF service realization.

Table 184 A is under surveillance

No of Steps	**1**	**2**	**3**
Messages	**1.1**	**1.4**	**1.3**
Calling DN	A	B	A
Called DN	B	C	C
SOSM Call #	01	01	01
Attribute of choice	01	40	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	04	00
MCL #	1	1	1
Code of operation	00	00	01
Feature Code	FF	CFX	FF

Table 185 B is under surveillance

No of Steps	**1**	**2**	**3**
Messages	**1.1**	**1.4**	**1.3**
Calling DN	A	B	A
Called DN	B	C	C
SOSM Call #	01	01	01
Attribute of choice	04	01	40
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	04	00
MCL #	1	1	1
Code of operation	00	00	01
Feature Code	FF	CFX	FF

Table 186 C is under surveillance

Steps	**1**	**2**	**3**
Messages	**1.1**	**1.4**	**1.3**
Calling DN	A	B	A
Called DN	C	C	C
SOSM Call #	01	01	01
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	04	00
MCL #	1	1	1
Code of operation	00	00	01
Feature Code	FF	CFX	FF

14.11.2.17 Completition of Calls to Busy Subscriber (CCBS)

The CCBS supplementary service enable user A, when encountering a busy destination B, to have the call completed without having to make a new call attempt when the destination B becomes not busy.

SOSM is responsible to report CCBS act/deact/int and usage to CP, if agent is being monitored.

14.11.2.17.1 CCBS Act

A dials B which is busy. A activates CCBS against B. When B on-hooks, A rings. When A off-hooks, the call is setup automatically established between A and B.

In this scenario, the following call steps will be reported to CP :

1- A dials B; **2-** B is busy; **3-** A activates CCBS against B; **4-** A on-hooks; **5-** A is notified that B is not busy and A initiates a CCBS call to B; **6-** B answers; **7-** disconnection of conversation A-B.

Table 187 A is under surveillance

No of Steps	**1**	**2**	**3**	**4**	**5**	**5**	**6**	**7**
Messages	**1.1**	**1.3**	**1.4**	**1.3**	**1.4**	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A	A	A	A	A	A
Called DN	B	B	B	B	B	B	B	B
SOSM Call #	1	1	2	2	3	3	3	3
Attribute of choice	01	01	01	01	01	01	01	01
Parameters of connection	1C	1C	1C	1C	1C*	1C	1C	1C
Code of supp. service phase	00	00	01	00	04	00	00	00
MCL #	1	1	FF	FF	FF**	3	3	3
Code of operation	00	03	FF	05	FF	00	00	05
Feature Code	FF	FF	CC BS	FF	CC BS	FF	FF	FF

Note 1: * Parameter of connection is always set as 1C in CCBS service usage message, since at this call step, SOSM is unable to determine whether B is a present exchange subscriber or not.

Note 2: ** In CCBS service usage message, MCL number is always set as FF.

Table 188 B is under surveillance

No of Steps	1	2	5	6	7
Messages	**1.1**	**1.3**	**1.1**	**1.2**	**1.3**
Calling DN	A	A	A	A	A
Called DN	B	B	B	B	B
SOSM Call #	1	1	2	2	2
Attribute of choice	04	04	04	04	04
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	00	00	00	00
MCL #	1	1	2	2	2
Code of operation	00	03	00	00	05
Feature Code	FF	FF	FF	FF	FF

14.11.2.17.2 CCBS Deact/Interrogation

BRI user can deactivate and interrogate CCBS service via using the BRI phone set menu (when on-hook). Deactivation and interrogation is performed according to the facility messages received from the phone set.

SOSM is responsible to report each facility message processed by DMS, which causes successful deactivation/interrogation of CCBS service, if agent was supervised before.

Please note that 1.3 - Disconnect message is not reported to CP, since no off-hook/on-hook occurs during CCBS deact/interrogation.

Following is the facility messages and SOSM message sequence reported during CCBS deactivation.

Figure 105 Facility Messages for CCBS Deactivation

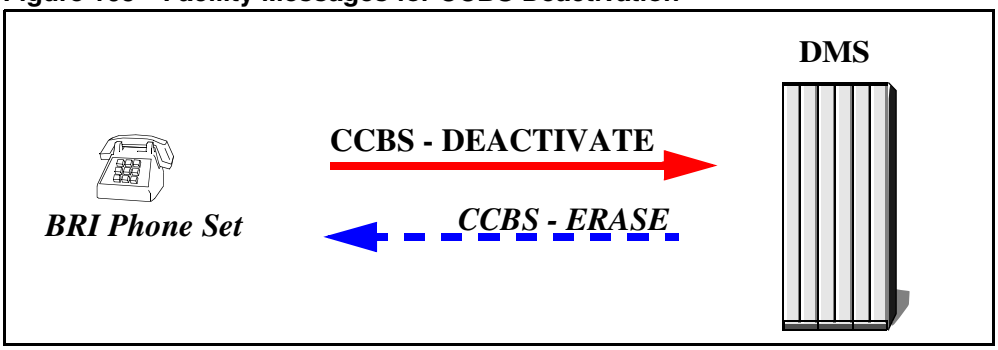


Table 189 A is under surveillance

No of Steps	**1**
Messages	**1.4**
Calling DN	A
Called DN	B*
SOSM Call #	1
Attribute of choice	01
Parameters of connection	1C**
Code of supp. service phase	03
MCL #	FF
Code of operation	FF
Feature Code	CCBS

Note 1: * B is the DN that CCBS was programmed for.

Note 2: ** Parameter of connection is always set as 1C in CCBS service usage message, since at this call step, SOSM is unable to determine whether B is a present exchange subscriber or not.

14.11.2.17.3 CCBS Usage

After CCBS is activated by subscriber A, A goes on hook, then A is notified that B is not Busy and A initiates a CCBS call to B. B answers and for the rest of the call , normal call clearing procedure is applied. Please see Table 187 for SOSM message sequences.

14.11.2.18 Completition of Calls on No Reply (CCNR)

CCNR supplementary service enables user A, encountering a destination B which does not answer the call (No Reply), to have the call completed without having to make a new call attempt when the destination B becomes not busy after having initiated an activity.

SOSM is required to send notification about activation/usage of CCNR service within SOSM ISDN BRI and PRI Supplementary Services Specifications document (SOSMISDN.AA01 in FMDOC library). However, this service can not be realized in NETAS lab, therefore, this requirement is not supported within this activity.

14.11.2.19 Automatic Line (AUL)

Functionality of BRI AUL feature is similar to IBN hot line (AUL) feature. BRI AUL is an administrator assigned feature, and administrator is responsible for activation , deactivation and programming.

SOSM message sequences for BRI AUL usage is the same as message sequences of IBN AUL. Please refer to Section “14.11.1.14 Automatic Line” on page 409.

14.11.2.20 Warm Line (WML)

Warm Line feature for BRI lines has an equivalent functionality to IBN Warm Line. Warm Line feature is assigned from servord, with WML line option. Subfield ’FTCODE’ of WML line option and office parameter WML_OCT_IS_LINE_OPT_PARM together defines the behavior of octothorpe (#) during feature activation (Please refer to FN Document of A59027828 - BRI Hot and Warm Line).

SOSM message sequences for WML act/deact/interrogation is the same as IBN Warm Line feature. Please refer to Section “14.11.1.15 Warm-Line” on page 410.

14.11.2.21 Wake Up Call Request (WUCR)

This feature allows the subscriber to ring his/her phone set at a specified time which can be programmed by the subscriber. For BRI lines WUCR line option provides this functionality.

SOSM Message sequences for WUCR act/deact/interrogation and wake up call is the same as IBN CEPT IWUC. Please refer to Section “14.11.1.17 Wake-up Call” on page 412.

14.11.2.22 Outgoing Call Barring (OCB)

This feature enables calls belonging to certain types to be rejected when they are originated by the served user. Restriction of outgoing calls are performed according to 11 classes of restriction.

In OCB - F (Fixed), the barring program to be restricted is specified while assigning OCB line option to the line. Only administrator has the capability to control OCB functionality (i.e. any user actions are not allowed).

In OCB - UD (User Defined), ISDN BRI subscriber who has OCB line option can actvate, deactivate, and interrogate his/her OCB functionality.

SOSM reports service usage messages to CP, during act/deact/int/usage of OCB service.

14.11.2.22.1 OCB Act/Deact/Interrogation using CEPT dialing Sequence

In this scenario A has OCB option. A activates the OCB feature using CEPT dialing sequence. The message sequence is given in the following table.

Table 190 Activation of OCB - A is under surveillance

	1.4	1.3
Calling DN	A	A
Called DN	Dialed Digits	Dialed Digits
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	1C	1C
Code of supp. service phase	01	00
MCL #	FF	FF
Code of operation	FF	05
Feature Code	OCB*	FF

14.11.2.22.2 OCB Usage

In this scenario, A is under surveillance and calls a restricted number. The message sequence is shown in the following table.

Table 191 OCB Usage - A is under surveillance

	1.1	1.4	1.3
Calling DN	A	A	A
Called DN	B	B	B
SOSM Call #	1	1	1
Attribute of choice	01	01	01
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	04	00
MCL #	1	1	1
Code of operation	00	00	01
Feature Code	FF	OCB*	FF

Note: * The same feature code is used by ILR.

If B is under surveillance no messages are reported to CP during OCB usage.

14.11.3 ISDN PRI Supplementary Services

"SOSM Message Sequences for ISDN Supplementary Services" (SOSMISDN in FMDOC library) document describes the SOSM behavior for BRI/PRI supplementary services.

In this document, reporting of service usage messages is mentioned as optional in several scenarios. SOSM reports optional service usage messages to CP if data regarding to usage of the service is available.

The services ETSIDIV, ECT, CCBS, CCNR, UUS1, MCID, CLIR (temporary mode) and COLR (temporary mode) can be assigned to PRI trunks on DMS. In fact, activation/ deactivation/ usage of these services are initiated from PBX, not on DMS, and since PRI is a trunk access, normally SOSM does not sent any notification about these services, unless the service changes the call topology. Therefore:

- Since the Call Forwarding with Partial Rerouting (ETSIDIV option) and ECT services cause call rerouting, the usage of these services are reported to Control Point (CP) in SOSM message No.1.4“SS usage” when the service is successfully realized upon the request.
- Since the CCBS, CCNR, UUS1, MCID, CLIR (temporary mode) and COLR (temporary mode) services do not cause call rerouting, the usage of

these services are not reported to CP. However, the usage of these services does not cause any abnormal messages to CP.

The remaining services do not have subscriber interactions (such as AOC-D, AOC-E, CLIP, COLP, CLIR-permanent mode, COLR-permanent mode, CUG, SUB, DDI) or the service functionalities are provided by PBX (such as CW, HOLD, 3PTY, CONF, TP). So the “No.1.4-SS usage” message is not reported for the usages of these services. These services calls are monitored as basic call.

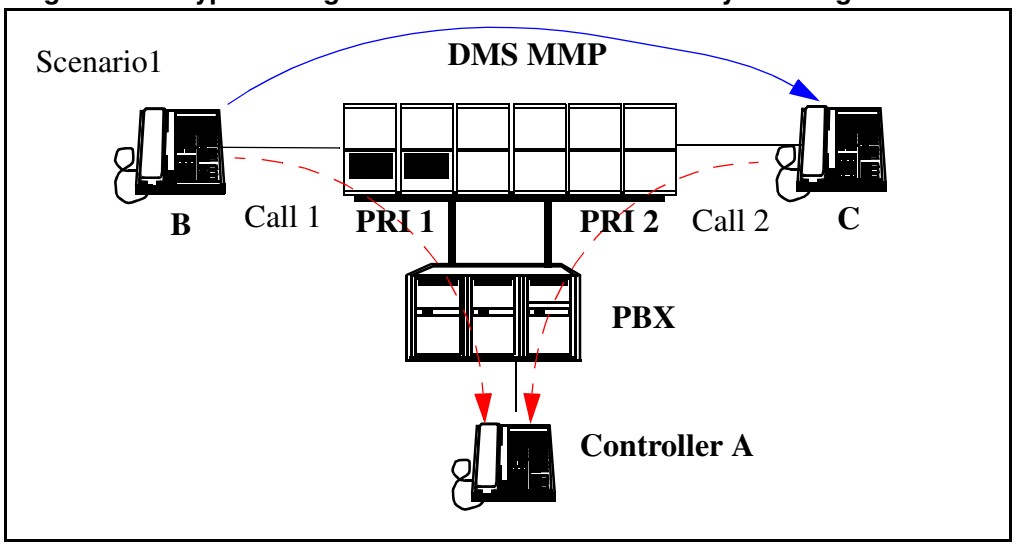
These PRI services can be enabled only via provisionning to related tables on DMS. There is no subscriber utility to activate/ deactivate/ interogate PRI services so the “No.1.4-SS usage” message is not reported for Act/Deact/Intg of ISDN PRI services.

14.11.3.1 ECT for PRI

Explicit Call Transfer is an ISDN supplementary service which enables a user who has two calls to connect the other parties and get out from the call. Any of these calls can be an incoming or an outgoing call.

ECT optimizes the use of ETSI PRI trunks when it is in effect. The ECT feature is associated with an ISDN PRI interface. The PRI interface may terminate on an Intelligent Peripheral (IP), a Private Branch Exchange (PBX) or other Customer Premise Equipment (CPE). Figure 106 and Figure 108 . show a typical usage of ECT for two scenario and the result of successfully invoking ECT.

Figure 106 Typical usage and the result of successfully invoking ECT



The following call steps are reported to CP : Please note that PRI1 and PRI2 are two members of a PRI trunk and A1 represents terminating agent A over

first member of PRI trunk , A2 represents terminating agent A over second member of PRI trunk.

1- B dials A1 over PRI1 ;

2- A1 answers;

3- C dials A2 over PRI2;

4- A2 answers;

5- A2 makes Explicit Call transfer.

6- disconnection of conversation C-A2;

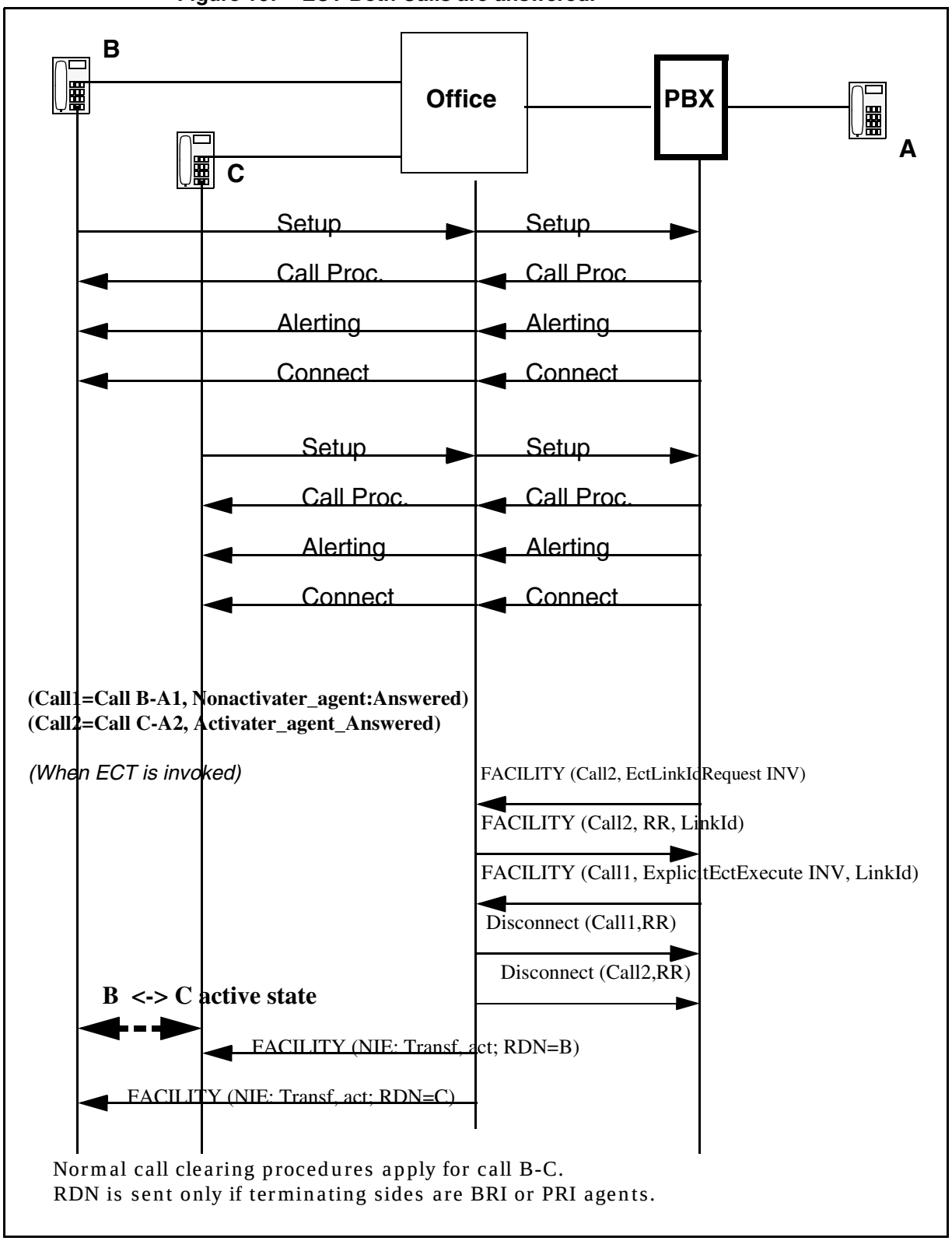
7- disconnection of conversation B-A1;

8- disconnection of transferred call C-B.

As a difference from BRI access, only explicit invocation method of ECT is supported for PRI access signalling. Please note that since the HOLD supplementary service is not supported on ISDN PRI, the “No.1.4 SS usage - HOLD” is not reported to Control Point.

Explicit Call Transfer can be realized while both calls are on talking states as illustrated in Figure.107.

Figure 107 ECT Both Calls are answered.



In the given call, before ECT is invoked, there are two calls between B-A1 (CALL1) and C-A2 (CALL2).

After successful activation of ECT service, a new C-B call is established.

Please note that the direction of the new call depends on the FACILITY messages received over PRI trunks. (i.e, in Figure.107, FACILITY-ExplicitEctExecute message is received within CALL2, and, B is transferred and connected to C to establish C-B call. In cases where FACILITY-ExplicitEctExecute message is received within CALL1, C will be transferred and connected to B. In such cases, B-C call will be established instead of C-B call.) The call steps for this scenario are as follows:

Steps 1,2,3 and 4 are same.

5- A1 makes Explicit Call transfer.*

6- disconnection of conversation B-A1;*

7- disconnection of conversation C-A2;*

8- disconnection of transferred call B-C.*

In tables below, detailed information is given on SOSM parameter values for each step of scenario1 above.

Table 192 Both A1 and A2 are under surveillance

No of step	1	2	3	4	5	6	7		5*	6*	7*
Messages	1.1	1.2	1.1	1.2	1.4	1.3	1.3		1.4	1.3	1.3
Calling DN	B	B	C	C	A2	C	B		A1	B	C
Called DN	A1	A1	A2	A2	B	A2	A1		C	A1	A2
SOSM Call #	1	1	2	2	2	2	1		1	1	2
Attribute of choice	04	04	04	04	01	04	04		01	04	04
Parameters of connection	11	11	11	11	12	11	11		12	11	11
Code of supp. service phase	00	00	00	00	04	00	00		04	00	00
MCL #	1	1	2	2	2	2	1		1	1	2
Code of operation	00	00	00	00	00	05	05		00	05	05
Feature Code	FF	FF	FF	FF	ECT	FF	FF		ECT	FF	FF

Table 193 A1 is under surveillance

No of step	1	2	7		5*	6*
Messages	1.1	1.2	1.3		1.4	1.3
Calling DN	B	B	B		A1	B
Called DN	A1	A1	A1		C	A1
SOSM Call #	1	1	1		1	1
Attribute of choice	04	04	04		01	04
Parameters of connection	11	11	11		12	11
Code of supp. service phase	00	00	00		04	00
MCL #	1	1	1		1	1
Code of operation	00	00	05		00	05
Feature Code	FF	FF	FF		ECT	FF

Table 194 A2 is under surveillance

No of step	3	4	5	6		7*
Messages	1.1	1.2	1.4	1.3		1.3
Calling DN	C	C	A2	C		C
Called DN	A2	A2	B	A2		A2
SOSM Call #	1	1	1	1		1
Attribute of choice	04	04	01	04		04
Parameters of connection	11	11	12	11		11
Code of supp. service phase	00	00	04	00		00
MCL #	1	1	1	1		1
Code of operation	00	00	00	05		05
Feature Code	FF	FF	ECT	FF		FF

Table 195 B is under surveillance:

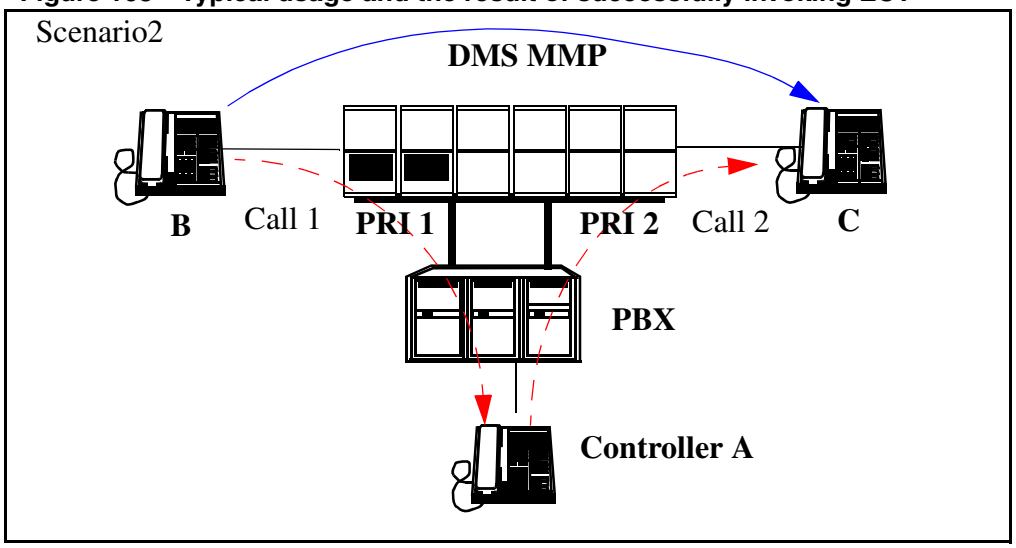
No of step	1	2	5	8		5*	8*
Messages	1.1	1.2	1.4	1.3		1.4	1.3
Calling DN	B	B	A2	C		A1	B
Called DN	A1	A1	C	B		C	C
SOSM Call #	1	1	1	1		1	1
Attribute of choice	01	01	40	04		40	01
Parameters of connection	11	11	12	1C		12	1C
Code of supp. service phase	00	00	04	00		04	00
MCL #	1	1	1	1		1	1
Code of operation	00	00	00	05		00	05
Feature Code	FF	FF	ECT	FF		ECT	FF

Table 196 C is under surveillance

No of step	3	4	5	8		5*	8*
Messages	1.1	1.2	1.4	1.3		1.4	1.3
Calling DN	C	C	A2	C		A1	B
Called DN	A2	A2	B	B		B	C
SOSM Call #	1	1	1	1		1	1
Attribute of choice	01	01	40	01		40	04
Parameters of connection	11	11	12	1C		12	1C
Code of supp. service phase	00	00	04	00		04	00
MCL #	1	1	1	1		1	1
Code of operation	00	00	00	05		00	05
Feature Code	FF	FF	ECT	FF		ECT	FF

A PRI agent can activate ECT service also during alerting (i.e. CALL1 is answered, and CALL2is alerting) as illustrated in Figure.108 and Figure.109 below.

Figure 108 Typical usage and the result of successfully invoking ECT



1- B dials A1 over PRI1 ;

2- A1 answers;

3- A2 dials C over PRI2;

4- C answers;

5- A2 makes Explicite Call transfer.

6- disconnection of conversation A2-C;

7- disconnection of conversation B-A1;

8- disconnection of transferred call B-C.

In tables Table 197 - Table 198 - Table 199 , detailed information is given on SOSM parameter values for each step of scenario2 given in Figure 108 .

Figure 109 ECT Nomactivater_ag:Answered./Activater_ag.:Alerting Msg Flow

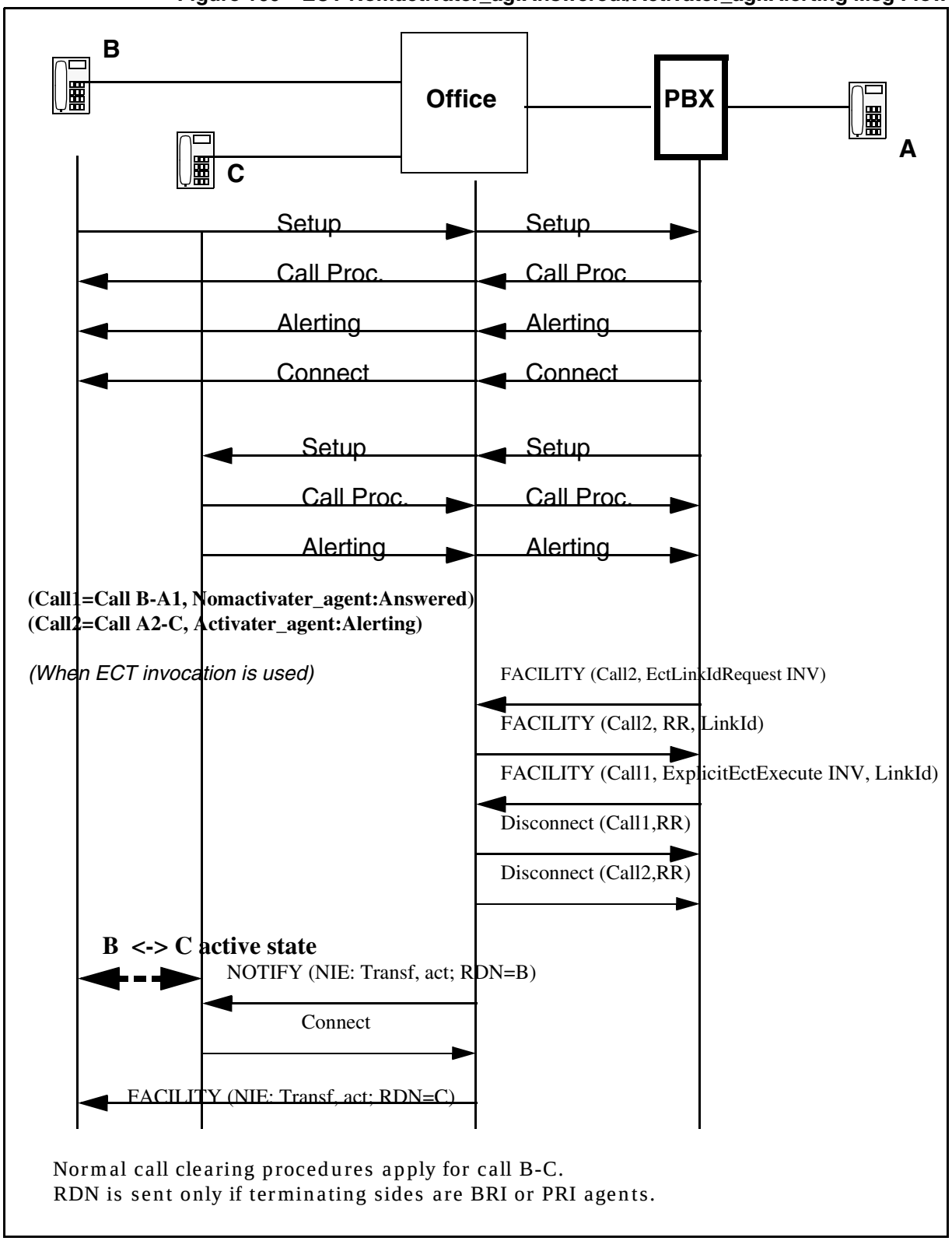


Table 197 A1 is under surveillance

No of step	1	2	7
Messages	1.1	1.2	1.3
Calling DN	B	B	B
Called DN	A1	A1	A1
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	11	11	11
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Since A2 is incoming PRI agent, it can not be chosen as target.

Table 198 B is under surveillance:

No of step	1	2	5	8
Messages	1.1	1.2	1.4	1.3
Calling DN	B	B	A2	B
Called DN	A1	A1	C	C
SOSM Call #	1	1	1	1
Attribute of choice	01	01	40	01
Parameters of connection	11	11	12	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	ECT	FF

Table 199 C is under surveillance

No of step	3	4	5	8
Messages	1.1	1.2	1.4	1.3
Calling DN	A2	A2	A2	B
Called DN	C	C	B	C
SOSM Call #	1	1	1	1
Attribute of choice	04	04	40	04
Parameters of connection	12	12	12	1C
Code of supp. service phase	00	00	04	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	FF	ECT	FF

14.11.3.2 ETSIDIV - ETSI PRI Diversion

ETSI PRI Diversion (ETSIDIV) is an ISDN supplementary service which enables a user to reroute an incoming call from a PRI agent to another telephone number. DMS MMP tries to route a call by sending out a SETUP message over ETSI PRI to a private network e.g. Private Branch Exchange (PBX). At the private network, it is decided that this call needs to be diverted. A partial rerouting request is sent to the DMS MMP in a FACILITY message. DMS MMP processes the request and reroutes the call.

There are two modes of ETSIDIV functionality:

Early Release: On receipt of a call rerouting request, the call towards the private network (B) is cleared immediately, and then a new call leg to the diverted-to user (C) is established.

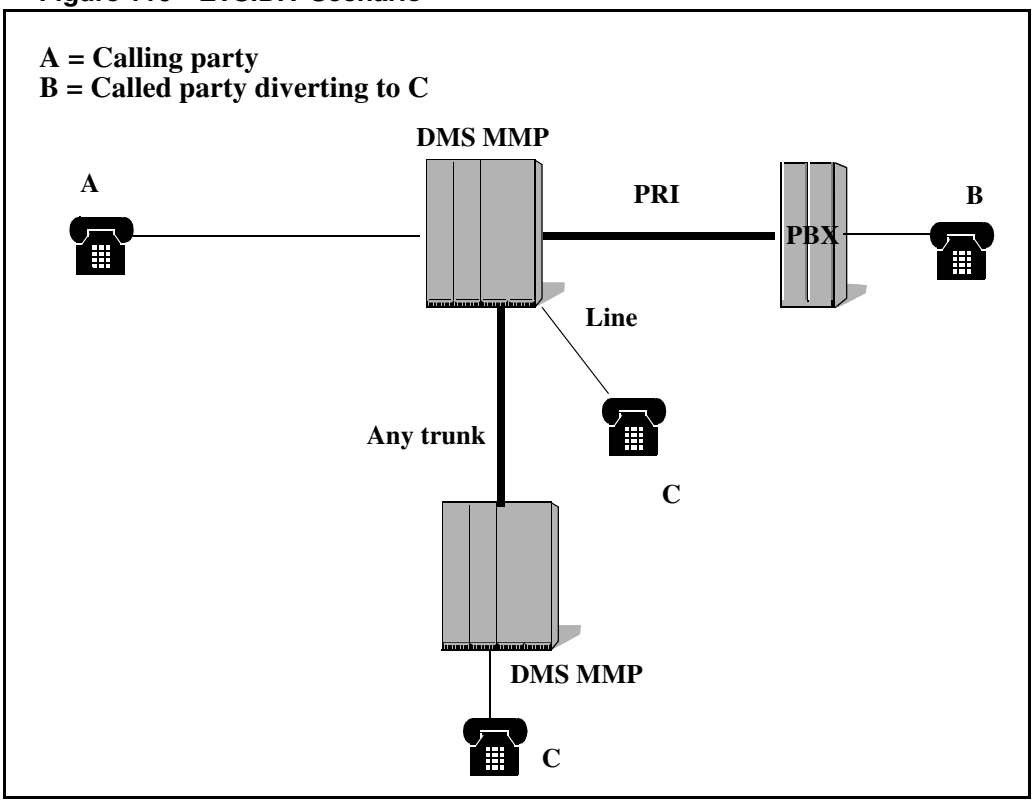
Late Release: First the new diverted call leg is established between the originator (A) and diverted-to user (C), then the call towards the private network (B) is cleared. The connection is maintained between the calling party (A) and the diverting party (B) until it is determined that the diverted-to party (C) is free thus avoiding the scenario where the caller first hears ringing tone then hears busy tone when the call diverts to a busy user.

According to A59007447 (EPRIDIV), Early release only applies to the diversion reasons of CFU, CFB or CD-I (CD-Immediate) and Late release only

applies to the diversion reasons of CFNR, CD-A (CD Alerting) or Unknown in FACILITY message.

ETSIDIV functionality applies to the call forwarding scenario given in Figure 110 :

Figure 110 ETSIDIV Scenario



In the following figures (Figure 111 and Figure 112), the subscriber A can also be POTS line. And the subscriber C can also be POTS line or another subscriber over any supported Russian trunk signallings.

ETSIDIV-Early Release:

The following call steps are reported to CP:

1- A dials B (B is a network subscriber);

2- ETSIDIV request is received and call is rerouted to C (alerting of C).

3- C answers.

4- disconnection

Figure 111 ETSIDIV with early release

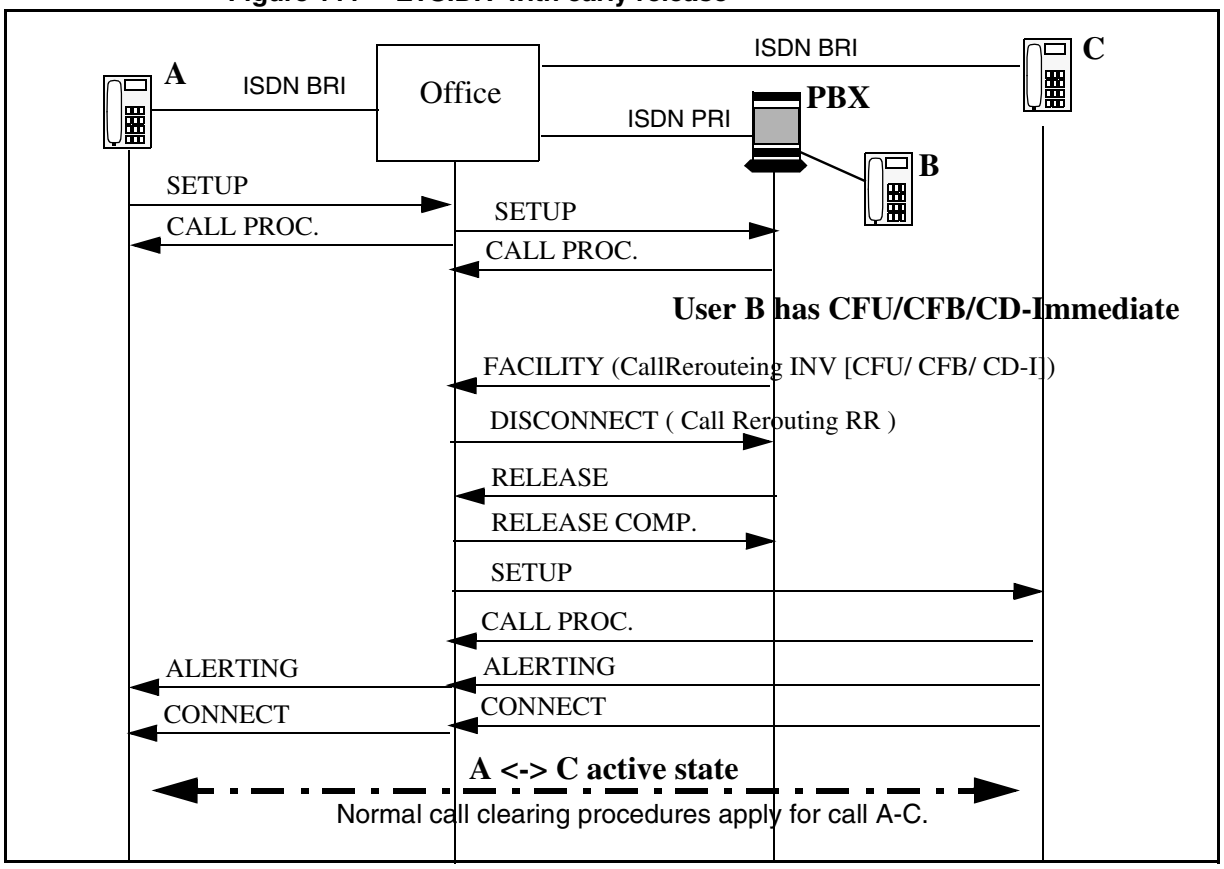


Table 200 A is under surveillance

No of step	1	2	3	4
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C*	C	C
SOSM Call #	1	1	1	1
Attribute of choice	01	40	01	01
Parameters of connection	11	12**	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05

Feature Code	FF	ETSI DIV	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

Table 201 B is under surveillance

No of step	**1**	**2**	**3**	**4**
Messages	1.1	1.4	1.2	1.3
Calling DN	A	B	A	A
Called DN	B	C*	C	C
SOSM Call #	1	1	1	1
Attribute of choice	04	01	40	40
Parameters of connection	11	12**	1C	1C
Code of supp. service phase	00	04	00	00
MCL #	1	1	1	1
Code of operation	00	00	00	05
Feature Code	FF	ETSI DIV	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

Table 202 C is under surveillance

No of step	**1**	**3**	**4**
Messages	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	C	C	C

SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Note: When ETSIDIV Early Release is invoked successfully, if C is target, ETSIDIV information can not be determined. Therefore, in Table 202 ,there is no 1.4 ETSIDIV usage message.

Please note that, in ETSIDIV service notification messages, C is the number (DN) which is received within PRI facility message. If this number is changed during a translation (with DMOD) which is terminating to a line, in 1.2 message, this number is changed with the terminating line DN.

ETSIDIV-Late Release, successful Diversion Attempt:

In this scenario, A-B call is retained until diverted-to user (C) begins to alert.

1- A dials B;

2- B requests ETSIDIV to C;

3- C alerts (call is forwarded);

4- C answers;

5- Call disconnection (A-C)

Figure 112 ETSIDIVP with late release

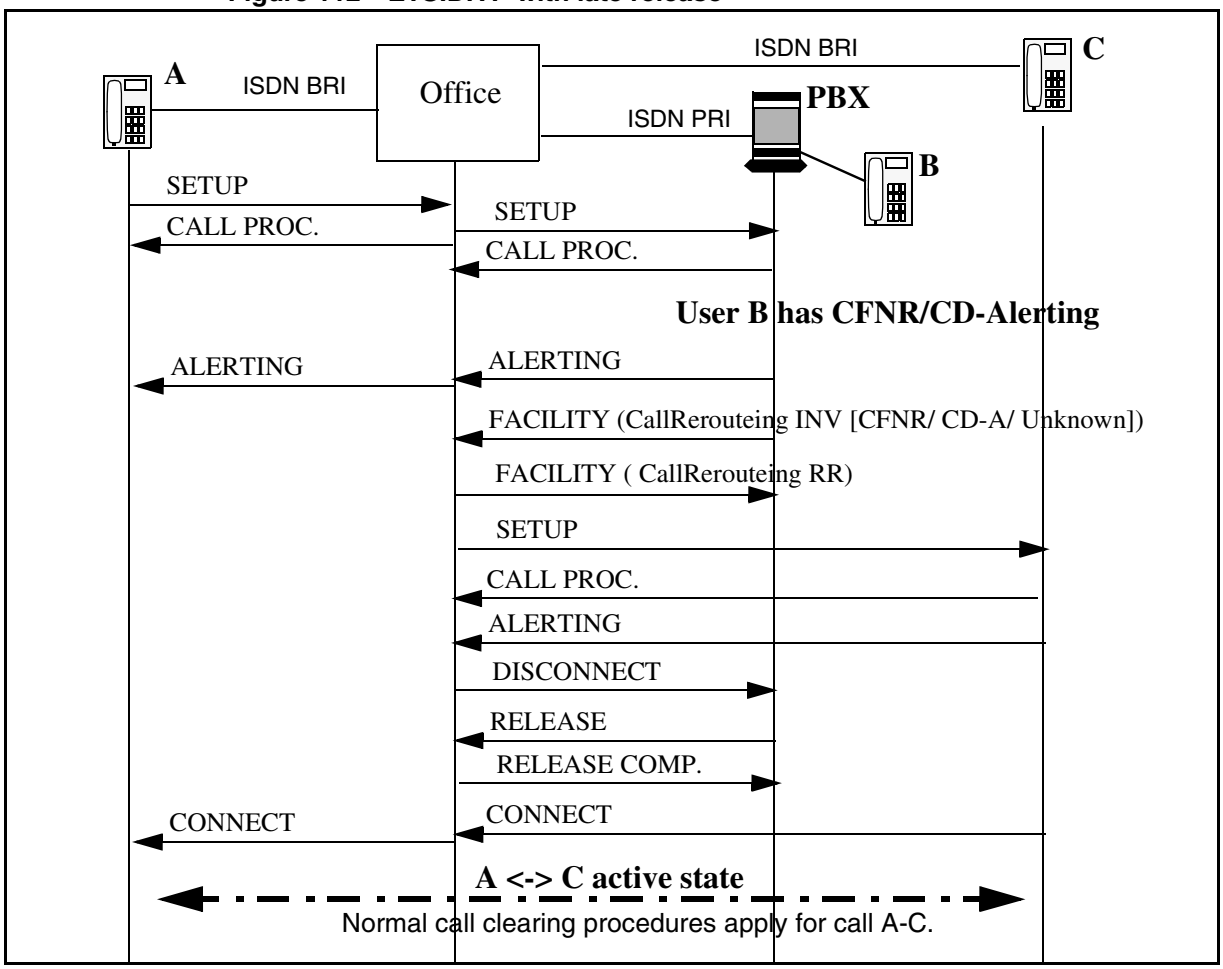


Table 203 A is under surveillance

No of step	1	2	2	3	4	5
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	B	C	C
SOSM Call #	1	**2**	**2**	1	**2**	**2**
Attribute of choice	01	40	01	01	01	01
Parameters of connection	11	12**	1C	11	1C	1C
Code of supp. service phase	00	04	00	00	00	00

MCL #	1	FF	**2**	1	**2**	**2**
Code of operation	00	00	00	**04**	00	05
Feature Code	FF	ETSI DIV	FF	FF	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

Table 204 B is under surveillance

No of step	**1**	**2**	**2**	**3**	**4**	**5**
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	B	C	C
SOSM Call #	1	**2**	**2**	1	**2**	**2**
Attribute of choice	04	01	40	04	40	40
Parameters of connection	11	12**	1C	11	1C	1C
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	1	**2**	**2**
Code of operation	00	00	00	**04**	00	05
Feature Code	FF	ETSI DIV	FF	FF	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

In ETSIDIV message, C is the number received within PRI. If this number is modified during a translation which is terminating to a line, the value of C will be changed with the number of this line in 1.1 message.

Table 205 C is under surveillance

No of step	2	3	4
Messages	1.1	1.2	1.3
Calling DN	A	A	A
Called DN	C	C	C
SOSM Call #	1	1	1
Attribute of choice	04	04	04
Parameters of connection	1C	1C	1C
Code of supp. service phase	00	00	00
MCL #	1	1	1
Code of operation	00	00	05
Feature Code	FF	FF	FF

Note: When ETSIDIV Late Release is invoked successfully, if C is target, ETSIDIV information can not be determined by SOSM. Therefore, in Table 205 , there is no 1.4 ETSIDIV usage message.

ETSIDIV-Late Release, Unsuccessful Diversion Attempt

This scenario is realized when the second leg can not be established successfully due to a problem. This is the case when C is busy. Since second leg is not established, the call is terminated to first leg terminating side. This scenario is only valid for ETSIDIV Late Release. This scenario does not exist for ETSIDIV Early release.

1- A dials B;

2- B requests call diverted to C with ETSIDIV;

3- Call forwarding fails (C is busy);

4- B answers;

5- Call disconnection (A-B).

Table 206 A is under surveillance

No of step	1	2	2	3	4	5
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	C	B	B
SOSM Call #	1	**2**	**2**	**2**	1	1
Attribute of choice	01	40	01	01	01	01
Parameters of connection	11	12**	1C	1C	11	11
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	2	**1**	**1**
Code of operation	00	00	00	**03/ 01**	00	05
Feature Code	FF	ETSI DIV	FF	FF	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

Table 207 B is under surveillance

No of step	1	2	2	3	4	5
Messages	1.1	1.4	1.1	1.3	1.2	1.3
Calling DN	A	B	A	A	A	A
Called DN	B	C*	C	C	B	B
SOSM Call #	1	**2**	**2**	2	**1**	**1**
Attribute of choice	04	01	40	40	04	04
Parameters of connection	11	12**	1C	1C	11	11
Code of supp. service phase	00	04	00	00	00	00
MCL #	1	**FF**	**2**	2	**1**	**1**

Code of operation	00	00	00	**01/ 03**	00	05
Feature Code	FF	ETSI DIV	FF	FF	FF	FF

Note 1: *: C in 1.4 service usage message in Step 2 is the diverted-to digits sent by the served user (B) over PRI agent.

Note 2: ** While sending ETSIDIV message parameter of connection is always set to 12 (even if terminating side is line or trunk agent), since B is a network number which is called over PRI trunks.

Table 208 C is under surveillance

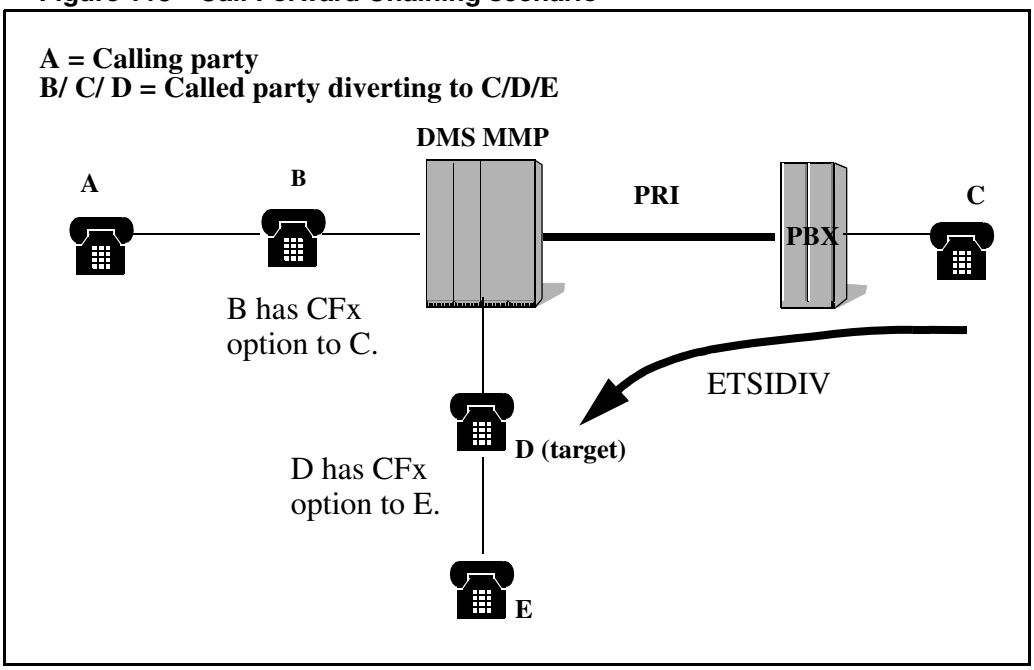
No of step	**3**	**3**
Messages	1.1	1.3
Calling DN	A	A
Called DN	C	C
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	1C	1C
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	01/ 03
Feature Code	FF	FF

Note: When ETSIDIV Late Release is invoked successfully, if C is target, ETSIDIV information can not be determined by SOSM. Therefore, in Table 208 , there is no 1.4 ETSIDIV usage message.

CFx chaining interaction with ETSIDIV and multiple ETSIDIV

An example scenario for call forward chaining interaction is given in Figure 113 in order to describe SOSM behavior in CFx and ETSIDIV interactions.

Figure 113 Call Forward Chaining scenario



While diverting the call due to ETSIDIV Late Release, data related to prior CFx attempts are lost due to ETSIDIV service functionality.

In the given scenario, C diverts the call using ETSIDIV service. In this scenario, SOSM does not send ETSIDIV service usage notification to CP if monitoring starts after ETSIDIV is activated (i.e. when D or E is the monitored subscriber).

Additionally, in this case, B forwards the call to C, however, as described above, B-to-C diversion data is also lost during realization of ETSIDIV Late Release service. Therefore, SOSM does not send any notification to CP about B-to-C diversion when ETSIDIV Late Release service is activated before monitoring starts (i.e. when D or E is the monitored subscriber).

Above conditions occur while monitoring D. The call steps are as follows:

1- A dials B;

2- B forwards the call to C over PRI;

3- C diverts the call to D by using ETSIDIV;

4- D forwards the call to E;

5- E answers;

6- disconnection.

Table 209 D is under surveillance ETSIDIV -call forwarding interaction

No of step	3	3*	4	5	6
Messages	1.1	1.4	1.4	1.2	1.3
Calling DN	A	B	D	A	A
Called DN	D	D	E	E	E
SOSM Call #	1	1	1	1	1
Attribute of choice	04	04	01	40	40
Parameters of connection	1C	1C	1C	1C	1C
Code of supp. service phase	00	04	04	00	00
MCL #	1	1	1	1	1
Code of operation	00	00	00	00	05
Feature Code	FF	CFX	CFX	FF	FF

Note: *This column is reported only if ETSIDIV Early Release is invoked.

ISDN BRI Call Deflection (CD) interaction with ETSIDIV

For detailed information, please refer to section 2.11.2.8.3 CD interaction with ISDN PRI ETSIDIV service.

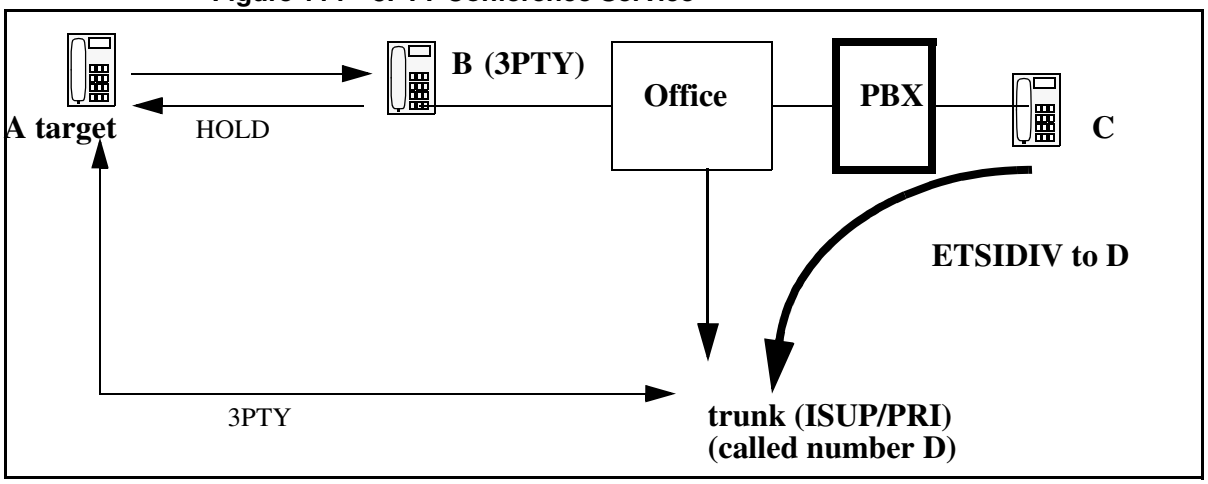
ETSIDIV interaction with multi-party services

When ETSIDIV is activated over a PRI trunk, original diverted-to number can not be determined after diverted-to subscriber alerts.

In multi-party services such as conference calls or call transfer, SOSM informs CP about all subscribers involved in the call, even if they are not monitored subscribers.

Below scenario illustrates an ETSIDIV and 3PTY service interaction. In this scenario, SOSM is expected to notify CP about the conference and the conferees (A, B and D), when B establishes conference between A, B and the trunk agent.

Figure 114 3PTY Conference Service



Due to the existing ETSIDIV service functionality, SOSM is unable to determine original forwarded to digits during activation of three party conference. Therefore, in 3PTY service notification message, C is sent to CP as the called number instead of D.

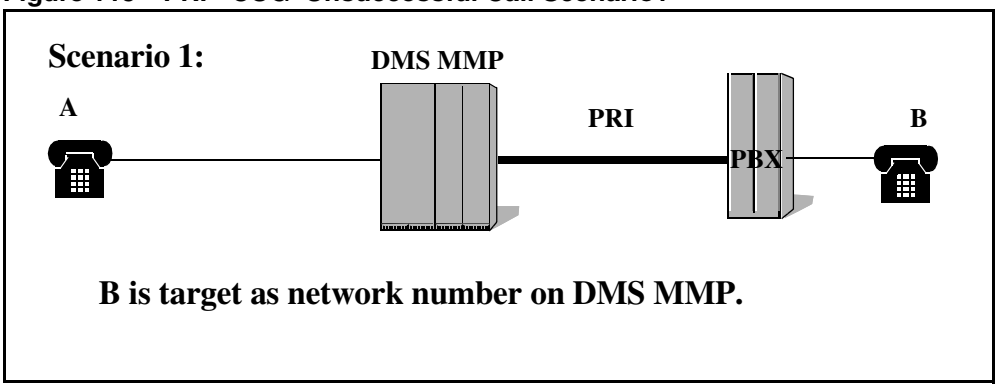
14.11.3.3 CUG - Closed User Group

CUG provides a mechanism for forming groups to and from which access is restricted. A specific user may be member of one or more Closed User Groups. Members of a specific CUG can communicate among each other but not, in general, with users outside of the group. CUG can be provisioned in table ETSIFEAT and LTDATA. These tables should be datafilled to activate this functionality.

CUG service do not have subscriber interactions, the service functionalities are provided by PBX. So the “No.1.4-SS usage” message is not reported for the usages of CUG. Since in SOSM, it is not required to send a special notification for CUG, there will be no special handling for successful call scenarios. So the CUG scenarios will have a similar behavior as normal calls.The operation code can change according to the treatment sent.

Figure 115 is a call failure due to CUG service. Table 210 and Table 211 describe the SOSM message sequence for unsuccessful CUG call scenario.

Figure 115 PRI - CUG Unsuccessful Call Scenario1



In this scenario, the following call steps are reported to CP:

1. A calls subscriber B over PRI trunk; **2-** The call fails due to realization of CUG service.

Table 210 CUG - A(originator) is under surveillance

No of Steps	**1**	**2**
Messages	**1.1**	**1.3**
Calling DN	A	A
Called DN	B	B
SOSM Call #	1	1
Attribute of choice	01	01
Parameters of connection	11	11
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	02/ 03
Feature Code	FF	FF

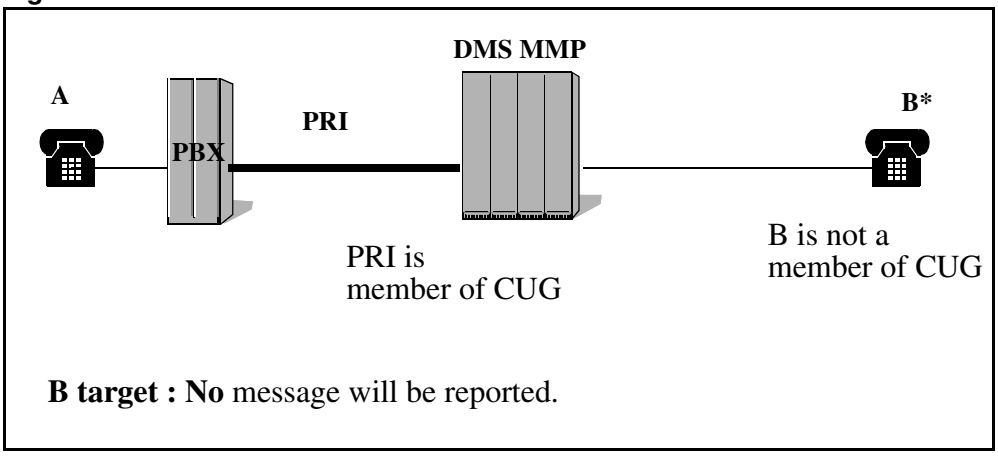
Table 211 CUG - B(terminator) is under surveillance

No of Steps	**1**	**2**
Messages	**1.1**	**1.3**
Calling DN	A	A
Called DN	B	B

No of Steps	1	2
Messages	**1.1**	**1.3**
SOSM Call #	1	1
Attribute of choice	04	04
Parameters of connection	11	11
Code of supp. service phase	00	00
MCL #	1	1
Code of operation	00	02/ 03
Feature Code	FF	FF

However, the unsuccessful call scenario given in Figure 116 -where the originator is a PRI agent, which has CUG option- the call does not terminate to the called subscriber if it is not a member of the closed user group. In such scenarios, if the terminating agent is a monitored line, SOSM does not start monitoring, and does not send any call data messages to the CP.

Figure 116 PRI - CUG Unsuccessful Call Scenario2



14.12 ONP, Restart and Swact Interactions

When a software upgrade is taking place via a One Night Process (ONP), all static SOSM data (data in tables SOSMTRK, SOSMMPC and SOSMPARM) is transferred to the new software load automatically.

However, dynamic SOSM data such as monitoring orders, MCL definitions are cleared, MCL's are disconnected and effective system password is initialized at CM swact (during ONP).

During TABXFR, The commands received are rejected with the reason of "dump restore in progress".

In PRESWACT step of ONP, SOSM is stopped. The commands received are rejected with the reason of **"dump restore in progress"** until SWACT is completed. When SWACT is completed, CP is notified via Exchange Restart message.

Upon any system restart (Warm, Cold or Reload) SOSM data is cleared and the CP is notified via Exchange Restart message. Since active calls survive warm restarts, any active call under surveillance will have its MCLs disconnected.

14.13 Restrictions/Limitations

14.13.1 Ring tone

During ringing, mechanical voice is listened from MCL connected to the called DN due to the relay switching because there will be physical connection between MCL and the ring relay in line card of called dn.

14.13.2 Conference circuits usage

The conference ports added to the exchange for SOSM are not pre-allocated to the SOSM system. If all ports are used by normal 3-way or 6-way calls, SOSM will be unable to allocate a conference bridge, and a monitored call will become statistically monitored. Upon conference bridge shortage, CP is informed by an clearing of MCL message (Msg.2.2) after reception of called party number (Msg.1.1).

Similarly, if all conference circuits are used by SOSM, local subscribers will be unable to use 3-way call features.

14.13.3 The restriction of Analog Line cards

By design, analog line cards contain a bridge which causes an echo on the backward speech path. If a party in a monitored call is off an analog line card, the party's MCL will contains a combination of his transmit and receive signals.The transmit signal predominates the other by approximately 20db.

14.13.4 Monitoring of network subscribers

SOSM triggers monitoring for **"telephone network subscriber with complete telephone number"** and **"telephone network subscriber with incomplete telephone number"** type of objects only in line-to-trunk calls where the specified number within the object is dialled.

In overlap outpulsed calls, SOSM starts monitoring the calls for complete network numbers as the received digits matches a DN within the corresponding monitoring order. SOSM does not make any further checks to verify whether the total number of the dialled digits are equal to the number of the digits in monitoring order.

14.13.5 Incoming group of connecting lines

The Incoming group concept is not supported in DMS MMP. DMS MMP always expects to receive FFFFH value for this field, otherwise the message will be rejected.

Additionally, DMS MMP sets this field to FFFFH in all call information messages from SOSM to CP, where ANI is available. Otherwise, incoming trunk number is sent within "Conditional number of incoming group".

14.13.6 SOSM under traffic

Under heavy SOSM traffic, it is possible that the conference circuits may fail. This is a limitation of the 3X67 conference circuit card on the MTM or CTM shelf. In those rare cases, failure message will be sent to the CP reporting Conference Circuit Failure, and the MCL using that conference port card will be released with message 52 (MCL cleared) reported to CP.

In addition, NET102 logs (not SOSM specific) will be generated in the office, reporting the card problem (Integrity Failure).

14.13.7 Image Dump and Restore

During the process of an Image Dump or Restore (when the DMS saves its active image to disk, or restores it from disk) the SOSM system operates in a LIMITED fashion. All Control Point commands are rejected:

- During DS dumping phase of load image,
- During TABXFR phase of ONP,
- After Preswact is started.

If any commands are received during a dump/restore, the command is rejected with negative reception confirmation code **"dump restore in progress"** with value **59H**.

14.13.8 IN Interaction

IN interaction is not supported.

14.13.9 Interaction with digit collection methods

DMS MMP has a flexible digit collection mechanism which means that user dialled digits can be reported to CM as provisioned in digit collection tables. In partial dialling cases, only collected digits that are reported from monitored

line's XPM are sent to the control point within call clearing message (Msg.1.3).

14.13.10 Failures in ISUP-Line call scenarios

SOSM does not monitor the unsuccessful calls when the call setup fails due incoming trunk (i.e. COT failures, ANI failure,...etc).

14.13.11 PM Swact (warm) interactions

If warm swact is applied on the PLGC/GPP of a monitored line in call setup phase, DMS MMP takes down the call. If the subscriber remains off-hook until completion of warm swact, the peripheral prepares the line for a new call origination.

If subscriber on-hooks after PLGC/GPP recovery is over, SOSM sends a call clearing message (Msg.1.3) to the control point with "partial dialling - 02H" operation code for the completion of the new origination.

If the subscriber is a V5.2 agent, GPP sends an additional origination message for this agent during recovery phase (please refer to GPPPRODS document in FMDOC library for detailed information about GPP recovery after warm swact), therefore SOSM reports an extra call clearing message (Msg.1.3) to the control point with "partial dialling - 02H" operation code.

14.13.12 Monitoring of SUSpended agents

SUSpended agents are not monitored by SOSM, although they exist in monitoring order database.

14.13.13 SOSM starting after restarts

After restarts, the recovering of X25 hardware does not complete, right away. So, SOSM cannot be started until X25 hardware is ready to work after restarts.

14.13.14 Call Release over PRI

The call disconnections over PRI are handled such as ISUP trunks when the same disconnection causes are received over PRI. In the case of no disconnection cause received over PRI (from PBX); since the call and PRI trunk are released when the originating party on-hooks, it is decided that the monitoring continues until the originating party on-hooks. Since the real reason of disconnection (busy etc.) is not known by DMS, the disconnection reason in No.1.3 message is set to "disconnection because of no answer" for the unanswered call scenarios.

14.13.15 Supported Line Agents

As present exchange subscribers, IBN, V5.2(IBN) and ETSI BRI lines are supported by SOSM (See “2.2 Feature Synopsis” on page 49 and “14.5.4

Agent Interactions" on page 268). Please note that EBS and V5.2(BRI) lines are not supported by SOSM software.

14.14 Service Codes mapping

14.14.1 Subscriber services codes

These codes are reported to the CP in responses to Monitored object information request and anywhere else where a Service code appears in a message.

A set of codes was supplied by ZNIIS and is used wherever possible. For services which are not covered in that list, the DMS service code is used.

The following table provides the complete list of services available in the Russia market, and their LONIIS code equivalent.

For services where mapping is possible between DMS codes and LONIIS codes, the LONIIS code is used (in field "Service Code"). For those services with no equivalent code in the LONIIS specification, the DMS code is used and placed in the "Service Code".

Note that some services defined by LONIIS do not exist on the DMS MMP in the Russia market. Other services may have two flavors in DMS MMP, but map to a single LONIIS code.

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
SCL,SCS,SCU	10H	Abbreviated Dialing
APS	74H	Attendant Pay Station
ACD	3BH	Automatic Call Distribution
ACRJ	18H	Anonymous Caller Rejection
AR	19H	Automatic Recall
BNN	25H	Bridged Night Number
CDA	4EH	Call Deflection Alerting
CDI	4FH	Call Deflection Immediate
CPC (RSRVD)	71H	CIS Subscriber Category 0
CPC (UNKNOWN)	53H	CIS Subscriber Category 1
CPC (ORD)	72H	CIS Subscriber Category 1
CPC (MAINT)	54H	CIS Subscriber Category 1

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
CPC (OPER)	55H	CIS Subscriber Category 1
CPC (VIS)	56H	CIS Subscriber Category 1
CPC (CNDB)	57H	CIS Subscriber Category 1
CPC (AU_ORD)	58H	CIS Subscriber Category 1
CPC (AU_PRIO)	59H	CIS Subscriber Category 1
CPC (HOTEL)	73H	CIS Subscriber Category 2
CPC (LOCAL)	2CH	CIS Subscriber Category 3
CPC (PRIOR)	2DH	CIS Subscriber Category 4
CPC (FOC)	2EH	CIS Subscriber Category 5
CPC (SPM)	2FH	CIS Subscriber Category 6
CPC (ITDN)	30H	CIS Subscriber Category 7
CPC (TRAN)	76H	CIS Subscriber Category 8
CPC (METER)	34H	CIS Subscriber Category 9
CPU / CP	32H	Call Pick Up
CBIL	35H	Centralized Billing
CCW	3AH	Cancel Call Waiting
CFWANN/CFU	21H	Call Forward With Announcement
CFU/CFU	21H	Call Forward Unconditional
CFF/CFU	21H	Call Forward Fixed
CFI/CFU	21H	Call Forward Intragroup
CHD	42H	Call Hold
CFB / CFB	29H	Call Diversion on Busy
CFD/CFNRY	2AH	Call Diversion on No Answer
CEPT	15H	CEPT
CEPTPW	16H	CEPT Password
CDTA/ All CF	20H	Call Diversion to Announcement
CDTO/All CF	20H	Call Diversion to Operator
CDS / CFU	21H	Call Diversion to Subscriber
- / CFNRC	2BH	Call diversion on mobil unreachable

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
- / CONDF	28H	All conditional forwarding
CIR / CUG	61H	Circular Hunt
CWT, ICWT / CWT	41H	Call Waiting
CW	62H	ISDN BRI Call Waiting
CUG	1CH	Closed User Group
Flash / HOLD	42H	Hold for Enquiry
HOLE	40H	Hold End
RAG / CCBS	43H	Ring Again
CCBS / CCBS	43H	Completion of Calls to Busy Subscriber
MPTY	51H	All Multi-Party Services
6WC, I6WC / CONF	50H	Six Way Calling
ECONF	63H	ISDN BRI Addon Conference
3WC, I 3WC/ TPTY	52H	Three Way Calling
3PTY	64H	ISDN BRI 3 Party Conference
CNAMD / CLIP	11H	Calling Name Display
CND/CLIP	11H	Calling Name Display
CLIP / CLIP	11H	Calling Line Identification Presentation
CNAB / CLIR	12H	Calling Name Display Blocking
CNDB/CLIR	12H	Calling Name Display Blocking
CLIR / CLIR	12H	Calling Line Identification Restriction
CNDBO	1EH	Calling Name Display Blocking Override
COIN	3EH	
COLP / COLP	13H	Connected Line Identification
COLR / COLR	14H	Connect Line ID. Blocking
DLH / CUG	61H	Distributed Line Hunting
DNH / CUG	61H	Directory Number Hunting
MLH / CUG	61H	Multi-Line Hunting
CFRA	80H	Call Forward Remote Access
CEPTRA	81H	CEPT Remote Access

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
ILR / OCB	91H	International Line Restrictions (ALL)
OCB / OCB	91H	Outgoing Call Barring
DOR/ BAOC	92H	Denied Origination
CDND / BIC	99H	International Do Not Disturb
DTM / BAIC	9AH	Denied Termination
- / BICRoam	9BH	Barring INcoming when PLMN, Country
ICT, ECT, CXR/ CXR	31H	International Call Transfer
TBI / -	98H	Toll Break In
DCF	38H	Denied Call Forwarding
DTBI	A9H	Denied Toll Break-In
ELN	B0H	Essential Line
EMW	D0H	Executive Message Waiting (Voice Mail)
ENQ	33H	Enquiry Calling
ESG	B3H	Emergency Service Groups
FDN	BAH	Features Denied
FNO	BEH	Free Number Origination
FNT	BFH	Free Number Terminating
GIC	3CH	Group Intercom
HOT	CFH	Hotel or Motel
ICR	D1H	International Call Recording
HTL, AUL / AUL	D7H	Hot Line/Automatic Line
LNR	D9H	International Last Number Re-dial
INDC	DDH	International No Double Connect
NDC	DDH	No Double Connect
WML	E4H	Warm Line
LOR	F0H	Line Overflow to Route
LDA	1AH	Long Distance Aler
LROA	F2H	Line Reversal on Answer
LRS	F4H	Line Reversal on Seizure

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
CLF	FCH	Malicious Call Trace
MCID	FCH	Malicious Call Identification
MCT2	FDH	Malicious Call Trace 2
MWT	D0H	Message Waiting (Voice Mail)
OFR	C1H	Overflow Hardware Register
OFS	C2H	Overflow Software Register
ONI	C3H	Operator Number Identification
PILOT	C4H	Pilot of a Hunt Group
PLP	C5H	Plug Up
PMC	C6H	Printed Meter Check
PR1	C7H	Priority 1 Subscriber
PR2	C8H	Priority 2 Subscriber
PRR_CFU, PRR_CFB, PRR_CDI	5AH	Partial ReRouting (ETSIDIV) Call Forward Unconditional, Call Forward Busy, Call Deflection Immediate
PRR_CFNR, PRR_CDA, PRR_Unknown	5BH	Partial ReRouting (ETSIDIV) Call Forward No Reply, Call Deflection Alerting
RCVD	CAH	Type of Terminating Billing
RESL	36H	Restricted Line
REV	27H	Reverse Charging
SCR	CBH	Selective Call Recording
SMDR	37H	
SPM	CCH	Subscriber Premise Meter
SUS	CDH	Suspended Service
SUPPRESS/CLIR	12H	Suppress
TFO	CEH	Terminating Fault Option
TP Suspend	4CH	Terminal Portability (Suspend call)
TP Resumed	4DH	Terminal Portability (Resumed call)
UCD	39H	Uniform Call Distribution

Table 212 Subscriber Services Codes

Feature Name DMS / LONIIS	Service Code	Description
UUS1	26H	User to User Service 1
VM	D0H	Voice Mail
IWUC / WUCR	D4H	Wake-Up Call
WUCR / WUCR	D4H	Wake-Up Call Request

14.14.2 Negative confirmation of command reception codes

The following table describes the expanded error codes for "confirmation of command reception" messages. For a detailed explanation of what causes each code to be sent, please refer to the relevant command in section "2.5.7 CP to SOSM Command Processing" on page 66.

Table 213 Command reception result codes

Code name	Value
command accepted	00H
incorrect preamble	01H
incorrect sosm number	02H
invalid message code	03H
message too long	04H
incorrect message length	05H
unsupported command	06H
invalid type and sign	07H
invalid MCL group number	08H
invalid MCL group type	09H
invalid MCL number	0AH
invalid object type	0BH
invalid sign of telephone number	0CH
incorrect sign of telephone number	0DH
invalid category of monitoring	0FH
invalid priority code	10H
invalid digit	11H
invalid number of digits	12H

Table 213 Command reception result codes

Code name	Value
number of digits mismatch	13H
invalid MCL B for group	14H
invalid password character	15H
unsupported parameter	16H
invalid group for category	17H
password mismatch	18H
command out of sequence	19H
invalid_conditional_number	1AH
dump restore in progress	1BH
command rejected	FFH

14.14.3 Negative confirmation of command execution

The following table describes the expanded error codes for "confirmation of command execution" messages. For a detailed explanation of what causes each code to be sent, please refer to the relevant command in section "2.5.7 CP to SOSM Command Processing" on page 66.

Table 214 Command execution result codes

Code name	Value
command executed	00H
duplicate MCL group	40H
MCL in use	41H
duplicate conditional number of object	42H
invalid parameter	43H
non-unique object	44H
object not found	45H
invalid call number	46H
invalid object number	47H
invalid object type	48H
invalid MCL group	49H
invalid MCL number	4AH

Table 214 Command execution result codes

Code name	Value
MCL information not found	4BH
command out of sequence	4CH
invalid number of digits	4DH
call already monitored	4EH
max num of objects exceeded	4FH
missing PCM-30 group data	50H
duplicate MCL number	51H
wrong MCL type for group	52H
sosm missing trkmem datafill	53H
object type mismatch	54H
digits mismatch	55H
sign of dn mismatch	56H
no services found	57H
invalid dn for exchange	58H
command not allowed during dump	59H
unsupported agent type	5AH
invalid MCL B for group	5BH
priority code mismatch	5CH
type and sign mismatch	5DH
unsupported parameter	5EH
invalid sign of telephone number	5FH
no data exists in database	60H
invalid MCL group type	61H
max num MCL exceeded	62H
object transfer in progress	63H
mcl transfer in progress	64H
invalid digit failure	65H
technical_problem	66H
sosm command failed	FFH

14.14.4 Expanded codes for MCL connection problem reporting

The following table describes the expanded error codes for “mcl unconnection code” in call related messages.

Table 215 MCL unconnection result codes

Code name	Value
Normal connection	0H
no free mcl	01H
mcl not idle (not ready)	1CH
mcl releasing failed	1DH
missing PCM-30 group data	1EH
no free conf. circuit	1FH
conf. circuit connection failed	20H
sosm hardware out of service	22H
invalid agent for connection	23H
Other failure (unknown)	FEH
for statistical monitoring	FFH

14.15 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema __X__
- User Interface __X__
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

14.16 References

[1] NTP 297-8991-500, Maintanence and Operations Manual.

[2] NTP 297-1001-592, DMS-100 Family Peripheral Modules Maintenance Guide.

[3] A00001919 - CEPT SERVICES PASSWORD ENHANCEMENT

[4] A59019083 - CEPT Call Diversion and CEPT Do Not Disturb

[5] A59034125 - ISDN BRI CEPT Call Forwarding

[6] A59028702 - Support of CFx (Call Forward Variants) for Multiple DNs on ETSI BRI

[7] A59027705 - ETSI ISDN BRI Outgoing Call Barring - Fixed (OCB - F)

[8] 590326661 - Outgoing Call Barring - User Defined (OCB - UD)

[9] 59027828 - BRI Hot and Warm Line

Glossary

Term	Description
SOSM	System of Operative-Searching Measures
DMS	Digital Multiplexing System
MMP	Multi Market Product
CP	Control Point
CFB	Call Forward Busy
CFD	Call forward Do Not Answer
CFU	Call Forward Unconditional
ICWT	International Call Waiting
I3WC	International Three Way Calling
I6WC	International Six Way Calling
NBD	Network Broadcast Delivery
MPC	Multi Protocol Controller
AMA	Automatic Message Accounting
PCM	Pulse Code Modulation

Term	Description
MCL	Monitoring Connecting Line
MTM	Maintenance Trunk Module
PDTC	Peripheral Digital Trunk Controller
LCC	Line Class Code
ONP	One Night Process
DTC	Data Transmission Channel
BRI	Basic Rate Interface
MSN	Multiple Subscriber Nuumber
AFC	Additional Functional Call
WUCR	Wake Up Call Request
OCB	Outgoing Call Barring
WML	Warm Line
AUL	Automatic Line
CW	Call Waiting
ETSI	European Telecommunications Standards Institute
ISDN	Integrated Services Digital Network
CFK	Call Forward Per Key
CD	Call Deflection
TP	Terminal Protability
MCID	Malicious Call Trace
CLIR	Calling Line Identification Restriction
COLR	Connected Line Identification Restriction
CUG	Closed User Group
UUS	User To User Signalling
CCBS	Completition of Calls to Busy Subscriber
CCNR	Completition of Calls on No Reply
ECT	Explicit Call Transfer
3PTY	Three Party
ECONF	ETSI BRI Addon Conference

Term	Description
ETSIDIV	ETSI PRI Diversion
PRR	Partial Re-Routing

14.17 APPENDIX

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
1		1.1	Exchange start, SW restart	No2
2	No1 SOSM start	2.1	No3 (before SOSM start)	No7-NOK
		2.2	No1 with wrong password	No7-NOK, No6
		2.3	No1 with right password	No7-OK, No8-OK
		2.4	No1 (repeatedly)	No7-OK, No8-NOK or **No7-NOK**
3	No3 Password setting	3.1	No3 with wrong password	No7-NOK, No6
		3.2	No3 with wrong SOSM No	No7-NOK
		3.3	No3 with right password	No7-OK, No8-OK
		3.4	No4 with factory password	NO7-NOK, No6

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
4	No4 Assignment of MCL to group	4.1	No4, Nogr=1, gr.type-01H (combined) NoMCLA=NoMCLB	No7-OK, No8-OK
		4.2	No4, Nogr=1, gr.type-01H (combined) NoMCLB=FF	No7-OK, No8-OK
		4.3	No4, Nogr=1, gr.type-01H (combined) NoMCLA in unadjacent time interval. That is if in test 4.2, MCLA=3 then in test 4.3, MCLA ^= 4	No7-OK, No8-OK
		4.4	No4,Nogr=1,gr.type-01H(combined) NoMCLA ≠ NoMCLB	No7-OK,No8-NOK or **No7-NOK**
		4.5	No4, Nogr=1, gr.type-01H (combined) NoMCLA is distributed. That is it has been already assigned to the group.	No7-OK, No8-NOK
		4.6	No4, Nogr=1, gr.type-01H (combined) NoMCLA from inexisting PCM primary group.	**No7-OK,No8-NOK** or No7-NOK
		4.7	No4,Nogr=2,gr.type-11H(separate) NoMCLA ≠ NoMCLB (in adjacent time interval. That is if for example MCLA is 5 then MCLB is 6)	No7-OK, No8-OK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		4.8	No4,Nogr=2,gr.type-11H (separate) NoMCLA ≠ NoMCLB (in unadjacent time interval. That is if for example MCLA is 5 then MCLB is value other than 6)	No7-OK, No8-OK
		4.9	No4, Nogr=2, gr.type-11H (separate) NoMCLA ≠ NoMCLB (different PCM primary groups)	**No7-OK,No8-NOK** or No7-NOK
		4.10	No11, all parameters=FF	No7-OK, No4, No8-OK
		4.11	No4, Nogr=1, gr.type-11H (separate) NoMCLA, NoMCLB	No7-OK, No8-NOK
		4.12	No4, Nogr=2, gr.type-01H (combined) NoMCLA =NoMCLB	No7-OK, No8-NOK
		4.13	No4, Nogr=2, gr.type-11H (separate) NoMCLA is distributed. (That is it has been already assigned to the group)	No7-OK, No8-NOK
		4.14	No4, Nogr=2, gr.type-11H (separate) NoMCLB is distributed. (That is it has been already assigned to the group	No7-OK, No8-NOK
		4.15	No4, Nogr=2, gr.type-11H (separate) NoMCLA=NoMCLB	No7-OK, No8-NOK or **No7-NOK**
		4.16	No4, Nogr=254(inexisting), gr.type- 01H (combined) NoMCLA=NoMCLB	No7-OK, No8-NOK or **No7-NOK**
		4.17	No4, Nogr=3, gr.type-inexisting NoMCLA=NoMCLB	No7-OK, No8-NOK or **No7-NOK**
		4.18	No4, Nogr=3, gr.type-01 NoMCLA - inexisting	**No7-OK, No8-NOK** or No7-NOK
5	No9 Exclusion of MCL from group	5.1	No9, Nogr=1, NoMCLA=NoMCLB	No7-OK, No8-OK
		5.2	No9, Nogr=1, NoMCLB=FF	No7-OK, No8-OK
		5.3	No9, Nogr=2, NoMCLA, NoMCLB	No7-OK, No8-OK
		5.4	No11, all parameters=FFH	No7-OK, No4, No8-OK
		5.5	No9,Nogr=1, NoMCLA ≠ NoMCLB and NoMCLB ≠ FFH	No7-OK, No8-NOK or **No7-NOK**
		5.6	No9, Nogr=1, NoMCLA not defined in TR for links	**No7-OK, No8-NOK** or No7-NOK
		5.7	No9, Nogr=1, NoMCLA is not assigned to a group	No7-OK, No8-NOK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		5.8	No9, Nogr=1, NoMCLA is from another group.	No7-OK, No8-NOK
		5.9	No9, Nogr=1, MCLA is engaged with conversation	No7-OK, No8-NOK
		5.10	No9, Nogr=2, NoMCLA=NoMCLB	No7-OK, No8-NOK
		5.11	No9, Nogr=2 NoMCLA not defined in TR for links.	**No7-OK, No8-NOK** or No7-NOK
		5.12	No9, Nogr=2, NoMCLB not defined in TR for links.	**No7-OK, No8-NOK** or No7-NOK
		5.13	No9, Nogr=2, NoMCLA is not assigned to a group	No7-OK, No8-NOK
		5.14	No9, Nogr=2, NoMCLB is not assigned to a group.	No7-OK, No8-NOK
		5.15	No9, Nogr=2, MCLA and MCLB are engaged with conversation	No7-OK, No8-NOK
		5.16	No9, Nogr is not defined, MCLA and MCLB are really distributed. (It means that MCLA and MCLB are assigned to a certain group in practice, but in this test case, number of a non-existent group is indicated.)	**No7-OK, No8-NOK** or No7-NOK
		5.17	No4, Nogr=3, gr.type=01 NoMCLA=5 from primary group 0, No4, Nogr=3, gr.type=01 NoMCLA=5 from primary group 1 No9, Nogr=3, NoMCLA=5 from primary group 1, No11, all parameters=FFH	No7-OK, No8-OK No7-OK, No8-OK No7-OK, No8-OK No7-OK, No4,No8-OK observation of MCLA=5 in the primary group 0

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
6	No5 Taking a subject under observation	6.1	No5, subject type-01H	No7-OK, No8-OK
		6.2	No5, subject type-02H	No7-OK, No8-OK
		6.3	No5, subject type-12H, FH in the end of phone No	No7-OK, No8-OK
		6.4	No5, subject type-03H (not for toll exchange)	No7-OK, No8-NOK
		6.5	No5, subject type-03H (for toll exchange)	No7-OK, No8-OK
		6.6	No5, conditional No is busy, subject type-01H	No7-OK, No8-NOK
		6.7	No5, conditional No is busy, subject type-02H	No7-OK, No8-NOK
		6.8	No5, phone No is already under observation	No7-OK, No8-NOK
		6.9	No5, phone No (complete) is already under observation in the list for incomplete number	No7-OK, No8-NOK
		6.10	No5, phone No (incomplete) is already under observation in the list for complete number	No7-OK, No8-NOK
		6.11	No5, phone No and incoming group conditional number are set.	No7-OK, No8-NOK
		6.12	No5, Nogr. does not comply with observation category.	No7-OK, No8-NOK
		6.13	No5, inexisting Nogr. (inexisting MCL group)	No7-OK, No8-NOK
		6.14	No5, amount of digits in phone No does not comply with the mentioned in byte 5	No7-OK, No8-NOK
		6.15	No5, subject type does not comply with phone No.	No7-OK, No8-NOK
		6.16	No5, number attribute does not comply with phone No.	No7-OK, No8-NOK
		6.17	No5, subject type not defined TR for links.	No7-OK, No8-NOK or **No7-NOK**
		6.18	No5, phone No attribute not defined in TR for links.	No7-OK, No8-NOK or **No7-NOK**
		6.19	No5, observation category not defined in TR for links	No7-OK, No8-NOK or **No7-NOK**

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		6.20	No5, group No not defined in TR for links	No7-OK, No8-NOK or **No7-NOK**
		6.21	No5, priority mark not defined in TR for links	No7-OK, No8-NOK or **No7-NOK**
		6.22	No5, during conversation of subscriber with statistical observation category	No7-OK, No8-OK observation since the next call (That is monitoring will begin with the first next call)
		6.23	No5, during conversation of subscriber with full observation category	No7-OK, No8-OK observation since the next call (That is monitoring will begin with the first next call)

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
7	No6 Cancellation of observation	7.1	No6, subject type-01H	No7-OK, No8-OK
		7.2	No6, subject type-02H	No7-OK, No8-OK
		7.3	No6, subject type-12H	No7-OK, No8-OK
		7.4	No6, subject type-03H (for toll exchange)	No7-OK, No8-OK
		7.5	No6 during conversation of subject who is under statistical observation	No7-OK, No8-OK
		7.6	No6 during conversation of subject who is under full observation	No7-OK, No8-OK No2.2 (Channel 2)
		7.7	No6, condition No and phone No not inserted into SOSM data base (That is we have correct conditional No and a non-existing phone No)	No7-OK, No8-NOK
		7.8	No6, phone No and conditional number not inserted into SOSM data base (That is we have correct phone No and a non-existing conditional No)	No7-OK, No8-NOK
		7.9	No6, conditional No of CL (incoming) group not inserted into SOSM data base	No7-OK, No8-NOK (**for toll only, local exchanges will always receive FFFFH**)
		7.10	No6, phone No does not comply with conditional No (both parameters are inserted into data base)	No7-OK, No8-NOK
		7.11	No6, subject type not defined in TR for links.	No7-OK, No8-NOK or **No7-NOK**
		7.12	No6, number attribute does not comply with phone No	No7-OK, No8-NOK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		7.13	No6,subject type does not comply with phone No	No7-OK, No8-NOK
		7.14	No6, amount of digits in phone does not comply with the mentioned in byte 5	No7-OK, No8-NOK
		7.15	No6, phone No and No of CL group are set	No7-OK, No8-NOK or **No7-NOK**
		7.16	No6, cancellation of observation from network subscriber by full number (taking under observation was provided by not full number)	No7-OK, No8-NOK
		7.17	No6, cancellation of observation from network subscriber by not full number (taking under observation was provided by full number)	No7-OK, No8-NOK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
8	No7 Connection to speech path	8.1	No7 during conversation of subject with observation category - statistical, Nogr.=1 (combined observation)	No7-OK, No8-OK No2.1 (channel 2)
		8.2	No7 during conversation of subject with observation category - statistical, Nogr.=2 (separate observation)	No7-OK, No8-OK No2.1 (channel 2)
		8.3	during conversation of subject with observation category - full the MCL was not separated due to absence of free ones; No7 after MCL release.	No7-OK, No8-OK No2.1 (channel 2)
		8.4	during conversation of subject with observation category - full the MCL was not separated due to absence of free ones; No7 when MCL are seized. *(That is Command 7 is executed while all MCLs are busy, and due to the higher priority of Command No7, MCLs used by another conversation are released and assigned to the corresponding call)*	No7-OK, No8-OK No2.1 (channel 2) No2.2(channel 2) MCL release by priority
		8.5	No7 during conversation of subject with observation category - statistical, inexisting Nogr.	No7-OK, No8-NOK
		8.6	No7 during conversation of subject with observation category - full combined, Nogr.=1 (after command No8)	No7-OK, No8-OK No2.1 (channel 2)
		8.7	No7 during conversation of subject with observation category - full combined, Nogr.=2 (after command No8)	No7-OK, No8-OK No2.1 (channel 2)
		8.8	No7 during conversation of subject with observation category - full combined and inexisting Nogr. Not coinciding with the mentioned in command No5 (after command No8)	No7-OK, No8-OK No2.1 (channel 2)

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		8.9	No7 during conversation of subject with observation category - full separate, Nogr.=1 (after command No8)	No7-OK, No8-OK No2.1 (channel 2)
		8.10	No7 during conversation of subject with observation category - full separate, Nogr.=2 (after command No8)	No7-OK, No8-OK No2.1 (channel 2)
		8.11	No7 during conversation of subject with observation category - full separate, inexisting Nogr (after command No8)	No7-OK, No8-OK No2.1 (channel 2)
		8.12	No7 during conversation of subject with observation category - full (combined or separate) with separate MCL *(already assigned MCL)*	No7-OK, No8-NOK
		8.13	No7 during conversation of subject with observation category - statistical subject type 03H, Nogr.=1 (combined observation)	No7-OK, No8-OK No2.1 (channel 2)
		8.14	No7 during conversation of subject with observation category - statistical subject type 03H, Nogr.=2 (separate observation)	No7-OK, No8-OK No2.1 (channel 2)

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
9	No8 Release of monitoring	9.1	No8 according to call identifier during conversation of subject with observation category - statistical, (after command No7)	No7-OK, No8-OK No2.2 (channel 2)
		9.2	No8 according to No MCL during conversation of subject with observation category - statistical, (after command No7)	No7-OK, No8-OK No2.2 (channel 2)
		9.3	No8 according to inexisting NoMCL during conversation of subject with observation category - statistical, (after command No7)	No7-OK, No8-NOK
		9.4	No8 according to call identifier during conversation of subject with observation category - statistical	No7-OK, No8-NOK
		9.5	No8 according to call identifier during conversation of subject with observation category - full combined	No7-OK, No8-OK No2.2 (channel 2)
		9.6	No8 according to No MCL during conversation of subject with observation category - full combined	No7-OK, No8-OK No2.2 (channel 2)
		9.7	No8 according to call identifier during conversation of subject with observation category - full combined and not assigned No MCL.	No7-OK, No8-OK No2.2 (channel 2)
		9.8	No8 according to not assigned No MCL during conversation of subject with observation category - full combined	No7-OK, No8-NOK
		9.9	No8 when MCL is not separated during conversation of subject (due to seizure) with observation category - full combined.	No7-OK, No8-NOK
		9.10	No8 according to call identifier during conversation of subject with observation category - full separate	No7-OK, No8-OK No2.2 (channel 2)
		9.11	No8 according to NoMCLA and NoMCLB during conversation of subject with observation category - full separate	No7-OK, No8-OK No2.2 (channel 2)
		9.12	No8 according to call identifier during conversation of subject with observation category - full separate and not assigned NoMCLA and NoMCLB	No7-OK, No8-OK No2.2 (channel 2)

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		9.13	No8 according to NoMCLA and NoMCLB set wrong during conversation of subject with observation category - full separate.	No7-OK, No8-NOK
		9.14	A and B - subscribers are subjects with observation category - full combined. No8 according to one out of two separate MCL	No7-OK, No8-OK No2.2 (channel 2) observation of conversation via another MCL.
		9.15	No8 according to call identifier during conversation of subject with observation category -full combined. Subject type 03H.	No7-OK, No8-OK No2.2 (channel 2)
		9.16	No8 according to NoMCL during conversation of subject with observation category -statistical; subject type 03H (after command No7)	No7-OK, No8-OK No2.2 (channel 2)

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
10	No10 Request for transmission of data about subject to be observed.	10.1	No10 with all parameters besides No of CL group	No7-OK, No3, No8-OK
		10.2	No10 according to No of CL group (for ATS)	No7-OK, No3, No8-NOK
		10.3	No10 according to conditional No	No7-OK, No3, No8-OK
		10.4	No10 according to object type	No7-OK, No3, No8-OK
		10.5	No10 according to attribute, digits amount and phone No	No7-OK, No3, No8-OK
		10.6	No10, all parameters=FFH	No7-OK, No3, No8-OK
		10.7	No10, conditional No does not comply with phone No	No7-OK, No3, No8-NOK
		10.8	No10, conditional No, unreal phone No	No7-OK, No3, No8-NOK
		10.9	No10, phone No and unreal conditional No	No7-OK, No3, No8-NOK
		10.10	No10, subject type not defined in TR for links	No7-OK, No3, No8-NOK
		10.11	No10, phone No attribute not defined inTR for links	No7-OK, No3, No8-NOK
		10.12	No10, number attribute does not comply with phone No	No7-OK, No3, No8-NOK
		10.13	No10, amount of digits in phone No does not comply with the mentioned in byte 5.	No7-OK, No3, No8-NOK
		10.14	No10, phone No and No of CL group are set	No7-OK, No3, No8-NOK
		10.15	No10, phone No is not a subject to be observed	No7-OK, No3, No8-NOK
		10.16	No10 with all FF parameters, there is no subscriber under observation	No7-OK, No3, No8-OK
		10.17	No10 with all set parameters, ther is no subscriber under observation	No7-OK, No3, No8-NOK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
11	No11 Request for transmission of information about compliance between MCL and groups	11.1	No11, all parameters=FFH	No7-OK, No4, No8-OK
		11.2	No11 according to Nogr.	No7-OK, No4, No8-OK
		11.3	No11 according to type of MCL group	No7-OK, No4, No8-OK
		11.4	No11 according to NoMCLA for gr.type-01H (combined)	No7-OK, No4, No8-OK
		11.5	No11 according to NoMCLA for gr.type-11H (separate)	No7-OK, No4, No8-OK
		11.6	No11 according to NoMCLB for gr.type-11H (separate)	No7-OK, No4, No8-OK
		11.7	No11, Nogr.=1, gr.type-01H(combined) MCLA is engaged with conversation	No7-OK, No4, No8-OK
		11.8	No11, Nogr.=2, gr.type-11H(separate) MCLA and MCLB are engaged with conversation	No7-OK, No4, No8-OK
		11.9	No11, Nogr.=1, gr.type-11H(separate)	No7-OK, No8-NOK
		11.10	No11, Nogr.=2, gr.type-01H(combined)	No7-OK, No8-NOK
		11.11	No11, Nogr.=1, gr.type-01H(combined) $\mathrm{NoMCLA} \neq \mathrm{NoMCLB}$	No7-OK, No8-NOK
		11.12	No11, Nogr.=1, gr.type-01H(combined) NoMCLA not assigned	No7-OK, No8-NOK
		11.13	No11, Nogr.=1, gr.type-01H(combined) NoMCLA is from another group	No7-OK, No8-NOK
		11.14	No11, Nogr.=2, gr.type-11H(separate) NoMCLA=NoMCLB	No7-OK, No8-NOK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		11.15	No11, Nogr.=2, gr.type-11H(separate) NoMCLA not assigned	No7-OK, No8-NOK
		11.16	No11, Nogr.=2, gr.type-11H(separate) NoMCLB not assigned	No7-OK, No8-NOK
		11.9 - 11.16	For these tests, the answer of EATS SOSM is admissible according to the first real parameters in the command	No7-OK, No8-NOK
		11.17	No11, Nogr. not defined in TR for links	**No7-OK, No8-NOK** or No7-NOK
		11.18	No11, type of MCL group not defined in TR for links	**No7-OK, No8-NOK** or No7-NOK
		11.19	No11, NoMCL for a given capacity of EATS not defined in TR for links	**No7-OK, No8-NOK** or No7-NOK
12	No15 Change of observation subject parameters	12.1	No15, change of observation category	No7-OK, No8-OK
		12.2	No10 according to conditional No	No7-OK, No3, No8-OK
		12.3	No15, change of No MCL gr.	No7-OK, No8-OK
		12.4	No10 according to conditional No	No7-OK, No3, No8-OK
		12.5	No15, change of priority mark	No7-OK, No8-OK
		12.6	No10 according to conditional No	No7-OK, No3, No8-OK
		12.7	No15, inexisting conditional No	No7-OK, No8-NOK
		12.8	No15, Nogr.does not comply with observation category	No7-OK, No8-NOK
		12.9	No15, observation category not defined in TR for links	No7-OK, No8-NOK or No7-NOK
		12.10	No15, not distributed Nogr (That is non-existing number of group).	No7-OK, No8-NOK
		12.11	No15, of priority mark not defined in TR for links	No7-OK, No8-NOK or No7-NOK
		12.12	No10 according to conditional No	No7-OK, No3, No8-OK
		12.13	No15, change of observation category during conversation	No7-OK, No8-OK observation of changed parameters since the next conversation.

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
		12.14	No15, change of NoMCL gr. during conversation	No7-OK, No8-OK observation of changed parameters since the next conversation.
		12.15	No15, change of priority mark during conversation	No7-OK, No8-OK observation of changed parameters since the next conversation.
13	No12 Request for transmission of supplementary services list	13.1	No12	No7-OK, No5, No8-OK
		13.2	No12, phone No is not a subject to be observed	No7-OK, No5, No8-OK
		13.3	No12, phone No of another exchange	No7-OK, No8-NOK
		13.4	No12, amount of digits in phone No does not comply with the mentioned in byte 2	No7-OK, No8-NOK
		13.5	No12 with attribute of phone No different from 01H	No7-OK, No8-NOK or No7-NOK
14	No13 Interruption of output of messages about tables contents	14.1	No10, all parameters=FFH	No7-OK, No3
		14.2	No13	No7-OK, No8-NOK, No8-NOK(c.No10)
		14.3	No11, all parameters=FFH	No7-OK, No4
		14.4	No13	No7-OK, No8-NOK, No8-NOK(c.No11)
		14.5	No10, all parameters=FFH	No7-OK, No3
		14.6	No9, Nogr.=1, gr.type-01H(combined) NoMCLA=NoMCLB	No7-NOK No8-OK(c.No10)
15	No14 Testing of data transfer channels	15.1	No14 over one of channels 1	No9 over channels 1, No2.3 over channels 2
		15.2	No14 over one of channels 1 with wrong SOSM No	No answer
		15.3	No10, all parameters=FFH	No7-OK, No3
		15.4	No14 over one of channels 1	No3, No9, No3, No2.3, No3, No8-OK(c.No10)
16	No17 SW release request	16.1	No17	No7-OK, No11, No8-OK

Tests for checking commands and messages transmitted via channel 1 between SOSM and CP.

No	Commands to be checked	No of tests	No of command sent from CP	Answer messages of exchange SOSM
17	No2 SOSM stop	17.1	No2 with wrong SOSM No	No7-NOK
		17.2	No2 with wrong password	No7-NOK, No6
		17.3	No2 with right password	No7-OK, No8-OK
		17.4	No2 repeatedly with initial password	No7-NOK
		17.5	No1 with initial password	No7-OK, No8-OK
		17.6	No10, all parameters=FFH	No7-OK, No3-NOK No8-NOK (No8-OK)

15: Functional description (FN): A00002252

15.1 Feature name

MG9K LINES PREPROVISIONING

- MG9K - Media Gateway 9000

15.2 Description

Feature 89009298 implements the core code changes required for increasing MG9K line provisioning throughput by preprovisioning. Please refer to ActID 89008025 which details the overall goals of the preprovisioning work effort.

The 89009298 core changes have three components:

1. The format of an MG9K LEN will reflect a physical location. Previously, no correlation existed between an MG9K LEN and its physical location. Instead the LEN correlated to the terminal id of the line. The new format shows a circuit range of 0 to 47. Currently, only 32 circuit line cards are supported for the MG9K.

   OLD FORMAT
   <SITE> <0 to 511> <0 to 9> <subgroup, 0 to 10> <circuit, 0 to 99>

   NEW FORMAT
   <SITE> <frame, 0 to 511> <shelf, 0 to 9> <slot, 2 to 9, 14 to 21> <circuit, 0 to 47>

2. When SESM provisions an MG9K node on shelves 0 to 3 and LGRP data, table LNINV will be automatically datafilled with the available circuits. Subsequent SERVORD+ commands issued by SESM will not add or delete MG9K line datafill from table LNINV. Essentially, autoprovisioning of table LNINV will be disabled for MG9K lines.

   This new functionality will supercede the setting of office parm RDT_SUCC_AUTOCREATE_LNINV for determining the autoprovisioning of table LNINV. This feature, however, does not restrict the MNO_DEFAULT value associated with RDT_SUCC_AUTOCREATE_LNINV. We can assume multiple gateway offices where setting the default MNO would be desirable for all gateways including MG9K. It is the ACTIVE setting that is ignored for MG9K lines.

3. Two new pad groups will be defined for use by gateway lines. PKLNL will be created for use by gateway lines that have LGRP GRPTYPE set to S. PKNIL will be created for use by gateway lines that have LGRP GRPTYPE set to C. These pad group will always be applied to gateway lines during SERVORD provisioning and during SESM provisioning and preprovisioning. Changing of gateway line pad group from these two new groups is permitted via changing the pad group in table LNINV. Default pad levels will also be set for Legacy interaction.

15.3 Hardware Requirements or Dependencies

None.

15.4 Software Requirements or Dependencies

The changes implemented under feature 89009298 require associated code changes in SESM line provisioning and MG EM in order to deliver the described functionality. However, the core changes are completely transparent to existing functionalities. Interactions are detailed below.

15.5 Limitations and restrictions

This feature is specific to MG9K lines.

15.6 Interactions

The feature 89008782 “MG EM - LINE CARD DATA DELIVERY TO SESM” implements the MG9K-EM part of the preprovisioning. It is required for this feature to work properly. It is a compliment of this feature.

The feature 89008025 implements the SESM line provisioning changes that are required by MG9K lines for this feature to work.

Feature 00000420 introduces the office parm RDT_SUCC_AUTOCREATE_LNINV which enables autoprovisioning for non-MG9K line gateways.

15.7 Applicable customer facing sections

Fault Management	
Logs	__X___
Alarms	_____
Configuration	
Data Schema	_____
User Interface	__X___
Element Management	_____
Security	_____
Service Order	__X___
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

15.8 Glossary

Term	Description
EM	Element Manager
LEN	Line Equipment Number
LGRP	Logical Group (of lines)
LNINV	Line Inventory (table)
MG	Media Gateway
MG9K	Media Gateway 9000
SESM	Succession Element and Sub-element Manager

16: Functional Description (FN): A00002291

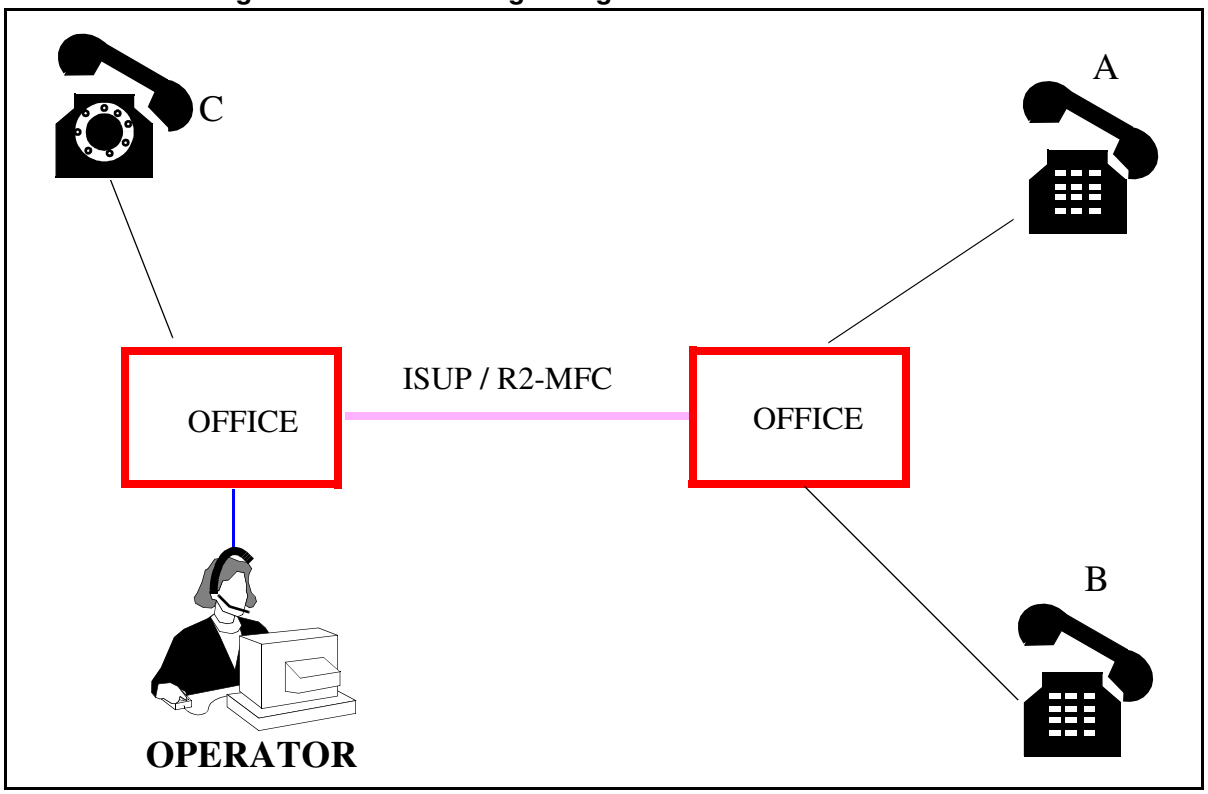
16.1 Feature name

Trunk Offering Expansion.

16.2 Description

“Trunk Offering” (TKO, TOF) is a software package that allows an operator to inform a busy subscriber that another subscriber wants to speak to him. The operator can break into an existing call and inform the busy subscriber verbally about a new, pending call. If the busy subscriber wants to receive the new call, One of the parties in the existing call should goes onhook, then the operator can connect him to the new caller immediately.

Figure 1 Trunk Offering configuration



TKO over ETSI ISUP trunks is already supported for some markets in the World-Trade software starting from the WT14 stream. This FN reflects the

functionality that supports the TKO feature both over ETSI ISUP and FDCP / MFC-R2 trunks for all markets using the default FDCP variant.

Table 1 TKO support today

	Telrad markets	other WT markets
ETSI ISUP trunks	supported in off-stream only.	supported.
FDCP/MFC trunks	supported in off-stream only.	not supported.

In order to provide Telrad markets with TKO feature in on-stream release, this feature propagates the TKO support to MMP20 for the following protocols:

- ETSI ISUP V2 for Ethiopia market,
- ETSI ISUP V2 for Costa-Rica market,
- ETSI ISUP V2 for Vietnam market,
- ETSI ISUP V2 for Georgia market,
- FDCP MFC / R2 and TYPE A.

In addition this FN reflects the Warning tone functionality for Ethiopia market.

Figure 1 LOGICAL VIEW

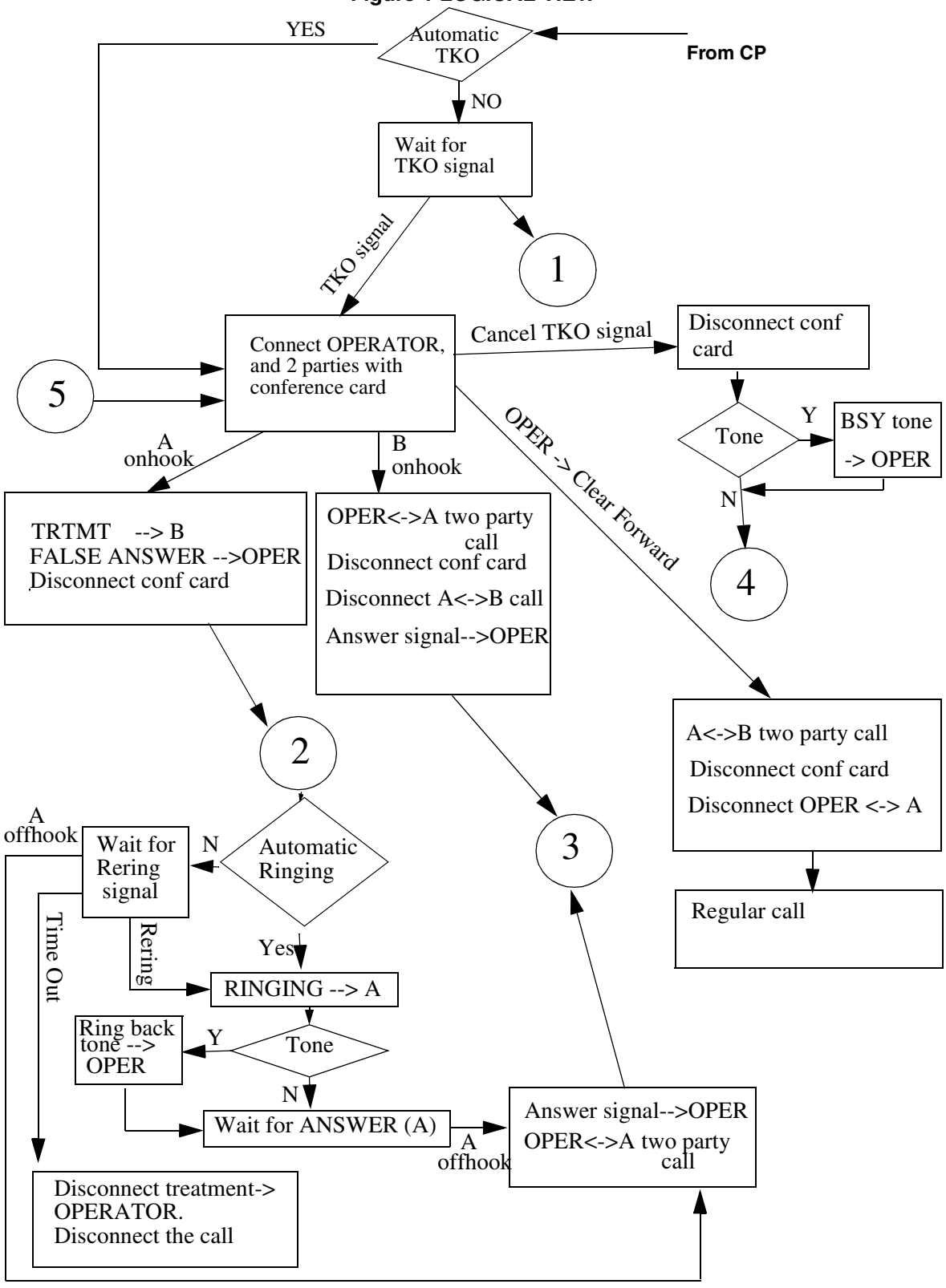


Figure 2 Logical View (continued)

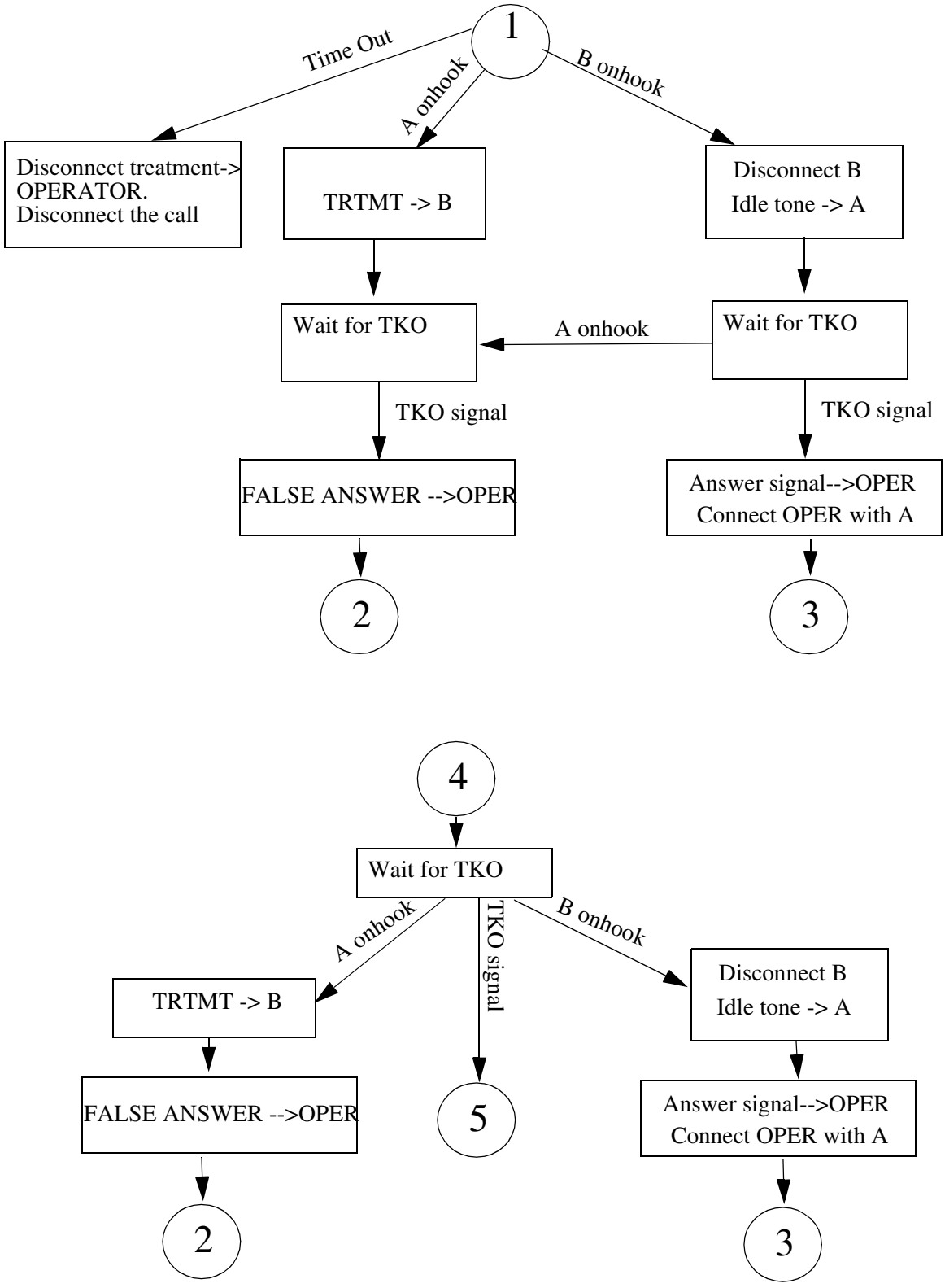
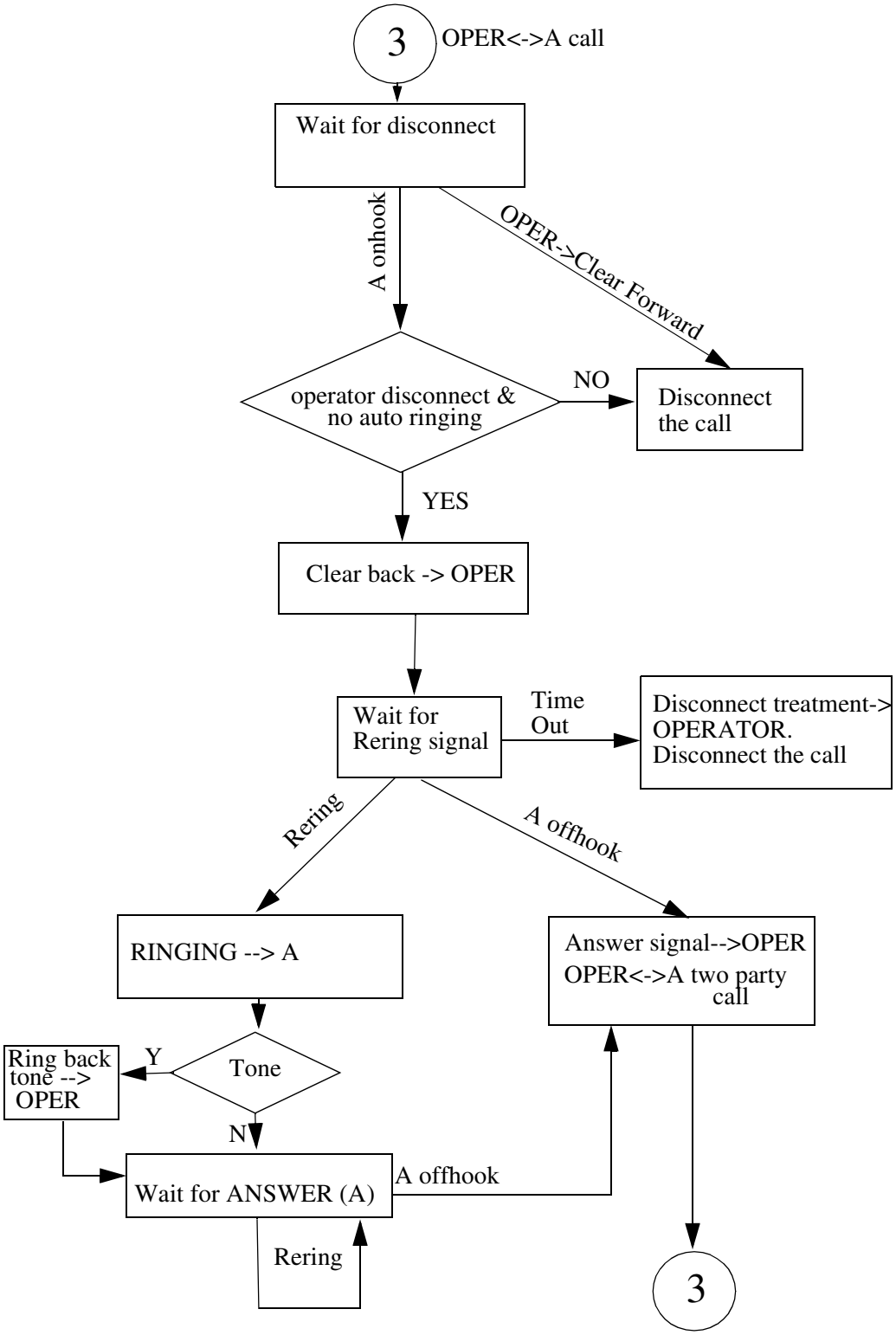


Figure 3 Logical View (continued)



16.2.1 TKO support over ETSI ISUP trunks.

Table 2 ETSI ISUP TKO protocol differences

Event	Variations for Telrad markets	Existing behaviour for other markets
TKO signal	Ethiopia, Vietnam, Georgia: ISUP_FF_NATL (#FF) Costa-Rica: ISUP_F9_NATL (#F9)	Various values, eg. ISUP_FF_NATL (#FF) (egypt), ISUP_FD_NATL (#FD) (Mexico), etc.
OPER Calling Party Cathegory	Vietnam, Costa-Rica, Georgia: ISUP_CPC_OP_NATIONAL (#09) Ethiopia: ISUP_CPC_TKO_OPERATOR (#E6)	Various values, eg. ISUP_CPC_OP_FRENCH (#01), ISUP_CPC_OP_ENGLISH (#02), ISUP_CPC_OP_GERMAN (#03), etc.
Party A goes OffHook in response to the operator Re-Ring signal	A sends SUS message only	A sends ANM message followed by SUS message
Party B goes OnHook to terminate the conference	A sends ANM message	A sends RES message

Figure 4 ISUP TKO messaging flow: Basic case A: A OnHook after conference.

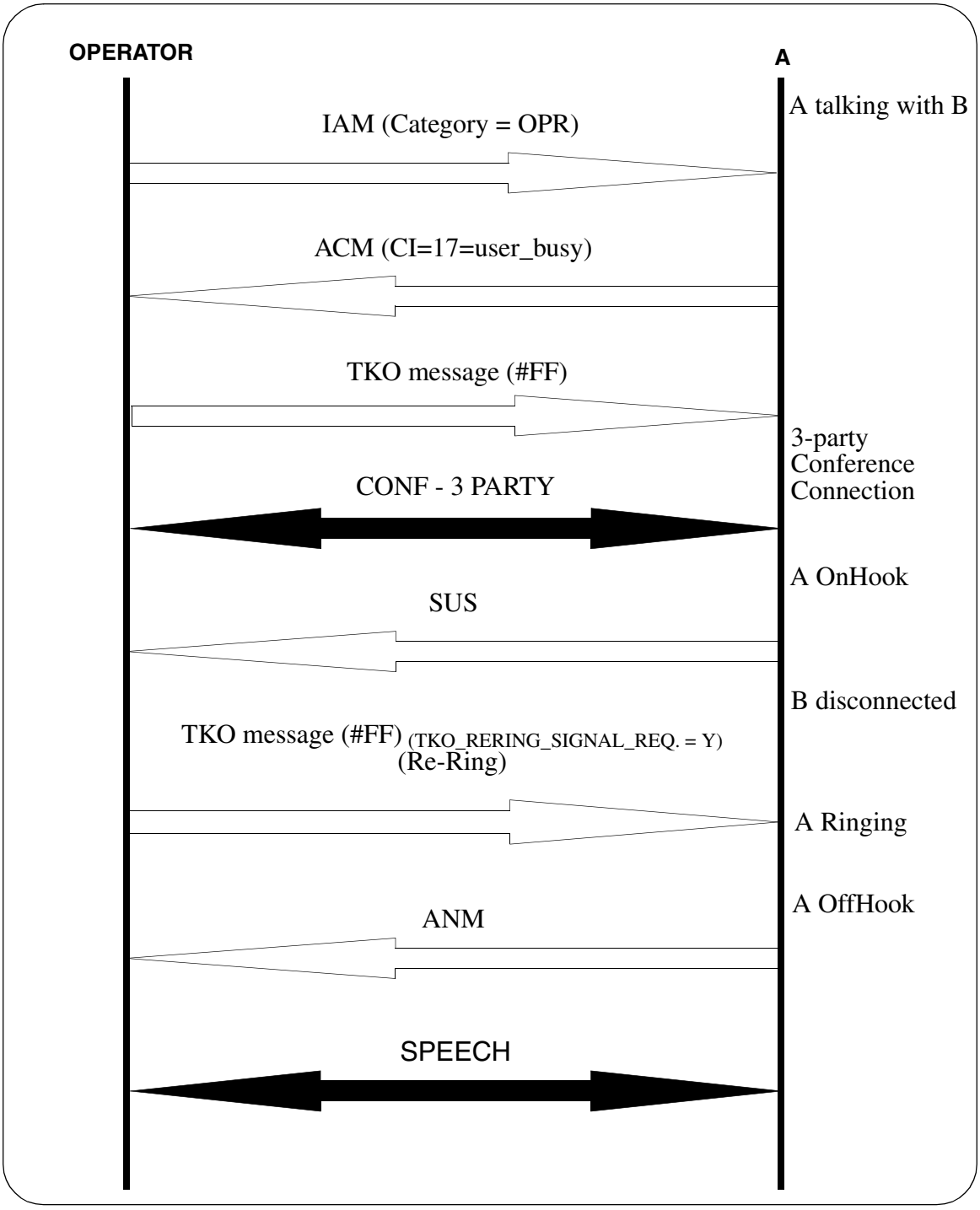


Figure 5 ISUP TKO messaging flow: Basic case B: B OnHook after conference.

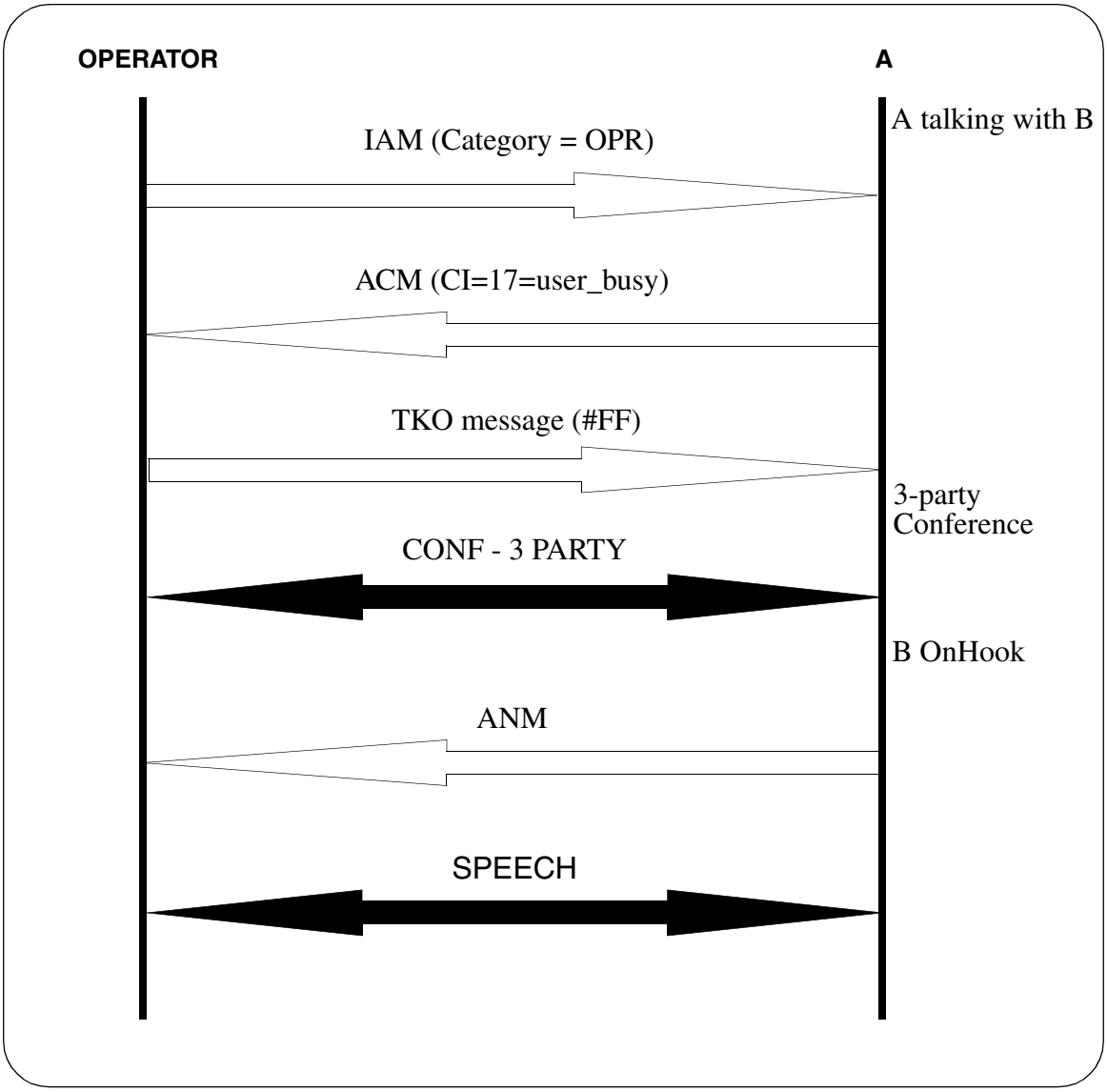
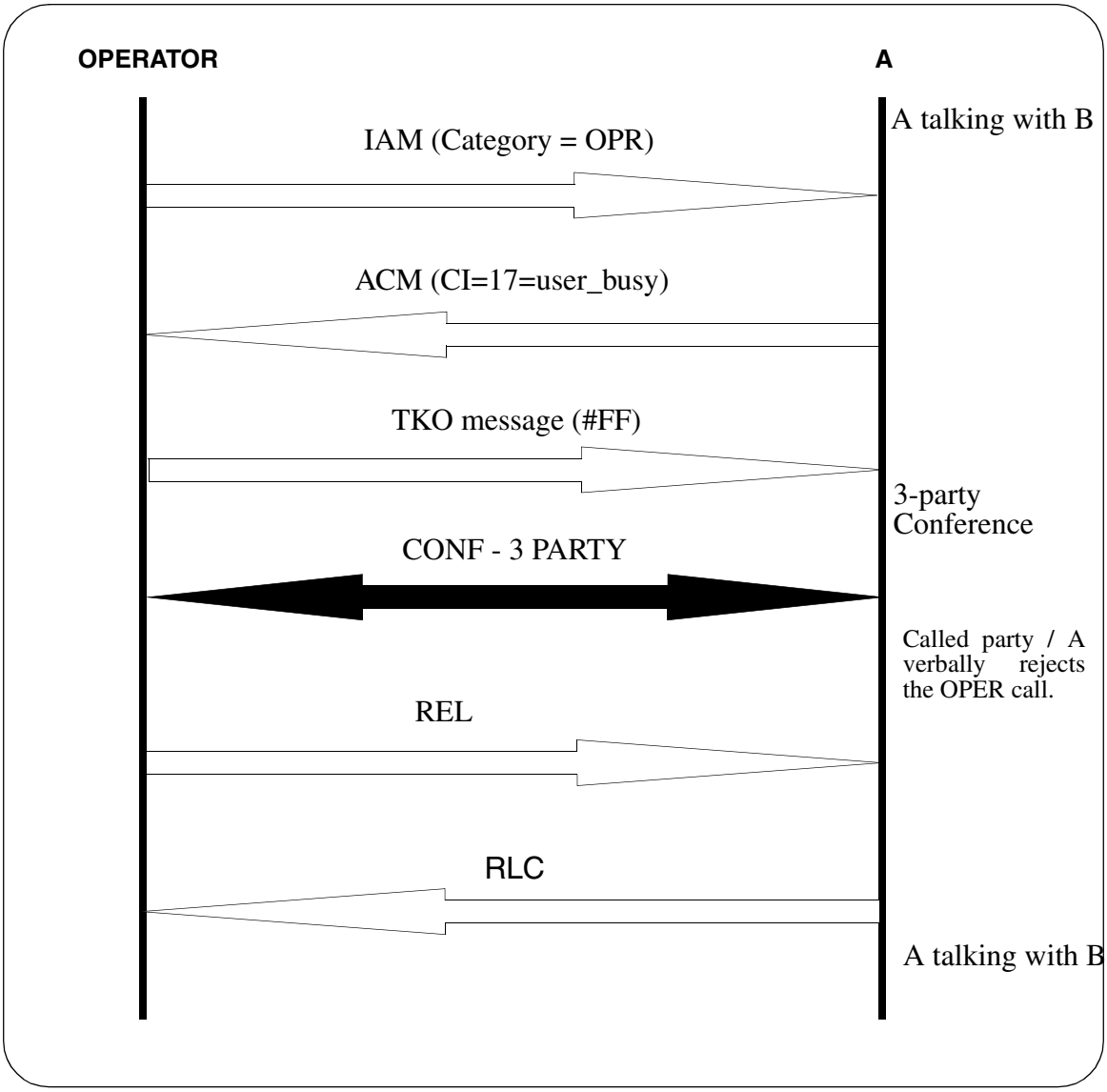


Figure 6 ISUP TKO messaging flow: Basic case C: A reject the operator call.



16.2.2 TKO support over FDCP MFC/R2 trunks.

Figure 7 MFC/R2 FOT messaging flow: Basic case A: A OnHook after conference.

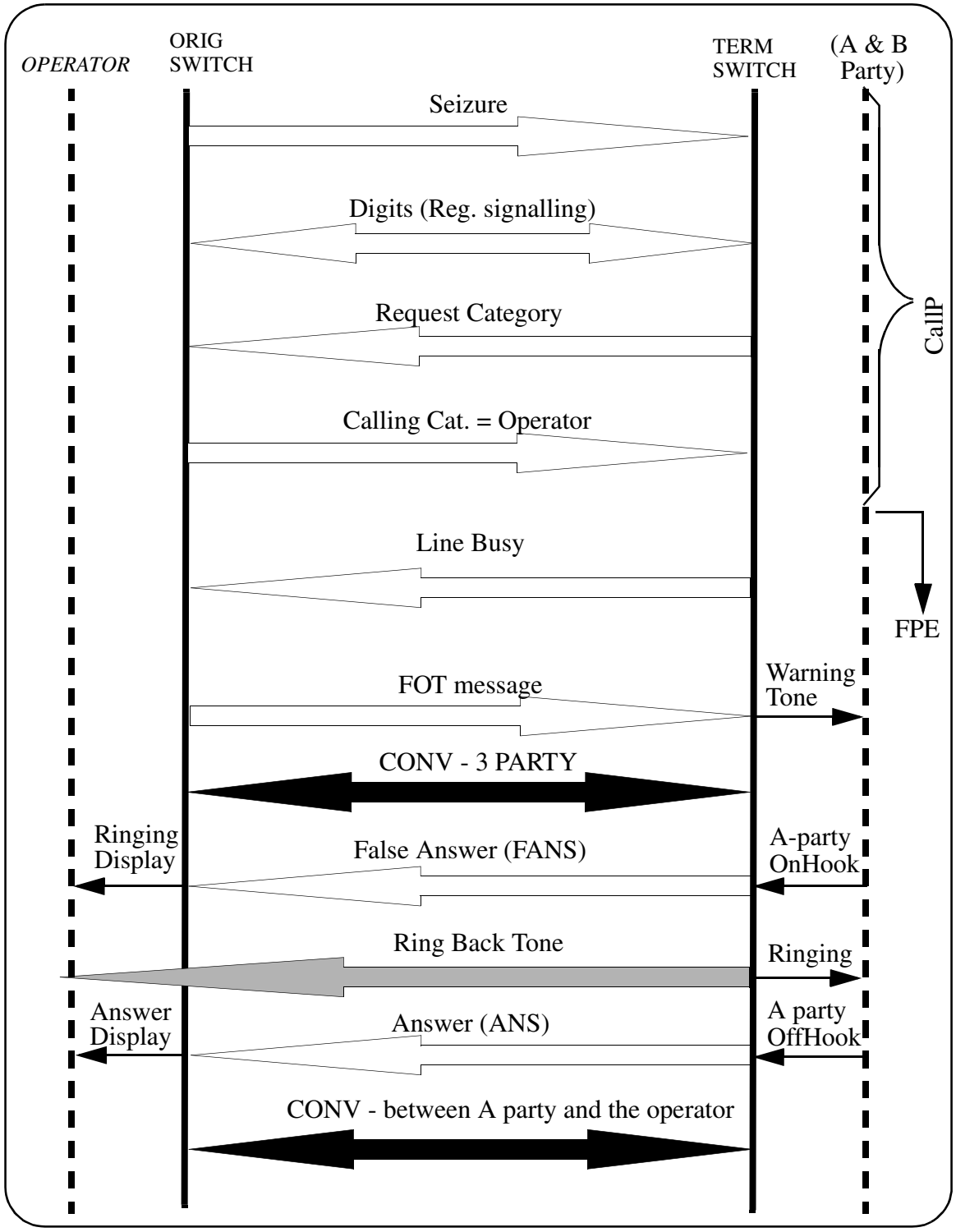


Figure 8 MFC/R2 FOT messaging flow: Basic case B: B OnHook after conference.

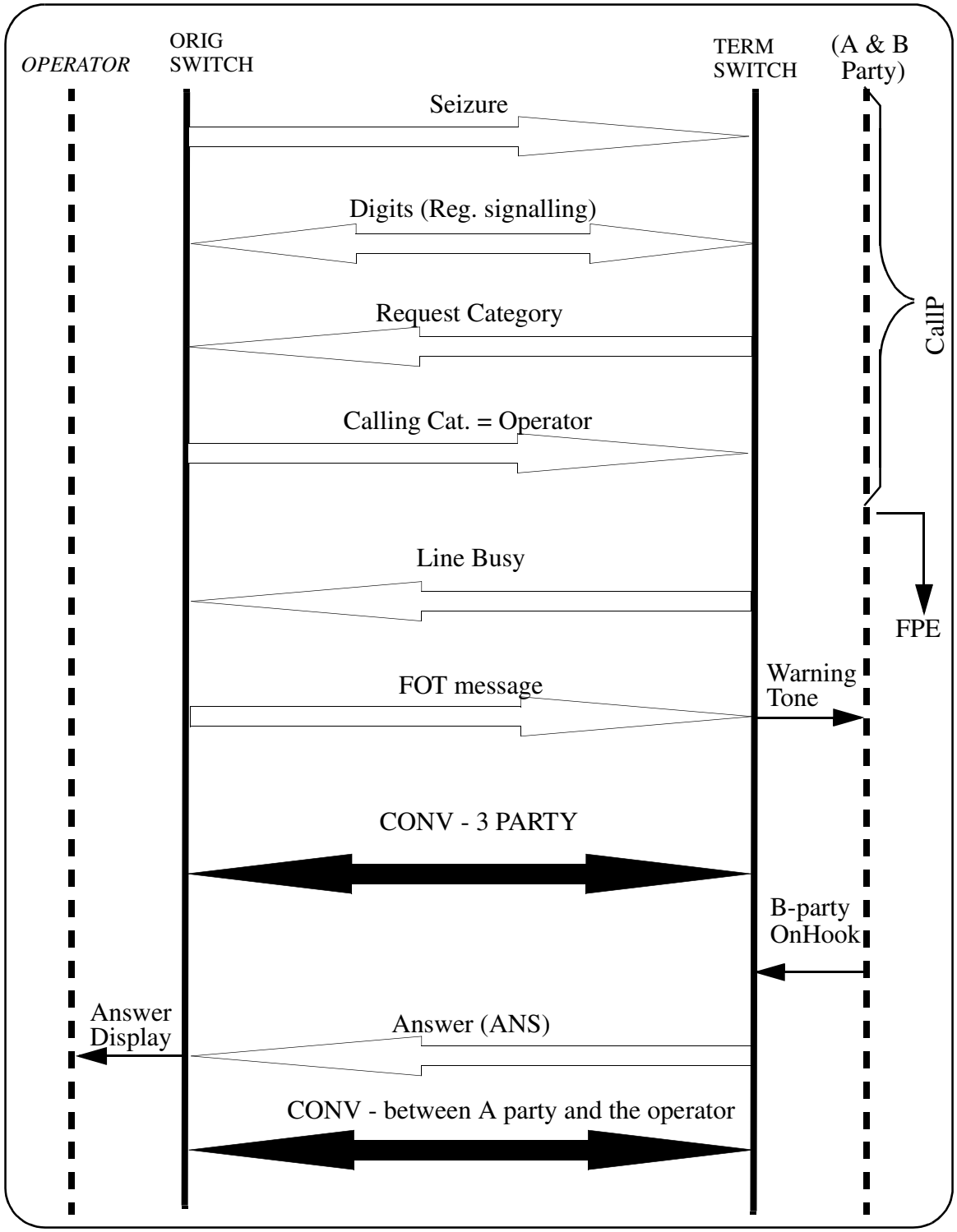
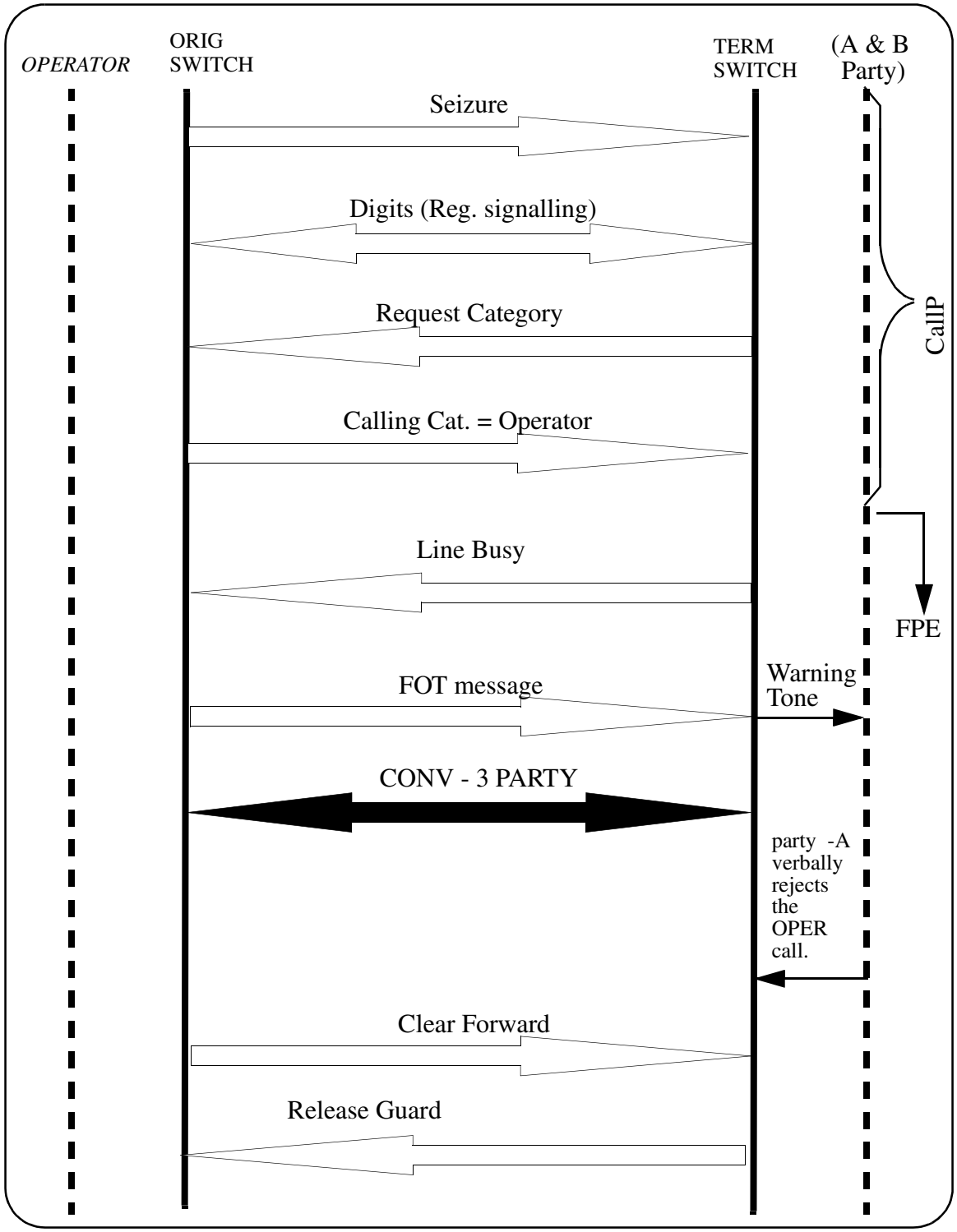


Figure 9 MFC/R2 FOT messaging flow: Basic case C: A reject the operator call.



16.2.3 TKO support in Interworking switch of FDCP <-> ETSI ISUP trunks cross.

This feature supports cross situations between the two protocols FDCP and ETSI ISUP in the tandem switch, that includes the following cases:

1. Interworking switch of ETSI ISUP to ETSI ISUP trunks cross.
2. Interworking switch of ETSI ISUP to FDCP trunks cross.
3. Interworking switch of FDCP to ETSI ISUP trunks cross.
4. Interworking switch of FDCP to FDCP trunks cross.

Table 3 ISUP - FDCP equivalence

ISUP Signal	R2 MFC Equivalent Signal	Notes
ISUP_ACM	**Line busy**	Sent as a response to IAM event by TKO. This is done because CPC=Operator, and ACM is sent instead of RLS. For R2-MFC, busy signal (B-3) is sent by CALLP BEFORE feature is activated, regardless of the fact that CPC=Operator.
ISUP_SUS	**FANS (False Answer)**	'FALSE_ANSWER' signal - Notify operator switch of one of the following events: • Terminator is onhook and operator-terminator call is now being established. • Terminator has gone onhook while talking with operator.
ISUP_ANM	**ANS (Answer Message)**	Used to notify operator that terminator has gone offhook.
ISUP_RES	**ANS (Answer Message)**	Used for notifying operator switch that call is re-established (i.e. parties are now talking again).

Figure 10 TKO call on tandem switch with ISUP-FDCP cross

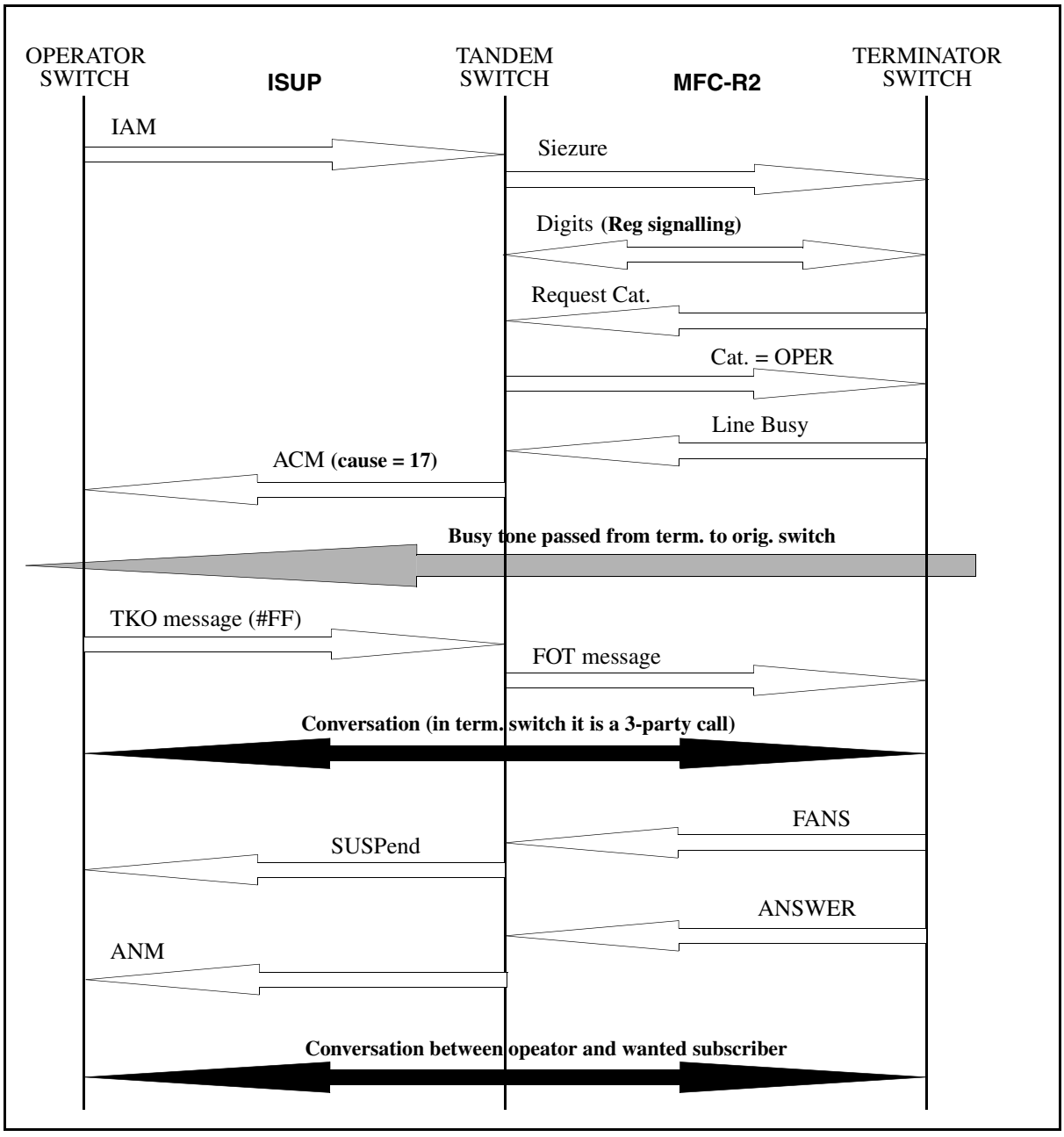
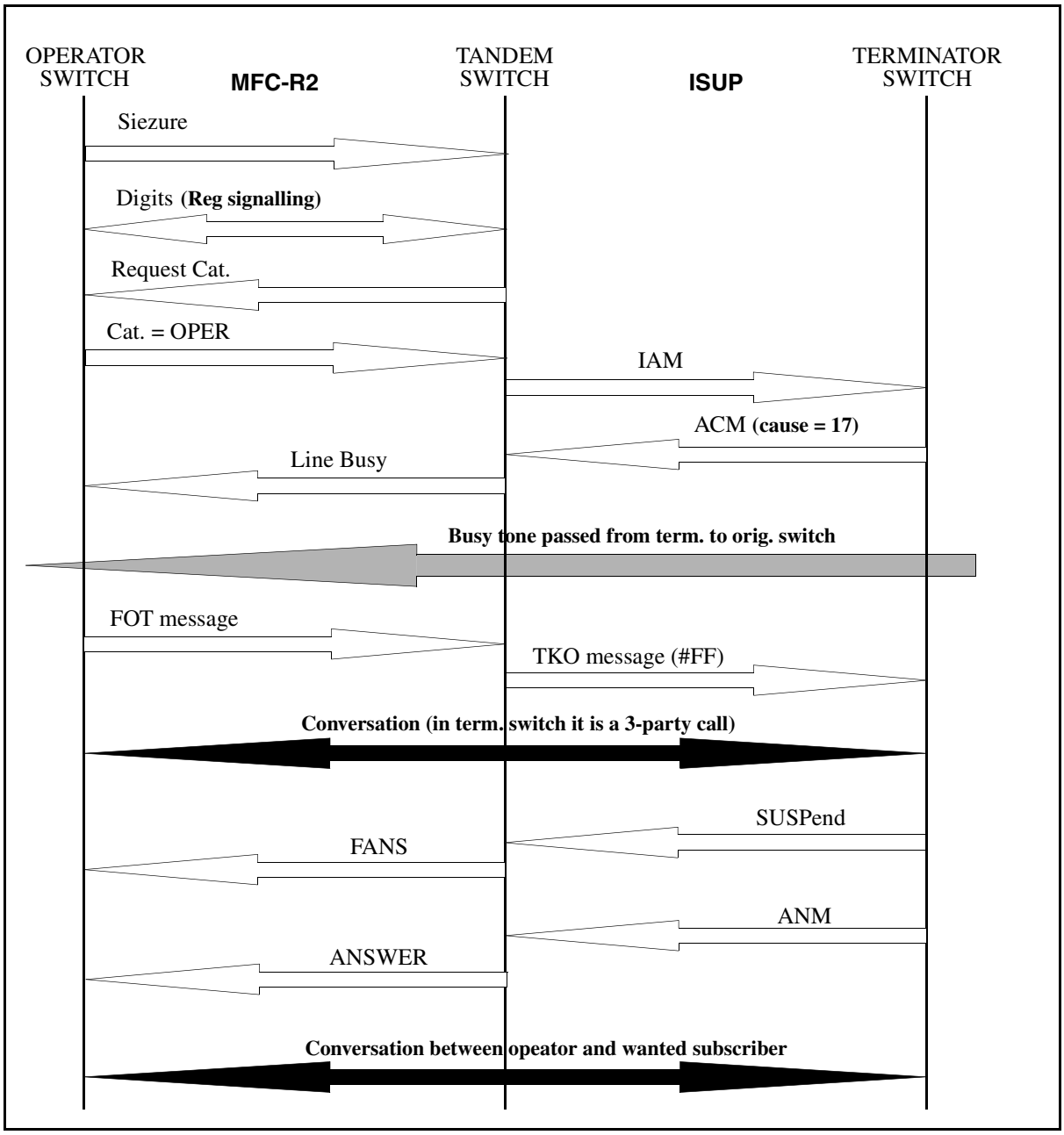


Figure 11 TKO call on tandem switch with FDCP-ISUP cross



16.2.4 Warning tone for Ethiopia market.

This feature supports warning tone for the existing TLR425 toneset.

The warning tone is used in the Fix Price Service (FPS) feature.
The warnong tone is given when FPS credit limit is exhausted and timer to clear call started.

Table 4 Warning tone requirements

Frequency (Hz)	Level (dbm0)	Tone Id. in hex
1400	-10	9D

The tone consists from 3 repeated patterns of tone 08 for 0.5 secs with a break for 11.5 secs between the tones (tone-brake-tone-brake-tone).

16.3 Hardware Requirements or Dependencies

N/A

16.4 Software Requirements or Dependencies

N/A

16.5 Data Requirements or Dependencies

To enable the Trunk Offering feature in the switch, the office parameter TBI_OFFER in table OFCVAR should be set to one of the following values:

- "MANUAL", which means that the operator has to send a TKO signal manually in order to enter into A-B call, or:
- "AUTO", which means that a TKO signal is not needed, and the operator enters A-B call automatically after the intrusion tone is heard.

In the off-stream TLR13 CM load, eight office parameters defined in tables OFCOPT and OFCENG are used for Trunk Offering.

In the on-stream MMP19 CM load, five office parameters defined in table OFCENG are already used for Trunk Offering.

Merging the off-stream parameters in the on-stream release is done as follows:

1. The parameters TBI_OFFER and TBI_OPR_TIMEOUT are used by this feature in MMP instead of the TLR off-stream parameters TKO_IS_ACTIVE, TKO_AUTO and TKO_TIMEOUT.
2. The parameters:
   — TKO_INTRUSION_TONE,
   — TKO_TONE,

— TKO_RERING_SIGNAL_REQ,

— TKO_OPER_ONLY_CAN_DISC,

— TKO_BREAK_FTR,

are added by this feature in MMP20.

3. The new parameters are added in table **OFCENG**, to comply with the definition of the existing parameters in MMP.

4. The new parameter TKO_INTRUSION_TONE is used in combination with the existing parameter TBI_BACKGROUND_TONE, thus allowing the user to select the desired tone from the toneset. The original hardcoded tone is used as default.

Table 5 Office parameters for TKO in MMP20

Table	Office Parameter	New / Unchanged in WT20	Range	Default value	Description	Notes
OFC VAR	TBI_OFFER	Unchanged	OFF, AUTO, MANUAL	OFF	Sets feature activity and mode	For Telrad markets, this paramater replaces TKO_IS_ACTIVE and TKO_AUTO used in TLR.
OFC VAR	TBI_OPR_TIMEOUT	Unchanged	100 TO 300 sec	100	Timeout value for operator message	Same as TKO_TIMEOUT in TLR.
OFC VAR	LOCAL_TBI_TONE	Unchanged	N,Y	Y	Indicates whether the call being broken into will hear any tone (offering tone and/or background tone) during the intrusion by the operator.	Telrad markets should use the default value “Y”.
OFC VAR	TBI_OFFERING_TONE	Unchanged	N,Y	N	If set to ‘Y’, an offering tone will be played from the toneset for one second only before the operator enters the call. The tone is hardcoded.	Not applicable for Telrad markets.

Table 5 Office parameters for TKO in MMP20

Table	Office Parameter	New / Unchanged in WT20	Range	Default value	Description	Notes
OFC VAR	TBI_BACKGROUND_TONE	Unchanged	N,Y	Y	If set to 'Y', a continuous intrusion tone will be played from the conference card during the conference call. If set to 'N', an intrusion tone will be played from the toneset for one second only before the operator enters the call. The tone is hardcoded, and is different from the offering tone.	Telrad markets should use the default value "Y". Up to this feature, the tone was hardcoded as 450HZ_15DBM. In this feature, the tone is defined by the parameter TKO_INTRUSION_TONE (see next). The previously hardcoded tone is used now as the default tone.
OFC ENG	TKO_INTRUSION_TONE	Unchanged	CONFERENCE_TONE_SET: a range of 7 tones or "no tone".	450HZ_15DBM	Defines the intrusion tone that is played from the conference card during the conference call.	The default tone is set to 450HZ_15DBM to comply with the existing application. In TLR off-stream release, any tone from the set can be used. The default is 450HZ_20DBM. Telrad customers using MMP20 release will retain their own tone either by ONP or by load building.
OFC ENG	TKO_TONE	Unchanged	N,Y	Y	Defines wether the operator receives 'busy' and 'ring-back' tones	Applicable for Telrad markets only.
OFC ENG	TKO_RERING_SIGNAL_REQ	Unchanged	N,Y	Y	Defines wether a "Re-Ring" signal is required (second operator message)	Applicable for Telrad markets only.
OFC ENG	TKO_OPER_ONLY_CAN_DISC	Unchanged	N,Y	N	Defines wether the terminator subscriber can disconnect the call with the operator, or the operator only can disconnect it.	Applicable for Telrad markets only.

Table 5 Office parameters for TKO in MMP20

Table	Office Parameter	New / Unchanged in WT20	Range	Default value	Description	Notes
OFC ENG	TKO_BREAK_FTR	Unchanged	N,Y	N	Enables/disables TKO to a subscriber that has features that disallow calls received (DTM)	Applicable for Telrad markets only.

16.6 Limitations and restrictions

The new trunk option TKO_FDCP should be assigned to incoming FDCP trunk in the table TRKOPTS. It will allow TKO feature **for specific incoming directions**.

TrunK Offering via ETSI ISUP Trunks will be supported only for Costa-Rica, Vietnam, Ethiopia ang Georgia markets.

TrunK Offering via FDCP Trunks will not be supported for 2W Trunks.

OPERATOR to Busy ISDN subscriber: OPERATOR can not break in.

16.7 TREATMENT

In case of TKO can not be applied, a PTOF (Premature_Trunk_OFfering) treatment should be applied to the InComing Trunk.

16.8 Interactions

16.8.1 OPERATOR to call with regret time.

In a scenario where the OPERATOR tries to call A and A is involved in a call with B: If A or B are in regret time, the OPERATOR can break in and disconnect B.

In case a scenario where A or B has been involved in a CWT or 3WC features before OPERATOR call, if A or B was On-Hook and now A or B are in regret time: in this case OPERATOR can not breake in.

Example for above mentioned case:

- A (CWT option) in call with B.
- C calls A. A was got CWT tone.
- C On-Hook.
- A and B continue to be in conversation.

- A On-Hook.
- OPERATOR can not breake in.

16.8.2 OPERATOR to call with OPERATOR on line.

In a scenario where the OPERATOR tries to call A and A is involved in a call with another OPERATOR, the operator can not break in.

.When an OPERATOR is in the process of breaking in to a call another OPERATOR can not initiate a break in process.

16.8.3 OPERATOR to noneTALKING call.

OPERATOR can not break in to the following call states: Off-Hook before dialing, dialing and ringing.

16.8.4 Call Wait (CWT).

The possible situations are:

A has the CWT feature but he is involved in a regular call - The OPERATOR can break in to the call (regular call).

A is involved in a CWT call - Break in can not be effected.

B is involved in a CWT call and A is on the same office - Break in can not be effected.

B is involved in a CWT call and A is not on the same office - There is therefor, no indication that B is involved in a CWT call - The OPERATOR can break in.

A cannot FLASH after OPERATOR enterd the call.

16.8.5 3WC.

The possible situations are:

A has the 3WC feature but he is involved in a regular call - The OPERATOR can break in to the call (regular call).

A is involved in a 3WC call - Break in can not be effected.

B is involved in a 3WC call and A is on the same office - Break in can not be effected.

B is involved in a 3WC call and A is not on the same office - There is therefor, no indication that B is involved in a 3WC call - The OPERATOR can break in.

A cannot FLASH after OPERATOR enterd the call.

16.8.6 Call Forward (CFW) / CFBL / CFDA.

The call forward is transferred. If the second call is BUSY the OPERATOR can break in.

16.8.7 Denied Terminator (DTM).

The OPERATOR can break in only if office parameter TKO_BREAK_FTR is set to Y.

Note. Office parameter TKO_BREAK_FTR for connection via FDCP trunks works only in case when calling paty category was received before all the called party digits were delivered to the switch. For this purpose appropriate entry in the table R2PROT should be datafilled with option ANI_AFTER_1_DIG or CAT_AFTER_1_DIG.

16.8.8 SUS / RSUS.

The OPERATOR can not break in.

16.8.9 MCT.

The OPERATOR can not break in to any call involving MCT.

The OPERATOR can not break in - When B has MCT and the AB call is a line to line call or the AB call is a line to trunk call and when A receives a holding indication.

The OPERATOR can not break in - When A has activated MCT by pressing FLASH.

A cannot FLASH after OPERATOR enterd the call.

16.8.10 OPERATOR to Line who was connected to TREATMENT or TONE call.

The OPERATOR can not break in.

16.8.11 OPERATOR to HUNT GROUP.

In case of all HUNT GROUP (DNH) members are in Busy state, the operator can breaks in last busy member call.

16.8.12 OPERATOR to Busy ISDN subscriber.

OPERATOR can not break in.

16.8.13 OPERATOR to Line with CLI option.

In case of OPERATOR calls Line with CLI option, no information Log will be printed - neither when line is in the call, nor when line is idle.

16.9 Applicable customer facing sections

Fault Management

- Logs ___N/A___
- Alarms ___N/A___

Configuration

- Data Schema ___Y___
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A____

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

16.10 Glossary

Term	Description
TKO, TOF	Trunk Offering
CP, CALLP	Call Process
FPE	Feature Processing Environment
CM	Computing Module
IAM	Initial Address Message
ISUP	ISDN User Part
MFC	Multi Frequency
OFFHK	Off Hook
ONHK	On Hook

Term	Description
OPR	Operator
RNG	Ring
ACM	Address Complete Message
FOT	Forward Operator Transfer
RGB	RinG Back
CPC	Calling Party Category

17: Functional Description (FN): A00002293

17.1 Feature name

Registered Call Line Option

17.2 Description

17.2.1 Introduction

The **Registered Call (RGC)** feature permits a subscriber with the RGC feature activated to redial automatically the last dialled number by going off-hook. When the Registered Call timer (the timeout can be programmed by the customer from 1 to 20 seconds) expires, and the subscriber does not start to dial any number, the feature provides call to the last dialled number.

The RGC feature allows automatic redialing to the last valid call that passed translation and routing (i.e. successfully route the call to terminating subscriber line or to outgoing trunk group or to BLDN treatment) in the switch.

The feature introduces a new line option RGC that supports IBN and ISDN (BRI) lines.

This activity allows automatic deactivation of RGC feature if a special timer expires. The timer value is determined by the new field **AUTO_DEACT_TIMEOUT** in the RGC tuple added to table ISERVOPT.

17.2.2 RGC Activation

- In order to activate RGC feature, subscriber should dial feature code activation (***66** - this number is used in this feature for example) and hang up.
- Subscriber will be able to activate RGC feature to only one destination.
- If subscriber has already activated RGC feature, the previous activation should be cancelled by a new one. The new RGC activation activates the feature to the new destination according to the last valid call performed before the new activation.
- Confirmation tone should be applied to subscriber in case of successful feature activation.
  Log LINE 138 is generated:
  TREATMENT SET = **CONF** CALLED NO = B66
- If dialed call did not pass translation and routing in the switch it will not be registered and activation will be done to the last valid call.

- When the new feature activation is done, the previous timing cycle is cancelled and the timer re-starts from the beginning.
- Log LINE 138 with FNAL treatment is generated when a subscriber, which has not the RGC option, tries to activate RGC feature by dialing *66:
  TREATMENT SET = **FNAL** CALLED NO = B66

17.2.3 RGC Deactivation

- Deactivation of RGC feature may be done by one of the following cases:
  - Automatically if the timer determined by the new field **AUTO_DEACT_TIMEOUT** of RGC option in table ISERVOPT expires.
  - After successful call establishment to registered destination and the terminator answer.
  - By dialling deactivation code (**#66** - - this number is used in this feature for example).
- Confirmation tone should be applied to subscriber in case of successful feature deactivation.
- If the subscriber has already deactivated RGC feature and a new RGC deactivation is done by dialing #66, then log LINE 138 with NACK treatment is generated:
  TREATMENT SET = **NACK** CALLED NO = C66

17.2.4 RGC Treatments

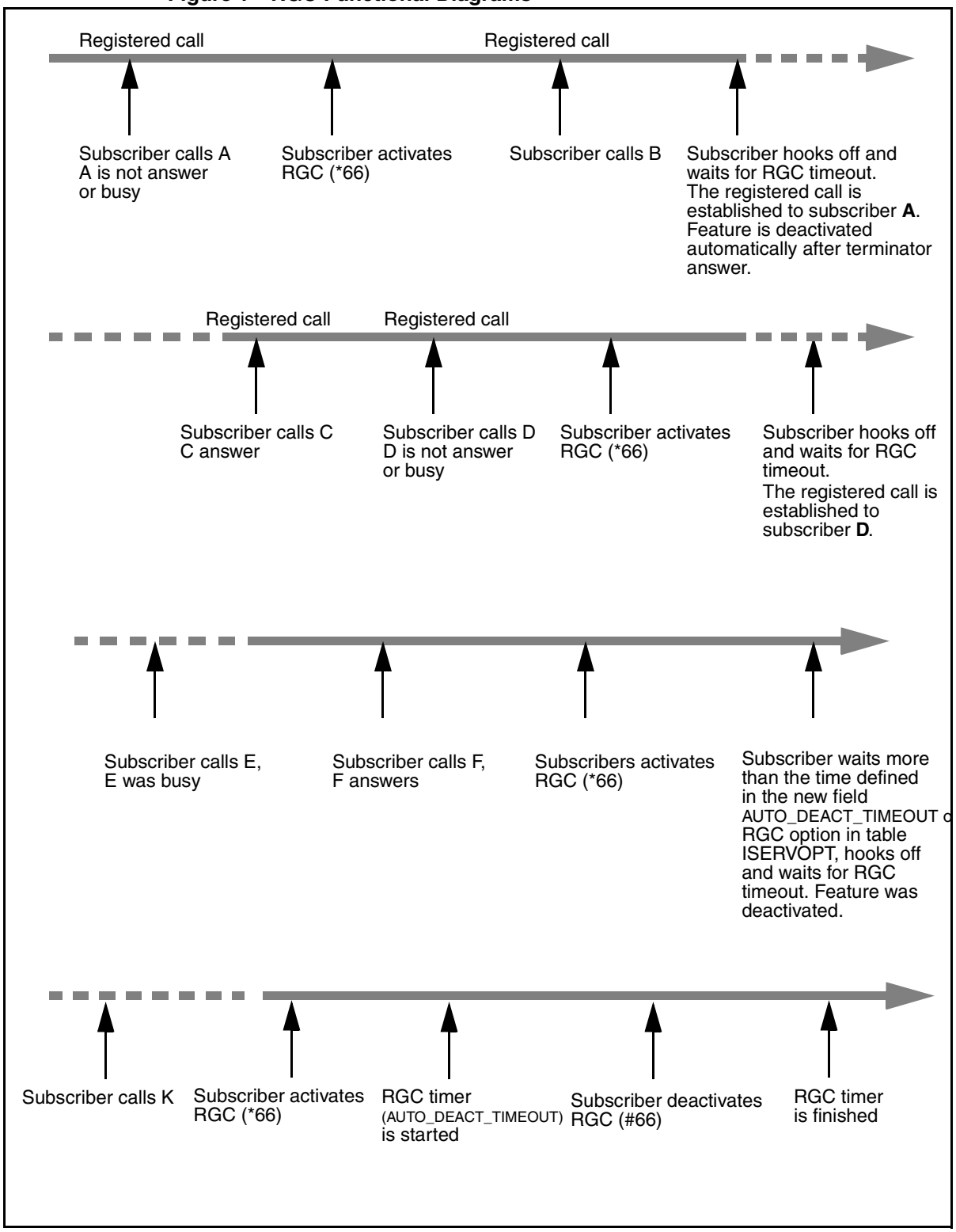
Table 1 Summary of treatments in log LINE138 after RGC activation/deactivation

Treatment	Action	Description of cases
FNAL	Activation	RGC feature is not defined on line
PSIG	Activation	RGC activation without last number stored
CONF	Activation/ Deactivation	Perform the successful RGC activation code
NACK	Deactivation	Double RGC deactivation by user
BLDN	Off-Hook	RGC feature was activated after BLDN call

17.2.5 RGC Functional Diagram

When the subscriber, which has activated RGC feature, goes off-hook, the feature waits for RGC activation timeout (defined in Servord TIMEOUT field). If the subscriber does not start to dial any number, the feature tries to establish a call to the last valid call that was performed before activation. Figure 1, "RGC Functional Diagrams" demonstrates same cases of RGC feature activation and deactivation interactions.

Figure 1 RGC Functional Diagrams



17.2.6 Controlling the RGC deactivation timer

Deactivation timer of RGC feature is fully controlled using the Table Control. A new tuple for RGC option is added to table ISERVOPT. If RGC option is not present in ISERVOPT table, then a value of deactivation timer is set to default (10). The customer can change the default value by adding/changing the RGC tuple to table.

Note: Restarts are not required to activate data changes after adding/ changing/deleting RGC tuple to/from table ISERVOPT.

17.3 Hardware Requirements or Dependencies

Not applicable.

17.4 Software Requirements or Dependencies

Not applicable.

17.5 Limitations and restrictions

- RGC line option is incompatible with WML, ACB, AR, AUL, GIC, MAN, MPB options and for HUNT group.
- Subscriber may activate RGC to one destination only.
- It can be allowed to activate simultaneously up to 1000 RGC requests per switch.
- RGC supports IBN and ISDN (BRI) lines.

17.6 Interactions

Not applicable.

17.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X

Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

17.8 Glossary

Term	Description
RGC	REGISTERED CALL
ACB	AUTOMATIC CALL BACK
RGC	REGISTERED CALL
ISDN	INTEGRATED SERVICES DIGITAL NETWORK
IBN	INTEGRATED BUSINESS NETWORK
AC	AUTOMATIC RECALL
AUL	AUTOMATIC LINE
GIC	GROUP INTERCOM
MAN	MANUAL LINE
MPB	MULTIPARTY BRIDGING
TCAP	TRANSACTION CAPABILITY APPLICATION PART

18: Functional Description (FN): A00002319

18.1 Feature name

MWI control via ISUP.

18.2 Description

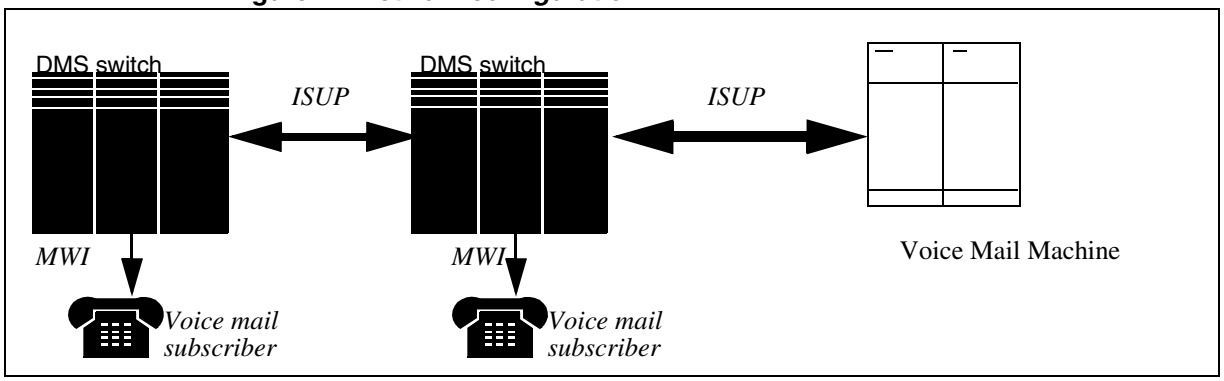
This feature provides Message Waiting Indication functionality via ETSI ISUP V2 protocol.

How this mechanism works:

— The MWT option is assigned to an IBN subscriber line with Voice Mail defined on it. The VMI option is assigned to a BRI subscriber line with Voice Mail defined on it.

— The ISUP IAM message with special activation code is sent from VMM to the DMS-100 switch (See Figure 1, "Network configuration."). The activation code includes 3 digits and may be defined in translation in accordind to customer requirements.

Figure 1 ***Network configuration.***



— For flexibility of the Vmi_Activation_Code definition, the code received in IAM message is replaced by the PXCODE table with constant values : 100 for Stuttered Dial Tone activation, 101 for Stuttered Dial Tone deactivation.

— To allow the MWI control via ISUP, the system invokes the Universal Translation using new ‘VMI’ conditional route selector from the PXRTE table (For details please refer the Configuration document).

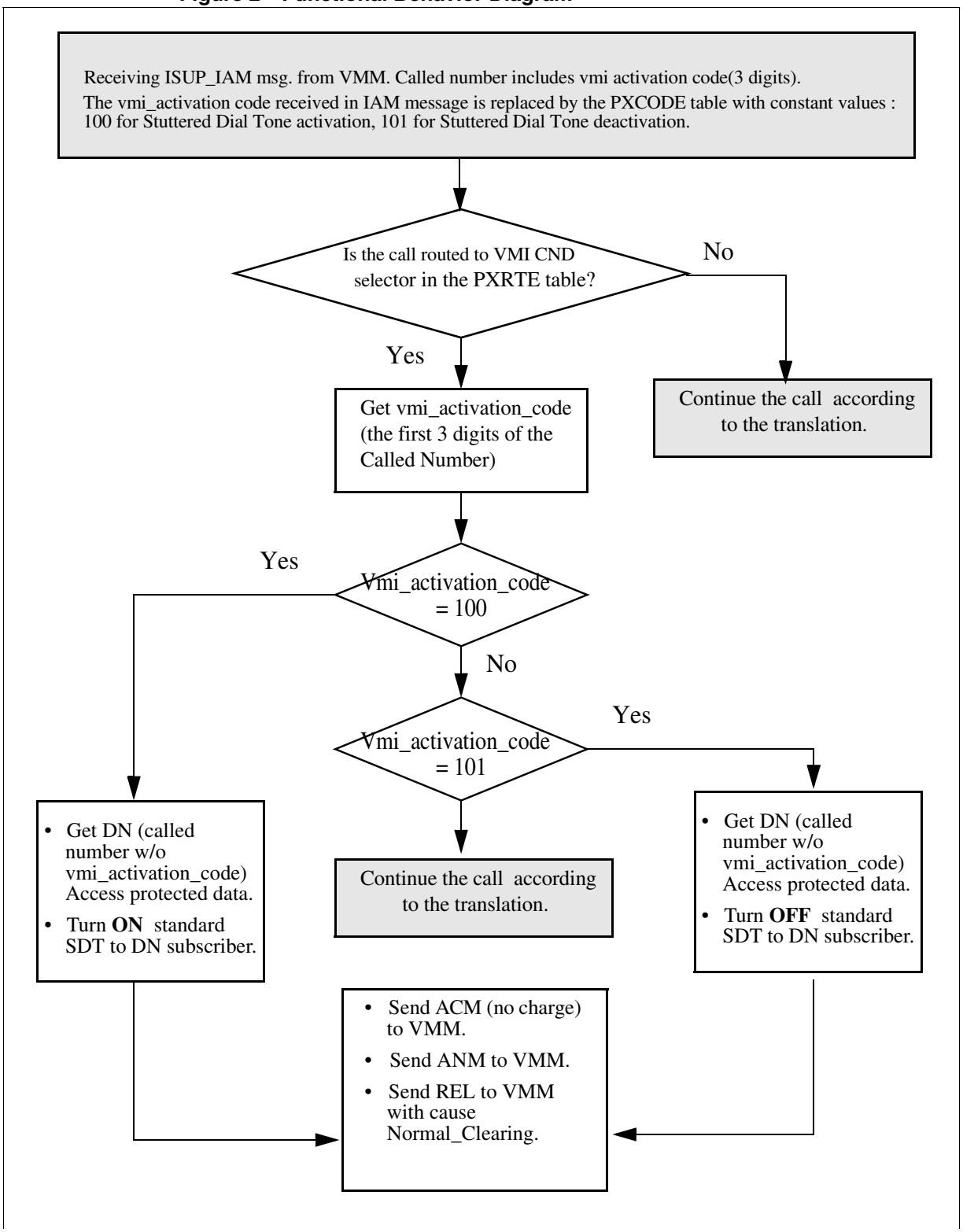
— After VMI Activation Code(the first 3 digits in the Called Number field of the IAM msg) is replaced in the PXCODE and the call pass translation via VMI’ conditional route selector in the PXRTE table, the SDT is set ON/OFF. The SDT is set for DN that is received in the IAM

msg (The Called Number digits without first 3 digits of activation code).

— After SDT tone is set, the ISUP ACM, ISUP ANM and ISUP REL with cause Normal_CLearing messages are sent to VMM. ISUP_REL message is sent as result of NORMCLR (Normal Clearing) defined in the TMTMAP table (For details please refer the Configuration document).

— If the call is not routed to the VMI' conditional route selector, the call is transferred according to defined translation.

Figure 2 Functional Behavior Diagram



18.3 Hardware Requirements or Dependencies

PDTC with SX05 processor or Shrink CPM.

18.4 Software Requirements or Dependencies

QDT20xx or QCI20xx load files for PDTC.

18.5 Limitations and restrictions

- The feature supports only PDTC with SX05 processor(QDT20xx or QCI20xx load files) or Shrink CPM.

18.6 Interactions

Not applicable.

18.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

18.8 Glossary

Term	Description
MWI	Message Waiting Indication
SDT	Stuttered Dial Tone
VMM	Voice Mail Machine

Term	Description
ISUP	Integrated Service User Part
DN	Dialled Number
IBN	Integrated Business Network
BRI	Basic Rate Interface
MWT	Message Waiting line option
VMI	Voice Mail Indication

19: Functional Description (FN): A00002358

19.1 Feature name

Feature A00002358 “H.323 tunneling over QSIG“ is part of the “Carrier Hosted Services and H.323 VPN Support“ project.

19.2 Description

The “Carrier Hosted Services and H.323 VPN Support“ project will provide support for tunneling H.323 messages through a CS2K Succession network, thus connecting remote sections of VPNs. It will allow H.323 components to be carrier hosted, with message tunneling done via the QSIG protocol.

The functionalities provided in the feature A00002358 include exclusively Basic Call as well as basic support for CAS and NCAS calls. No supplementary services on CS2K are explicitly supported.

19.3 Hardware Requirements or Dependencies

In the scope of A00002358 the following H.323 call management components are currently envisioned as registering with the GWC:

- BCM
- Meridian M1

The following table indicates, which basic call interworkings between such components will be supported by A00002358.

Table 20 Interworking support for basic call provided by A00002358 based on H.323 component

	BCM	Meridian M1
BCM	yes	yes
Meridian M1	yes	yes

For the exact testing environment which is used to evaluate the above interworkings under feature A00002358, please refer to section 3.1 below.

No other software or hardware line-ups outside the ones mentioned in section 3.1 are used under the scope of this feature for interworking testing between H.323 components.

All other interworkings with H.323 components not mentioned here are outside the scope of A00002358.

19.4 Software Requirements or Dependencies

The following software releases are required on the H.323 components for the functionality provided by A00002358:

BCM software release: BCM3.0

Meridian M1 software release: 25.15

As agents on the above listed H.323 components will be supported:

BCM: Nortel i2400 (model NTEX00)

Meridian: Meridian Business set M2008

19.5 Limitations and restrictions

Feature A00002358 provides trial quality functionality for a customer trial only.

A00002358 only covers Basic Call from a CS2K perspective.

Robustness delivered by A00002358 is to be considered on par with „trial ready“ software. This implies that limited error handling and recovery functionality will be provided.

No commitment is made regarding traffic completion rates for traffic employing the functionality provided by A00002358.

Feature A00002358 delivers support for intra switch calls only (CAS and NCAS); no interworkings to any trunk variants is provided.

19.6 Interactions

A00002358 uses existing call processing functionality within the CM and GWC software and makes extensive use of QSIG as tunneling protocol.

For additional interactions in the area of provisioning and datafill, please refer to feature A00001913 H.323 Provisioning.

19.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	N/A
User Interface	N/A

Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

19.8 Glossary and Additional Information

Term	Description
New term	Definition

20: Functional Description (FN): A00002364

20.1 Feature name

A00002364 : CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20.

20.2 Description

This feature provides the following functions:

1. Provide new option OCN in table CLICNTL
   - This feature adds a new option named OCN in table CLICNTL. This option is one of the selectors of BILLING_OPTIONS.
2. CLI/RDN/OCN capture in CDR for ANSI ISUP and HK ISUP
   - This feature provides CLI/RDN/OCN and corresponding indicator within CDR records generated on calls whose originating physical port is ISUP trunk according to the capture logic (please refer to Table 1). OCN option, which is introduced by this feature, is available in table CLICNTL.

***Note:** Both CLI and RDN capture in CDR feature have already been implemented for ISUP trunks on DRU GSP.*

Note: This feature is implemented on DRU GSP20 and patched back to GSP10.

20.2.1 Background

CLI and RDN capture in CDR have been implemented for ISUP trunks according to the datafill of table CLICNTL.

The field BILLING_OPTIONS of table CLICNTL specifies a list of numbers from:

- Screening Number (SCRN_NUM)
- Calling Line Identity (CLI)
- Redirecting Number (RDN)
- Charge Number (CHARGE)
- Generic Number (GENERIC_NO)
- Contractor Number (CONTRACTOR)
- Presentation Number (PN)

Table CLICNTL specifies a datafillable precedence order for the customer. The list of BILLING_OPTIONS is checked from left to right, searching for an address that is present. Once an address is found that is presented in the call, then this address is selected for billing purposes.

20.2.2 Detail Description

This feature provides the ability to enable CLI/RDN/OCN and corresponding indicator capture in CDR for ANSI ISUP and HK ISUP on DRU GSP20 according to the capture logic.

This feature is involved in ANSI ISUP and HK ISUP originating calls.

The following is the capture logic.

Table 1 CLI, RDN, OCN capture logic

Situation	Number put in the CDR	Indicator set in the CDR
Both RDN and CLI exist from ISUP message	RDN	10
Both OCN and CLI exist from ISUP message	OCN	01
Only CLI exists from ISUP message	CLI	00
No RDN/OCN/CLI exists from ISUP message	None	11
None of the above	RDN/OCN/ CLI *	10/01/00**

RDN/OCN/CLI * means if RDN exists, put RDN, then OCN if OCN exists, otherwise put CLI.

10/01/00 ** means if RDN is captured, put 10, then 01 if OCN is captured, otherwise put 00 if CLI is captured.

Two spare bits in existing CDR are used as indicator in this feature. The detailed information is listed in the following table.

Table 2 Spare bits usage information in CDR

Situation	Number put in CDR	Word 28/Bit	
		10	9
RDN and CLI existing	RDN	1	0
OCN and CLI only	OCN	0	1
CLI only	CLI	0	0
No RDN, OCN nor CLI	None	1	1
None of Above	RDN/OCN/ CLI*	1/0**	1/0**

Remark: Word 28/Bit 8 is "Answer"

RDN/OCN/CLI* means if RDN exists, put RDN, then OCN if OCN exists, otherwise put CLI.

1/0** means if RDN is captured, put 10, then 01 if OCN is captured, otherwise put 00 if CLI is captured.

The following table shows the current structure of CDR.

Table 3 The structure of CDR

No	Field Name	Offset	Bytes/ Bits	Encoding Type	Field Contents
1	RECCD +Type of call + VPN Cust Type + INAP Call + EXPANSION_REC	0	2	BINARY	Record Code + Type of Call + VPN Customer + INAP Call + E XPANSION_REC
2	ORIGDATE	2	2	BCD	Origination Date
3	ORIGTIME	4	3	BCD	Origination Time
4	DISCDATE	7	2	BCD	Disconnect Date
5	DISCTIME	9	3	BCD	Disconnect Time
6	CALLDUR	12	4	BINARY	Call Duration Time
7	ORIGCLLI	16	2	BINARY	Origination Trkgrp CLLI
8	ORIGMEM	18	2	BINARY	Origination Member Number
9	TERMCLLI	20	2	BINARY	Termination Trkgrp CLLI
10	TERMMEM	22	2	BINARY	Termination Member Number
11	CLGNUM	24	12	TBCD	Calling Number
12	TNSVALUE	36	3	TBCD	TNS Value

Table 3 The structure of CDR

No	Field Name	Offset	Bytes/ Bits	Encoding Type	Field Contents
13	CUSTCOST	39	4	TBCD	Cost Center Account Code
14	BILLTYP	43	1	BINARY	Billing Type
15	DIALNUM	44	12	TBCD	Dialed Number
16	SRVCODE	56	7 bits	BINARY	Service Code
17	TNSSENT	56.7	1 bit	BINARY	TNS Sent
18	ANSWER	57.0	1 bit	BINARY	Answer flag
19	SPARE_1	57.1	7 bits + 1 byte		Spare, with a hex value of 0
20	TRMTCD	59	1	BINARY	Call Treatment Code
21	COMPCD	60	2	BCD	Call Completion Code
22	CLASSMK	62	2	BINARY	IMT ClassMarks
23	CLISAT	64	2	BINARY	CLI Index + Disposition Qualifier + Satellite Indicator
24	SEQNUM	66	4	BINARY	Call Sequence Number
25	NODEID	70	2	BCD	Node Identification
26	DESTNUM	72	12	TBCD	Destination Number
27	SPARE_2	84	3		Spare, with a hex value of 0
28	BILLNUM	87	15	TBCD	Billing Number
29	T_FCI_NUM	102	1	BINARY	Total Number of FCI
30	CCD	103	2	BCD	Carrier Connect Date
31	CCT	105	3	BCD	Carrier Connect Time
32	CustID	108	1 byte + 4 bits	BINARY	Customer Identification Value
33	TTON		4 bits	BINARY	Terminating Type of Number
34	ACCT_EXT	110	5	TBCD	Account Code Extension
35	CPC	115	1	BINARY	Calling Party Category
36	OUTP_NUM	116	12	TBCD	Outpulsed Number
	Total		128		

20.2.2.1 New option “OCN” in table CLICNTL

OCN option is available for incoming direction in table CLICNTL by this feature.The OCN option can be assigned to any CLICTKEY whose direction is incoming, but only when the CLICTKEY with OCN option is assigned to an ANSI ISUP or HK ISUP trunk, the OCN option can work. If the OCN option is assigned to a CLICTKEY whose direction is outgoing, then an error is given. When the OCN option is datafilled with the highest priority for an ISUP trunk, then OCN is captured in CDR. Thus, CLI/RDN/OCN can be captured in CDR according to the datafill in table CLICNTL. As long as these 3 options are datafilled in the proper order, then CLI/RDN/OCN can be captured in CDR following the capture logic. An example of these 3 options datafill is shown in the figure 1.

Figure 2 CLI/RDN/OCN datafill in table CLICNTL

```
TABLE: CLICNTL

CLICTKEY DIRECTN
---------------
NONE IC $ (RDN) (CLI) $ Y

CLI_ONLY IC (CLI) $ (CLI) $ Y

RDN_ONLY IC (RDN) $ (RDN) $ Y

CLI_THEN_RDN IC (CLI) (RDN) $ (SCRN_NUM) $ Y

RDN_THEN_CLI IC (RDN) (CLI) $ (SCRN_NUM) $ Y

RDN_OCN_CLI IC $ (RDN) (OCN) (CLI) $ Y
```

The following is the example of the error message and warning message.

error message: "OCN option cannot be used for outgoing direction!"

In table CLICNTL, BILLING_OPTIONS and OUTPULSE_OPTIONS use the same list of selectors. So the OCN option is also one of the selectors of OUTPULSE_OPTIONS. But OCN option can not be datafilled as a OUTPULSE_OPTIONS because OUTPULSE_OPTIONS is only used for outgoing direction, but OCN option can only be used for incoming direction. The following is the data structure of table CLICNTL.

Figure 3 Data structure of table CLICNTL

```
TABLE: CLICNTL
>ran
 1 CLICTKEY         CLICNTL_KEY
 2 DIRECTN          DIR_OPTION_AREA
LOGICAL TUPLE TYPE: CLICNTL_LOGTUPLE
>ran DIRECTN
 2 DIRECTN          DIR_OPTION_AREA
TYPE IS DIR_OPTION_AREA       MULTIPLE WITH
      DIRECTN              {IC,OG} REFINEMENTS:
      {IC}                 MULTIPLE WITH
         CLISCRN_OPTIONS  VECTOR OF UP TO 16 CLISCRN_OPTION_RANGE'S
         BILLING_OPTIONS  VECTOR OF UP TO 16
                                              BILL_AND_OUTP_OPTION_RANGE
         CLIDELV          {Y,N}
      {OG}                 MULTIPLE WITH
         OUTPULSE_OPTIONS VECTOR OF UP TO 16
                                              BILL_AND_OUTP_OPTION_RANGE
>ddedit
DDE:
>zz BILL_AND_OUTP_OPTION_RANGE
  TYPE BILL_AND_OUTP_OPTION_RANGE       STRING RANGE
      'SCRN_NUM'                        0
      'CLI'                              1
      'RDN'                             2
      'CHARGE'                          3
      'CONTRACTOR'                      4
      'GENERIC_NO'                       5
      'PN'                               7
      'OCN'                             8
  END STRING RANGE
```

20.2.2.2 Capture CLI/RDN/OCN for ANSI ISUP and HK ISUP

On originating side, after receiving the IAM message, this feature puts CLI/ RDN/OCN in existing CLG_NUM field of CDR according to the capture logic. At the same time, set according indicator in the spare bits of the DMS-GSP-specific CDR unit structure.

If receiving the INF message, because only CLI will be contained in INF message, we have to consider the previous IAM message of this call to see if RDN or OCN exist, then capture corresponding number and set indicator in CDR according to the capture logic.

Furthermore, there is no indicator of the content of the CLG_NUM field in the CDR601 log currently. This feature adds a new field named CLGNUM_IND to CDR601 log report to include the corresponding indicator set in CDR, the new field is appended in the end of CDR601 log report. According to the capture logic, "00", "01", "10", "11" is displayed as the content of the indicator. Figure 3 is an example of the new CDR601 log.

Figure 4 CDR601 log example

```
NORTEL    CDR601 SEP20 16:44:09 1700 INFO CDR LONG LOG

        REC_CODE      F0
        TYPE_CALL     1
        INAP_CALL     0
        VPN_CUST      0
        CALL_DUR      00000000
        ORIG_CLLI     0775
        ORIG_MEM      0005
        TERM_CLLI     0774
        TERM_MEM      0005
        CLG_NUM       1066020003
        TNS_VALUE
        CUST_COST
        BILL_TYP      255
        DIAL_NUM      6020024
        SRV_CODE
        TNS_SENT
        ANSWER
        TRMT_CODE     000
        COMPL_CODE    125
        CLASS_SERV    00
        DATA_CALL     0
        PART_NUM      0101
        CLI_INDEX     000
        DISP_QUAL     001
        SATE_IND      0
        SEQ_NUM       00000015
        NODE_ID       000
        DEST_NUM
        BILL_NUM
        T_EXT_NUM     00
        CCD           263
        CCT           60243
        CUST_ID       0000
        TTON          NAT
        ACCT_EXT
        CPC           255
        OUTP_NUM      6020024
        CLGNUM_IND    01
```

20.3 Hardware Requirements or Dependencies

N/A

20.4 Software Requirements or Dependencies

N/A

20.5 Limitations and restrictions

Only ANSI ISUP and HK ISUP GSP trunks are supported in this feature.

20.6 Interactions

N/A.

20.7 Applicable customer facing sections

Fault Management

- Logs ___X___
- Alarms ___N/A___

Configuration

- Data Schema ___X___
- User Interface ___N/A___
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___N/A___

Accounting (includes AMA billing) ___X___

Performance (includes operational measurements) ___N/A___

20.8 Glossary

Term	Description
CDR	Call Detail Record
CLI	Calling Line Identification
GSP	Global Services Platform
IAM	Initial Address Message
IC	Incoming
INF	Information
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
OCN	Original Called Number

Term	Description
OG	Outgoing
RDN	Redirecting Number

20.9 References

1. DMS-Global Services Platform Billing Records Reference Manual, NTP 297-2651-119
2. DMS-GSP Logs Reference Manual Vol . 2 of 6, NTP 297-2651-8402
3. CLI Screening Enhancements for International Applications, A59023556

21: Functional Description (FN): A00002365

21.1 Feature name

"CWR Support over Trunks for Brazil Market"

21.2 Description

This activity adds the support for the Call Waiting Ringback (CWR)[1] service over ETSI ISUP including national variants, SIP-T, IBN7 and R2 trunks for the Brazilian Market.

When a call is made to a subscriber with CWR and Call Waiting Terminating (CWT) enabled, the CWR service provides an indication to the originating line as to the state of the terminating line. If the terminating line is currently engaged in a stable two-port call that is available for call waiting, a distinctive audible ringback is returned to the originating agent. Otherwise standard audible ringback or busy tone is provided.

The CWR feature is already available. A detailed description of the feature CWR is available in the following documents:

- Activity AF1271 (PLS OLDOC3)

This activity focuses on the support for CWR over trunks (ETSI ISUP including national variants, SIP-T, IBN7 and R2) for both TDM and CS2K. This feature enables the support of CWR over trunks if the CWR option is set for the specific trunk types in table ISERVOPT.

As an additional part, a CWR deactivation utility is provided for specific trunk groups. This option provides the possibility to exclude specific trunk groups from the support of CWR.

21.2.1 CWR Option in Table ISERVOPT

In table ISERVOPT a new option (CWR_ON_TRUNK) is introduced to support CWR over specific trunk types. The CWR_ON_TRUNK option contains the following trunk types:

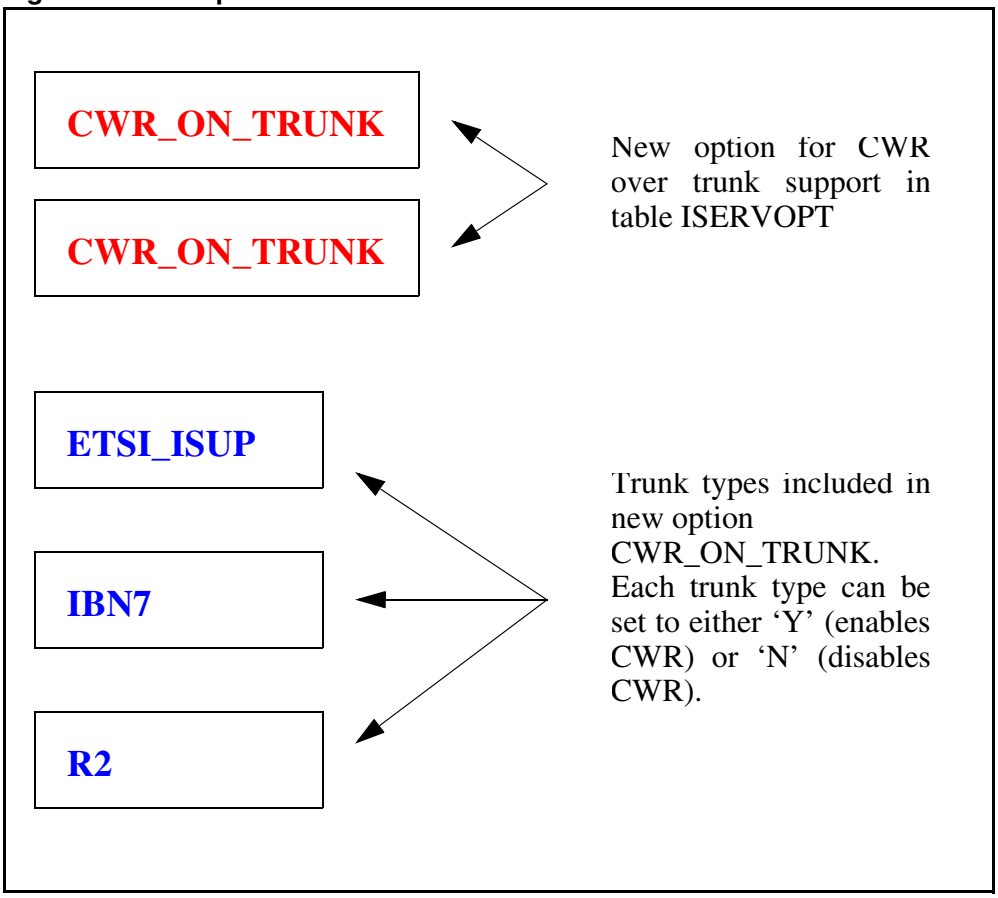
- ETSI_ISUP
- IBN7
- R2

If CWR is desired for a trunk type the corresponding trunk type in option CWR_ON_TRUNK needs to be set to 'Y'. All the trunks groups that belong

[1]GVT Anatel 252 Compliance

to a trunk type listed above will support CWR as soon as the trunk type is set to ‘Y’ in table ISERVOPT. Figure 1 shows the structure of the new option CWR_ON_TRUNK.

Figure 1 New Option in Table ISERVOPT



21.2.1.1 CWR Activation for Trunk Type

The standard audible ringback is the default tone for CWR over trunk that is provided to the originating party. The new option CWR_ON_TRUNK needs to be added in table ISERVOPT to allow distinctive audible ringback (CWR tone) for a trunk type. Every trunk type can be set to either ‘Y’ or ‘N’ individually. The trunk type in option CWR_ON_TRUNK is set to ‘Y’ if the activation of CWR over this trunk type is desired. Figure 2 shows an example on how the option CWR_ON_TRUNK is added and activated for the trunk types ETSI_ISUP and R2 in table ISERVOPT.

Figure 2 Example for Adding and Activating CWR_ON_TRUNK

```
>table iservopt
>pos cwr_on_trunk
TUPLE NOT FOUND
>add cwr_on_trunk
>y
OPTION:
>cwr_on_trunk
ETSI_ISUP:
>y
IBN7:
>n
R2:
>y
TUPLE TO BE ADDED:
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y N Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y N Y
>
```

The following Figure 3 shows an example of how to change the content of the existing option CWR_ON_TRUNK. The trunk type IBN7 will be enabled for CWR over trunk.

Figure 3 Example for Changing Option CWR_ON_TRUNK

```
>table iservopt
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y N Y
>cha
>y
OPTION: CWR_ON_TRUNK
>
ETSI_ISUP: Y
>
IBN7: N
>y
R2: Y
>
TUPLE TO BE CHANGED:
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y Y
>
```

21.2.1.2 CWR Deactivation for Trunk Type

The option CWR_ON_TRUNK controls the settings for the trunk types ETSI_ISUP, IBN7 and R2. Each trunk type is considered individually, therefore it is possible to enable or disable CWR over trunk for each trunk type. If the deactivation of CWR over trunk is desired, the corresponding trunk type is set to ‘N’ in option CWR_ON_TRUNK.
There are two possibilities to disable CWR over trunk for the trunk type:

- Change the setting for a trunk type from ‘Y’ to ‘N’:
  In this case only the trunk type that does not require the CWR over trunk ability is disabled. The option CWR_ON_TRUNK remains in table ISERVOPT. The deactivation of a trunk type is shown in Figure 4.

Figure 4 Deactivation of a Trunk Type

```
>table iservopt
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y Y
>cha
>y
OPTION: CWR_ON_TRUNK
>
ETSI_ISUP: Y
>
IBN7: Y
>
R2: Y
>n
TUPLE TO BE CHANGED:
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y N
>
```

- Remove the option CWR_ON_TRUNK from table ISERVOPT:
  The CWR over trunk ability is disabled for all the trunk types in option CWR_ON_TRUNK if the option is deleted in table ISERVOPT. The deletion of the CWR option is shown in Figure 5.

Figure 5 Deletion of Option CWR_ON_TRUNK

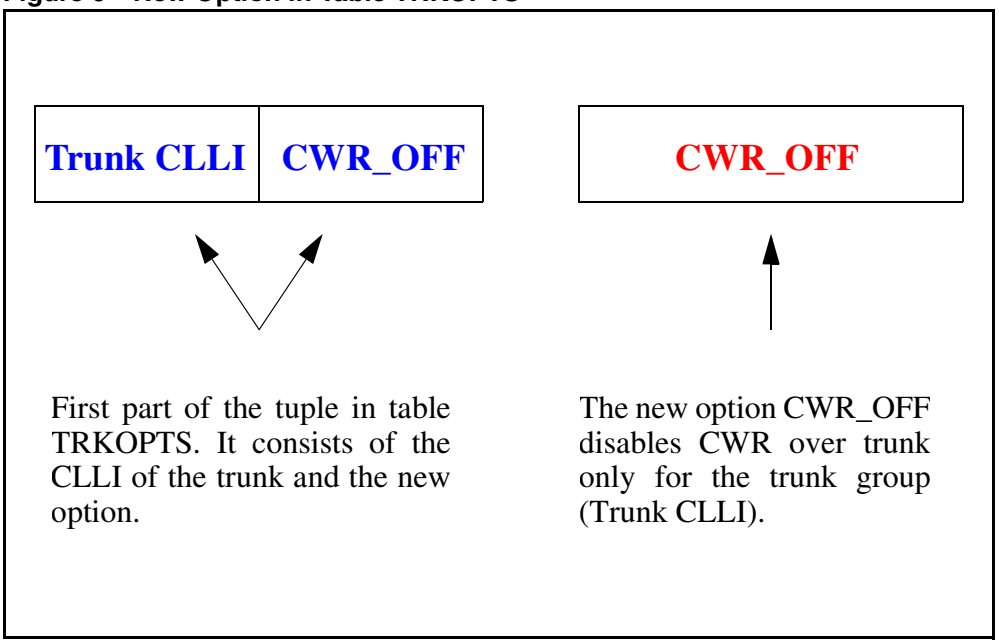
```
>table iservopt
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y N
>del
>y
TUPLE TO BE DELETED:
        CWR_ON_TRUNK
                                        CWR_ON_TRUNK Y Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE DELETED
>pos cwr_on_trunk
TUPLE NOT FOUND
>
```

21.2.2 CWR_OFF Option in Table TRKOPTS

The option CWR_ON_TRUNK in table ISERVOPT enables CWR over trunk for the trunk type including all the trunk groups of this trunk type. The new option CWR_OFF in table TRKOPTS provides the possibility to disable CWR over trunk for a specific trunk group without the need of disabling the whole trunk type.

If the CWR_OFF option is assigned to a trunk group in table TRKOPTS the CWR over trunk ability is disabled for the trunk group even if the trunk type is enabled for CWR in option CWR_ON_TRUNK. The option CWR_OFF is independent of the settings in option CWR_ON_TRUNK in table ISERVOPT. Figure 6 shows the structure of the new option in table TRKOPTS.

Figure 6 New Option in Table TRKOPTS



21.2.2.1 Deactivation of CWR for Specific Trunk Group

The new option CWR_OFF is assigned to the trunk group in table TRKOPTS to disable CWR over trunk only for this trunk group. An example of assigning the new option to a trunk group is shown in Figure 7.

Figure 7 Deactivate CWR for Specific Trunk Group

```
>table trkopts
>add rua501isupv2lp cwr_off
>y
OPTION:
>cwr_off
TUPLE TO BE ADDED:
 RUA501ISUPV2LP        CWR_OFF
                                    CWR_OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>pos rua501isupv2lp cwr_off
 RUA501ISUPV2LP        CWR_OFF
                                    CWR_OFF
>
```

The CWR_OFF option in table TRKOPTS disables CWR over trunk for the specific trunk group independent from the settings of option CWR_ON_TRUNK in table ISERVOPT.

If the CWR_OFF option is removed from a trunk group the settings in option CWR_ON_TRUNK are considered again for CWR over trunk ability. The Figure 8 shows how the CWR_OFF option is removed from a trunk.

Figure 8 Remove CWR_OFF from Trunk Group

```
>table trkopts
>pos rua501isupv2lp cwr_off
 RUA501ISUPV2LP        CWR_OFF
                                          CWR_OFF
>del rua501isupv2lp cwr_off cwr_off
>y
TUPLE TO BE DELETED:
RUA501ISUPV2LP        CWR_OFF
                                          CWR_OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE DELETED
>pos rua501isupv2lp cwr_off
TUPLE NOT FOUND
>
```

Note:
There is no explicit relationship or dependency between the settings in table ISERVOPT and TRKOPTS. It is possible to assign the CWR_OFF option to a trunk group even if the trunk type of the trunk group is disabled in option CWR_ON_TRUNK.

21.3 Hardware Requirements or Dependencies

N/A - Refer to “21.5 Limitations and restrictions”

21.4 Software Requirements or Dependencies

N/A - Refer to “21.5 Limitations and restrictions”

21.5 Limitations and restrictions

21.5.1 TDM Trunks

This activity instructs the PDTC to play distinctive audible ringback (CWR tone) to the originating party. The PDTC must be capable of providing the CWR tone.
The Brazilian toneset, e.g. on the PDTC, supports the CWR tone.

21.5.2 Succession Trunks

This activity instructs the trunk gateway to play distinctive audible ringback (CWR tone) to the originating party. The gateway must be capable of providing the CWR tone.

21.5.2.1 SIP-T Trunks

SIP-T trunks require an APG in order to play distinctive audible ringback (CWR tone) to the originating party. The APG must be capable of providing the CWR tone.

21.6 Interactions

The interactions are unchanged.
Please refer to Activity AF1271 (PLS OLDOC3)

21.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

21.8 Glossary

Term	Description
APG	Anchor Packet Gateway
CLLI	Common Language Location Identifier
CS2K	Call Server 2000
CWR	Call Waiting Ringback
CWT	Call Waiting Terminating
ETSI	European Telecommunications Standards Institute
IBN7	Integrated Business Network CCS7
ISUP	ISDN User Part
PDTC	PCM-30 Digital Trunk Controller
R2	Regional No.2
SIP-T	Session Initiation Protocol for Telephony
TDM	Time Division Multiplexing

21.9 Appendix

The following Table 1 shows an abstract of the translation of “GVT Anatel 252 Compliance”. It contains the characteritics of the CWT and CWR signals.

Table 1 Abstract of GVT Anatel 252 Compliance

Signal Identification	Visual Form	Audible Form				
		Periods, Continuous				Frequency
		Presence	Absence	Presence	Absence	
Call Waiting Alerting Signal	Calling	60 +- 06 ms	250 +- 25 ms	60 +- 06 ms	9000 +- 900 ms	425 +- 25 Hz
Call Waiting Alerting Control Signal	Waiting	400 +- 40 ms	5000 +- 500 ms	400 +- 40 ms	5000 +- 500 ms	425 +- 25 Hz

22: Functional Description (FN): A00002367

22.1 Feature name

A00002367 - BRI Preset Conference Base

22.2 Description

This activity allows an ETSI BRI (p-to-mp) station or ETSI ISUP V2 trunk to set up a preset conference with up to 35 conferees by dialling a specific directory number. This invokes simultaneous ringing of preselected conference members. The originator of a preset conference (served user) which has AFC & HOLD line options, is able to addon additional local conferees once the conference is established.

This activity is based on the existing IBN Preset Conference and uses same datafill requirements and restrictions for IBN Preset conference. See the appendix A- section for IBN preset conference background.

In additional, this feature also provides supporting IEs related to CGN, GAP, MLPP, UUI to be sent to conferees.

22.2.1 Preset Conference Call establishment and termination

22.2.1.1 Preconditions

The datafill of existing IBN preset preconf table PRECONF meets the BRI preset Conference requirements.
According to the requirements of spec ‘SIM : PRCONF_BRI issue3’ related to conference call establish , addon functionality and takedown process, the existing table PRECONF should be datafilled as follows:

- BRI Preset Conference should be datafilled to be allowed for the customer group. And the preset conference originator (served user) is a member of the preset conference’s customer group. Conferees does not need to belong to the same customer group.
- ADDON bool must be set to ‘yes’ in the existing table PRECONF. Only originator can add on conferees.
- In order to enable addon functionality, line options AFC and HOLD should be assigned to preset conference originator via Servord first.
- The conferees are specified in advance in a data table. According to the existing feature AF2014 -Preset conference (large), already allows 50

conferee numbers can be assigned to each preset conference DN (Directory Number). In other words, the preset conference can have up to 50 conferees. This includes the originator, all preset conferees and all add on conferees.

- Maximum 64 preset conference DN can be datafilled per office.
- The preset conference may be datafilled upto 14 digits and conferee numbers may be a string of up to 30 digits
- It is required that when the first conferee answers, the conference begins. In order to provide this functionality, the field IMMSTART of PRECONF should be datafilled as ‘yes’
- The field ORIGCONT should be set to ’yes’ to allow that the served user is in control of the conference. when he goes on-hook, the conference is taken down even if there are conferees still on the bridge.
- Associated with each conferee DN will be timeout interval of 15 to 60 seconds and an optional one alternate DN. If the conferee does not answer within the timeout interval, the call attempt ends. But if an alternate DN is datafilled, two call attempts are made on primary address with no answer, then the call is routed to alternate address. Two call attempts will be also directed to the alternate address

22.2.1.1.1 Example of BRI Preset Conference

The table 1 gives the example of BRI preset conference datafill. In this datafill example;

a. 7835599 is the predefined preset conference DN. The customer group of the originator should be ‘CONF6C’ option in the table CUSTENG to be activated conference. Up to 64 preset conference DN can be datafilled in the table PRECONF.

b. 7831016 and 7831002 are the conferees for preset conference DN by index 0. 35 conferees can be datafilled for preset conference DN (7835599).First conferee has the alternate address. Second conferee has no alternate address. The timeouts interval is 15 seconds for both conferees and its alternate address.

-If the conferee 7831002 does not answer within the timeout interval , the call attempt ends.

-If the conferee 7831016 does not answer within two trials, two call attempts will be directed to alternate address.

For the more details datafill for PRECONF table , Please see appendix - A.

Table 1 PRECONF Datafill example

PCNFKEY CONFADDR PCNFVAR OPTIONS
0 0 1027835599 D IBN CUST783A 0 Y N Y N N N $
0 1 7831016 A 7831003 15 $
0 2 7831002 C 15 $

Table 2 CUSTENG datafill example

CUSTNAME ADNUM NONCOS NOIBNTMT CONSOLES DOMAIN GROUPID
CUST783A 22 256 63 Y PRIVATE 105 (CONF6C 12)$

22.2.1.2 Preset conference initiation

A served user initiates one preset conference (PRCONF) by dialling a predefined DN, which is associated with conference. The directory number is recognized as a request for a preset conference. Translations check the originator's data against the data of preset conference DN. A check is made if required number of six-port conference bridges can be seized for the conference and the conference is not already in use .If call is valid, the originator will hear audible ringing while calls are originated to all the addresses stored for the desired preset conference. If invalid, the originator will be routed to treatment.

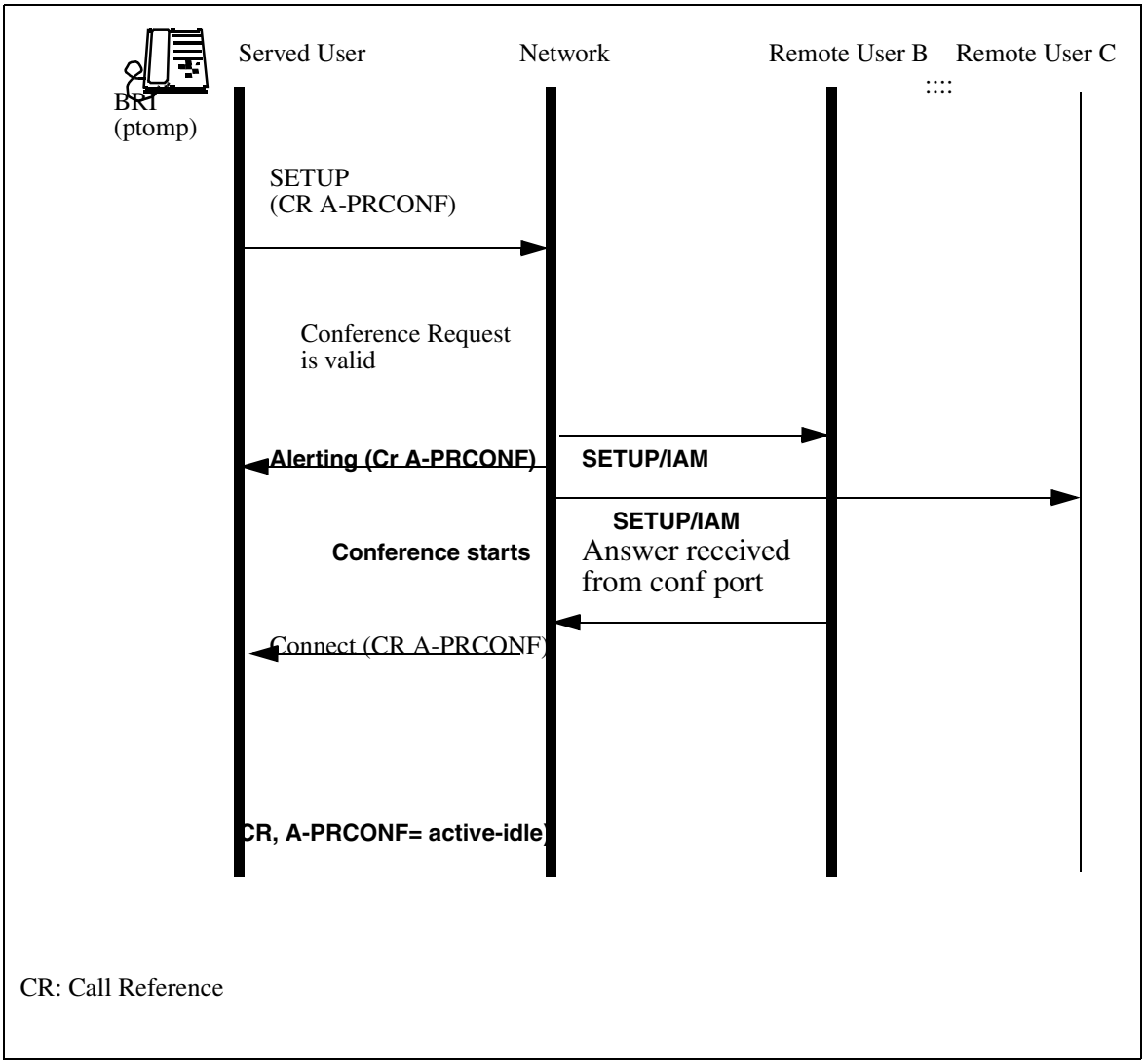
Dialling PRCONF DN invokes simultaneous ringing of the preselected conference members.

There could be more than one served user for a conference, when an attempt is made to originate a conference which has already been initiated, the second served user will be routed to busy tone.

The served user's directory number (DN) can be part of preset conference list of numbers. But originator can not be called as conferee for this preset conference. In other words, if the originator is a predefined preset conferee, we do not call this conferee unless the call is over trunk call.

The conference starts as soon as the first conferee answers (IMMSTART = Y in PRECONF). In this case , the answer will cause the audible ringing to the originator to stop and the conference to begin. Attempts to complete the calls to unanswered conferees will continue, with no audible ringing to originator.

Figure 1 Preset Conference Initiation



22.2.1.3 Add-on functionality

The originator of a preset conference can add on conferees as local call, once the preset conference is established. In order to provide this functionality , the field ADDON of the table PRECONF should be set to ‘yes’ and line options AFC and HOLD. Once the maximum number of conferees is reached , no more conferees may be added.The addon functionality is based on the existing ETSI BRI 6-part conference

22.2.1.3.1 Coding Requirements for DSS1

All components (invoke, return result, return error and reject) is included within a Facility information element. Facility information element can be

conveyed in any appropriate message.Setup, Connect, Facility and Disconnect messages are used within this specification.

Figure 2 ETSI -Q.931 FACILITY Information Element (FIE) with a Service Component embedded.

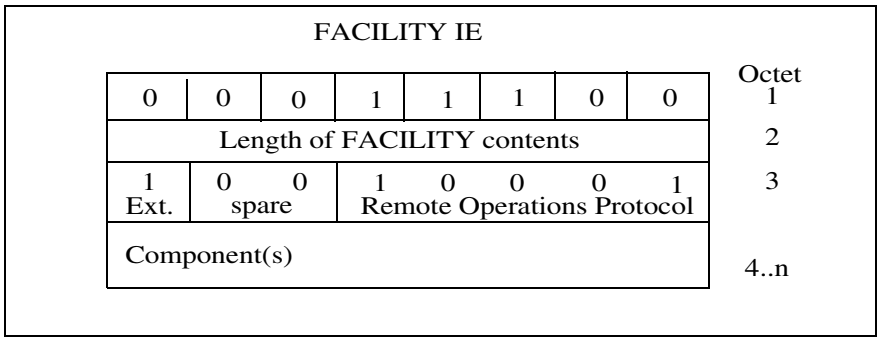


Table-1 shows the definition of the operations and errors required for the addon functionality of ETSI BRI preset conference ,using ASN.1.

Table 3 Definition of Operations and Errors for PRCONF

```
Conference-Add-On-Operations { ccitt identified organization etsi (0) 185
operations - and- types (1) }

DEFINITIONS EXPLICIT TAGS::=
BEGIN

EXPORTS              BeginCONF, AddCONF,

                     IllConferenceId, NumberOfPartiesExceeded,
                     NotAllowed, PartyId, ConferenceId, ConfSize;

IMPORTS              OPERATION,
                     ERROR
                     FROM Remote-Operation-Notation
                              { joint-iso-ccitt remote- operations(4) notation(0) }


                     notAvailable,
                     invalidCallState,
                     supplementaryServiceInteractionNotAllowed
                     FROM General-Error-List
                      { ccitt identified organization etsi (0) 196 general-errors (2)};

BeginCONF(40)::=     OPERATION
                     ARGUMENT          ConfSize--optional
                     RESULT            SEQUENCE {
                                              ConferenceId,
                                               PartyId OPTIONAL }
                     ERRORS            { notAvailable,
                                       supplemntaryServiceInteractionNotAllow,
                                        invalidCallState }

 AddConf(41)::=      OPERATION
                     ARGUMENT          ConferenceId
                     RESULT            PartyId
                     ERRORS            { IllConferenceId,
                                       NumberOfPartiesExceeded,
                                       NotAllowed,
                                    supplementaryServiceInteractionNotAllowed,
                                       InvalidCallState }


   IllConferenceID(28)::=ERROR
   NumberOfPartiesExceeded(30) ::=ERROR
   Notallowed(32)::=ERROR

     PartyId, ConferenceID,ConfSize ::=INTEGER(0..127)
```

The served user sends a Facility message with the call reference of the existing call and a facility information element including beginCONF-invoke component.This component may contain a ConfSize parameter, if not the conference size sets to a network dependent value by the network. The beginCONF-return-result component sent to the user includes a ConferenceId and a PartyId parameter which is used to identify the remote user.

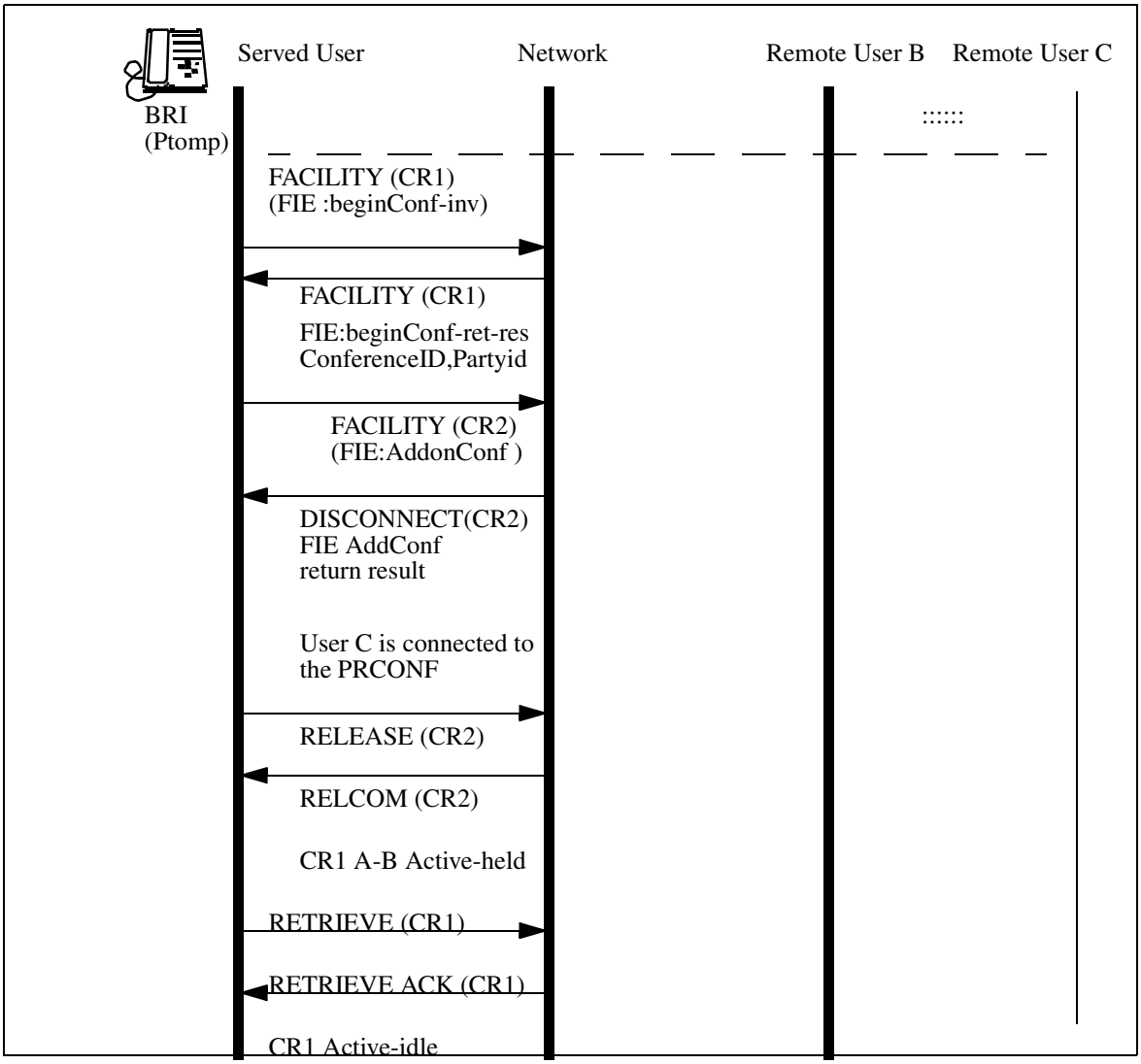
To add a new party, the connection to the conference bridge can be either in the (Active,Idle) state or in the (Active,Held) state and the connection to the party to be added can either be in (Active, Idle) state or in the (Active, Held) state. Which means that one of the connections should be held and other should be in (active, idle) state. A Facility message with the call reference of the call to be added and an Add-CONF-invoke component including conferenceId parameter is sent by the user to the network. Then the network sends a DISCONNECT message with AddCONF-return-result component including PartyId parameter which identifies the added party.

CRx, CRy: Call Reference used-
A-B :call between user A and PRCONF
A-C :call between user A and user C
FIE:Facility information element

CR1, A-B (Active, Held)

CR2, A-C(Active, Idle)

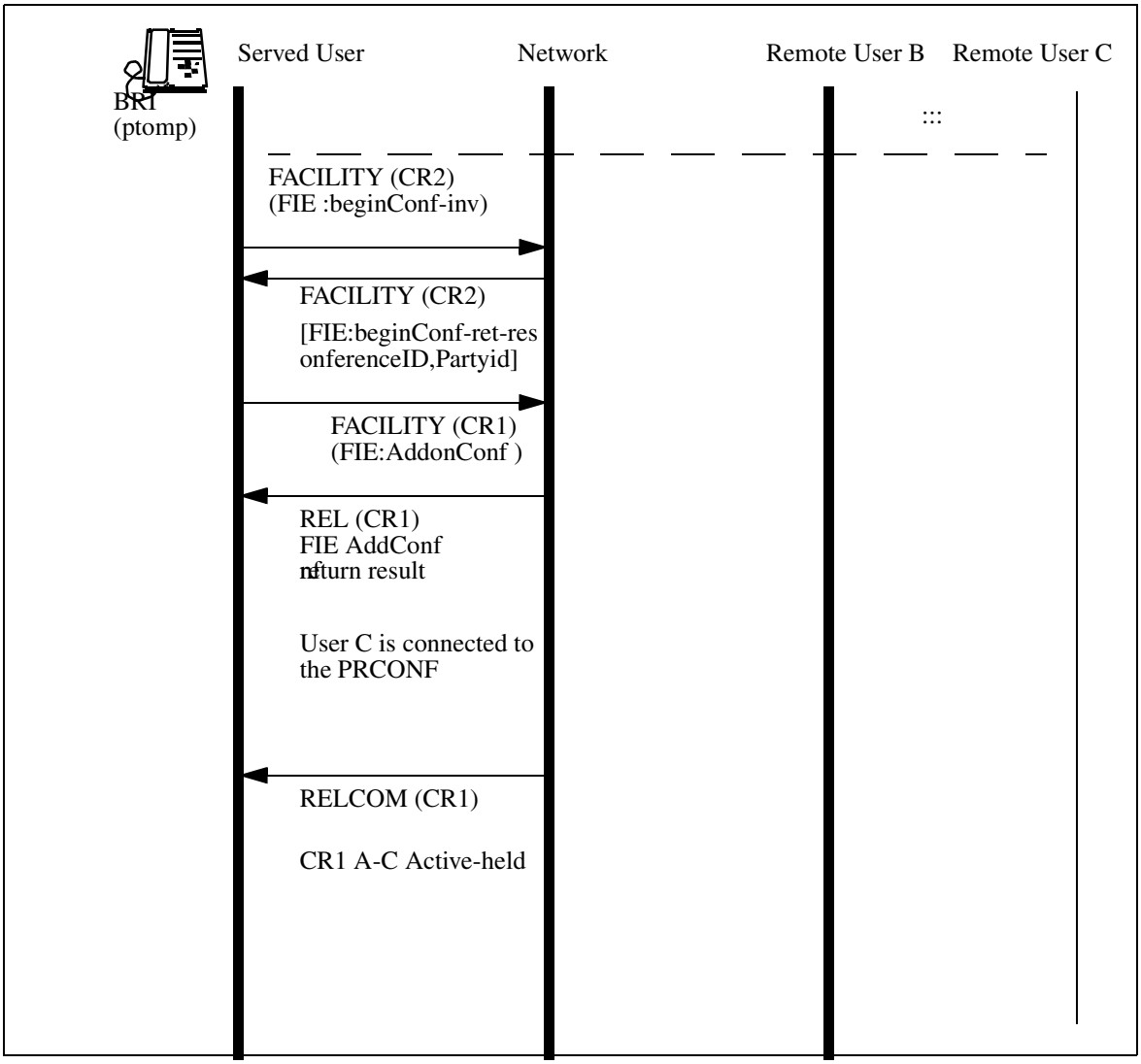
Figure 3 Addon conferee, when preset conference is in held state



CR1, A-C (active-held)

CR2, A-B (active, idle)

Figure 4 Addon conferee, when preset conference is active



22.2.1.4 Unsuccessful cases

Figure 5 Network receives a BeginCONF-inv in a state other then Active(N10)

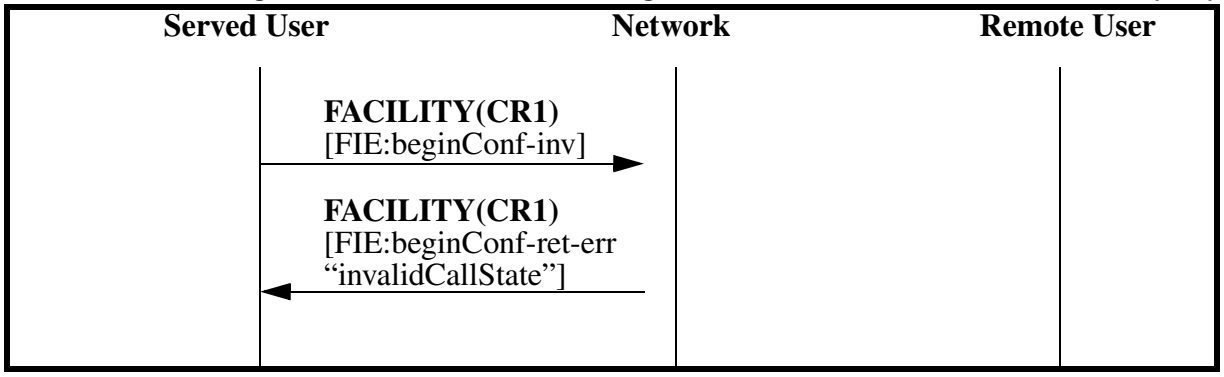


Figure 6 Adding a party which causes interworking restriction violations

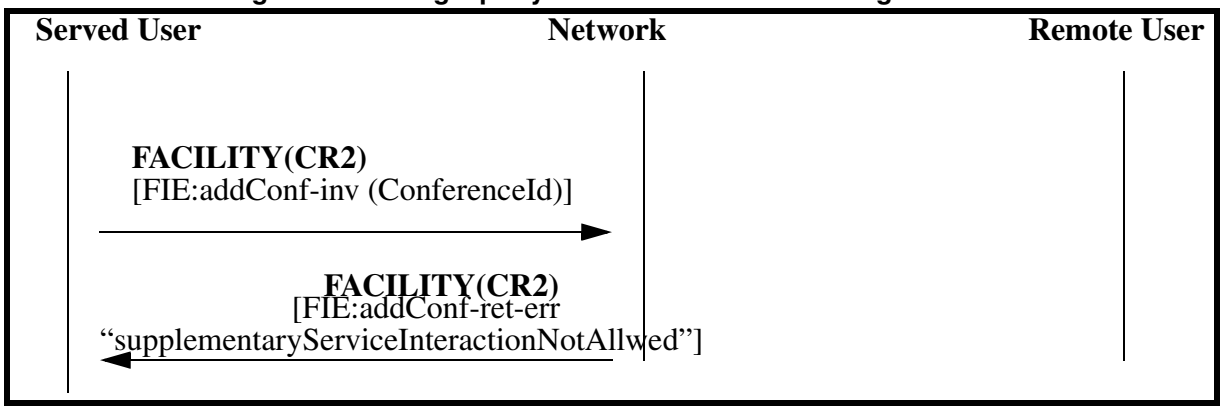


Figure 7 Served user indicates an inappropriate bearer capability.

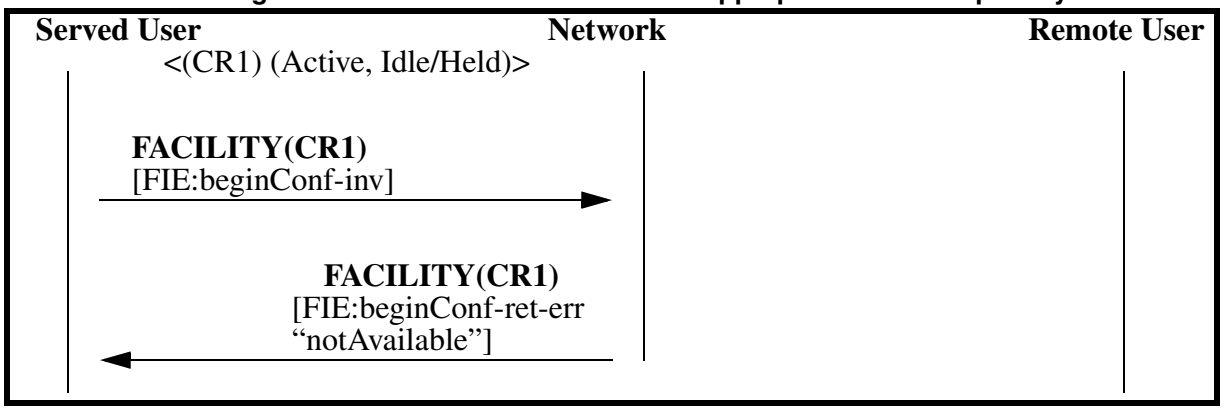


Figure 8 ConferenceId used is not associated with a conference known to the network

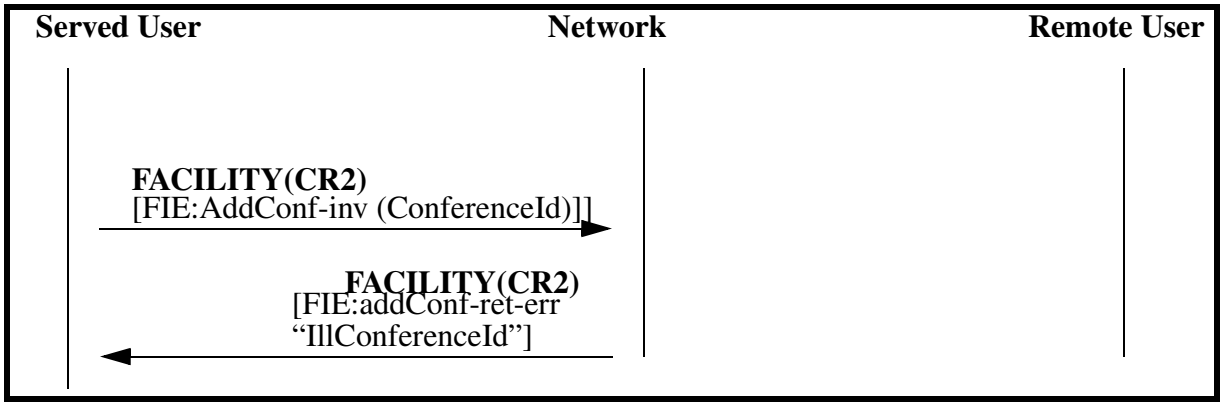
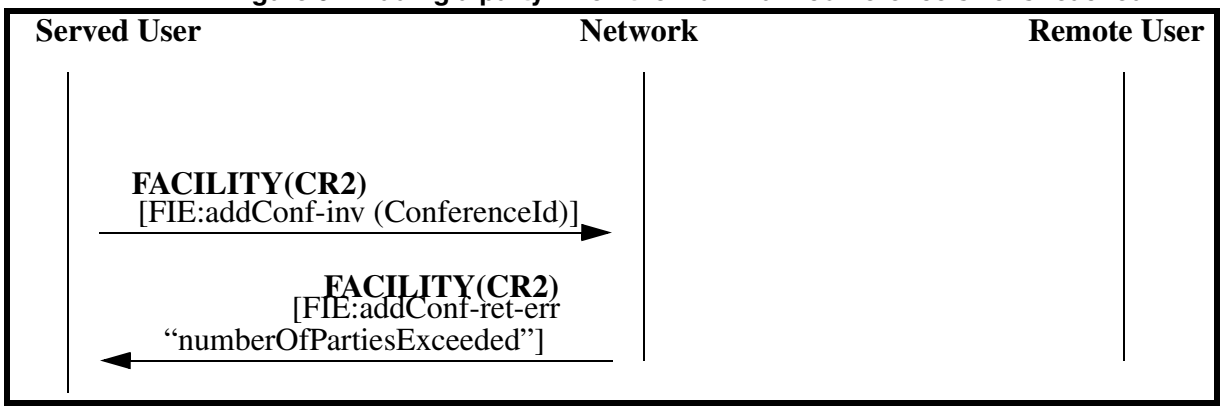


Figure 9 Adding a party when the maximum conference size is reached



22.2.1.4.1 BRI Facility information Element formats

Table 4 BEGINCONFinvoke

Hex Value	Description
1C	Facility
0B	Facility Length
91	Supplementary Service Spare
A1	Invoke Operation
09 (depending on the length of invoke identifier field)	Invoke Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
A unique identifier for the identifier	Invoke Identifier

Table 4 BEGINCONFinvoke

02 - Universal Integer	Operation Tag
01	Operation Length
28 - BCONF	Operation Identifier
02 - Universal Integer	Parameters Tag
01	Parameters Length
05	Parameters identifier (ConSIze) optional

Return Result component of the BEGINCONF operation is sent by the network to the terminal to inform the terminal .

Table 5 BEGINCONF Request.ReturnResult

Hex Value	**Description**
1C	Facility
11	Facility Length
91	Supplementary Service Spare
A2	Return Result Operation
0E (depending on the length of invoke identifier field)	Return Result Length
02 - Universal Integer	Invoke ID Tag
01 (depending on the length of invoke identifier field)	Invoke ID Length
Invoke identifier from the previous BEGINCONF FAC IE Invoke component	Invoke ID
30 - Universal Sequence	Opcode and Param Tag
09	Sequence Length
02 - Universal Integer	--- Opcode Tag
01	--- Opcode Length
28 -BCONF	--- Opcode
02 - Universal Integer	--- Parameter Tag
01	--- Parameter Length

Table 5 BEGINCONF Request.ReturnResult

00 -Conference id-	--- Parameter Identifier
02 - Universal Integer	--- Parameter Tag
01	--- Parameter Length
7F Partyid (optional)	--- Parameter Identifier

Return Error component of the BEGINCONF operation is sent by the network to the terminal to inform the terminal about any problems.

Table 6 BEGINCONF .ReturnError

Hex Value	Description
1C	Facility
09	Facility Length
91	Supplementary Service Spare
A3	Return Error Operation
06	Return Error Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
Invoke identifier from the previous BEGINCONF FAC IE Invoke component	Invoke ID
02 - Universal Integer	Error Value Tag
01	Error Value Length
NotSubscribed Not available invalid callstate	Error Value

Invoke component of the ADDCONF operation is sent by the network to the terminal

Table 7 ADDCONF.Invoke

Hex Value	Description
1C	Facility
0B	Facility Length
91	Supplementary Service Spare
A1	Invoke Operation
09	Invoke Length

Table 7 ADDCONF.Invoke

02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
A unique identifier for the operation	Invoke Identifier
02 - Universal Integer	Operation Tag
01	Operation Length
29 -ADDCONF	Operation Identifier
02 - Universal integer	Parameters Tag
01	Parameters Length
01 -Confid	Parameters Identifier

Return Result component of the ADDCONF operation is sent by the network to the terminal in DISCONNECT messageto inform the terminal about the result of the ADDCONF service invocation.

Table 8 ADDCONF Request.ReturnResult in DISC message

Hex Value	**Description**
1C	Facility
F	Facility Length
91	Supplementary Service Spare
A2	Return Result Operation
0C	Return Result Length
02 - Universal Integer	Invoke ID Tag
01 (depending on the length of invoke identifier field)	Invoke ID Length
Invoke identifier from the previous ADDCONF FAC IE Invoke component	Invoke ID
30 - Universal Sequence	Opcode and Param Tag
07	Sequence Length
02 - Universal Integer	--- Opcode Tag
01	--- Opcode Length
29 -ADDCONF	--- Opcode

Table 8 ADDCONF Request.ReturnResult in DISC message

02 - Universal Integer	--- Parameter Tag
02	--- Parameter Length
00 Party iid-	--- Parameter Identifier
08 -party id	

Return Error component of the ADDCONF operation is sent by the network to the terminal to inform the terminal about any problems.

Table 9 ADDCONF .ReturnError

Hex Value	Description
1C	Facility
09	Facility Length
91	Supplementary Service Spare
A3	Return Error Operation
06	Return Error Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
Invoke identifier from the previous ADDCONF FAC IE Invoke component	Invoke ID
02 - Universal Integer	Error Value Tag
01	Error Value Length
Number of parties exceeded Not allowed supplementary serviceinteraction notallowed invalid callstate	Error Value

22.2.1.5 Preset Call Termination

According to the datafill (ORIGCONT field is set to yes) , the originator is in control of conference. In this case when he goes on-hook, the conference is taken down, even if there are conferees are still on the bridge.

22.2.2 Supporting Information Elements

If information elements (IEs) explained below, is preset in the SETUP message which is sent by originator of preset conference, it is required that these IEs are included in SETUP/IAM messages to all conferees.

The following IEs are supported by this activity:

1 Calling Number (CGN) IE

2 Generic Address Parameter (GAP) IE

> **Note:** NOSCREEN should be datafilled for origination in LTDEF table. And CGN IE should be exist in SETUP message sent by originator.

3 Multi Level Precedence Preemption (MLPP) IE

4 User to User Implicit (UUI) IE

Mapping of the IEs to conferees are supported for the following interworkings:

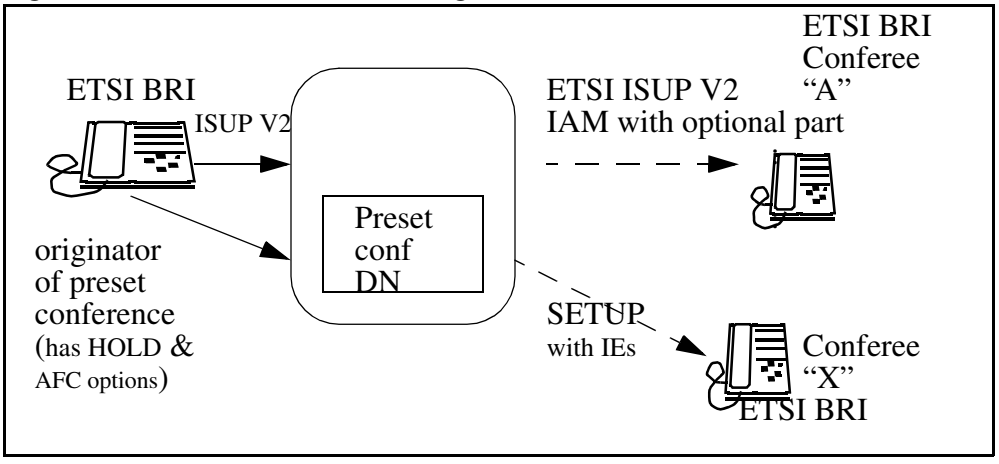
— ETSI BRI(ptomp)-CONF port- ETSI BRI(ptomp),

— ETSI BRI(ptomp)- CONF port-ETSI ISUP V2,

— ETSI ISUP V2-CONF port- ETSI BRI (ptomp) ,

— ETSI ISUP V2-CONF port-ETSI ISUP V2

Figure 10 Functional Behavior Diagram



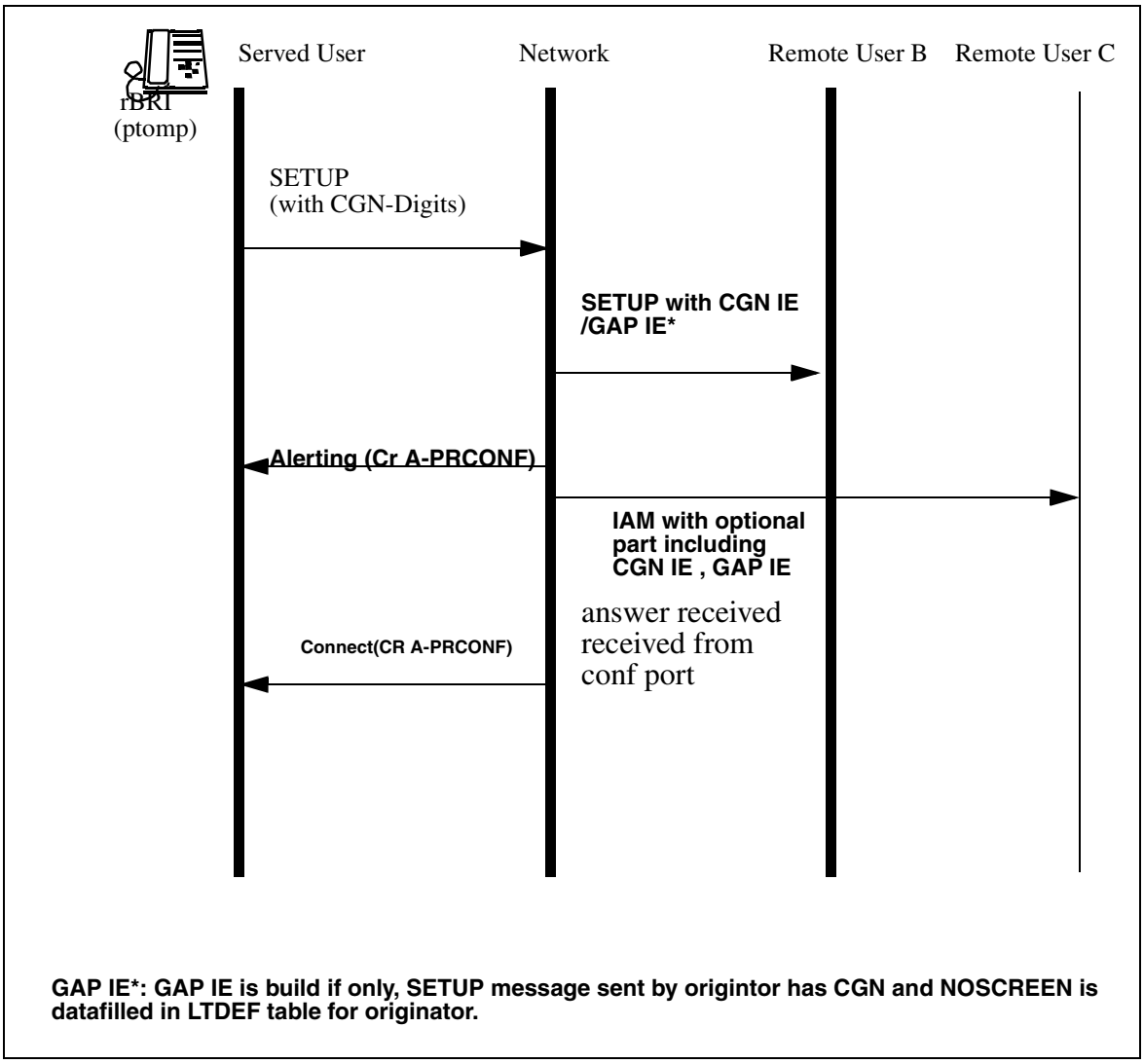
22.2.2.1 CGN IE and GAP IE

The purpose of the calling party number information element is to identify the origin of a call.This information element may be present in the SETUP

message transmitted by the originator to network and in the SETUP message transmitted by the network to conferees. Calling party number field in the SETUP message which is sent from originator may be either actual network number or presentation number (GAP IE is available when NOSCREEN datafill is entered) that the originator wishes to display .In other word, the user is allowed to send any CGN to the switch and the switch does not screen this CGN and does not override it with the provisioned DN. (NOSCREEN datafill is not required for incoming ISUP)

According to spec SIM.PRCONF_BRI issue3, It is required that CGN IE sent by originator (in the SETUP) and GAP IE are sent to all conferees in the SETUP/IAM messages

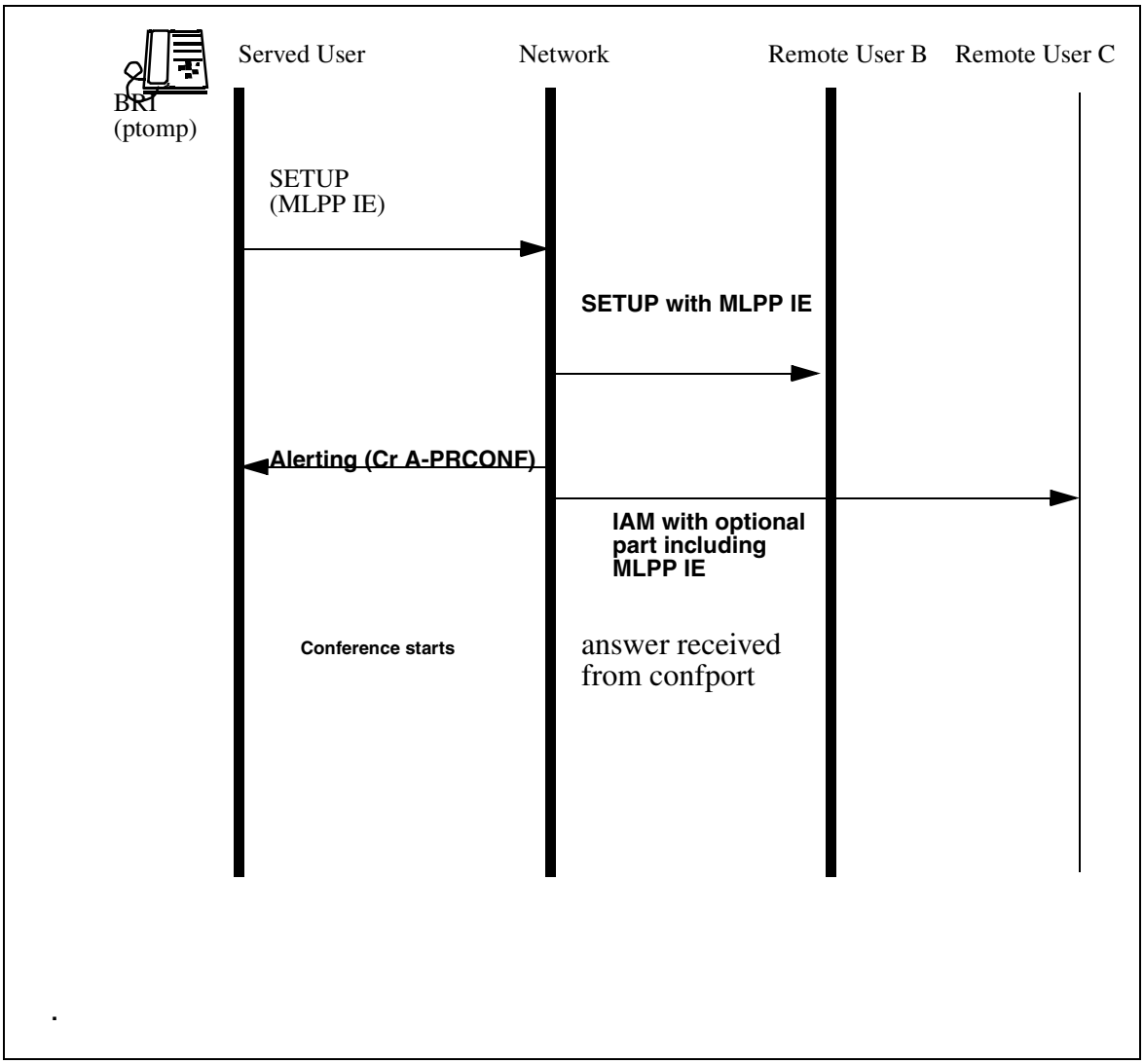
Figure 11 Mapping CGN IE/GAP IE



22.2.2.2 MLPP IE

The MLPP IE may be present in the SETUP message sent by origination which has MLPP line option to network. It is required that in the SETUP/IAM messages sent by network to conferees should includes MLPP IE, if originator has MLPP

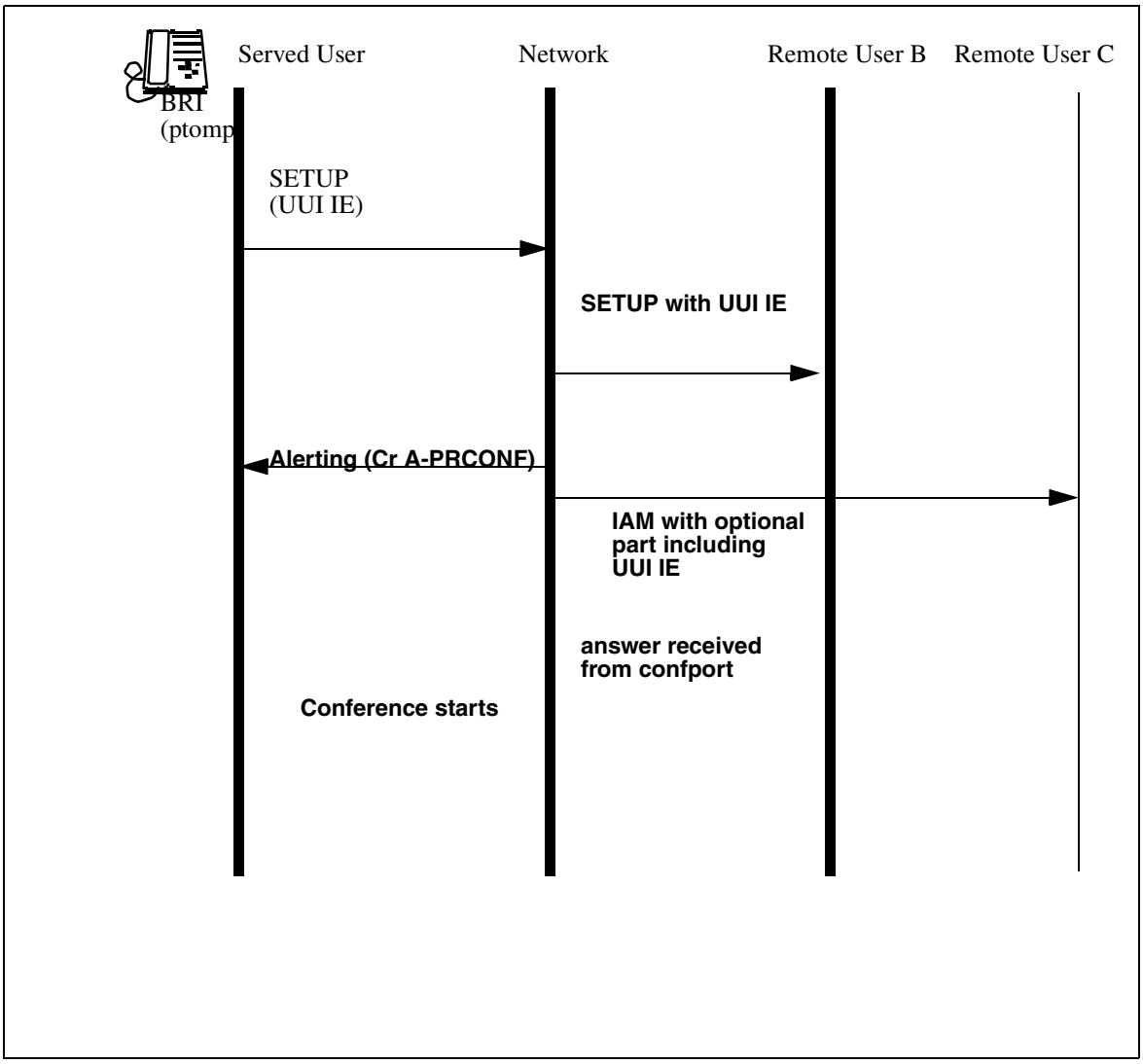
Figure 12 Mapping MLPP IE



22.2.2.3 UUI IE

Only User to User implicit IE will be propagated to conferees , if originator sends SETUP message with UUI IE.

Figure 13)Mapping UUI IE



22.2.3 OM class for Preset Conference

Since this activity is based on the existing IBN preset conference , the existing OM class PCNF is used.

22.2.4 Billing

No AMA/Billing changes for this activity.

22.3 Hardware Requirements or Dependencies

The NT3X67 six-party conference card provides conference facilities on a single card for use with DMS-100 switches. This activity uses same hardware as IBN Preset Conference.

22.4 Software Requirements or Dependencies

The existing IBN preset Conference is used by this activity.

22.5 Limitations and restrictions

Since the feature is based on the existing IBN Preset Conference , the restrictions of IBN preset conference are also valid for this activity.

Only Local calls can be add-on to conference.

The originator of Preset Conference can not start another preset conference.

The call attempts end to a conferee when it is unplugged.

Recommended datafill explained in this FN , should be provided for required functionality

- Served user is in the control of conference (ORIGCONT field is set to yes)
- When the first conferee answers, the conference begins (IMMSTART field is set to yes)
- In order to enable the addon functionality , ADDON field is set to yes.
- 35 conferee can be datafilled in PRECONF.

This activity is implemented for the following interworkings only, the rest of the interworkings are out of scope of this feature:

— ETSI BRI(ptomp)-CONF port- ETSI BRI(ptomp),

— ETSI BRI(ptomp)- CONF port-ETSI ISUP V2,

— ETSI ISUP V2-CONF port- ETSI BRI (ptomp) ,

— ETSI ISUP V2-CONF port-ETSI ISUP V2

22.6 Interactions

Calling Line Identification Presentation/Presentation Restriction

This activity only supports CGN IE to be sent to the conferees in the terminating message. For Special Arrangement (no screening option), if required datafill exists, GAP IE is sent to conferees.

User to User Signalling

This activity only provides UUI IE in setup message to conferees.UUS1 explicit is ignored. But if the originator requests in the FAC IE of the SETUP message that UUS1 is required and the terminator does not accept it, the call should be released according to the UUS1 ETSI spec.

MLPP

The served user provides MLPP information, the same MLPP Information is included into call setup to conferees.

For all feature interactions please refer to the activity A00002884 -'ETSI BRI Preset Conference service interactions'.

22.7 Applicable customer facing sections

Fault Management	
Logs	no
Alarms	no
Configuration	
Data Schema	n/a
User Interface	n/a
Element Management	n/a
Security	n/a
Service Order	n/a
Office Parameters	n/a
Accounting (includes AMA billing)	n/a
Performance (includes operational measurements)	n/a

22.8 Glossary

Term	Description
BRI	Basic Rate Interface
CGN	CallinG Number
MLPP	Multi Level Precedence Preemption
UUI	User to User implicit

22.9 Appendix A- IBN Preset Conference background

The originator (conference controller / served user) dials the predefined DN(specified in table PRECONF) to start the Preset Conference. One the DN is dialled, the preset conference feature will try to connect to all of the pre-selected conference members simultaneously.Audible ringing is provided to all of the conferees.These conferees are specified in advance in a data table PRECONF indexed by conference number and conferee number.(The preset conference DN is always first entry and the conferee number is zero)

These conferees are datafilled in table PRECONF indexed by conference number and conferee number.If the preset predefined DN is dialled a check is made if the required number of six-port conference bridges can be seized for the conference.There are enough six-port conference bridges available the originator receives audible ringing while calls are originated to all the addresses stored for the desired preset conference.

An IMMSTART option can be set in the PRECONF table so that the conference starts as soon as the first conferee answers.

Associated with each conferee DN is a timeout interval and an optional alternate DN. Automatic retrial is attempted on all conferees that have not returned answer within a customer datafillable interval (TIMEOUT option of table PRECONF) of 15 to 60 seconds after the call to conferee was initiated.If a call to a primary address fails to complete within two retrials, and the conferee is provided with an alternate address (ALTADDR option of table PRECONF), then two additional attempts are made on the alternate DN.

Once the preset conference is established, addon of additional conferees can begin if allowed by PRECONF table option ADDON.

The conference is terminated when all conferees disconnect, or if specified by ORIGCONT option in table PRECONF, when the originator of the conference goes on hook.

The following figure gives the brief description of the fields of PRECON.

Table 10 Table PRECONF

Datafilling PRECONF
PRECONF : is a number (0-63) assigned to the preset conference assigned by operating company.
CONFEREE: is a number (0-49) assigned to conferee by the operating company. Conferee 0 which is used to hold the conference's DN must be entered first.
CONFADDR:Conference address Enter the 1-29 digit conference address.
CLASS: Conference Class.
CUSTGRP: Is used to indicate the customer group that owns this preset conference
NCOS: is used to indicate NCOS
ALTADDR: Is used when the class is A.
ORIGCOUNT: is used to indicate whether the originator has control of the conference.
TIMEOUT: Variable Timeout.
ADDON: is used to add additional conferees, if yes, the origintor is allowed to addon conferee.
DIDORIG: DID Origination allowed
IMMSTART:Is used to indicate immediate start.

22.9.1 The range information for the fields of PRECONF

.

Table 11 Table PRECONF

Range of fileds in PRECONF
PRECONF : {0 TO 63}.
CONFEREE: {0 TO 49}
CONFADDR: VECTOR OF UP TO 30 DIGIT'S.(THIRTY_DIGIT_REGISTER.)
CLASS: {P,A,C,D} .
CUSTGRP: CUSTOMER_GROUP when D is selected.
NCOS:{0 TO 511} .
ALTADDR: VECTOR OF UP TO 30 DIGIT'S (THIRTY_DIGIT_REGISTER .)
ORIGCOUNT:{N,Y} ..
TIMEOUT: {15 TO 300}..
ADDON: {N,Y}..
DIDORIG: {N,Y.
IMMSTART:{N,Y}..

The preset conference DN can be datafilled up to 14 digits according to universal numbering plan .The conferee DN and alternate DN can be datafilled up to 30 digits.

23: Functional Description (FN): A00002377

23.1 Feature name

10 AFC Keys for BRI Directory Number

23.2 Description

This feature is required as part of the requirements for the German DBArt in ISN07. This feature allows up to 10 AFC (Additional Functional Call) Keys (and therefore 11 calls) on one DN (Directory Number). The master DN, known as SFC (Single Functional Call) key can have up to 10 AFC Keys associated with it.

This activity allows 11 Call Hold (all calls can be HELD calls) on one DN and 8 Call Waiting per loop if the customer is subscribed to these services.

This service is supported only in point to multipoint configurations.

The old capability allowed provisioning up to 4 AFC Keys (and therefore 5 calls) on one DN. This activity increases the provisioning number of AFC Keys to 10 per DN (and therefore 11 calls) for the DMS ETSI BRI implementation.

ETSI does not limit the number of calls on a TEI (Terminal Endpoint Identifier).

The old capability restricted the maximum call waiting calls per access with 2 and the maximum number of calls allowed on loop with six for terminations. Maximum call waiting calls per access is increased to 8 and maximum number of calls restriction for terminations is removed by this activity.

Summary of the provided capabilities by this activity are as follows:

- The maximum number of calls within an ETSI BRI (p-mp) configuration are 11 calls per DN.

  Number of calls per loop depends on the terminal capabilities.

  The maximum number per DN is provisionable in a range from 1 to 11.

- The maximum number of held calls within an ETSI BRI (p-mp) configuration are 11 calls per DN.

All calls can be HELD calls.

These values are not provisionable.

- The maximum number of waiting calls within an ETSI BRI (p-mp) configuration is 8 calls per access.

  These values are not provisionable.

  The summary of the number of the AFC Keys per DN, HELD calls per DN and CW calls per loop depending on PtoMP and PtoP configurations are shown in Table 1:

Table 1

	Before the activity		After the activity	
	PtoMP	**PtoP**	**PtoMP**	**PtoP**
Number of AFC Keys per DN	4	4	10	4
Number of HELD calls per DN	5	-	11	-
Number of CW calls per loop	2	-	8	-

Note: This activity is only applied to Point-to-Multipoint configurations and Point-to-Point configurations are kept unchanged as before the activity.

23.2.1 Software Optionality Control (SOC) Option

A new SOC option SULN0028, ‘SULN BRI Call Queuing’ is introduced to restrict the usage of the “10 AFC KEYS for BRI DIRECTORY NUMBER” functionality. Following “10 AFC KEYS for BRI DIRECTORY NUMBER” functionality is depend on the SOC option:

- Provisioning of 10 AFC Keys for a DN is possible only for Point-to-Multipoint configuration of ETSI BRI variant and if the SOC is in active state.

The SOC option restricts the datafilling of more than 4 AFC keys instead of restricting functionality of the AFC keys in this activity. In order to prevent the

10 AFC keys option is functioned while the SOC state is IDLE (this can be occur if 10 AFC keys option is assigned to a DN while SOC state is ON and then the SOC state is changed to the IDLE), referring to the Software Optionality Control Application Guidelines, prior to the SOC state transition from ON to IDLE, existing customer datafills for more than 4 AFC keys are determined and a warning is returned to the SOC. Also, a new CI command AFCLIS is created to list the available LTIDs with more than 4 AFC keys. After removing all datafills for more than 4 AFC keys, it can be possible to change the SOC state from ON to IDLE.

23.3 Hardware Requirements or Dependencies

N/A

23.4 Software Requirements or Dependencies

N/A

23.5 Limitations and Restrictions

N/A

23.6 Interactions

Since the number of AFC keys for BRI directory number and the number of waiting calls per loop are changed, there are some service interactions with some of the available BRI services. These service interactions are explained in this section.

23.6.1 Call Hold

23.6.1.1 Background

Call Hold supplementary service allows a user to interrupt communications on an existing call and then, if desired, re-establish the communication.

When the Call Hold supplementary service is invoked, communication on a B-channel is interrupted and the B-channel is released from use by the existing call. A B-channel shall be reserved for use by the terminal (based on the TEI of the terminal) used to invoke Call Hold supplementary service and enable the user to retrieve a call from hold, originate a new call, and establish connection to an incoming call (Activity AR2179 Multi Party Services).

23.6.1.2 Changes on the supplementary service with this activity

This feature allows up to 10 AFC Keys (and therefore 11 calls) on one DN (Directory Number). The master DN, known as SFC (Single Functional Call) key can have up to 10 AFC Keys associated with it. This allows 11 Call Hold (all calls can be HELD calls) on one DN if the customer is subscribed to this service.

This activity increases the AFC range from {1 to 4} to {1 to 10} per DN.

This activity only increases the number of AFC and indirectly affect the HOLD supplementary service. This activity does not make any change on the functionality of HOLD supplementary service.

23.6.2 Call Waiting

23.6.2.1 Background

Call waiting supplementary service enables the call can be offered without a B-channel. In CM terminating utilities exists that are dealing with B-channel idle or busy determination (Activity AR2179 Multi Party Services).

23.6.2.2 Changes on the supplementary service with this activity

This activity allows 8 Call Waiting per loop if the customer is subscribed to this service.

This activity increases the AFC range from {1 - 4} to {1 - 10} per DN and waiting call limit from 2 to 8 per loop.

This activity does not make any change on the functionality of CW supplementary service.

23.6.3 ECT

23.6.3.1 Background

The user is engaged in a telephone call and additional connections have been established. The user can interconnect two of the partners (ECT - Explicit Call Transfer) (Activity A59023626 BRI Explicit Call Transfer).

23.6.3.1.1 Implicit ECT Background

If there is only one held call on a DN, an ECTExecute message is sent from that HELD call and network connects that call with the active idle call. If there are more than one HELD call on a DN, user selects one of the HELD call. Then an ECTExecute message is sent from that selected call and network connects that selected HELD call with the active idle call.

23.6.3.1.2 Explicit ECT Background

A LinkIDRequest message is sent from the active idle call. Then, network sends a LinkID to the user. If there is only one held call on a DN, an ECTExecute message is sent from that HELD call with the LinkID and network connects that call with the active idle call. If there are more than one HELD call on a DN, user selects one of the HELD call. Then an ECTExecute message is sent from that selected call with the LinkID and network connects that call with the active idle call.

23.6.3.2 Changes on the supplementary service with this activity

23.6.3.2.1 Implicit ECT

Because the active held call is selected using the CR in the FAC message, there is no impact to ECT of allowing additional HELD calls.

This activity does not make any change on the implicit ECT supplementary service.

23.6.3.2.2 Explicit ECT

Because the active held call is selected using the CR in the FAC message, there is no impact to ECT of allowing additional HELD calls.

This activity does not make any change on the explicit ECT supplementary service.

23.6.4 Three Party Conference

23.6.4.1 Background

The Three Party Conference (3PTY) supplementary service enables the subscribed user to establish, participate in and control a three-way conversation. It is invoked by the subscribed user who is involved in two calls (one active call and one held call), either of which may be an incoming or outgoing call. The connections are established on each of the two calls prior to invocation of 3PTY supplementary service (Activity AR2179 Multi Party Services).

23.6.4.2 Changes on the supplementary service with this activity

In the old code, if there were more than one Active-Idle connection exists for the same TEI, the network accepted the transfer request and connected the parties.

This activity does not change this behavior and rejects the request if there are more than one Active-Idle connection exists for the same TEI.

23.6.4.3 Hunt Groups (MLH, DNH, DLH)

23.6.4.4 Background

ETSI BRI lines can have only one AFC assigned if they are in MLH (Multiline Hunt), DNH (Directory Number Hunt), DLH (Distributed Line Hunt) hunt groups. More than one AFC can not be assigned.

Up to two terminations are allowed on ETSI BRI terminals in hunt groups. One on the SFC key and on one AFC key.

23.6.4.5 Changes on the supplementary service with this activity

This activity does not change this restriction and therefore this activity has no interaction with hunt groups.

23.6.5 Six Party Conference / Add On Conference

23.6.5.1 Background

The conference (Add On CONF) supplementary service enables a user who is connected to the network via a point to multipoint ISDN ETSI BRI to establish, participate in and control a simultaneous communication involving a number of users. The DMS implementation of the Add On CONF supplementary service restricts the total number of conference parties to 6 Activity A59027439 ETSI BRI 6 PARTY CONFERENCE).

23.6.5.2 Changes on the supplementary service with this activity

Since only one active held call on a DN was possible before this activity, adding a new party which is on HELD state to the CONFERENCE while conference is also on HELD state (two HOLD method) was not possible.

After the activity, since more than one HELD call on a DN is possible, adding a new party which is on HELD state to the CONFERENCE while conference is also on HELD state (two HOLD method) is possible.

This activity does not make any change on the Add On Conference supplementary service. It just allows two hold method as mentioned above.

23.6.6 Preset Conference

The service interaction with ‘Preset Conference’ is handled under ‘Preset Conference’ activity.

Please refer to the ISN07 activity “A00002884 - ETSI BRI Preset Conference Service Interactions”.

23.7 Applicable Customer Facing Sections

Fault Management

Logs ..... N/A

Alarms ..... N/A

Configuration

Data Schema ..... N/A

User Interface ..... N/A

Element Management ..... N/A

Security ..... N/A

Service Order X

Office Parameters ..... N/A

Accounting (includes AMA billing) ..... N/A

Performance (includes operational measurements) ..... N/A

Please see Service Orders section of the Configuration document for details.

23.8 Glossary

Term	Description
AFC	Additional Functional Call
BRI	Basic Rate Interface
CM	Computing Module
CW	Call Waiting
DLH	Distributed Line Hunt
DN	Directory Number
DNH	Directory Number Hunt
DRU	Development Release Unit
ECT	Explicit Call Transfer European Telecommunications
ETSI	Standard Institute
MLH	Multiline Hunt
PTOMP	Point to Multipoint
PTOP	Point to point
SFC	Single Functional Call
SOC	Software Optionality Control
TEI	Terminal Endpoint Identifier
3PTY	Three Party Conference
XPM	eXtended Peripheral Module

23.9 Recommended Reading/References

a. AR2179FN - Functional Description (FN) document of the feature ND ISDN SVCS:WT:Multi Party Services

b. A59023626 - Functional Description (FN) document of the feature BRI Explicit Call Transfer

c. A59027439 - Functional Description (FN) document of the feature ETSI BRI 6 Party Conference

d. A00000154 - Functional Description (FN) document of the feature ETSI BRI (Basic Rate Interface) MLPP (Multi Level Precedence and Preemption) Service

e. A00003465 - Functional Description (FN) document of the feature ETSI BRI Channel Reservation Overwrite

f. A00003466 - Functional Description (FN) document of the feature MLPP Default Precedence Level on Terminations

24: Functional Description (FN): A00002470

24.1 Feature name

Fixed Price Service for Turkey.

24.2 Description

The purpose of this activity ;

- FPS (Fixed Price Service) support for agent interworkings in Turkish network;
  a. IBN line to Turkish R1 (NTLS01, NTLS02, NTLS09)
  b. IBN line to Turkish ETSI ISUP V1
  c. IBN line to Turkish ETSI ISUP V2

  interworkings.
- FPS on V5.2 IBN line support.
- FPS Warning tone definition is added to Turkish tone set.

24.2.1 Supported Agent interworkings for FPS in Turkish network

The all supported agent interworkings for FPS feature in Turkish network is shown in Table 1.

Table 1 Supported Agent interworkings for FPS in Turkish network

Originator with FPS data feature	Terminating Agent									
	Analog IBN lines	ETSI BRI lines	Pphone	V5.2 IBN line	V5.2 BRI line	ETSI PRI	Global R2	Turkish R1 (NTLS01, NTLS02, NTLS09)	Turkish ETSI ISUP V1	Turkish ETSI ISUP V2
Analog IBN line	S	S	S	S	S	S	S	S*	S*	S*

Table 1 Supported Agent interworkings for FPS in Turkish network

Originator with FPS data feature	Terminating Agent									
	Analog IBN lines	ETSI BRI lines	Pphone	V5.2 IBN line	V5.2 BRI line	ETSI PRI	Global R2	Turkish R1 (NTLS01, NTLS02, NTLS09)	Turkish ETSI ISUP V1	Turkish ETSI ISUP V2
V5.2 IBN line	S*	S*	S*	S*	S*	S*	S*	S*	S*	S*

S Supported agents for FPS feature in Turkish network

S* Newly Supported agents for FPS feature by this activity.

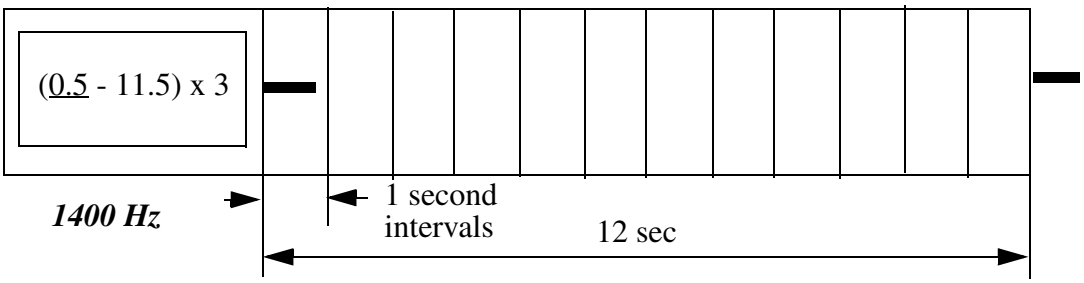
FPS data feature can be assigned to Analog and V5.2 IBN lines.

For detail information about FPS service please refer to A89007209 “Fixed Price Service for Bangladesh” document . All FPS capabilities in FN section of A89007209 document is also supported with newly supported interworkings in Turkish market.

24.2.2 FPS warning tone

When FPS counter reach zero during a call a tone is generated and after 30 seconds call is taken down. This tone is WARNING TONE that is already used by Papua New Guinea (PNG) and Bangladesh market via PNG and Bangladesh tonesets and will be added to TURKISH tone set by this activity.

Tone Cadence of *Warning Tone*

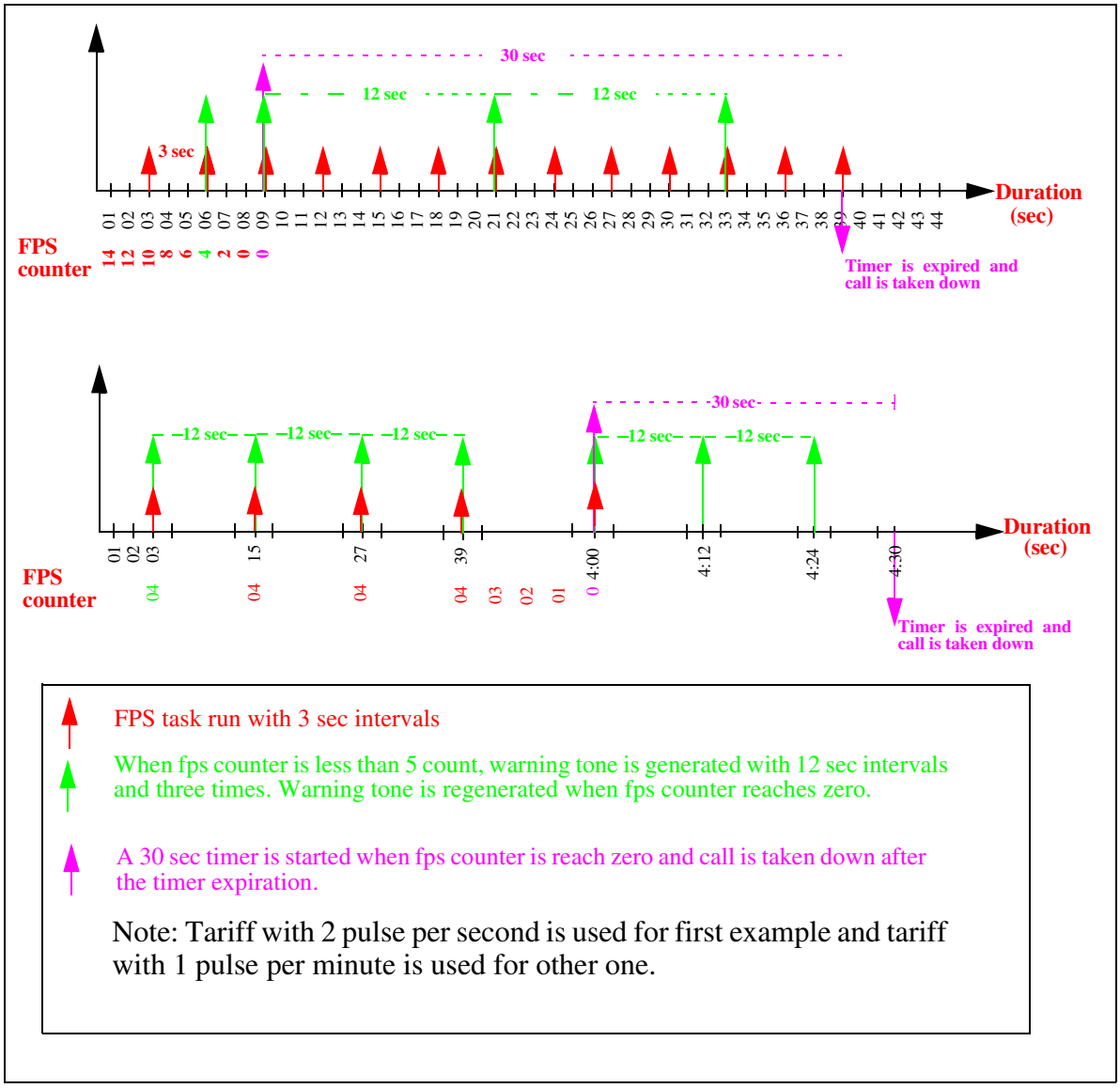


Note: cadence - 3 cycle, 36 sec duration.

Table 2 Tone requirement

Tone Name	Frequency (Hz)	Frequency Tolerance	Level (dbm0)	Cadence Rate Tolerance
Warning Tone	1400	2,5%	- 10	± 10%

Figure 1 Examples of Warning tone generation



24.3 Hardware Requirements or Dependencies

N/A

24.4 Software Requirements or Dependencies

N/A

24.5 Limitations and restrictions

None

24.6 Interactions

None

24.7 Applicable customer facing sections

Fault Management

- Logs __N/A__
- Alarms __N/A__

Configuration

- Data Schema __N/A__
- User Interface __N/A__
- Element Management __N/A__
- Security __N/A__
- Service Order __N/A__
- Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

24.8 Glossary

Term	Description
FPS	Fixed Price Service
TT	Turkish Telephone
ETSI	European Telecommunications Standards Institute
ISUP	ISDN User Part

24.9 References

PLS Name	Description of Reference
A89007209	Fixed Price Service for Bangladesh
AF7173	Hardware Metering and Fixed Price Service CM

25: Functional Description (FN): A00002512

25.1 Feature name

GWC-EM Internet Transparency VCAC Provisioning.

25.2 Description

The Internet Transparency ("ITrans") solution, implemented in the SN06.x stream, provides a means for CS2K to enable IP-telephony across and between VPNs (Virtual Private Networks). This is achieved by taking into account the presence of NAT (Network Address Translator) middleboxes between MGs (Media Gateways) and the 'outside world', and inserting publicly-addressable MP (Media Proxy) devices into the media path where required.

The SN06 provisioning component of this work dealt with:

- datafilling of Media Proxy and (virtual) NAT devices
- association of MGs to an 'adjacent' NAT.
- association of MPs to GWCs (Gateway Controllers)
- downloading of MP/NAT information to GWCs as necessary.

See feature ACTIDs 89007809, 89007814 and 89007657 for further information on the SN06 provisioning functionality.

The present feature (SN07) builds on this provisioning functionality to add support for:

- datafilling of LBL (Limited Bandwidth Link) middleboxes in addition to NATs
- datafilling of RU (Resource Usage) data for use in the VCAC (Virtual Connections & Admissions Control) function of LBLs
- manual or automatic assignment of a GWC to carry out the RU capacity counting function on behalf of an LBL
- 'chaining' of middleboxes (NATs/LBLs) in a hierarchical network topology.
- downloading of MP/NAT/LBL/RU information to GWCs as necessary.

VCAC Background
LBLs are a virtual representation of 'policed' capacity-restricted links in the network. An LBL carries a number ("max count") representing maximum

capacity through the link. Call set-up through the link causes a running total of used capacity to be incremented, and call take-down causes the running total to be decremented. If call set-up will cause the running total to exceed the LBL's maximum capacity figure, the call attempt is rejected and routed to treatment (congestion tone).

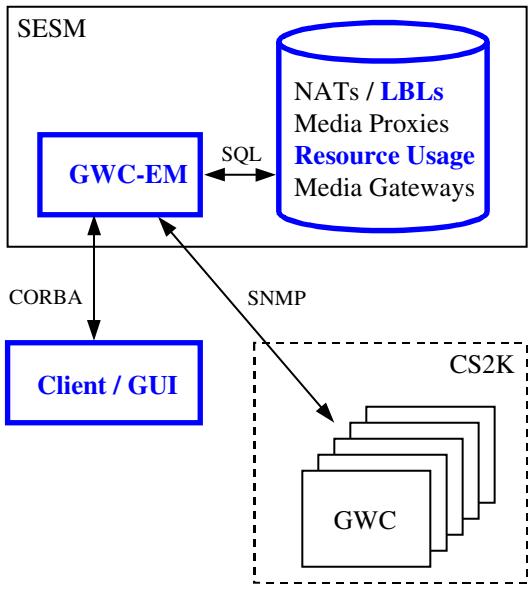
The specific amount used to increment/decrement the running total is supplied by the Resource Usage entry used by the LBL. Each Resource Usage entry has a set of 'capacity-used-per-call' values, depending on the codec and packetization rate in use on the call.

The running total is maintained by a counting device - in the SN07 release this device is a GWC. The counting device for a particular LBL is identified by entering the counter's address into the LBL's IP address field. There is one method for allocating the LBL's counting device:

- "auto-generated" - the LBL's address field is filled automatically when the LBL is first downloaded to a GWC.

25.3 Hardware Requirements or Dependencies

Figure 1 System Configuration



Note: The components outlined in blue will be affected by this provisioning activity.

Requirements for the whole Pre-midcom solution:

- CS2K.

- SESM Platform (Succession Element and Sub-Element Manager).

- IMS manager to handle provisioning of the Media Proxy.

- Uncontrolled NATs.

- Media Proxies.

- MGs.

25.4 Software Requirements or Dependencies

Dependencies:

- GWC should be running a software load of an equivalent stream to that of the SESM/GWC-EM, and should be running under a profile that enables ITrans functionality.

25.5 Limitations and restrictions

- There is only one NAT exit point from a local network.
- A Media Gateway has one or no adjacent middlebox. A NAT/LBL has one or no parent middlebox.
- The maximum length of sequentially 'chained' middleboxes (e.g. A --> B --> C, etc) is five.
- If two gateways are behind the same NAT then they can set up a call without requiring a Media Proxy.
- If two gateways are behind the same LBL, a call between them is not considered to use capacity on that LBL.
- The DQoS IAC solution (ACTID 59039082/59006771) uses "PepServer" middleboxes. The ITrans IAW solution uses NAT/LBL middleboxes. These two solutions are mutually exclusive as defined in the gateway profile service type (i.e. DQOS and ITRANS cannot be defined together in a profile).
- Where an LBL is 'shared' between two or more Succession Call Server networks (see ACTID.A00002644 "Common Topology Identifier Provisioning"), the LBL must be provisioned with exactly the same details on each network.

25.6 Interactions

The provisioning of LBL/RU data brings changes to the following GUIs:

- GWC-EM Network Panel (figures 2, 3, 4)
- Associate Media Gateway window (section 2.7.1.4).

The following features will also make changes in the Network Panel GUI:

- ACTID.A00002644 "Common Topology Identifier Provisioning"
- other [AT LEAST ONE OTHER... get details from Keith Raker]

This feature provisions data for use by the SN07 GWC CallP feature ACTID A00002739 "Virtual Connections Admissions Control".

25.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	_N/A_
User Interface	**_X_**
Element Management	**_X_**
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

25.7.1 User Interface - GUI

The upper section of the GWC-EM Network Panel GUI is reorganised to put the exisiting three subsections into tabbed panes. VCAC Resource Usage data is provisioned via the new RU table in a fourth tab in the upper section.

NATs are provisioned as before, except that:

— the tab is renamed “IP-VPNs (Virtual NATs)”

— a new field is added to provision a “Parent” (northbound neighbour) middlebox in the topology.

LBLs are provisioned via a table in a new tab added to the central section of the Network Panel.

Figures 2 and 3 and 4 show the Network Panel:

— before reorganisation (SN06 version)

— after reorganisation, NAT table visible

— after reorganisation, new LBL table visible

The new RU data table can be seen in the upper part of the reorganised view.

Figure 2 Unmodified (SN06) view of GWC-EM Network Panel

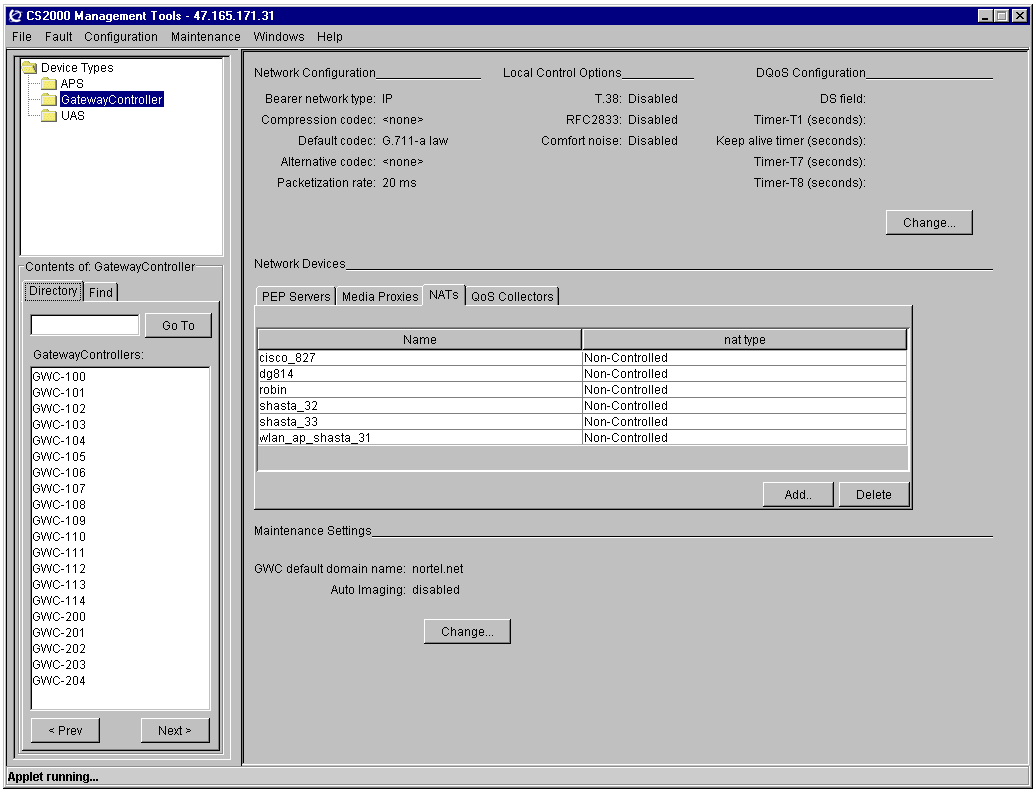


Figure 3 Modified Network Panel (1)

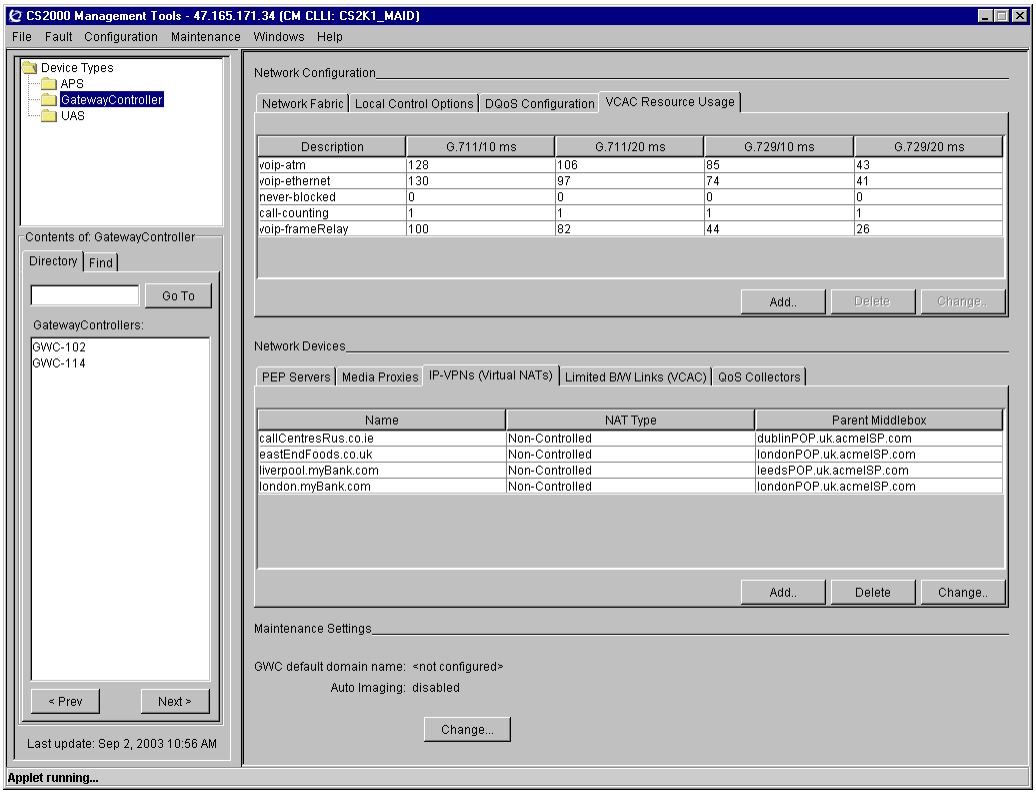
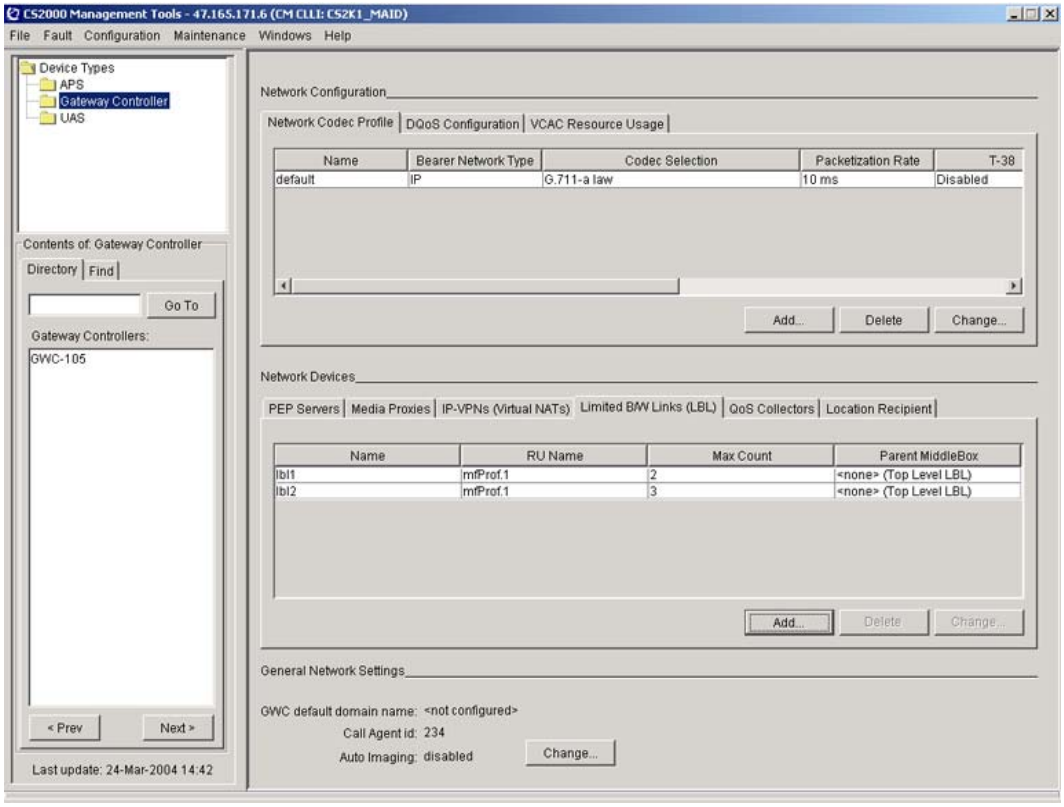


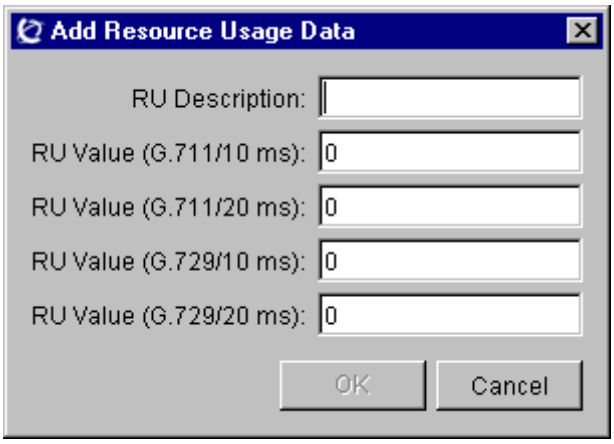
Figure 4 Modified Network Panel (2)



25.7.1.1 Provisioning Resource Usage data: Add, Change, Delete

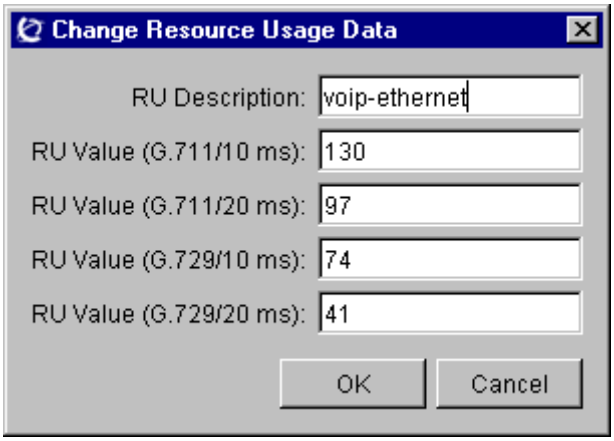
These operations are accessed by clicking the appropriate buttons on the tabbed pane of the VCAC Resource Usage table (figure 3).

Add Resource Usage data: click the “Add” button in the Resource Usage tab to obtain the following box.



Enter a valid text description, and non-negative integer entries for each “RU Value” (zero is provided as a default). Click “OK” to confirm.

Change Resource Usage data: select an RU table entry and click the “Change” button to obtain the following box:



Modify the required data fields and click “OK” to confirm.

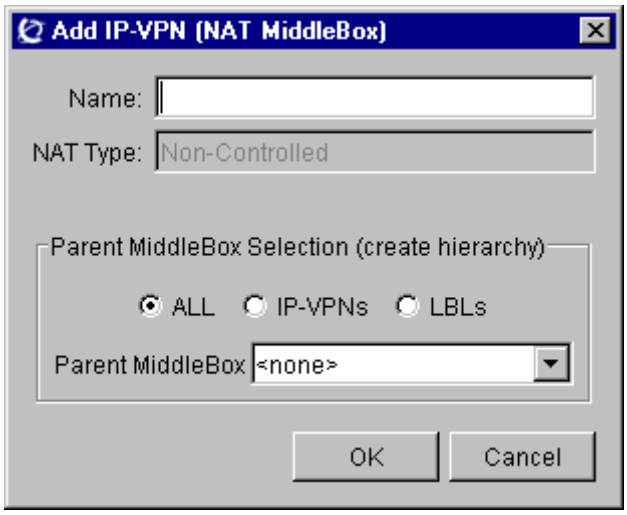
Delete Resource Usage data: select an RU table entry and click the “Delete” button to obtain the following confirmation box:

Click “Yes” to confirm. Note that the operation will be rejected if the RU Factor is currently ‘in use’, i.e. is currently referred to by an LBL.

25.7.1.2 Provisioning NAT middleboxes: Add, Change, Delete

These operations are accessed by clicking the appropriate buttons on the tabbed pane of the IP/VPN table (figure 3).

Add NAT middlebox: click the “Add” button on the “IP-VPNs (Virtual NATs)” tab to obtain the following box:

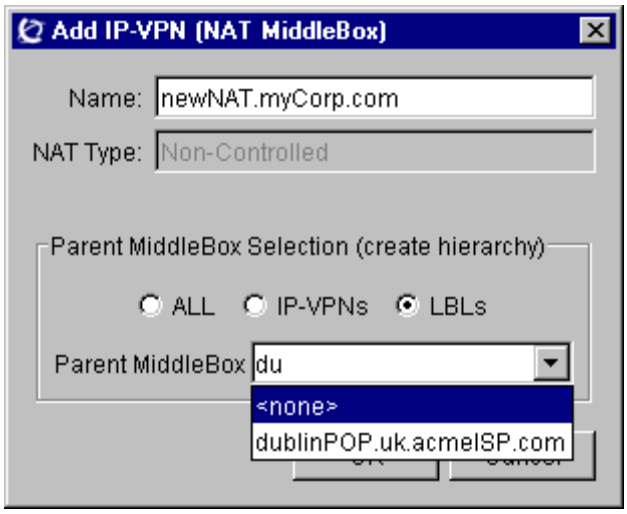


Enter a unique (DNS compliant, see ref 1) name. If appropriate use the filtered selection box to select a Parent Middlebox. Filtering is performed by one or both of:

— radio button selection to limit the choice to only NATs or only LBLs

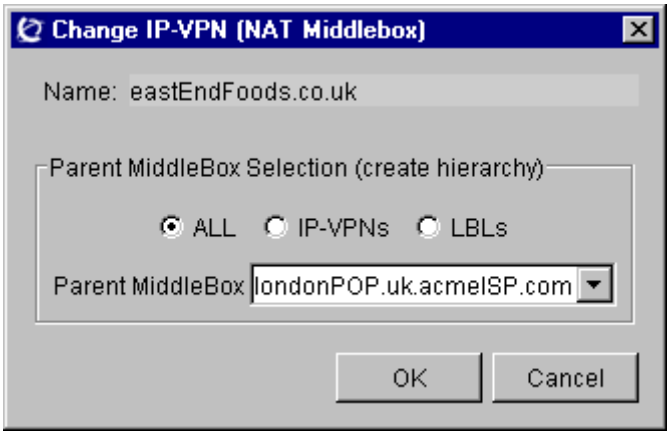
— typing the starting letters of the Parent middlebox name to limit selection to those with matching starting letters.

An example of filtered selection is shown below:



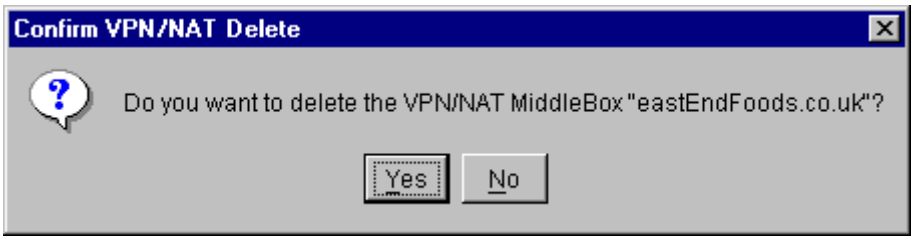
Selection of Parent middlebox is restricted to already provisioned middleboxes. Both NAT and LBL middleboxes can have either a NAT or an LBL as parent. Click “OK” to confirm.

Change NAT middlebox: select a NAT table entry and click the “Change” button to obtain the following box:



Modify the selected Parent middlebox as required (i.e. select another middlebox or <none>), and click “OK” to confirm.

Delete NAT middlebox: select a NAT table entry and click the “Delete” button to obtain the following confirmation box:



Click “Yes” to confirm. Note that the operation will be rejected if the NAT is currently ‘in use’, i.e. is currently referred to:

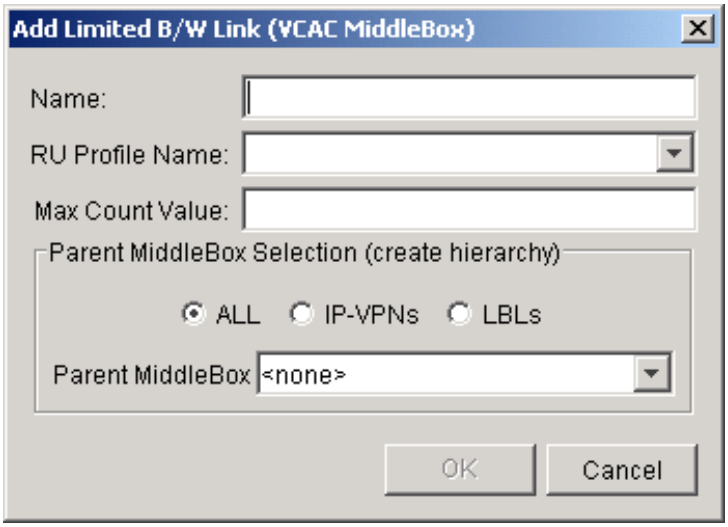
— as a parent by another middlebox

— as an adjacent middlebox by a Media Gateway.

25.7.1.3 Provisioning LBL middleboxes: Add, Change, Delete

These operations are accessed by clicking the appropriate buttons on the tabbed pane of the Low B/W Links table (figure 4).

Add LBL middlebox: click the “Add” button on the “Low B/W Links (VCAC)” tab to obtain the following box:

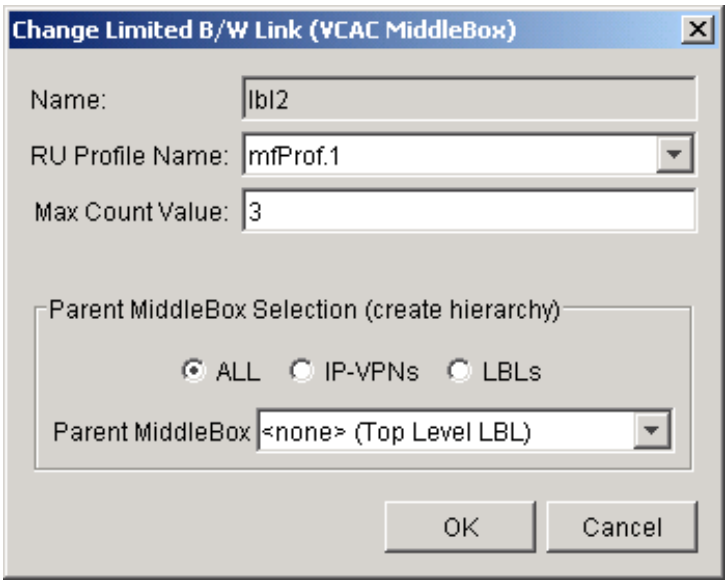


Enter the following information:

- valid text name (DNS compliant, see ref. 1)
- select RU Factor from the list provided
- enter a non-negative integer value for “Max Count Value”
- select Parent middlebox from the (filtered) list. Remember that an LBL can have either another LBL or a NAT as Parent middlebox.

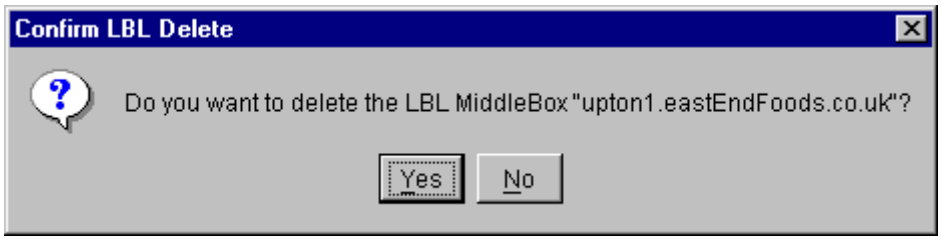
Click “OK” to confirm.

Change LBL middlebox: select an LBL table entry and click the “Change” button to obtain the following box:



The name field is not modifiable, other fields may be edited as required. Parent middlebox may be changed to either another middlebox or <none>. Click “OK” to confirm. NB: the RU Factor and the Parent may not be changed in the same operation - they must be modified in separate change operations.

Delete LBL middlebox: select an LBL table entry and click the “Change” button to obtain the following confirmation box:



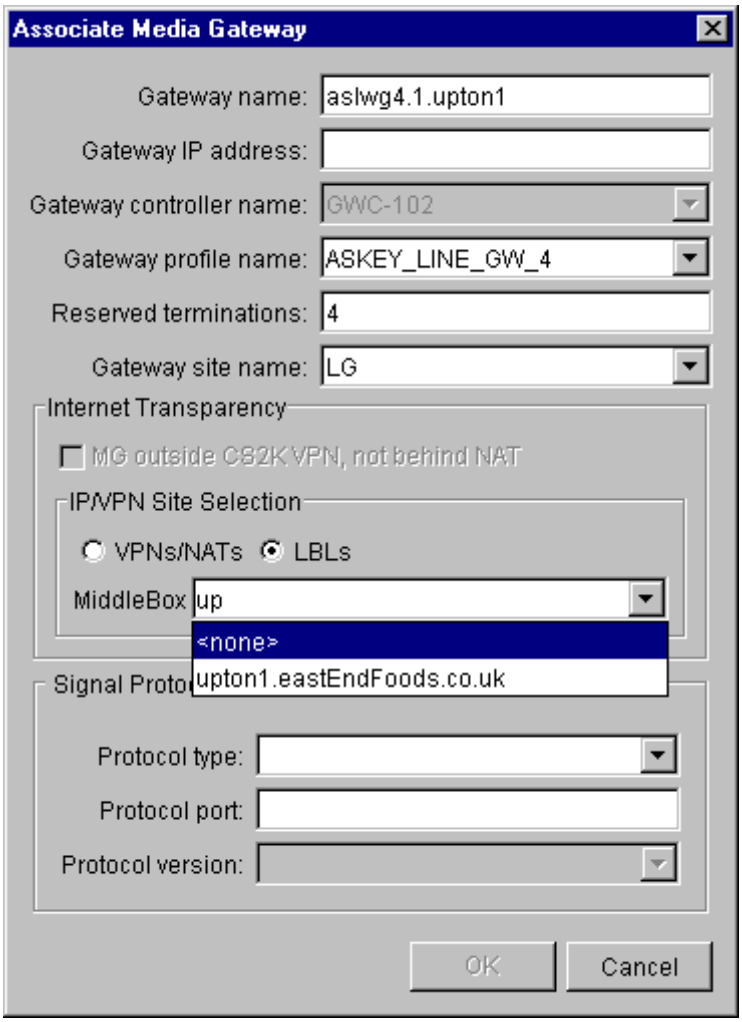
Click “Yes” to confirm. Note that the operation will be rejected if the LBL is currently ‘in use’, i.e. is currently referred to:

— as a parent by another middlebox

— as an adjacent middlebox by a Media Gateway.

25.7.1.4 Associate/Change Middlebox to a Media Gateway

This is unchanged from SN06 functionality except that filtered selection is used to choose an Adjacent Middlebox, as shown below for the Associate operation:



Note: attempting to remove an adjacent middlebox from a Media Gateway will be rejected if the middlebox or any member of it's 'northbound' topology chain is a NAT.

25.7.2 XML Interfaces

Modified Interfaces in Sn07

- Add/Query NATs - added parent middlebox attribute

New Interfaces introduced in Sn07 are as follows:

- Change NATs
- Add/Delete and Change Media Proxies.
- Add/Delete/Query and Change Resource Usage profiles
- Add/Delete/Query and Change LBL entries.
-

25.7.2.1 Add NAT XML command

Add NAT is modified SN07 the <parentMB> tag has been added. The value of this tag must have been previously provisioned into the system to successfully complete this command.

The XML for this command is shown in Figure 5, Figure 6 . Error messages returned are described in Appendix B.

Figure 5 XML command to Add NAT device.

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addNAT usn="1" version="1.0">
      <Parameters>
        <NATname>NAT-A</NATname>
        <ParentMB>VPN-Eastenders</ParentMB>
      </Parameters>
     </addNAT>
    </Methods>
  </Command>
 </CommandList>
```

Figure 6 XML response to Add NAT

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <addNAT usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </addNAT>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.2 Query NAT XML command

The Query NAT response is modified SN07 the <parentMB> tag has been added

The XML for this command is shown in Figure 7, Figure 8. Error messages returned are described in Appendix B.

Figure 7 XML command to Query a NAT

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <Parameters>
        <NATname>NAT-A</NATname>
      </Parameters>
     </queryNAT>
    </Methods>
  </Command>
 </CommandList>
```

Figure 8 XML response to Query NAT

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <queryNAT usn="1" version="1.0">
       <ReturnData>
          <NATname>NAT-A</NATname>
         <ParentMB>VPN-Eastenders</ParentMB>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </queryNAT>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.3 Change NAT XML command

Change NAT is new to SN07 because there was no data in the SN06 releases to change, in Sn07 the only attribute that can change is the <ParentMB> tag.The value of this tag must have been previously provisioned into the system to successfully complete this command.

The XML for this command is shown in Figure 9, Figure 10. Error messages returned are described in Appendix B.

Figure 9 XML command to Change specified NAT parent middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeNAT usn="1" version="1.0">
      <Parameters>
        <NATname>NAT-A</NATname>
        <ParentMB>VPN-Eastenders</ParentMB>
      </Parameters>
     </changeNAT>
    </Methods>
  </Command>
 </CommandList>
```

Figure 10 XML response to Change specified NAT

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <changeNAT usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </changeNAT>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.4 Add Media Proxy XML command

Media Proxy provisioning via XML is new to SN07.

The XML for this command is shown in Figure 11, Figure 12. Error messages returned are described in Appendix B.

Figure 11 XML command to Create a new Media Proxy

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addMP usn="1" version="1.0">
      <Parameters>
        <MPname>MP-A</MPname>
        <IPAddress>47.165.32.23</IPAddress>
         <Protocol>MGCP+</Protocol>
         <ProtocolVersion>2.0</ProtocolVersion>
       </Parameters>
     </addMP>
    </Methods>
  </Command>
```

Figure 12 XML response to Creating a new Media Proxy command

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <addMP usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </addMP>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.5 Change Media Proxy XML command

Media Proxy provisioning via XML is new to SN07.

The XML for this command is shown in Figure 13, Figure 14. Error messages returned are described in Appendix B.

Figure 13 XML command to Change IP data of a Media Proxy

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeMP usn="1" version="1.0">
      <Parameters>
        <MPname>MP-A</MPname>
        <IPAddress>47.165.32.22</IPAddress>
         <Protocol>MGCP+</Protocol>
         <ProtocolVersion>2.0</ProtocolVersion>
       </Parameters>
     </changeMP>
    </Methods>
  </Command>
```

Figure 14 XML response to Change Media Proxy IP data.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <changeMP usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </changeMP>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.6 Delete Media Proxy XML command

Media Proxy provisioning via XML is new to SN07.

The XML for this command is shown in Figure 15, Figure 16. Error messages returned are described in Appendix B.

Figure 15 XML command to Delete a Media Proxy

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteMP usn="1" version="1.0">
      <Parameters>
        <MPname>MP-A</MPname>
       </Parameters>
     </deleteMP>
    </Methods>
  </Command>
 </CommandList>
```

Figure 16 XML response to Deleting Media Proxy .

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <deleteMP usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </deleteMP>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.7 Creating RU profile command

Resource Usage provisioning is new to SN07. To successfully create an RU profile the XML client must provide every Codec/packetRate combination that has been entered into the CS2K config manager.

The XML for this command is shown in Figure 17, Figure 18. Error messages returned are described in Appendix B.

Figure 17 XML command to Create an RU profile

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
     <Methods>
         <addRU usn="1" version="1.0">
         <Parameters>
               <RUDescription>AAL1/IP40</RUDescription>
               <RUValue>
                       <Codec>G.711</Codec>
                       <PacketRate>10 ms</PacketRate>
                       <Value>103</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.711</Codec>
                       <PacketRate>20 ms</PacketRate>
                       <Value>133</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.729</Codec>
                       <PacketRate>10 ms</PacketRate>
                       <Value>132</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.729</Codec>
                       <PacketRate>20 ms</PacketRate>
                       <Value>103</Value>
               </RUValue>
         </Parameters>
         </addRU>
    </Methods>
   </Command>
</CommandList>
```

Figure 18 XML response to Creating an RU profile .

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <addRU usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </addRU>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.8 Changing RU profile command

Resource Usage provisioning is new to SN07. To successfully change an RU profile the XML client must either provide and <RUNewDescription> OR every Codec/packetRate combination that has been entered into the CS2K config manager.

The XML for this command is shown in Figure 19, Figure 20, Figure 21. Error messages returned are described in Appendix B.

Figure 19 XML to Change an RU profile Description.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <changeRU usn="1" version="1.0">
        <Parameters>
              <RUDescription>AAL1/IP40</RUDescription>
              <RUNewDescription>AAL1/IP71 </RUNewDescription>
         </Parameters>
      </changeRU>
    </Methods>
   </Response>
</CommandList>
```

Figure 20 XML command Change RU profile data

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
     <Methods>
         <changeRU usn="1" version="1.0">
         <Parameters>
               <RUDescription>AAL1/IP40</RUDescription>
               <RUValue>
                       <Codec>G.711</Codec>
                       <PacketRate>10 ms</PacketRate>
                       <Value>123</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.711</Codec>
                       <PacketRate>20 ms</PacketRate>
                       <Value>133</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.729</Codec>
                       <PacketRate>10 ms</PacketRate>
                       <Value>152</Value>
               </RUValue>
               <RUValue>
                       <Codec>G.729</Codec>
                       <PacketRate>20 ms</PacketRate>
                       <Value>163</Value>
               </RUValue>
         </Parameters>
         </changeRU>
    </Methods>
   </Command>
</CommandList>
```

Figure 21 XML response to Changing an RU profile .

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <changeRU usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </changeRU>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.9 Query RU profile XML command

Resource Usage provisioning is new to SN07. The XML client has the option to either Query all the RU profiles, or the RU data for a particular profile.

The XML for this command is shown in Figure 22, Figure 23, Figure 24, Figure 25. Error messages returned are described in Appendix B.

Figure 22 XML command to Query all RU Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryRU usn="1" version="1.0">
      <Parameters>
     </Parameters>
     </queryRU>
    </Methods>
  </Command>
 </CommandList>
```

Figure 23 XML response to query all RU profiles.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <queryRU usn="1" version="1.0">
        <ReturnData>
              <RUDescription>AAL1/IP40</RUDescription>
              <RUDescription>AAL2/IP40</RUDescription>
              <RUDescription>AAL1/IP40-B</RUDescription>
              <RUDescription>AAL2/IP40-B</RUDescription>
             <ReturnCode value="0" text="Successful result" />
        </ReturnData>
       </queryRU>
    </Methods>
   </Response>
</CommandList>
```

Figure 24 XML command to Query an RU Profile data

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryRU usn="1" version="1.0">
      <Parameters>
        <RUDescription>AAL1/IP40</RUDescription>
       </Parameters>
     </queryRU>
    </Methods>
  </Command>
 </CommandList>
```

Figure 25 XML response to Querying an RU profile.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <queryRU usn="1" version="1.0">
       <ReturnData>
              <RUDescription>AAL1/IP40</RUDescription>
              <RUValue>
                      <Codec>G.711</Codec>
                      <PacketRate>10 ms</PacketRate>
                      <Value>123</Value>
              </RUValue>
              <RUValue>
                      <Codec>G.711</Codec>
                      <PacketRate>20 ms</PacketRate>
                      <Value>133</Value>
              </RUValue>
              <RUValue>
                      <Codec>G.729</Codec>
                      <PacketRate>10 ms</PacketRate>
                      <Value>152</Value>
              </RUValue>
              <RUValue>
                      <Codec>G.729</Codec>
                      <PacketRate>20 ms</PacketRate>
                      <Value>163</Value>
              </RUValue>

        <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </queryRU>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.10 Delete RU profile XML command

Resource Usage provisioning is new to SN07.

The XML for this command is shown in Figure 26, Figure 27. Error messages returned are described in Appendix B.

Figure 26 XML command to Delete an RU Profile

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteRU usn="1" version="1.0">
      <Parameters>
        <RUDescription>AAL1/IP40</RUDescription>
       </Parameters>
     </deleteRU>
    </Methods>
  </Command>
 </CommandList>
```

Figure 27 XML response to Deleting an RU profile.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <deleteRU usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </deleteRU>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.11 Add LBL XML command

Limited Bandwidth Links provisioning is new to SN07. The <CounterGWC> tag is optional, if omitted the the counterGWC is automatically assigned. The <RUDescription> and <ParentMB> values must have been previously provisioned into the system to successfully complete this operation.

The XML for this command is shown in Figure 28, Figure 29. Error messages returned are described in Appendix B.

Figure 28 XML command to Create a LBL device

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
     <Methods>
     <addLBL usn="1" version="1.0">
       <Parameters>
         <LBLname>LBL1</LBLname>
         <CounterGWC>47.132.132.12</CounterGWC>
         <RUDescription>AAL1/ip40</RUDescription>
         <MaxCount>1000</MaxCount>
         <ParentMB>VPN-A</ParentMB>
      </Parameters>
     </addLBL>
    </Methods>
</Command>
```

Figure 29 XML response to Creating a LBL device.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <addLBL usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </addLBL>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.12 Change LBL XML command

Limited Bandwidth Links provisioning is new to SN07. The <LBLname> tag is required the other changing data tags are optional. The <RUDescription> and <ParentMB> values must have been previously provisioned into the system to successfully complete this operation.

The XML for this command is shown in Figure 30, Figure 31. Error messages returned are described in Appendix B.

Figure 30 XML command to Change a LBL device RU profile.

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
     <Methods>
     <changeLBL usn="1" version="1.0">
       <Parameters>
         <LBLname>LBL1</LBLname>
          <RUDescription>AAL2/ip40</RUDescription>
       </Parameters>
     </changeLBL>
    </Methods>
</Command>
 </CommandList>
```

Figure 31 XML response to Changing a LBL device.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <changeLBL usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </changeLBL>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.13 Query LBL XML command

The Query LBL is new to SN07

The XML for this command is shown in Figure 32, Figure 33. Error messages returned are described in Appendix B.

Figure 32 XML command to Query a LBL

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
      <Parameters>
        <LBLname>LBL-A</LBLname>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>
```

Figure 33 XML response to Query LBL

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <queryLBL usn="1" version="1.0">
       <ReturnData>
          <LBLname>LBL1</LBLname>
         <CounterGWC>47.132.132.12</CounterGWC>
         <RUDescription>AAL1/ip40</RUDescription>
         <MaxCount>1000</MaxCount>
         <ParentMB>VPN-A</ParentMB>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </queryLBL>
    </Methods>
   </Response>
</CommandList>
```

25.7.2.14 Delete LBL XML command

Limited Bandwidth Links provisioning is new to SN07.

The XML for this command is shown in Figure 34, Figure 35. Error messages returned are described in Appendix B.

Figure 34 XML command to Delete a LBL device

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteLBL usn="1" version="1.0">
      <Parameters>
        <LBLname>LBL1</LBLname>
       </Parameters>
     </deleteLBL>
    </Methods>
  </Command>
 </CommandList>
```

Figure 35 XML response to Deleting a LBL device.

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <deleteLBL usn="1" version="1.0">
       <ReturnData>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </deleteLBL>
    </Methods>
   </Response>
</CommandList>
```

25.8 Authorization for Commands

The security for the GUI Client and OSSgate interface includes support for permission or ‘Authorization’ levels for commands. Each command is associated with one or more user groups. In order to execute a command, a user must belong to at least one of the associated user groups. The user groups associated with the new /modifed commands associated with this feature are specified in the table below.

Table 1 Internet Transparency Commands Authorization

Command	User Group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
addNat	X	X			
changeNAT	X	X			
queryNAT	X	X	X	X	X
addMP	X	X			
changeMP	X	X			
deleteMP	X	X			
addRU	X	X			
changeRU	X	X			
queryRU	X	X	X	X	X
deleteRU	X	X			
addLBL	X	X			
changeLBL	X	X			
queryLBL	X	X	X	X	X
deleteLBL	X	X			

25.9 References

1. DNS naming conventions: see for example IETF RFC 1034, or http://www.dns.net

25.10 Glossary

Term	Description
CORBA	Common Object Request Broker Architecture
DNS	Domain Naming System
GUI	Graphical User Interface
GWC	Gateway Controller
GWC-EM	GWC Element Manager
IAC	Cable solution
IAW	Wireline
IP	Internet Protocol
ITrans	Internet Transparency solution
LBL	Low Bandwidth Link
MG	Media Gateway
MP	Media Proxy
NAT	Network Address Translation
RU	VCAC Resource Usage
SESM	Succession Element and Sub-Element Manager
SNMP	Simple Network Management Protocol
VCAC	Virtual Connection Admission Control
VPN	Virtual Private Network

25.11 Appendix A: ITrans/VCAC Provisioning Steps

This section provides a high-level overview of the provisioning steps required to set up the ITrans VCAC functionality NEW installtion SN07.

1 Network Analysis/Modelling: identify the key locations in the network for NAT and LBL **functions** (not physical devices). Model and provision the Resource Usage values required for the VCAC functionality (see the Engineering Information section of this document. ***TO DO: Julian M. to supply the Engineering Information section***).

2 On the CS2K Config Manager provision model as defined by step 1. Starting with individual NAT/LBL middleboxes: these are provisioned in top-down hierarchical order, i.e. starting with those closest to the network core. Remember that a 'parent' middlebox must be already provisioned before a 'child' that refers to it can be provisioned.

3 On the CS2K Config Manager provision MGs: select the appropriate ITrans middlebox (NAT or LBL) from the topological model as the 'adjacent middlebox' for the MG.

Existing ITrans network models (SN06.x stream, NATs and MGs) may be adapted to the SN07 form by:

1 following steps 1 and 2 above for new middleboxes.

2 changing the parent middlebox fields of existing (NAT) middleboxes as required to insert them at the correct location in the topology.

3 changing the adjacent middlebox field of existing MGs as required to associate them to the appropriate middlebox (NAT or LBL) in the topology.

25.12 Appendix B: XML validation schemas

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addNATparamsType">
    <xsd:sequence>
      <xsd:element name="NATname" type="NoSpaceNameType" />
     <xsd:element name="ParentMB" type="NoSpaceNameType" />
    <xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeNATparamsType">
     <xsd:sequence>
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addMP Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addMPmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addMPparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
```

```
  </xsd:complexType>
  <xsd:complexType name="addMPparamsType">
    <xsd:sequence>
      <xsd:element name="MPname" type="NoSpaceNameType" />
      <xsd:element name="IPAddress" type="IPAddressType" />
      <xsd:element name="Protocol" type="NoSpaceNameType" />
      <xsd:element name="ProtocolVersion" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeMP Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeMPmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeMPparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeMPparamsType">
     <xsd:sequence>
      <xsd:element name="MPname" type="NoSpaceNameType" />
      <xsd:element name="IPAddress" type="IPAddressType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define deleteMP Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteMPmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteMPparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteMPparamsType">
    <xsd:sequence>
      <xsd:element name="MPname" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addRU Method Parameters -->
  <!-- ********************************************************************************************** -->
```

```
  <xsd:complexType name="addRUmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addRUparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addRUparamsType">
    <xsd:sequence>
      <xsd:element name="RUDescription" type="xsd:string" />
      <xsd:element name="RUValue" type="CodecPacketValue" maxOccurs="unbounded" />
    </xsd:sequence>
  </xsd:complexType>
   <xsd:complexType name="CodecPacketValue">
    <xsd:sequence>
      <xsd:element name="Codec" type="CodecType" />
      <xsd:element name="PacketRate" type="PacketType" />
      <xsd:element name="Value" type="NoSpaceNumberType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeRU Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeRUmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeRUparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeRUparamsType">
    <xsd:sequence>
      <xsd:element name="RUDescription" type="xsd:string" />
      <xsd:choice minOccurs="0">
         <xsd:element name="RUNewDescription" type="xsd:string" />
         <xsd:element name="RUValue" type="ChangeCodecPacketValue" maxOccurs="unbounded" />
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
   <xsd:complexType name="ChangeCodecPacketValue">
    <xsd:sequence>
      <xsd:element name="Codec" type="CodecType" />
      <xsd:element name="PacketRate" type="PacketType" />
      <xsd:element name="Value" type="NoSpaceNumberType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define queryRU Method Parameters -->
```

```
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="queryRUmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryRUparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryRUparamsType">
    <xsd:choice minOccurs="0">
      <xsd:element name="RUDescription" type="xsd:string" />
    </xsd:choice>
  </xsd:complexType>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define deleteRU Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteRUmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteRUparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteRUparamsType">
    <xsd:sequence>
      <xsd:element name="RUDescription" type="xsd:string" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

!!!!!TO DO LBL XSDs

25.13 Appendix C: Error codes and messages

Table 2 Return codes when command is unsuccessful

Cause of error	Return code	Example return messages
Incorrect command version in query	301	Unsupported version
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error
Unable to provision requested Itrans data because of a database error occurred	303	Database error occurred during setting of RU data
Unable to provision requested Itrans data because of invalid input data	304	Cannot set LBL Max count, value must be between 1 and <Max int> Cannot set LBL ParentMB ,value not configured. Cannot set LBL RUDescription, value not configured. Cannot provision RU profile, RUvalue missing
No Itrans data for this query. e.g. no NAT meets selection criteria or the NAT/GWC specified does not exist	305	NAT not found No NAT found for GWC
User is not a member of any of the user groups allowed to perform this action	501	Insufficient permissions to perform this operation

25.13.1 Example Error Message

```
<?xml version='1.0'?>
    <CommandList>
       <Response>
         <Interface>ITransIf</Interface>
            <Methods>
                <queryNAT usn="1.0" version="1.0">
                 <ReturnData>
                    <NATname>nat1111</NATname>
```

```
                    <ReturnCode value= "305" text="NAT not found"/>
                </ReturnData>
               </queryNAT usn="1.0">
            </Methods>
        </Response>
    </CommandList>
```

25.14 Appendix D: XML Commands: description of method parameters

25.14.1 Parameter definitions (new in SN07)

- **ParentMB** - The name of the parent Middlebox for this device. This allows ITrans devices to be connected into a hierarchy. A value of <none> indicates that this device has no parent. TYPE *NoSpaceNameType* .(32 character token without spaces, see xsd definitions in Appendix A).
- **MPname** - The unique name of the Media Proxy. This must be in a valid DNS format . TYPE *NoSpaceNameType*.
- **IPAddress** - The Media Proxy IP address. *TYPE IPAddressType.*
- **Protocol** - The Media Proxy communication protocol (GWC to MP). This must be either MGCP+ or MPCP. *TYPE NoSpaceNameType.*
- **ProtocolVersion** - The Media Proxy communication protocol version. This must be 1.**0 or 2.0 ?????? TO DO** . *TYPE NoSpaceNameType.*
- **RUDescription** - The Resource Usage profile name. *TYPE NoSpaceNameType.*
- **RUValue** - a composite of the following parameters. Codec,PacketRate,Value *TYPE CodecPacketValue*
- **Codec** - A valid codec that has been entered in the CS2K config manager. E.G. G.711 or G.729. *TYPE CodecType*
- **PacketRate** - A valid Packetisation rate. E.G. 10 ms , 20 ms. *TYPE PacketType*
- **Value** - A resource usage value that one call will use. This is the basic call count value that VCAC uses to measure calls through a Limited Bandwidth Link. *TYPE NoSpaceNumberType*
- **RUNewDescription** - The new name of an RU profile. *TYPE NoSpaceNameType*
- **LBLName** - The unique name of the Limited Bandwidth Link device. This must be in a valid DNS format . TYPE *NoSpaceNameType*.
- **CounterGWC** - The VCAC counter GWC IP address. *TYPE IPAddressType*
- **MaxCount** - The VCAC count maximum limit. TYPE ?
-

25.14.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **addNAT** - Method to create a new NAT (virtual NAT function). This method has the following parameters:

- Input data:
  - usn
  - version
  - NATname. The unique name of the NAT device
  - ParentMB (Optional). The name of the parent Middlebox for this device. This allows ITrans devices to be connected into a hierarchy. A value of <none> indicates that this device has no parent. (default = <none>)
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - CallAgentId **-** The value of the Call Agent Id for this Call Agent (CS2k).
  - ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

2. **queryNAT** - Method to list the NATs. Optional parameters allow the client to choose the data returned. This method has the following parameters:

- Input data:
  - usn
  - version
  - NATname (Optional, cannot be included as well as GWCname)- A Unique Name of a NAT device, to get full info on a device
  - GWCname (Optional, cannot be included as well as NATname) - To obtain a list of all NATs on a GWC (Use GWC-XX format)
  - ListNATid (Optional) - Set to true if the NAT ids are required.
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - GWCname (only when the GWCname option requested)

– NATname
– ParentMB (only when the full details are requested)
– NATType (returned only when the full details are requested)
– NATid (returned only when ListNATid is set to ‘true’ in the input data)
– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

3. **changeNAT** - Method that changes a provisioned NAT information into the CS2k Mgr. This method has the following parameters:

• Input data:
– usn
– version
– NATname - unique name for the NAT to be changed
– ParentMB - The new parent middlebox name. Enter <none> to remove the topology for this NAT device. Note: the parent Middlebox name entered must have been already provisioned into the CS2k Mgr.

• Output data:
– usn (value should be the same as the input)
– version (value should be the same as the input)
– ReturnCode

4. **addMP** - Method that creates a Media Proxy device into the CS2k Mgr. This method has the following parameters:

• Input data:
– usn
– version
– MPname - unique name for the MP to be provisioned
– IPAddress - The IP address of the MP device
– Protocol - Enter “MGCP+” for the control protocol of the device
– ProtocolVersion - Enter “1.1” for the control protocol version.

• Output data:
– usn (value should be the same as the input)
– version (value should be the same as the input)
– ReturnCode

5. **changeMP** - Method that changes a provisioned MP information into the CS2k Mgr. This method has the following parameters:

- Input data:
  - usn
  - version
  - MPname - unique name for the MP to be changed
  - IPAddress - The new IPAddress of the MP device.
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - ReturnCode

6. **deleteMP** - Method that deletes provisioned MP information from the CS2k Mgr. This method has the following parameters:

- Input data:
  - usn
  - version
  - MPname - unique name for the MP to be deleted
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - ReturnCode

7. **addRU** - Method that creates resource usage information into the CS2k Mgr. This method has the following parameters:

- Input data:
  - usn
  - version
  - RUDescription - A unique String to label this RU profile
  - RUValue - an RU Value must be entered for every Codec/Packetrate combination that has been created in the CS2k Mgr. An RUValue consists of the following three parameters.
  - Codec - The Codec that this value refers to
  - PacketRate - The packetisation rate this value refers to
  - Value - The VCAC value for a call using this codec/packetrate.
- Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

8. **changeRU**- Method that changes provisioned RU information into the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– RUDescription - The RU profile to change

– RUNewDescription (Optional - not allowed with RUValue)- The New name of the RU profile

– RUValue (Optional - not allowed with RUNewDescription) - The full list of RU values for this RU profile, this will overwrite the existing values.

– Codec (Optional - not allowed with RUNewDescription) - The Codec that this value refers to

– PacketRate (Optional - not allowed with RUNewDescription) - The packetisation rate this value refers to

– Value (Optional - not allowed with RUNewDescription) - The VCAC value for a call using this codec/packetrate.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

9. **queryRU** - Method that queries provisioned RU information from the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– RUDescription (Optional if omitted all RU profiles are returned)- The RU profile to query

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– RUDescription - If RUDescription ommitted from query then a list of multiple dexcription fields are returned.

– RUValue returned if a RUDescription query was requested. A value for every Codec/Packetrate combination is returned, this comprises of the following three parameters.

– Codec returned if a RUDescription query was requested.

– PacketRate returned if a RUDescription query was requested.

– Value returned if a RUDescription query was requested.

– ReturnCode

10. deleteRU - Method that deletes provisioned RU information from the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– RUDescription - The RU profile to be deleted

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

–

11. addLBL - Method that creates Limited Bandwidth Link information into the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– LBLname - A unique name for the LBL device

– CounterGWC (optional) a Counter GWC IP address, if ommited the Counter IPaddress is automatically allocated.

– RUDescription - The RU profile that this LBL device is using, the RU profile must exist already in the CS2k Mgr.

– MaxCount - The maximum value that this LBL can handle with respect to the number of calls using the Codec/Packetrate as defined in the RU profile.

– ParentMB - The parent middlebox name, a link into a middlebox hierarchy. The parent middlebox device must already be in the CS2k Mgr.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

12. changeLBL- Method that changes provisioned LBL information in the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– LBLname - The name for the LBL device to change.

– CounterGWC (optional) a new Counter GWC IP address.

– RUDescription (optional) - The new RU profile, the RU profile must exist already in the CS2k Mgr.

– MaxCount (Optional)- The new maximum value.

– ParentMB (Optional)- The new parent middlebox name. The parent middlebox device must already be in the CS2k Mgr.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

13. queryLBL - Method that queries provisioned LBL information from the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– LBLname (Optional, cannot be included as well as GWCname)- A Unique Name of a LBL device, to get full info on a device

– GWCname (Optional, cannot be included as well as LBLname) - To obtain a list of all LBLs on a GWC (Use GWC-XX format)

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– LBLname - if GWCname option used above, then a list of LBLnames returned without the full info on each device

– CounterGWC returned if LBLname option used.

– RUDescription returned if LBLname option used.

– MaxCount returned if LBLname option used.

– ParentMB returned if LBLname option used.

– ReturnCode

14. deleteLBL - Method that deletes provisioned LBL information from the CS2k Mgr. This method has the following parameters:

• Input data:

– usn

– version

– LBLname - The LBL device to be deleted

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

26: Functional Description (FN): A00002638

26.1 Feature name

PCA SW Metering Support for Billing

26.2 Description

26.2.1 Scope

The actual activity will extend the existing NAOC [1] - [7] and PCA [8] - [9] implementation to provide the availability of the software metering counter in the AMA extensions. This approach is needed in order to be fully compliant to the Spanish Metering Requirements [10]. The choosen approach is generic, so it can be reused for any International markets requesting this functionality.

The activity will reuse the existing NAOC tariff database and framework to provide tariff information for every single call. The existing PCA charge calculation routines will be extended to allow charge calculation

The pieces of functionality listed below are planned to be deployed with the current activity:

- Triggering the calculation of call charges for either
  a. all supported NAOC and PCA subscribers on a global (per switch) basis:
     – IBN
     – V5.2 IBN
     – PRI/QSIG
  b. specific PCA subscribers on a per line basis:
     – IBN
- Writing the calculated call charges into a newly introduced extension of the AMA module code 612
- Providing overall SOC control for the functionality mentioned above.

26.2.2 Value for the operator

The main area where PCA SW metering support for Billing can be used is the improvement of the billing process. By having call charges registed in real-time, billing process will be speeded up.

26.2.3 Brief Background Information

26.2.3.1 NAOC (Tariff Database Part)

Network **A**dvice **O**f **C**harge (NAOC) implements the tariffing of calls over the network boundaries. Two network configurations are supported:

1. It operates in a single/multiple carrier environment, where the originating exchange is able to determine the tariff. This improves the performance and reduces the messaging over the network (see Figure 1, "CGP tracking for a Combined CGP and CDP is supported (generic)"). This is generic functionality which supports all versions of ETSI ISUP interconnection trunks.
2. It operates in a multiple carrier environment, where the originating exchange (named Charged Generation Point, CGP) does not know the tariff that will be applied to the call for every call, so it has to retrieve the information over the network from the selected carrier's exchange called Charge Determination Point (CDP, see Figure 2, "NAOC messages are exchanged between different networks (Gemany only)").

Figure 1 CGP tracking for a Combined CGP and CDP is supported (generic)

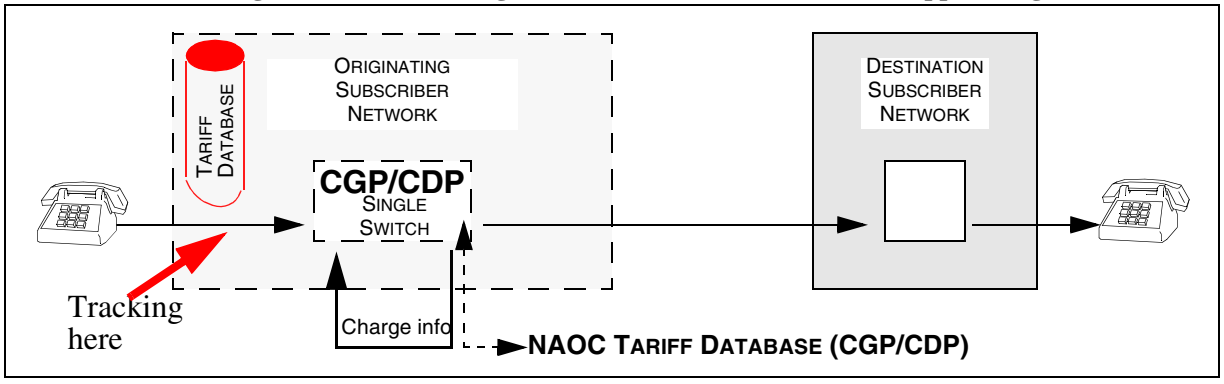
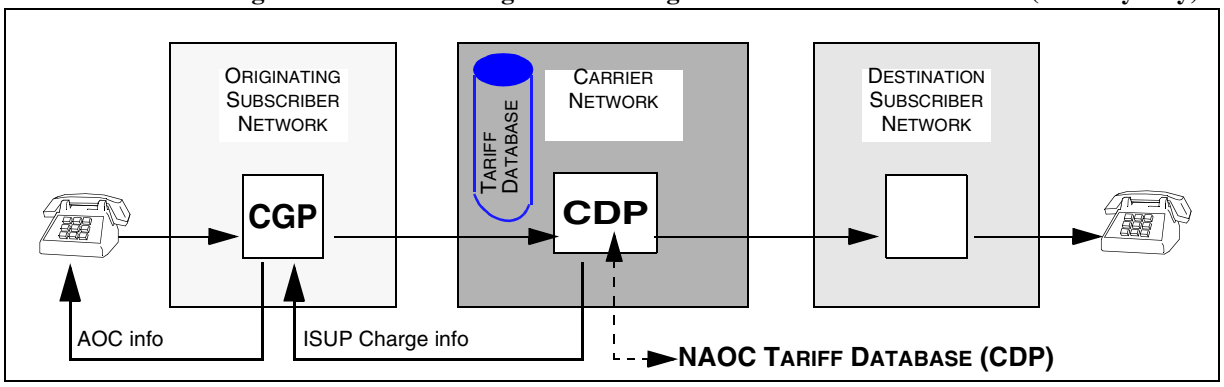


Figure 2 NAOC messages are exchanged between different networks (Gemany only)



NAOC support for basic call scenarios was developed during MMP12 - MMP13 [1] - [6]. The support for compex call scenarios was introduced in SN05 [7].

26.2.3.2 PCA (Hot Billing Part)

The Payment Ceiling Advice (***PCA***) feature provides a hot-billing functionality for the subscriber's account which allows a customer to meet Regulatory requirements [11] - [13]. The base PCA feature which reuses NAOC functionality was developed for IBN subscribers in the SN04 release for the Succession platform [8]. Additional Regulatory and market requirements were included in SN05 [7] and SN06 [9]. From SN06 onwards, PCA is also available for

1. for TDM IBN subscribers
2. for V5.2 IBN subscribers ob both TDM and CS2K

26.2.3.2.1 PCA feature description

An analogue line subscriber with Line Class Code (LCC) ***IBN*** may request that the ***PCA*** option be added to his or her primary directory number (DN). When ordering this service, the subscriber must specify a particular payment ceiling amount. This amount applies to each of the subscriber's billing cycle (generally every 29 - 32 days, but it can be any period of the year in terms of PCA). If no billing cycle is provided, the subscriber's account will never get resetted.

PCA comes with the following abilities:

- When performing a call, the subscriber's charges are counted during the call and written into the PCA database (PCADB) at the end of the call. This operation is done in real time, so that PCA can provide hot-billing abilities
- The PCA database can be queried at any point of time to retrieve the information regarding a specific subscriber's account.
- The PCA database information can be displayed in either currency units or virtual pulses (which correspond to 1/1000 of one currency units)
- Complex tariff structure described by the NAOC tariffs is fully supported
- Several complex calls scenarios as described in [12] are supported
- PCA database can be automatically resetted based on the provisioned information
- Announcements are provided for approaching or exceeding the PCA limit:
    - ***i. Prepaid or tracking phone bill***

- When a subscriber approaches the PCA limit by exceeding the 80% PCA limit, he hears a (provisionable) announcement he is approaching his limit
- When he exceeds his PCA limit, he hears the announcement, that he exceeds his limit. Depending on the datafilled information, he might not be able to do any additional phone calls (prepaid) or only some specific call classes

ii. Bonus notification

- When a subscriber exceeded the 80% limit, he hears an announcement that encourages him to perform additional calls to get the discount
- When he exceeded his PCA limit, he hears the announcement that he qualified to get a bonus

• PCA supports prepaid functionality and selective force release:

— *Prepaid:*

- When exceeding his PCA limit, the subscriber cannot perform any calls except emergency calls and charge free calls
- When the prepaid account expires, the account is resetted, so that the subscriber cannot perform any calls except emergency calls and charge free calls

— *Selective force release:*

- Depending of the datafilled information, only specific call classes are allowed after the subscriber reached his PCA limit during a call or during the last call

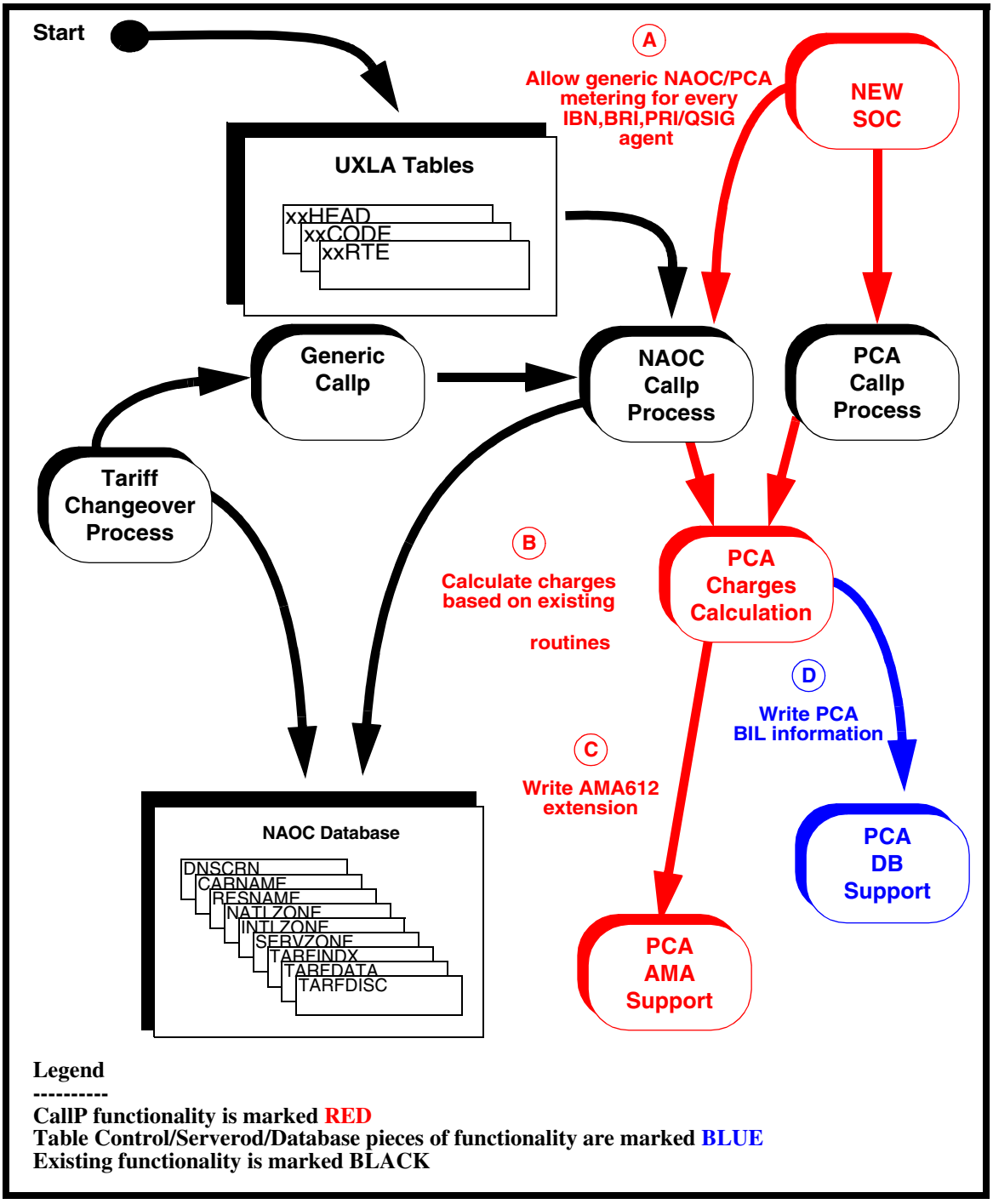
26.3 General Feature Description

The current activity contains of several independant components listed in Chapter “26.2.1 Scope” on page 709. Therefore, the behaviour will be described on a component basis in the chapters below. A brief overview is given in “Figure 3 Interactions with existing NAOC/PCA features” on page 713.

26.3.1 Behaviour

The feature activation will be done by turning SOC on or by assigning the new PCA mode “BIL” to a PCA line.

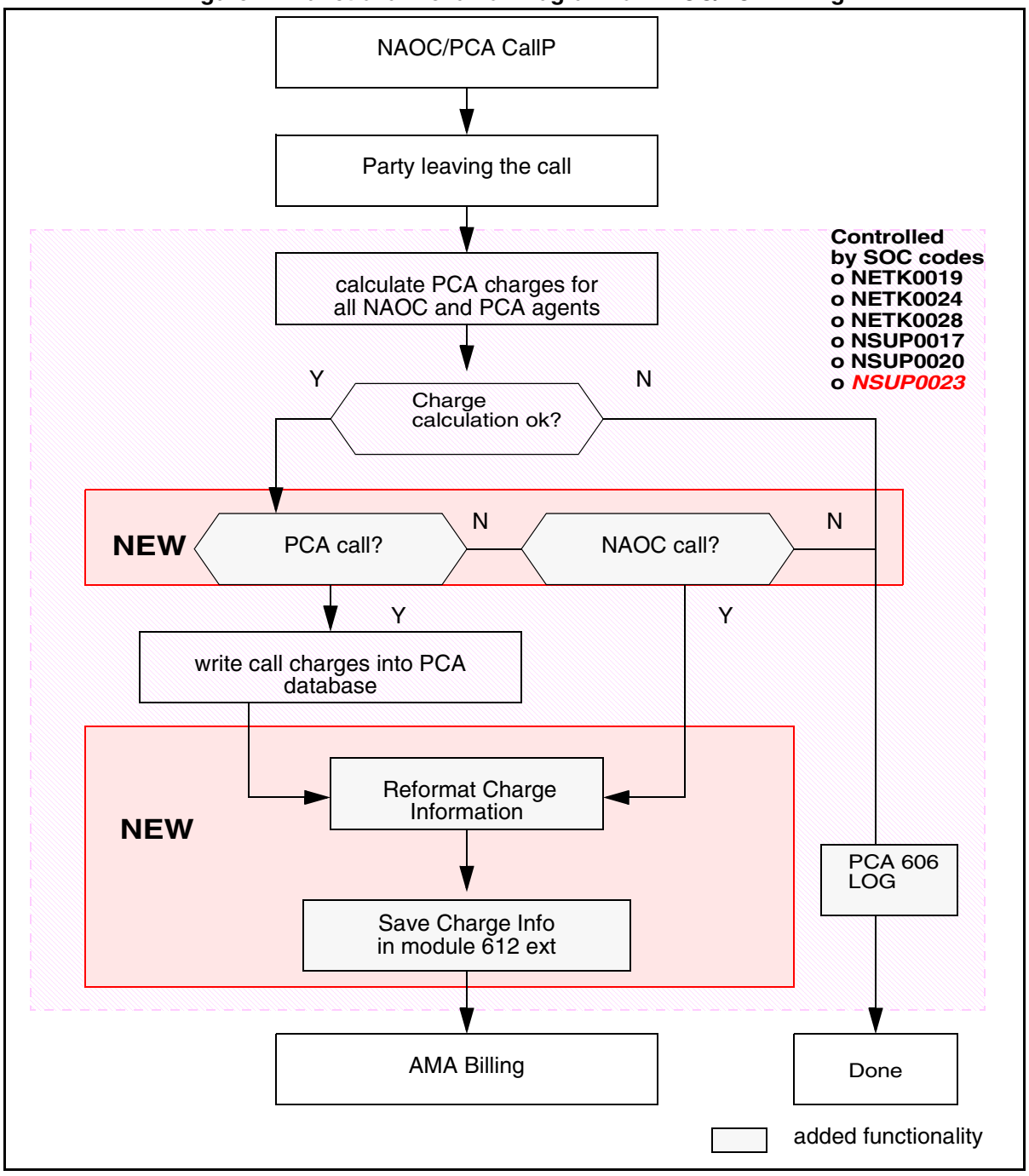
Figure 3 Interactions with existing NAOC/PCA features



Changes are done to both NAOC and PCA CallP code to trigger the call calculation when one party leaves the call. (“Figure 4 Functional Behavior Diagram for NAOC/PCA Billing” on page 714). The calculated call charges

are written in pulse units in the AMA record and if PCA BIL is assigned to the line, they are added to the PCA database.

Figure 4 Functional Behavior Diagram for NAOC/PCA Billing



The calculation of call charges is triggered by the PCA framework. In addition to writing the call charges into the PCADB the just calculated call charges are added to an AMA record as a module 612 extension.

The 30 BCD characters contained in this module 612 extension would be distributed as follows:

Figure 5 New module 612 extension used for NAOC/PCA billing

BCD Char	Length	Meaning
1 - 3	3	**Rating Class at the beginning of the Call** If the billing record is generated by basic call this field will contain the tariff index used for this call from Table TARFDATA, bound by an upper limit of 511 for the Spanish market. If the billing record is generated by a feature action this field will always be set to the value of "511".
4 - 11	8	**Used Meter** The total number of meter pulses **used** for this call or feature action.
12 - 15	4	**Initial meter value MS** The 4 most significant digits of the initial meter pulse value.
16 - 19	4	**Initial meter value LS** The 4 least significant digits of the initial meter pulse value.
20 - 27	8	**Final Meter value** The final meter pulse value, i.e., initial value + used value.
28 - 29	2	**Call Type** This field describes if this is a **basic call** or a **feature action**. If the billing record is generated by basic call this field will be equal to "00". If the billing record is generated by a feature action this field will be equal to a value based on the particular feature as it is provisioned in table NAOCFEAT (per the carrier/reseller).
30	1	**Feature Action**[a] This field describes the type of feature action If the billing record is generated by basic call this field will be equal to "2". If the billing record is generated by a feature action this field will be equal to one of 10 values based on the type of action: (0) assign (1) deassign (2) administrative activation (3) administrative deactivation (4) administrative programming (5) subscriber activation (6) subscriber deactivation (7) subscriber programming (8) usage (9) interrogation

a. Feature billing is described in PLS FMDOC, Module a00002654.

Figure 11, "AMA Record with Module 612 extension" contains an example of an AMA record with the 612 extension.

Figure 6 Sample AMA Record With Module 612 Extension

```
HEX ID:                              AA
STRUCTURE CODE:                      40510C
CALL CODE:                           006C       STATION PAID
SENSOR TYPE:                         036C       DMS 100F
SENSOR ID:                           0250250C
REC OFFICE TYPE:                     036C       DMS 100F
REC OFFICE ID:                       0250250C
DATE:                                30903C     SEPTEMBER 03, 2003
TIMING IND:
    TIMING GUARD FLAG                0          UNUSED
    SHORT CLD PARTY OFF-HOOK IND     0          UNUSED
    LONG DUR/SERV PTY CAPABILITY IND 0          UNUSED
    UNUSED                           0
    UNUSED                           0C
STUDY IND:
    STUDY TYPE A                     0          UNUSED
    STUDY TYPE B                     2          NETWORK COMPLETION
    STUDY TYPE C                     0          UNUSED
    TEST CALL IND                    0          UNUSED
    UNUSED                           0
    ORIG/TERM NANP NUM IND           0          UNUSED
    OPERATOR SERV IND                0C         UNUSED
CLD PTY OFF-HK:                      0C         CLD OFF-HOOK DETECTED
SERVICE OBSERVED:                    0C         NONE
OPER ACTION:                         0C         ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:                     000C       OTHER
SIG DIGITS NEXT FIELD:               010C
ORIG OPEN DIGITS 1:                  01418420317C
ORIG OPEN DIGITS 2:                  FFFFFFFFFF
ORIGINATING CHARGE INFO:             FFFF
DOMESTIC/INTL INDICATOR:             1C         DOMESTIC
SIG DIGITS NEXT FIELD:               007C
TERM OPEN DIGITS 1:                  00008406301C
TERM OPEN DIGITS 2:                  FFFFFFFFFF
CONNECT TIME:                        000000000C 000000:00.0
ELAPSED TIME:                        000011204C 000011:20.4
MODULE CODE:                         612C       GENERIC MOD: TWO DGT STR FMT
GENERIC CONTEXT ID:
    PARSE RULES                      80070      NAOC PCA CHARGING INFO
    SIGNIFICANT DIGITS               00C        NIL
GENERIC DIGIT STRING ONE:
    RATING CLASS                     010
    USED METER                       00000028
    INITIAL_METER_MS                 4000
GENERIC DIGIT STRING TWO:
    INITIAL_METER_LS                 0000
    FINAL METER                      40000028
    CALL_TYPE                        00
    FEATURE ACTION                   2
MODULE CODE:                         000C       FINAL MODULE
```

26.3.2 How To Convert Virtual Pulses To Meter Pulses

The **used meter** value in the AMA module 612 is a function of virtual meter pulses as used by the PCA feature and the provisioning in table CURRCONV.

In order to understand the conversion function you will need some background information:

- The value of a single virtual pulse is equal to 0.001 monetary units, this **cannot** be changed via provisioning.
- The value of a single meter pulse is based on the provisioning in table CURRCONV, specifically the third tuple. This is shown below in Figure 7.

Figure 7 Table CURRCONV - meter pulse value

```
>table currconv
>list all
TOP
CURRNAME CURRVAL
----------------
CHARGING 1 0
DEFAULT 1 0
EURO 6 -2        <-- one meter pulse is 0.06 Euros
BOTTOM
```

The function for the conversion is as follows:

```
meter pulses = (vpa/cv_val) * (1/10^[3+cv_exp])
```

Where:

- **vpa** is equal to the actual number of virtual pulses used.
- **cv_val** is equal to the **value** from the third tuple of table CURRCONV.
- **cv_exp** is equal to the **exponent** from the third tuple of table CURRCONV.

So if we have a call that has used 5630 virtual pulses, the calculation of the number of meter pulses is as follows (based on the provisioning shown in Figure 7):

```
vpa     = 5630
cv_val  = 6
cv_exp  = -2

meter pulses = (5630/6) * (1/10^[3+(-2)])
meter pulses = 93.83
meter pulses = 94 (rounded off)
```

The PCADB level of the NAOCCI tool has been updated with a new command called “convert”. This new command can be used to view this conversion function (including the information from table CURRCONV). The command simply takes the **vpa** as input and it prints out the number of meter pulses based on the **vpa** and data in table CURRCONV, as shown in Figure 8.

Figure 8 CI ‘convert’ command - pcadb level of the naocci tool

```
PCADB:
>convert 5630
Result: 5630 virtual pulses are equal to 94 meter pulses
```

26.4 Interworking

A brief overview of the supported agent interworkings is given below. The combinations of supported interworkings depend on the available NAOC and PCA agents and are listed in “Figure 9 Agent interworking for the current feature” on page 718.

Figure 9 Agent interworking for the current feature

Platform	Originator	Terminating agents							
		IBN lines	ETSI PRI	QSIG (95)	PUSI)	SIP-T	ETSI ISUP V1	ETSI ISUP V2/V2+	BRI
CS2K	IBN	X							
	V5.2 IBN	X							
	PRI/QSIG	X							

As the current functionality ties into the NAOC/PCA framework, the actual feature is able to exist with the features listed below in “Figure 10 Agent interworking for the current feature” on page 718. Red fields mark functionality that has not been implemented while blue fields stand for functionality which was not defined

Figure 10 Agent interworking for the current feature

Platform	Originator for SW Metering Support for Billing	Feature to interact		
		Line HW Metering[a]	AOC[b]	PCA
CS2K	IBN	X		X
	V5.2 IBN			X
	PRI/QSIG		X	

a. Line HW Metering on CS2K is not supported for V5.2 IBN and and not defined for PRI/QSIG
b. AOC is not defined for IBN and V5.2 IBN. Line HW Metering is used instead

26.5 Activation

26.5.1 Global activation via SOC

If all agents have to write their call charges in the AMA records extension, a global activation is needed. This is done by using the SOC code ***NSUP0023*** to activate the trigger for all supported NAOC / PCA agents. This avoids the need to assign AOC or PCA to every single agent.

For this approach, charge calculation will be done in the background. Line agents which have not subscribed PCA will not be seen in the PCA database.

26.5.2 Per line PCA billing activation

26.5.2.1 Provisioning

If a per line activation is needed for PCA functionality is needed, the ***BIL*** option has to be set. This implies that no credit limit tracking will be needed, so no PCA Limit or FRLS information will be neededA provisioning example for the prepaid functionaliy is given below (Figure 11, "How to datafill the PCA per line billing functionality")

Figure 11 How to datafill the PCA per line billing functionality

```
>ado
SONUMBER:      NOW   2  5 24 PM
>
DN_OR_LEN:
>8838441000
OPTION:
>pca
BASE_DN:
>$
CAR_RES_NAME:
>car88
ESSENTIAL:
>Y
PCA_CURRENCY:
>EUR
PCA_MODE
>BIL
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 2 5 24 PM 8838441000 ( PCA $ CAR88 Y EUR BIL) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

26.5.2.2 PCA tracking per access interworking with BIL

PCA tracking per access provides a possibility to use one base DN for multiple lines with separate DNs. That is, call charges for all lines of that access are

tracked via one dedicated DN (referred to as base DN). There is specific limit for the number of DNs that can be linked to a base DN.

Call charges will be accumulated to the subscriber's account balance after the call was finished. This number will be used as a source for the billing number.

26.6 Hardware Requirements or Dependencies

This feature does not add any additional hardware requirements and dependencies on top of those one used for NAOC and PCA or for the features that NAOC/PCA do interact with.

26.7 Software Requirements or Dependencies

This feature requires the following features to be activated by SOC:

- ***NETK0019*** Network AOC
- ***NETK0024*** Network AOC Tariff
- ***NETK0028*** CGP Network AOC
- ***NSUP0017*** Payment Ceiling
- ***NSUP0020*** NAOC/PCA Supp Svcs
- ***NSUP0023*** PCA SW Metering Support for Billing (this feature)

NAOC tariff information is required, since ***PCA*** reuses the ***NAOC*** functionality. If no ***NAOC*** information is provided, the payment ceiling counter cannot be updated for that call. NAOC datafill including the NAOC tables and translation options have to be set up in a appropriate way. Please refer to [1] - [7] for additional information.For the per line assignment (PCA BIL), the PCA framework has to be datafilled in a proper way according to [9]. The PCA announcement for the 80-99.9% notification must be datafilled with the announcement CLLI ***PCA1***. The announcement for exceeding the 100% limit must be datafilled with the announcement CLLI ***PCA2***.

26.8 Limitations and restrictions

1. The following limitations and restrictions were inherited from the former PCA features [8], [9]. They have to be considered only if the per line activation (PCA BIL option) is turned on. They will have no effect for the case where the feature is activated by SOC:
   - — PCA and ELN [14] are mutually exclusive, since PCA would restrict the ability of the subscriber to perform calls in emergency cases. Therefore PCA is not allowed on ELN lines.
   - — Emergency calls take priority over PCA, so if the subscriber makes an emergency call, the PCA announcement will not be activated.

— Overlap outpulsing is not supported when a line with PCA has reached at least 80% of its payment ceiling limit.

— PCA may be assigned only to the primary DN of line accesses with multiple DNs (e.g. SDNs). All charges made to that line access will count towards a single payment ceiling limit.

— Fixed Price Service (FPS) and PCA are mutually exclusive and may not be assigned to the same analogue line.

— The Announcement Before Routing (ABR) feature and PCA are incompatible and may not be assigned to the same IBN line. Servord prevents the craftsperson from making such an assignment.

— PCA can be assigned to a maximum number of 65,535 lines per node.

— Per node, there can be up to 65,535 DNs linked to a single base DN

— Nevertheless, the PCA accuracy will be always 1/1000 of one unit datafill with SERVORD. So if the meaning of the value datafilled is 1 million currency units (e.g. Turkish Lira), the accuracy will be 1000 currency units (1000 Turkish Lira)

26.9 Recommendations

1. The following recommendations were inherited from the former PCA development [8], [9]. They have to be considered only if the PCA BIL option is turned on. They will have no effect for the case where the feature is activated by SOC:

- It is not recommended to reset the PCA entries during an active call, if the subscriber has not exceeded his limit yet. Doing so may result in the subscriber hearing the mid-call warning tone prematurely (if limit is being increased) or erroneously not hearing the tone when the 100% limit is reached (if limit is being decreased).
- It is recommended that fax and modems have any Voice Detection Features deactivated, if possible. It is also recommended that these devices have their connection set-up timers set to at least 60 seconds. Announcement length should not exceed 60 seconds.

26.10 Interactions

1. All ***NAOC*** [1] - [7] and ***PCA*** [8], [9] feature interactions also apply to this feature.

2. On a TDM platform, AOC Hardware Metering and PCA can coexist and function independently

26.11 Applicable customer facing sections

Fault Management	
Logs	___X___
Alarms	__N/A__
Configuration	
Data Schema	__N/A__
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A_
Service Order	___X__
Office Parameters	__N/A_
Accounting (includes AMA billing)	___X__
Performance (includes operational measurements)	___X__

26.12 NAOC and PCA history

Figure 12 Overview of the NAOC and PCA development

Type	Stream	Activity	ACTID	Description of Reference
NAOC	MMP12	SIM	ND0076	*German Network-AOC Support over ISUP*, Issue AA03, Version: Pre 1.1, PLS MDIVDOC module: *ND0076*.
			ND0035	*AOC for NLOs Strategic Interface Management (SIM)*, Issue AA03, Release: ISSUE 2.7, PLS MDIVDOC module: *ND0035*.
		Feature	59007987	*ETSI ISUP - Network AOC (CDP+CGP)*, Issue AA25, PLS FMDOC module: *network_aoc_etsi_isup.*
			59008229	*ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)*, Issue AA67, PLS FMDOC module: *naoc_etsi_isup_tariff_db_tco.*
		Feature	59007780	*Network AOC CGP Function*, Issue AA18, PLS FMDOC module: *A59007780.*
	MMP13		59012308	*ETSI ISUP Network AOC - analog enhancement,* Issue AA15, PLS FMDOC module *A59012308 (TDM only)*
			59012315	*ETSI ISUP Network AOC - V5.2 enhancement,* Issue AA02, PLS FMDOC module *A59012315*
		Feature	59013775	*Network AOC: Integrated CGP and CDP,* Issue AA27, PLS FMDOC module: *A59013775.*
	ISNH03		59032878	*NAOC on PRI,* Issue AA05, PLS FMDOC module: *A59032878.*
PCA	SN04		59034497	*Payment ceiling for Succession Intl. Cable IP,* Issue AA32, PLS FMDOC module: *A59034497.*
	SN05		59039121	*NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD,* Issue AA30, PLS FMDOC module: *A59039121.*
NAOC	SN06		89007454	*NAOC Regulatory Enhancements,* Issue AA17, PLS FMDOC module: *A89007454.*
PCA			89007461	*Payment Ceiling Regulatory Enhancements,* Issue AA40, PLS FMDOC module: *A89007461.*
NAOC	SN06.2		A00001927	*Line Hardware Metering,* Issue AA03, PLS FMDOC module: *A00001927.*
			A00002625	*Full Line HW Metering / Billing Compliance*, Issue AA01, PLS FMDOC, module: *A00002625.*
			A00002737	*NAOC Trunk Metering Enhancements,* Issue AA02, PLS FMDOC module: *A00002637.*

26.13 Glossary

Term	Description
AOC	Advice of Charge
CDN	Called Party Directory Number
CDP	Charge Determination Point
CGN	Calling Party Directory Number
CGP	Charge Generation Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000
ELN	Essential Line
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
MMP	Multi Market Platform
NAOC	Network Advice of Charge
PCA	Payment Ceiling Advice
PVG	Passport Voice Gateway
PRI	Primary Rate Interface
PUSI	National variant of ETSI ISUP in Spain
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol - Telephony
SNP	Service Number Portability
UXLA	Universal Translations
XLA	Translations

26.14 References

REF #	Description of Reference
[1]	Feature 59008229, *ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)*, Issue AA62, PLS FMDOC module: *naoc_etsi_isup_tariff_db_tco.*
[2]	Feature 59007987, *ETSI ISUP - Network AOC (CDP+CGP)*, Issue AA20, PLS FMDOC module: *network_aoc_etsi_isup.*
[3]	Feature 59007780, *Network AOC CGP Function*, Issue AA17, PLS FMDOC module: *A59007780.*
[4]	Feature 59013775, *Network AOC: Integrated CGP and CDP* Issue AA27, PLS FMDOC module: *a59013775.*
[5]	Feature 59032878, *NAOC on PRI* Issue AA05, PLS FMDOC module: *a59032878.*
[6]	Feature 89007454, *NAOC Regulatory Enhancements,* Issue AA17, PLS FMDOC module: *A89007454*
[7]	Feature 59039121, *NAOC and PCA Feature Interworking,* Issue AA32, PLS FMDOC module: *A59039121*
[8]	Feature 59034497, *Payment Ceiling for Intl. Cable IP*, Issue AA32, PLS FMDOC module: *A59034497*
[9]	Feature 89007461, *Payment Ceiling Regulatory Enhancements*, Issue AA40, PLS FMDOC module: *A89007461*
[10]	Rating in the digital switching exchanges, GT.ER.d4.463 (Spanish Metering specification)
[11]	German Telecommunikation Decree, “Telekommunikations Kundenschutzverordnung” - Article 18 http://www.regtp.de/gesetze/00991/03/index.html
[12]	EU “Universal Service” Directive 2002/22 - Article 10 (Control of expenditure) http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00510077.pdf
[13]	Directive of the Spanish Minister of Science and Technology from Dec 28th, 2001http://www.derecho.com/cometatech.com?producer=Legislacion&op=detalle_legislacion&id_legislacion=114384&process=html&stylesheet=legislacion/mcyt/detalle-ley.xsl
[14]	Feature ICCMSEROPTELM, *ELN - Essential LIne,* Issue AC01, PLS MICA module: ICCMSEROPTELM
[15]	Feature 00002654, *CEPT AR (Class Callback for Telefonica)*, Issue AA21, PLS FMDOC module: *a00002654.* (This contains the feature billing documentation for Table NAOCFEAT)

27: Functional Description (FN): A00002639

27.1 Feature name

"CEPT PSTN: Analogue Call Waiting Indication"

27.2 Description

This activity provides the following functionality in addition to the existing CEPT Analogue Call Waiting Indication functionality implemented by the activity A59019288, CEPT Call Waiting (FMDOC):

- "Caller Call Waiting" announcement: The waiting party gets an announcement played, that the call is waited. Then normal ringing tone is played. The announcement is optional and controlled by datafill.
- "Called Party Ignores Waiting Call" announcement: After 30sec period (hardcoded), the waiting party hears an announcement followed by a datafillable treatment (please refer to the bullet "Call Waiting Timeout Treatment" below). The announcement is optional and controlled by datafill.
- "Call Waiting Timeout Treatment" . After 30 secs timer expiry (and after the Called Party Ignores Waiting Call announcment, if being applied), a treatment (busy, answer, no_service_circuit timeout etc.) is applied to the Call Waiting Line. The treatment is defined by datafill.

27.2.1 Caller Call Waiting Announcement

The Caller Call Waiting Announcement is applied to the Calling Party if:

- The Called Party has ICWT line option datafilled and activated as covered in section Figure 27.2.3, "Datafilling and activating ICWT (CEPT CWT) option",

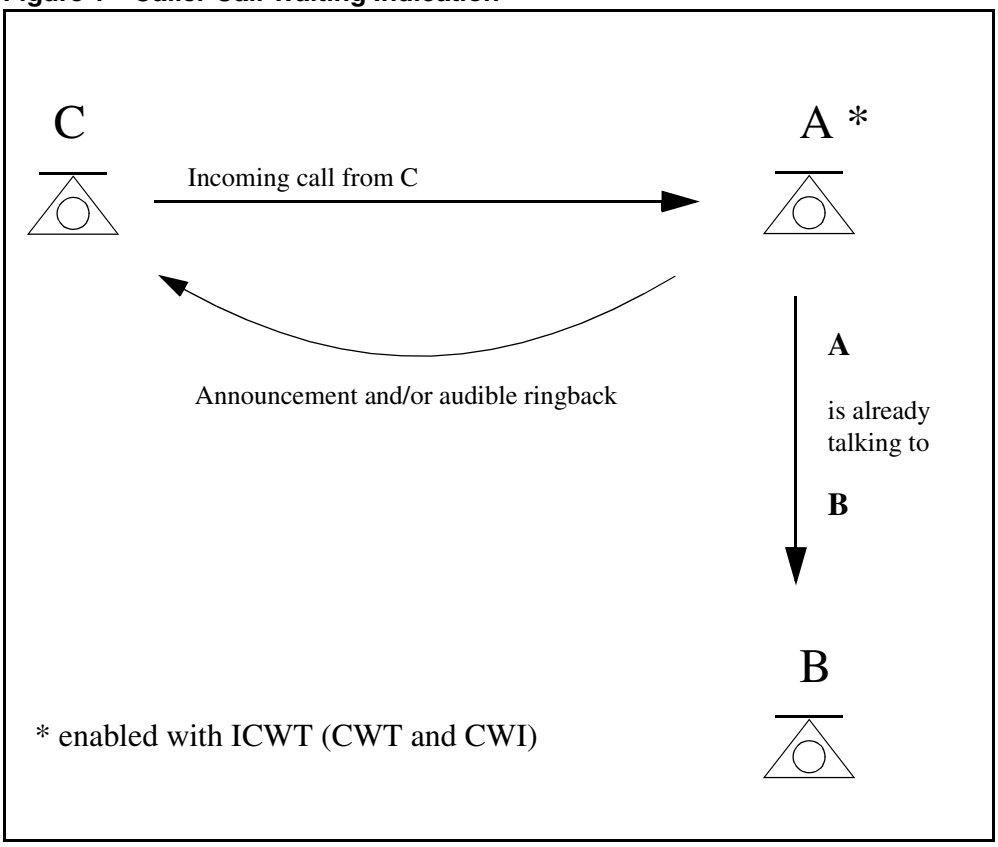
  or

- the Customer Group of the Called Party has ICWT option datafilled in table CUSTSTN and activated by the Called Party as covered in section Figure 27.2.4, "Datafilling and activating Customer Group Based ICWT option",
- The ICWT announcement datafill covered in section "Datafilling ICWT Announcements" on page 730, is done, and
- The boolean ICWT_ANN_ACTIVE of option ICWT is activated (i.e. is set to 'Y') as described in section Figure 27.2.6.1, "Activation of boolean ICWT_ANN_ACTIVE".

The announcement is followed by the standard ring back tone.

If the boolean ICWT_ANN_ACTIVE of option ICWT is set to ‘N’ and if the Called Party has ICWT option datafilled, the standard ring back tone is applied to the Calling Party.

Figure 1 Caller Call Waiting Indication



27.2.2 “Called Party Ignores the Waiting Call” Announcement

If the Called Party ignores the Waiting Call, the “Called Party Ignores the Waiting Call” announcement is applied to the Calling Party to indicate that the Called Party ignored the call if:

- The Called Party has ICWT line option datafilled and activated as covered in section Figure 27.2.3, "Datafilling and activating ICWT (CEPT CWT) option",

  or

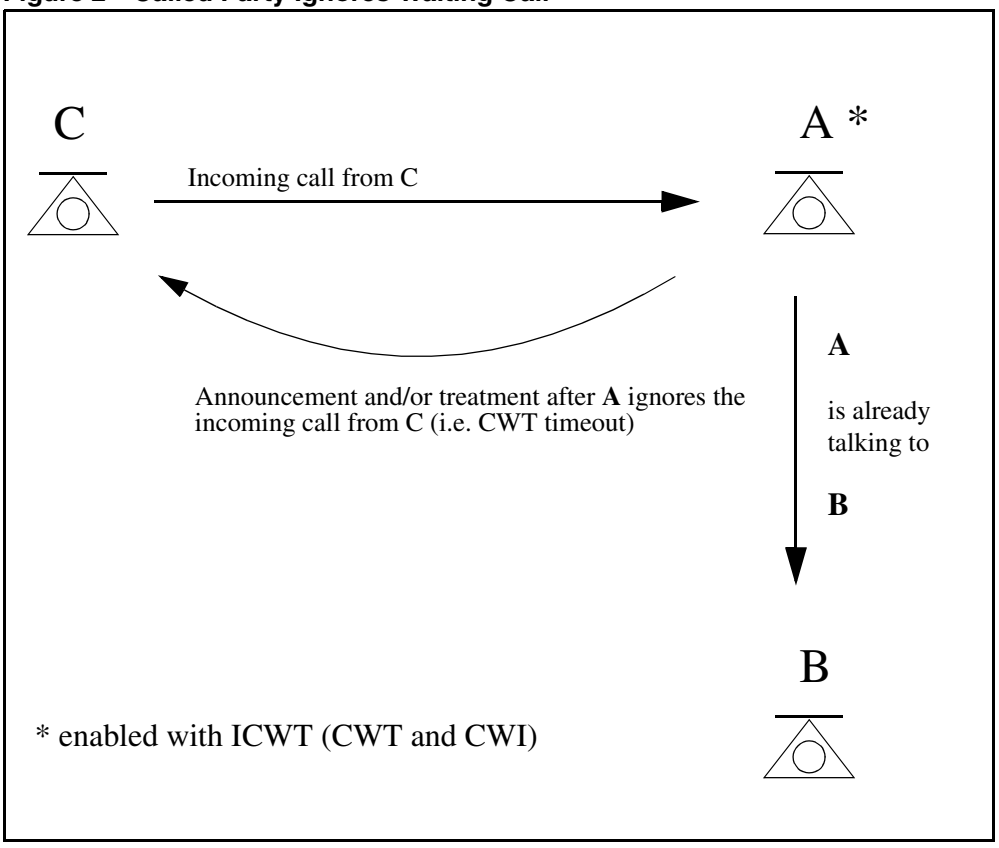
  the Customer Group of the Called Party has ICWT option datafilled in table CUSTSTN and activated by the Called Party as covered in section Figure 27.2.4, "Datafilling and activating Customer Group Based ICWT option",

- The ICWT announcement datafill covered in section “Datafilling ICWT Announcements” on page 730, is done, and
- The boolean ICWT_TMO_ANN_ACTIVE of option ICWT is activated (i.e. is set to ‘Y’) as described in section Figure 27.2.6.2, "Activation of boolean ICWT_TMO_ANN_ACTIVE".

The announcement is followed by the treatment datafilled in ICWT_TMO_ANN_ACTIVE sub-field of ICWT tuple.

If the boolean ICWT_TMO_ANN_ACTIVE is set to ‘N’ and if the Called Party ignores the Waiting (Calling) Call, the treatment datafilled in ICWT_TMO_ANN_ACTIVE sub-field of ICWT tuple is applied to the calling party. For datafilling the ICWT timeout treatment, please refer to section Figure 27.2.6.3, "Datafilling of ICWT_TIMEOUT_TREATMENT".

Figure 2 Called Party Ignores Waiting Call



27.2.3 Datafilling and activating ICWT (CEPT CWT) option

The following figure shows the steps for adding and activating the ICWT line option to the Called Party:

Figure 3 Steps for adding and activating ICWT line option to the Called Party

```
>servord
SO:
>ado $ 8888587771001
OPTION:
>CEPT
OPTION:
>ICWT
ICWT_ACTIVE:
>y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 6 7 PM 8888587771001 ( CEPT ) ( ICWT Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

27.2.4 Datafilling and activating Customer Group Based ICWT option

The following figure shows the steps for adding and activating the Customer Group Based ICWT option to the Customer Group of Called Party:

Figure 4 Steps for adding and activating Customer Group Based ICWT option

```
>table custstn
>pos ruacept cept
>cha
OPTION: CEPT
>
DEFAULT_FEATURE_ON: N
>y
DEFFTR:
>icwt
DEFFTR:
>$
TUPLE TO BE CHANGED:
RUACEPT CEPT CEPT Y (ICWT) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

For activating the ICWT option by the user, please refer to the FN section of activity A59019288, CEPT Call Waiting (sub-section, Feature Activation, Deactivation, Interrogation).

27.2.5 Datafilling ICWT Announcements

The “Call Waiting” and “Called User Ignores Waiting Call” announcements are datafilled using the existing CS2K announcement capabilities. Please, note that the CLLIs used for “Call Waiting” and “Called User Ignores Waiting Call” announcements are **hardcoded** to **ICWTANN** and **ICWTTMOANN**, respectively.

The following figure shows the steps for datafilling the ICWT announcements:

Figure 5 Example for datafilling ICWT Announcements

```
table clli
ove; ver off;
add ICWTANN 70 10 ICWT_ANNOUNCEMENT y y
add ICWTTMOANN 71 10 ICWT_ANNOUNCEMENT y y
quit

table anns
ove; ver off;
add ICWTANN NETWK 5 10 1 STND N 5
add ICWTTMOANN NETWK 5 10 1 STND N 5
quit

table annmems
ove; ver off;
add ICWTANN 0 UAS AUD 0 AUD 0
add ICWTTMOANN 0 UAS AUD 0 AUD 0
quit

table annphlst
ove; ver off;
add ICWTANN 0 AUD_546 $
add ICWTTMOANN 0 AUD_547 $
quit
```

The following figure shows the steps for bringing the ICWT announcement trunks inservice:

Figure 6 Steps for bringing the ICWT announcement trunks Inservice

```
mapci;mtc;trks;ttp

post g ICWTANN
bsy; rts

post g ICWTTMOANN
bsy; rts

quit all
```

27.2.6 ICWT Tuple in Table ISERVOPT

In table ISERVOPT, a new option, ICWT, is introduced to indicate whether the Call Waiting Announcements to be applied to the Waiting (Calling) party.

Option ICWT has three sub fields, ICWT_ANN_ACTIVE, ICWT_TMO_ANN_ACTIVE and ICWT_TIMEOUT_TREATMENT which activate/deactivate “Caller Call Waiting” announcement , “Called Party Ignores Waiting Call” announcement and datafills “Timeout Treatment Value”, respectively.

The Call Waiting Announcements can be activated/deactivated independent from each other.

27.2.6.1 Activation of boolean ICWT_ANN_ACTIVE

The standard audible ringback is the default tone for ICWT feature provided to the Calling Party. The new boolean ICWT_ANN_ACTIVE of option ICWT needs to be activated (i.e. set to ‘Y’) in table ISERVOPT to allow Caller Call Waiting announcement to the Calling party.

The following figure shows an example of how to add and activate the boolean ICWT_ANN_ACTIVE.

Figure 7 Example for adding and activating ICWT_ANN_ACTIVE boolean

```
>table iservopt
>add icwt
>y
OPTION:
>icwt
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y/n
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)
TUPLE TO BE ADDED:
ICWT ICWT Y    Y/N BUSY


ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

The following figure shows an example of how to activate the boolean ICWT_ANN_ACTIVE if it is already deactivated.

Figure 8 Example for activating ICWT_ANN_ACTIVE boolean

```
>table iservopt
>format pack
>pos icwt
        ICWT ICWT N   Y/N BUSY
>cha
>y
OPTION: ICWT
>
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y/n
ICWT_TIMEOUT_TREATMENT:
> BUSY_LINE (one of the EXTENDED_TREATMENT)
TUPLE TO BE CHANGED:
        ICWT ICWT Y   Y/N BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
```

27.2.6.2 Activation of boolean ICWT_TMO_ANN_ACTIVE

The standard busy tone is the default tone for ICWT feature provided to the Calling Party if the Called Party ignores the Waiting Party. The new boolean ICWT_TMO_ANN_ACTIVE of option ICWT needs to be activated (i.e. set to 'Y') in table ISERVOPT to allow announcement to the Calling party indicating that the Called Party ignores the Waiting Party.

The following figure shows an example of how to add and activate the boolean ICWT_TMO_ANN_ACTIVE.

Figure 9 Example for adding and activating ICWT_TMO_ANN_ACTIVE boolean

```
>table iservopt
>add icwt
>y
OPTION:
>icwt
ICWT_ANN_ACTIVE:
>y/n
ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)
TUPLE TO BE ADDED:
ICWT ICWT Y/N   Y BUSY

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

The following figure shows an example of how to activate the boolean ICWT_TMO_ANN_ACTIVE if it is already deactivated.

Figure 10 Example for activating ICWT_TMO_ANN_ACTIVE boolean

```
>table iservopt
>format pack
>pos icwt
        ICWT ICWT   Y/N  N BUSY
>cha
>y
OPTION: ICWT
>
ICWT_ANN_ACTIVE:
>y/n
>ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)

TUPLE TO BE CHANGED:
        ICWT   ICWT   Y/N   Y BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
```

27.2.6.3 Datafilling of ICWT_TIMEOUT_TREATMENT

The third sub field of ICWT tuple in ISERVOPT is ICWT_TIMEOUT_TREATMENT which is used to select timeout treatment value. The type of the treatment is EXTENDED_TREATMENT (please refer to following table).

UNDT (Undefined_Treatment) is not supported as an ICWT Timeout Treatment and datafilling is prevented by the table control.

If the ICWT tuple is removed from the ISERVOPT table the default value of ICWT_TIMEOUT_TREATMENT is NOSC (no_service_circuit) treatment.

Figure 11 Example for ICWT_TIMEOUT_TREATMENT datafill

```
>table iservopt
>format pack
>pos icwt
          ICWT ICWT    Y/N  N BUSY
>cha
>y
OPTION: ICWT
>
ICWT_ANN_ACTIVE:
>y/n
>ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
>ss
 ***  ERROR  ***
SS
|
TYPE OF ICWT_TIMEOUT_TREATMENT IS EXTENDED_TREATMENT
ICWT_TIMEOUT_TREATMENT:
>ss
 ***  ERROR  ***
SS
|
TYPE OF ICWT_TIMEOUT_TREATMENT IS EXTENDED_TREATMENT
TYPE IS EXTENDED_TREATMENT
{UNDT,NOSC,PDIL,PSIG,INAC,CNDT,VACT,MSCA,MSLC,
                  NBLH,NBLN,EMR1,EMR2,UNCA,SYFL,CQOV,HNPI,UNDN,
                 BLDN,BUSY,UNOW,TDND,UNIN,SSTO,NCRT,RODR,MANL,
                 ORSS,TESS,OPRT,TRBL,ANCT,PNOH,DNTR,NECG,FECG,
.....
                   CCRG,CCRP,CCRM,CCRH,CCRT,MSOA,RTEE,CRTC,CBFC,
                 CMGA,CMGD,RMIA,RMID,PODN,RL00,RL01,RL02,RL03,
                 RL04,RL05,RL06,RL07,RL08,RL09,RL10,RL11,RL12,
                 RL13,RL14,RL15,RL16,RL17,RAGC,UNMC,FACJ,ICCB,
                 RDIR}
ICWT_TIMEOUT_TREATMENT:
>BUSY


TUPLE TO BE CHANGED:
          ICWT    ICWT    Y/N    Y BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
```

27.2.7 Deactivation of Caller Call Waiting Announcement

There are four ways of deactivation of applying Caller Call Waiting announcement to the Calling Party:

27.2.7.1 By deactivating or deleting ICWT option

The following figure shows the steps for deleting the ICWT line option from the Called Party:

Figure 12 Steps for removing ICWT line option from the Called Party

```
>servord
SO:
>deo $ 8888587771001
OPTION:
>ICWT
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 6 13 PM 8888587771001 ( ICWT ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

27.2.7.2 By deactivating or deleting Customer Group Based ICWT option

For deactivation of the ICWT option, please refer to the FN section of activity A59019288, CEPT Call Waiting (sub-section, Feature Activation, Deactivation, Interrogation).

The following figure shows the steps for deleting the Customer Group Based ICWT option from the Customer Group of Called Party:

Figure 13 Steps for removing ICWT line option from the Called Party

```
>table sutstn
>pos ruacept cept
RUACEPT CEPT CEPT Y (CFU) (ICWT) $
>cha
OPTION: CEPT
>
DEFAULT_FEATURE_ON: Y
>
DEFFTR: CFU
>
DEFFTR: ICWT
>$
TUPLE TO BE CHANGED:
RUACEPT CEPT CEPT Y (CFU) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

27.2.7.2.1 By deleting the ICWT announcement datafill

The Call Wait announcement is disabled if whole or one part of the announcement datafill for ICWTANN covered in section "Datafilling ICWT Announcements" on page 730, is deleted.

Then, only the standard ringing tone is applied to the Waiting Party.

27.2.7.2.2 By changing the value of ICWT_ANN_ACTIVE to 'N'

The Caller Call Waiting announcement is disabled if the value of the boolean ICWT_ANN_ACTIVE of option ICWT is set to 'N' in table ISERVOPT.

The following figure shows an example of how to deactivate the boolean ICWT_ANN_ACTIVE.

Figure 14 Example for deactivating boolean ICWT_ANN_ACTIVE

```
>table iservopt
>format pack
>pos icwt
        ICWT   ICWT   Y    Y/N BUSY
>cha
>y
OPTION: ICWT
>
ICWT_ANN_ACTIVE:
>n
ICWT_TMO_ANN_ACTIVE:
>y/n
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)
TUPLE TO BE ADDED:

TUPLE TO BE CHANGED:
        ICWT    ICWT    N   Y/N BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
```

27.2.7.2.3 By removing the option ICWT:

The ICWT announcements are disabled if the option ICWT is deleted from table ISERVOPT. The following figure shows an example of how to delete the option ICWT.

Figure 15 Deletion of Option ICWT

```
>table iservopt
>pos icwt
        ICWT ICWT Y   Y/N BUSY
>del
>y
TUPLE TO BE DELETED:
        ICWT ICWT Y    Y/N BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

27.2.7.3 Deactivation of ICWT Announcement for "Called Party Ignores Waiting Call"

There are four ways of deactivation of applying ICWT "Called Party Ignores the Waiting Call" announcement to the Calling Party:

27.2.7.4 By deactivating or deleting ICWT option

The following figure shows the steps for deleting the ICWT line option from the Called Party:

Figure 16 Steps for removing ICWT line option from the Called Party

```
>servord
SO:
>deo $ 8888587771001
OPTION:
>ICWT
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 6 13 PM 8888587771001 ( ICWT ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

27.2.7.5 By deactivating or deleting Customer Group Based ICWT option

For deactivation of the ICWT option, please refer to the FN section of activity A59019288, CEPT Call Waiting (sub-section, Feature Activation, Deactivation, Interrogation).

The following figure shows the steps for deleting the Customer Group Based ICWT option from the Customer Group of Called Party:

Figure 17 Steps for removing ICWT line option from the Called Party

```
>table sutstn
>pos ruacept cept
RUACEPT CEPT CEPT Y (CFU) (ICWT) $
>cha
OPTION: CEPT
>
DEFAULT_FEATURE_ON: Y
>
DEFFTR: CFU
>
DEFFTR: ICWT
>$
TUPLE TO BE CHANGED:
RUACEPT CEPT CEPT Y (CFU) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

27.2.7.5.1 By deleting the ICWT announcement datafill

The Call Wait announcement is disabled if whole or one part of the announcement datafill for ICWTANN covered in section "Datafilling ICWT Announcements" on page 730 is deleted.

Then, only the standard no service circuit is applied to the Waiting Party.

27.2.7.5.2 By changing value of ICWT_TMO_ANN_ACTIVE to 'N'

The ICWT " Called Party Ignores the Waiting Call" announcement is disabled if the value of the boolean ICWT_TMO_ANN_ACTIVE of option ICWT is set to 'N' in table ISERVOPT.

The following figure shows an example of how to deactivate the boolean ICWT_TMO_ANN_ACTIVE.

Figure 18 Example for deactivating boolean ICWT_TMO_ANN_ACTIVE

```
>table iservopt
>format pack
>pos icwt
        ICWT   ICWT   Y/N  Y BUSY
>cha
>y
OPTION: ICWT
>
ICWT_ANN_ACTIVE
>y/n
ICWT_TMO_ANN_ACTIVE:
>n
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)

TUPLE TO BE CHANGED:
        ICWT   ICWT   Y/N   N BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

27.2.7.5.3 By removing the option ICWT:

The ICWT announcements are disabled if the option ICWT is deleted from table ISERVOPT. The following figure shows an example of how to delete the option ICWT.

Figure 19 Deletion of Option ICWT

```
>table iservopt
>pos icwt
        ICWT ICWT Y/N   Y BUSY
>del
>y
TUPLE TO BE DELETED:
        ICWT ICWT Y/N   Y BUSY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

27.3 Hardware Requirements or Dependencies

Standard CS2K hardware.

27.4 Software Requirements or Dependencies

Intl Succession Core and GWC loads.

27.5 Limitations and restrictions

- The duration of ICWT Timeout is hardcoded to 30 seconds.
- The CLLIs of the ICWT announcement trunks are hardcoded to ICWTANN and ICWTTMOANN.
- If UNDT (undefined_treatment) is tried to be datafilled for ICWT_TIMEOUT_TREATMENT sub field , it is prevented by the table control since it is not supported as ICWT Timeout Treatment.

27.6 Interactions

- The interactions supported by the activity A59019288, CEPT Call Waiting, (FMDOC) also supported by this activity.
- When the Called User ignores the Waiting Call and if the Calling User has CCBS option, CCBS procedures take precedence over “Called Party Ignores the Waiting Call” announcement procedures.
- The limitations for ICWT interactions with IN also applies for this activity.

27.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	Y
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

27.8 Glossary

Term	Description
CLLI	Common Language Location Identifier
CWT	Call Waiting Terminating

28: Functional Description (FN): A00002640

28.1 Feature name

CEPT Call Forward Delayed Programming.

28.2 Description

28.2.1 Introduction

This activity caters to telefonica requirements to enhance Call Forward and Call Pickup functionalities in CEPT standards.

Following services are enhanced/provided on CEPT lines:

- Concurrent Call Forwarding, Denied Call Forwarding.
- Subscriber Programmable RINGing for Call Forward Don't Answer.
- Call Pickup, Directed Call Pickup.

28.2.2 Functional Description

28.2.2.1 Concurrent Call Forwarding

The Call Forwarding Simultaneous/Screening (CFS) option allows a user to forward more than one call through a station at a time.

This feature make it possible to forward upto 256 calls simultaneously. However CFS feature allows upto 1024 calls to be forwarded simultaneously.

The administrator is authorized to assign, deassign CFS on a line via Service Order. Administrator can specify maximum number of simultaneous call forwarding for each user and for each flavour of forwarding (Unconditional, Busy, Don't Answer) via Service Order. Once, the number of simultaneous call forward reaches maximum limit, any further calls shall not be diverted.

Alternatively the Control Multiple Call Forwarding (CMCF) option can be used for concurrent call forwarding. The administrator is authorised to assign CMCF option in CUSTSTN table for a customer group.

Subscriber can prevent calls to be forwarded towards his line.

28.2.2.2 Subscriber Programmable RING (SPRING) for CEPT CFD

This activity utilizes the existing feature Call Forward Variable Timer (CFDVT) to provide the functionality of delay programming for CFD.

The administrator is authorized to assign, deassign CFDVT on a line via Service Order. Administrator is able to specify and modify the period of ringing in the case of Call Forwarding by No Answer. PRGRING is suggested for CFDVT ring control attribute. We do not check for FIXRING vs PRGRING.

Subscriber is able to activate, deactivate CFDVT by dialing access code. Subscriber is able to specify or interrogate time-interval in case of Call forwarding by No Answer by dialling access code. Subscriber can be charged for modifications/interrogations of the time-interval which is implemented by the activity A00002638 “Software Metering Support for Billing”.

28.2.2.3 Service of Call Pickup

This activity enables Call Pickup (CPU), Directed Call Pickup (DCPU) feature for a CEPT line. Call Pickup option allows a station to answer incoming calls to another station in the same pickup group. Directed Call Pickup option allows a station to answer a ringing line in the same customer group before the called party answers the ringing line.

For Limitations/Restrictions refer to section 2.5

28.2.3 Operation Procedures

The functionality provided by this activity can be controlled by the following procedures:

* Administrator assignment

* Administrator deassignment

* Subscriber activation

* Subscriber deactivation

* Subscriber interrogation

28.2.3.1 Administrator assignment

Administrator can assign CFS, CFX, CPU, DCPU, DCF using ADO (Add Option) command via Service Order.

Example of CFS option datafill in prompt mode

>ADO

SONUMBER: NOW 92 3 37 AM

>

DN_OR_LEN:

>6210001

OPTION:

>CFS

SIMULT:

Y

NCFUIF:

>5

NCFB:

>1

NCFD:

>1

SCREEN:

>N

CFXNCOS:

>100

OPTION:

>CFB

CFBCNTL:

>F

CFBDN:

>8107602

OPTION:

>$

Example of DCF option datafill in compact mode

ADO 8206211 DCF $

Example of CMCF option datafill in table CUSTSTN

CSCEPT CFXOPT CFXOPT Y Y Y Y Y Y Y Y $

CSCEPT CMCF CMCF 2 2 $

28.2.3.2 Administrator deassignment

Administrator can deassign CFS, CFX, CPU, DCPU, DCF using DEO (Delete Option) command via Service Order.

Example of CFS option datafill in prompt mode

>DEO

SONUMBER: NOW 92 3 37 AM

>

DN_OR_LEN:

>8107601

OPTION:

>CFB

OPTION:

>CFS

OPTION:

>$

28.2.3.3 Subscriber activation

Subscriber can activate CFDVT features that is provisioned on his line by using following dialling sequence:

SC[No of B](*[Time in seconds])#

The third '*' sign and the time is optional. If not used the time delay is not modified from last change. Timer range is 1 to 60s.

If the activation is successful subscriber gets positive acknowledgement, otherwise a negative acknowledgement is played.

28.2.3.4 Subscriber deactivation

Subscriber can deactivate CFDVT features that is provisioned on his line by using following dialling sequence:

#SC#

If the deactivation is successful subscriber gets positive acknowledgement, otherwise a negative acknowledgement is played.

28.2.3.5 Subscriber interrogation

Subscriber can interrogate CFD/CFDVT features that is provisioned on his line by using following dialling sequences:

i. Status of CFD by dialing *#SC#

ii. Verification of DN by dialing *#SC*DN#

iii. Verification of timer value by dialing *#SC*DD#

Here DD is the timer value given for the CFDVT feature that is provisioned on his line, DN is call forward number.

If the timer value dialled by the subscriber matches exactly with the timer value set on the line, subscriber gets a positive acknowledgement. Otherwise a negative acknowledgement is played.

As DN and DD both are numbers, following assumption is made to differentiate between interrogation of DD vs DN:

- If the dialled number of digits is 1 or 2, assume interrogation for timer value.
- If the dialled number of digits is more than 2, assume interrogation for the DN.

28.2.4 Billing for SPRING

The subscribers meter is pegged for changing and interrogation of the CFD delay timer as datafilled in table MTRFEAT against CFDVT feature. Activity A00002638 records the charges in the AMA.

28.2.5 Call Forward Chaining

A call can be forwarded mupltiple times forming a chain, i.e. A->B->C->D->E->F, with the limit of maximum of five call diversions in the chain. Sixth call diversion will not take place, fifth diverted-to station will keep on ringing and the originator will get ring back tone.

28.3 Hardware Requirements or Dependencies

No new hardware will be required for this feature.

28.4 Software Requirements or Dependencies

None.

28.5 Limitations and restrictions

There are some limitations for CPU. These are:

- Uses *SC instead *SC# for invocation.
- Does not support interrogation.

CFDVT option is not available as casual service.

28.6 Interactions

None.

28.7 Applicable customer facing sections

Fault Management

Logs	___N/A___
Alarms	___N/A___

Configuration

Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___

Security ___N/A___

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) ____N/A___

Performance (includes operational measurements) ___N/A____

28.8 Glossary

Term	Description
AMA	Automatic Message Accounting
CDR	Call Detail Record
CEPT	Conference of European Posts and Telecommunications Administrations
CFX	Call Forwarding (Universal/Busy/Don't Answer)
CFS	Call Forward Simultaneous/Screening
CFDVT	Call Forward Don't Answer Variable Timer
CFD	Call Forward Don't Answer/ Denied
CPU	Call Pickup
DCPU	Directed Call Pickup
DCF	Denied Call Forwarding
SC	Service Code
SPRING	Subscriber Programmable Ringing

28.9 Recommended Reading/References

a. A59019083.AC01 - CEPT Call Diversion

b. A59034502.AA17 - CEPT services for Succession Intl. Cable

c. A00002638 - Software Metering Support for Billing

29: Functional Description (FN): A00002641

29.1 Feature name

CEPT PSTN: Analogue Outgoing Call Barring

29.2 Description

29.2.1 Overview

This activity covers the requirements stated in Telefonica General Specification “SERVICE OF RESTRICTION OF OUTGOING CALLS “GT.Eg.d4.017 1ª 4-97

This activity addresses the Telefonica specific changes for the CEPT International Line Restriction” ILR supplementary service. It adds more flexibility to the original ILR activity 59019295.

29.2.2 ILRCLASS table

The ILRCLASS table stores the definition of the barring programs for the ILR service. The International Line Restriction line option references this table.

Figure 1 Example entry in table ILRCLASS

```
TABLE ILRCLASS
DIDD 02 (CNTL) (ICNTL) (INTL) $(09000) (09001)$
```

This entry indicates that the barring program DIDD or Deny International Direct Dial uses the code ‘02’ and bars the international translation classes CNTL, ICNTL and INTL. Additionally calls to the dialled DNs ‘09000’and ‘09001’ are restricted under this barring program. The dialled DN is in this context the DN dialled by the subscriber. The only option influencing this dialled DN string is the NO_ACCODE_DIGITS field in table IBNXLA for selectors like NET. This allows to use the DN barring in Centrex environment for public calls.

Table ILRCLASS can hold up to maximum of 100 tuples and the same should be the number of R-Codes, that is R-code range varies from 00 to 99. The R-Codes values are unique in table ILRCLASS, except ‘NN’

Table ILRCLASS entries with R-Code ’NN’ can not be used in the ILR line option and NIL barring class tuple can’t be deleted from the table ILRCLASS.

During ONP the ILRCLASS table is populated with the previously hard coded barring programs and the R-codes of the ILRCLS tuple in table ISERVOPT. The R-codes are not stored in the ILRCLS tuple in ISERVOPT any more.

During ONPs to this activity, the default tuples are restored.

29.2.3 Privileged user access

Changing the barring programs in table ILRCLASS needs to be communicated to the subscriber base. Therefore this table should be only changeable for a limited number of operators. Therefore it is suggested to set fairly high values for the command classes to update this table. This can be achieved via table CUSTPROT datafill:

Figure 2 Example of ILRCLASS table in CUSTPROT table

```
TABLE CUSTPROT
ILRCLASS 15       25 25 OFF    OFF
```

Only operators with a command class of 25 can change existing tuples and delete and add tuples to this table

29.2.4 ILRCLASS OM

The ILRCLASS OM are adopted to support the flexible definition of the barring programs in table ILRCLASS. The ILRCLASS OM provides per OM group the number of activations, deactivations, usages and unsuccessful deactivations:

Figure 3 flexible ILRCLASS OM group

```
ILRCLASS:   ACTIVE
START:2003/05/10 18:30:00 SAT; STOP: 2003/05/10 18:47:12 SAT;
SLOWSAMPLES:        11 ; FASTSAMPLES:        103 ;
       KEY (ILR_CLASS)
          ACT   DEACT USAGE UNDACT

   02 DIDD
       10 1 25 5
```

The ILR1 OM group is deleted, because all information is stored in the flexible ILR OM group.

The example above shows an OMSHOW output for the new ILRCLASS OM group. It shows for the OM group DIDD with 10 activations, 1 deactivation, 25 times a call was barred due to this program and 5 times the deactivation failed.

29.2.5 ILR OM

ILR OM provides the following information.

Figure 4 ILR OM group

```
ILR:   ACTIVE
START:2003/05/10 18:30:00 SAT; STOP: 2003/05/10 18:47:12 SAT;
SLOWSAMPLES:        11 ; FASTSAMPLES:        103 ;
      ILRCERR    ILRUINT    ILRINTG    TEMPDAC
      TEMPUDAC
      2           0         2           4
      2
```

29.3 Hardware Requirements or Dependencies

This activity is available for MMP and CS2k product.

29.4 Software Requirements or Dependencies

N/A

29.5 Limitations and restrictions

- This table does not apply to the BRI line option OCB.
- The barring programs apply to the whole office. Different barring programs for different customer groups are not possible
- The option if the subscriber can change the barring program or not is set for the office. It is not possible that some subscribers may change their barring program and some are not allowed to change their barring program.
- Announcement is not supported for this activity.
- The table ILRCLASS DN restriction based is supported only for the following ILR feature interactions.
  a. WML
  b. CDX
  c. SCS/SCL
  d. I3WC
  e. ICT
  f. LNR
  g. CND

h. AR

- DN digits in table ILRCLASS will be restricted on all endblock outpulsing calls (where translation has MIN and MAX of equal values).
- For overlap outpulsing calls, if the MIN is less than the number of digits in dialled DN, then the DN will not be restricted.
- The MIN restriction digits should be greater than the number of digits in dialled DN.
- As usual, DN digits as per the Telefonica General Specification "SERVICE OF RESTRICTION OF OUTGOING CALLS "GT.Eg.d4.017 1ª 4-97" is 3 digits and MIN digits should be three.

29.6 Interactions

Unchanged by this activity. Please refer to the NTPs for current interactions or ILR

29.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema ___X___

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

29.8 Glossary

Table 1

Term	Explanation
CEPT	Conference of European Posts and Telecommunications Administration

Table 1

Term	Explanation
CS2K	Call Server 2000 a super class soft switch
GWC	Gateway controller. One component in the CS2K which handles the messaging between the CSK2 and the gateways.
ILR	International Line Restrictions.
OM	Operational Measurements. Statistics provided by applications on the CS2k

29.9 References

The following activities are enhanced by this activity

i. A59019295 - CEPT International Line restriction

j. A59034536 - Wake-Up Call, Call Control

30: Functional description (FN): A00002642

30.1 Feature name

CEPT PSTN: Analogue Query and 3Party

30.2 Description

30.2.1 Overview

Activity A00002642 provides support for “Analogue Query and 3PTY” according to the Telefonica Specification ER.D4.062-6 “SUPPLEMENTARY TELEPHONE SERVICE CONSULT AND THREE PARTY CALL“

Additionally this activity covers a interworking issue between international call transfer and international warm line as documented in Telefonica Specification GT.ER.D4.462-16 “SUPPLEMENTARY TELEPHONE SERVICE CONSULTS AND CALLS TRANSFERENCE “.

As a last item this activity adds the option to turn off playing a hold tone to the held party via table ISERVOPT.

The supplementary services 3wc and call transfer covered in this activity had been implemented in MMP14 activity 59019281 “CEPT 3WC and ICT”

30.2.2 Warning Tone During 3WC Conferences

This activity introduces a new field to the ICONF tuple in table ISERVOPT. If this field is set the CS2k conference circuit of the conference controller is supervised with the H.248 signal “cg/wt”. This field is initialized to “No” to retain existing behaviour

The following tone definition is suggested:

- Frequency: 1400Hz
- Level: -25dB
- On: 400ms, Off: 18000ms, repeated endless

This field can only be set to “Yes” if an audio controller is datafilled in table SERVSINV. This warning tone is not played, if the conference uses a TDM conference circuit.

30.2.3 Warmline Interaction with Enquiry Mode

This activity introduces a new field to the ICONF tuple in table ISERVOPT. If this field is set, the CS2k prevents WML during enquiry mode. This field is initialized to “No” to retain existing behavior.

30.2.4 Hold Tone during Enquiry Mode

This activity introduces a new field to the ICONF tuple in table ISERVOPT. If this field is set, the CS2k does not play the hold tone to the held party.

30.2.5 Example

Below an example of the ICONF tuple after this activity

Figure 1 ICONF tuple in ISERVOPT

```
>add iconf
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
OPTION:
>iconf
ALLOW_ICT_IN_I3WC:
>y
CLF_FLASH_IGNORE:
>y
WARNING_TONE:
>Y
PREVENT_WML_DURING_ENQUIRY
>Y
PREVENT_HELD_TONE
>Y
TUPLE TO BE ADDED:
                    ICONF
                                                          ICONF Y Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

30.3 Hardware Requirements or Dependencies

The option to play the warning tone to the conference is only available to CS2k. All other functionality described in this document is applicable both to the DMS and the CS2k.

30.4 Software Requirements or Dependencies

None

30.5 Limitations and restrictions

- Warning Tone does not apply to other conference types than I3WC. I6WC or Meet Me conferences do not use the warning tone
- I3WC does not support chaining of conferences on the same office[1]
- In case I3WC conferences are chained via trunks, multiple warning tones might be encountered, if the other office also supports the warning tone

[1]existing limitation, which is not changed by this activity

- If PREVENT_WML_DURING_ENQUIERY bool is set to “Y” it impacts the Bellcore versions of CT and 3WC in a manner, that WML is still possible on CT and 3WC. But it will use the initial digit time out instead of the WML time out
- When the option PREVENT_WML_DURING_ENQUIRY is set to Y, the first digit timeout is set to the value in LN_PERM_SIG_TIME
- When the enquiry/consult call leg triggers IN queries- InfoCollected TDP or Info Analyzed TDP, the inquiry/consult call is not permitted
- The AudioCodes Media Server (AMS) does not support the warning tone. Please set WARNING_TONE to “N” while using the AMS. (Q00937489)
- The SAM16 UAS does not support the H.248 Empty Event Parameter without curly brackets used by the GWC. This takes down the conference, when the conference leader tries to toggle between the other parties (Q00726512)

30.6 Interactions

This activity does not change feature interactions unless documented above

30.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema ___X___

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

30.8 Glossary

Term	Description
3wc	Servord line option to allow 3 party conferences
CEPT	Conference of European Posts and Telecommunications Administration
CS2K	Call Server 2000 a super class soft switch
GWC	Gateway controller. One component in the CS2K which handles the messaging between the CSK2 and the gateways.
I3wc	Servord line option to allow international 3 party conferences according to former CEPT specification
UAS	Universal Audio Server - A media gateway being capable of providing announcements, conferences and tones
WML	Warm Line. After a short time out a pre configured DN is called.

31: Functional Description (FN): A00002644

31.1 Feature name

Common Topology Identifier Provisioning - Activity ID A00002644

31.2 Description

The Internet Transparency feature, which allows Voice-Over-IP calls to take place in the presence of Network Address Translation(NAT)/IP VPNs, was introduced into Succession in release 6.1. This feature optimises network resource utilisation by determining whether the call path crosses NAT/VPNs and inserting Media Proxies if necessary.

However, calls spanning multiple Call Agents (CS2ks) may result in the insertion of one or more Media Proxies into the call path, even if the call is contained within a single VPN. To avoid this, the inter-Call Agent trunks can be configured to be ‘intra-domain’ SIP-T trunks, thus causing the NAT/VPN information for both ends of the call to be compared. However, for this comparison to operate correctly, the following requirements must be met by the NAT’s numerical identifier within the Call Agents (CS2ks), ie by the NAT’s ‘Middlebox ID’:

— the middlebox ID for each NAT must be unique across all Call Agents

— each NAT must have the same Middlebox ID in all Call Agents

An example of this is shown in Figure 1.

This requirement on middlebox IDs is provided by the feature described in this note, hence allowing the configuration and use of intra-domain SIP-T trunks in SN07.

Each CS2k within the VoIP network must be allocated a unique Call Agent Identifier between 1 and 255. The user is responsible for administration of this number and its allocation among the CS2ks. Once a CS2k has been allocated a Call Agent ID, it should be provisioned into the CS2k Mgr using the capabilites provided by this feature. Ideally this should be co-ordinated with the CS2k upgrade to SN07, as described in 31.11.

When a NAT is provisioned, a middlebox ID is automatically generated by the CS2k Mgr. From SN07 onwards, the CS2k Mgr incorporates the Call Agent

into this automtically generated number, using the provisioned Call Agent ID for that CS2k. This helps to ensure uniqueness of middlebox IDs across multiple CS2ks.

For the special case in which the same NAT is provisioned into multiple CS2ks, it is necessary to ensure that the middlebox ID used for this NAT is the same in all CS2ks. Hence the middlebox ID allocated when the NAT is first provisioned into a CS2k must be used when the NAT is provisioned in subsequent CS2ks. In order to enable this, this feature provides the capability to

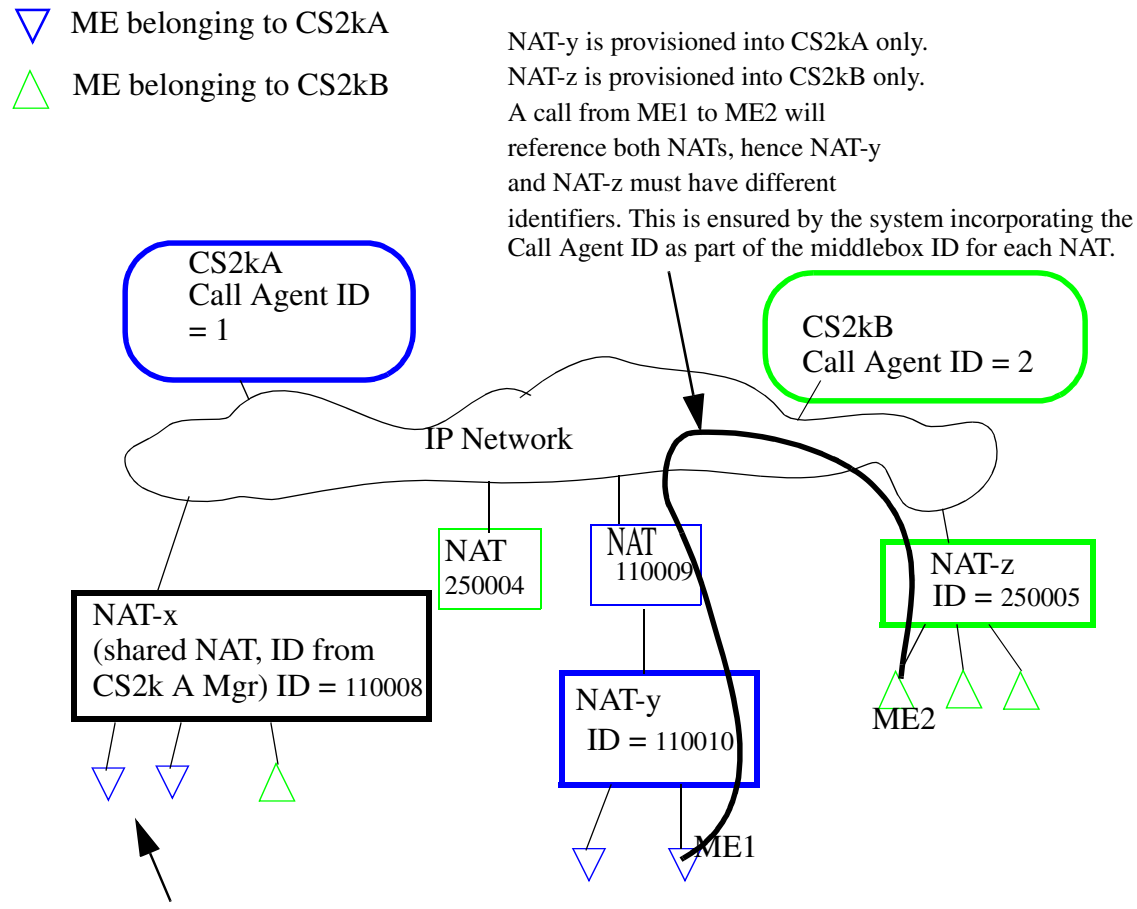
- read the middlebox ID of a provisioned NAT
- specify the middlebox ID as part of the data when provisioning a NAT.

Alternatively, the user may manually allocate any valid unique middlebox ID to a NAT and provision this value into all CS2ks, by-passing the CS2k Mgr middlebox-ID-auto-generation step. The middlebox ID must be an integer between 2 and 16777215 (ID = 1 is reserved by the system for internal use).

An example of ID allocations for a VoIP network with 2 CS2ks in shown in Figure 1 .

If a NAT is provisioned into a CS2k Mgr and the automatically generated middlebox ID is then provisioned into other CS2k Mgrs, care must be taken when deleting this NAT. The NAT must be deleted last from the CS2kMgr that generated the middlebox ID - ie only after it has been deleted from all other CS2k Mgrs.

Figure 1 VoIP network with multiple Call Agents (CS2ks)



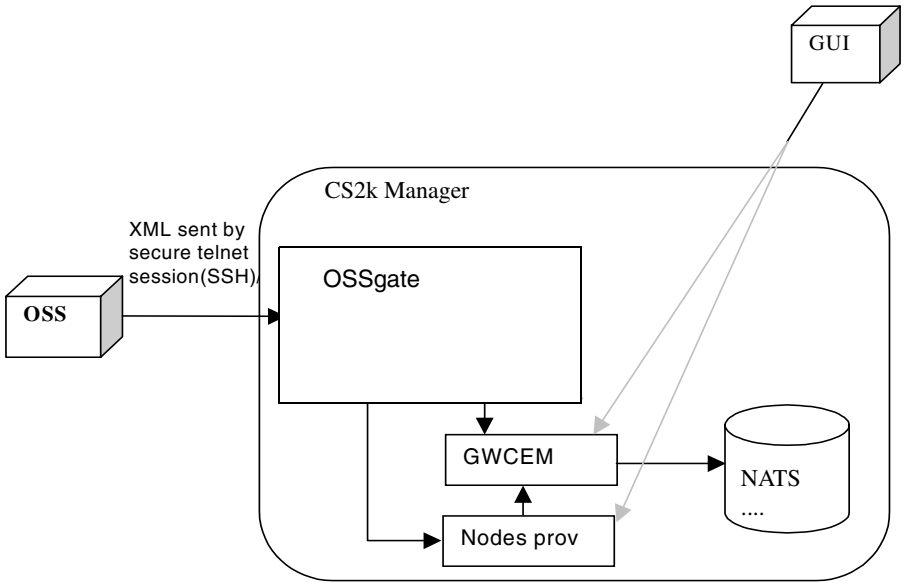
The user operations provided by this feature, which available via the GUI client and via the XML OSS interface, (Figure 2) are:

- Provision/set the Call Agent ID
- Display/list the Call Agent ID
- Specify the NAT middlebox ID during NAT provisioning
- Display/list the NAT Middlebox ID for a selected NAT
- Warning message on deletion of NAT middlebox.

In addition, the following internal functionality changes have been made as part of this feature:

- Automatic update of middlebox ids when Call Agent set for the first time
- Auto-generation of NAT and Pep Server middlebox id based on provisioned Call Agent ID

Figure 2 GUI Client and OSSGate interfaces



31.3 Hardware Requirements or Dependencies

No new hardware is required or introduced by this feature. The application components provided by this feature execute as part of the SESM.

31.4 Software Requirements or Dependencies

Dependencies:

- CR.Q00768898: Extend range in middlebox id in Gatway Controller

31.5 Limitations and restrictions

Upgrade to SN07 should be carried out as described in section 31.11

31.6 Interactions

The following existing GUIs have been modifed:

- Maintenance Settings Panel (see Figure 5).
- Change Maintenance Settings Dialog (see Figure 6).
- Network Devices Panel, NATs tab (see Figure 12).
- Add NAT middlebox Dialog (see Figure 14, Figure 15)
- Delete NAT confirmation Dialog (see Figure 26)

The following existing XML commands have been modified:

- queryNAT (see Figure 9, Figure 20, Figure 22).
- addNAT (see Figure 24).

The following GUIs have been added:

- NAT middlebox ID display dialog (see Figure 13).

The following XML commands have been added:

- queryCallAgentId (see Figure 8)
- setCallAgentId (see Figure 10)

The on-line help facility will be updated with information on the use, syntax and valid values for all the above modifications/additions.

31.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	**_X_**
User Interface	**_X_**
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_

Performance (includes operational measurements) _N/A_

31.8 Call Agent Identifier

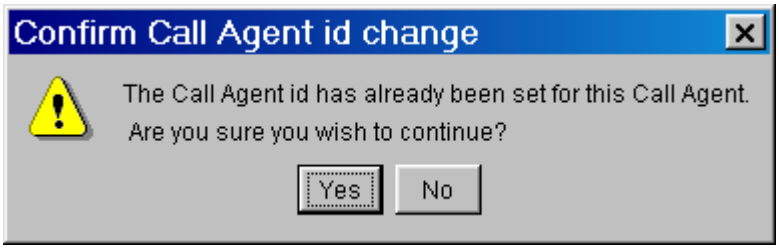
The Call Agent ID has an initial value of <not configured> in newly installed SN07 SESM systems. The Call Agent ID value should be set to a integer value between 1 and 255 by the user for normal operation. The Call Agent ID value must be set before the user can specify Middlebox IDs for NATs during NAT provisioning.

Note that in order to ensure optimum system operation is maintained during an upgrade, the Call Agent Id should be set just prior to upgrade of GWCs to SN07. Details of this are described in section 31.11.

The first time the Call Agent ID is set by the user, the system performs any necessary internal changes for NAT middleboxes which have already been provisioned, to incorporate the newly provisioned Call Agent ID into the NAT middlebox IDs. GWC units which need to be synchronised to this new data wil be identified by having data synchronisation alarms raised against them. (See sections 31.2, 31.11 for more details).

Ideally, the Call Agent ID should only be set once and then not changed. However, setting the Call Agent Id more than once is not prohibited by the CS2k mgr. Note that, for subsequent changes, the new Call Agent ID will only be used in the middlebox ID for NATs provisioned after the change has been made. The middlebox IDs of previously provisioned NATs are not modified. This ensures consistency, in case NATs have been provisioned into multiple Call Agents. If the user does attempt change the Call Agent ID, a warning confirmation message is displayed.

Figure 3



31.8.1 GUI Client

31.8.1.1 Display Call Agent ID

The Call Agent ID is displayed in the Gateway Controller Main Panel, in the ‘Maintenance Settings’ area. This is shown in Figure 4 and Figure 5.

Figure 4 Maintenance Setting Area, GWC management panel

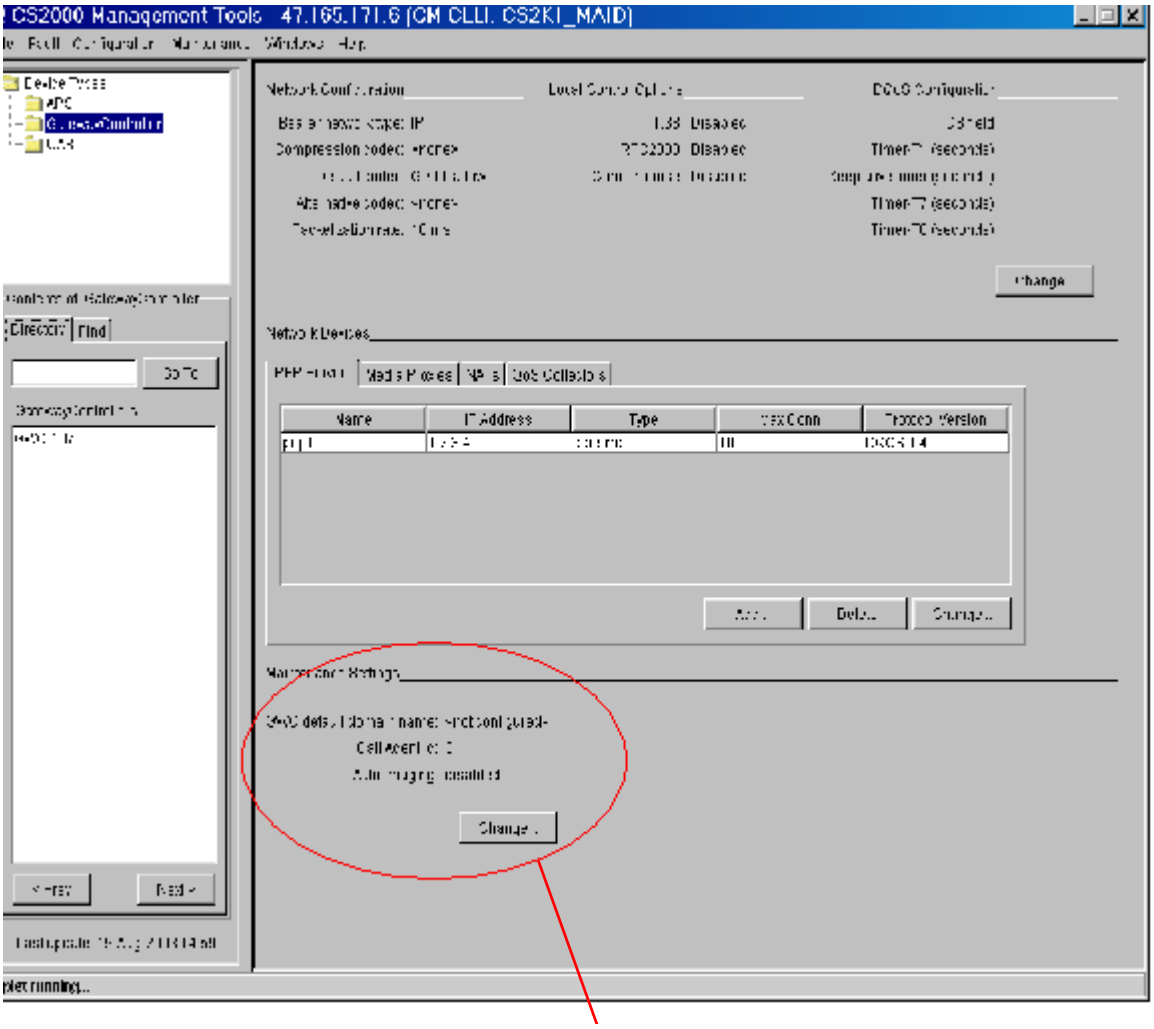
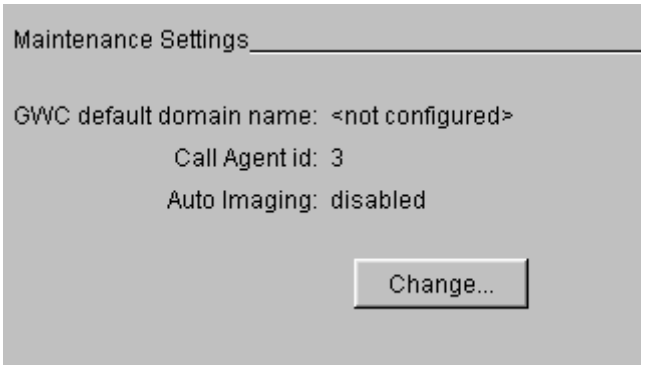


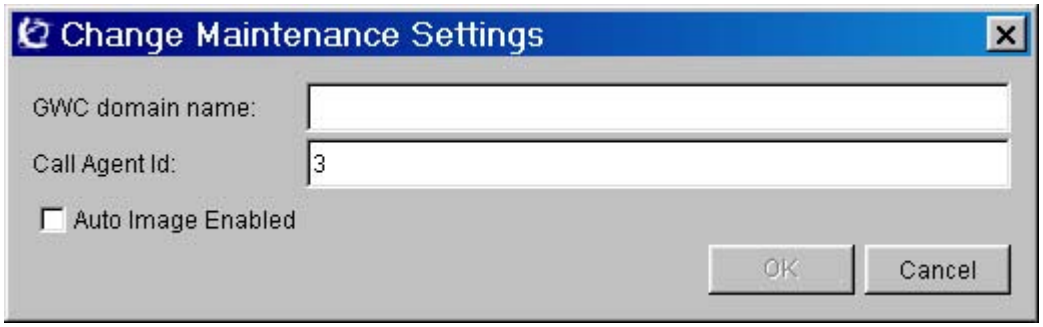
Figure 5 Call Agent ID display and Change button



31.8.1.2 Provision Call Agent ID

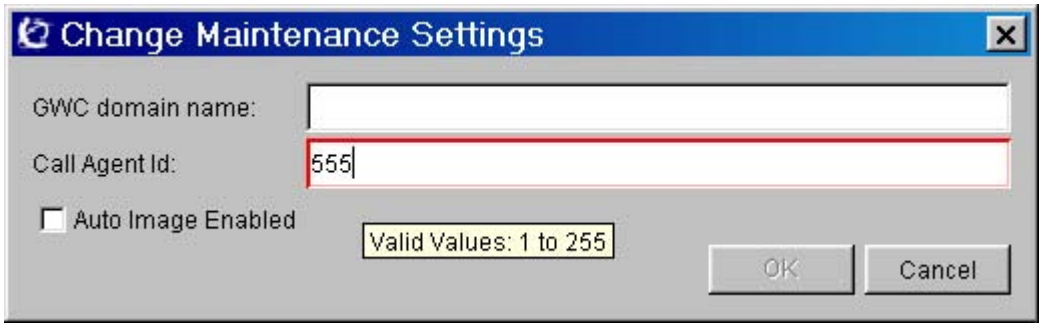
The Call Agent ID can be provisioned/set using the ‘Change’ button in the Maintenance Setting area display (Figure 5). This displays the Maintenance Settings change dialog (Figure 6), which allows the user to set the Call Agent ID to an integer value between 1 and 255. Other maintenance settings may optionally be changed at the same time.

Figure 6 Change Maintenance Settings Dialog



Tool tips for the Call Agent ID are displayed when the cursor is placed within the text field. If the entered value is invalid, the text field is outlined in red and the OK button is disabled (Figure 7).

Figure 7 Invalid Call Agent Id value



31.8.2 XML Interface

31.8.2.1 List Call Agent ID

The Call Agent ID may be retrieved via the XML interface using the following command (Figure 8). If the request is unsuccessful, an error message is returned as described in Appendix B.

Figure 8 XML command queryCallAgentId

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryCallAgentId usn="1" version="1.0"/>
    </Methods>
  </Command>
 </CommandList>
```

Figure 9 XML Response for queryCallAgentId

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <queryCallAgentId usn="1" version="1.0">
       <ReturnData>
        <CallAgentId>3</CallAgentId>
        <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </queryCallAgentId>
    </Methods>
   </Response>
</CommandList>
```

31.8.2.2 Provision Call Agent ID

The Call Agent ID can be specified via the XML interface using the setCallAgentId command (Figure 10). If the Call Agent Id cannot be set, an error message is returned as described in Appendix B:

Figure 10 XML Command: setCallAgentId

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <setCallAgentId usn="1" version="1.0">
      <Parameters>
       <CallAgentId>3</CallAgentId>
      </Parameters>
     </setCallAgentId>
    </Methods>
  </Command>
 </CommandList>
```

Figure 11 XML Response for setCallAgentId

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <setCallAgentId usn="1" version="1.0">
       <ReturnData>
        <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </setCallAgentId>
    </Methods>
   </Response>
</CommandList>
```

31.9 NAT middlebox Identifier

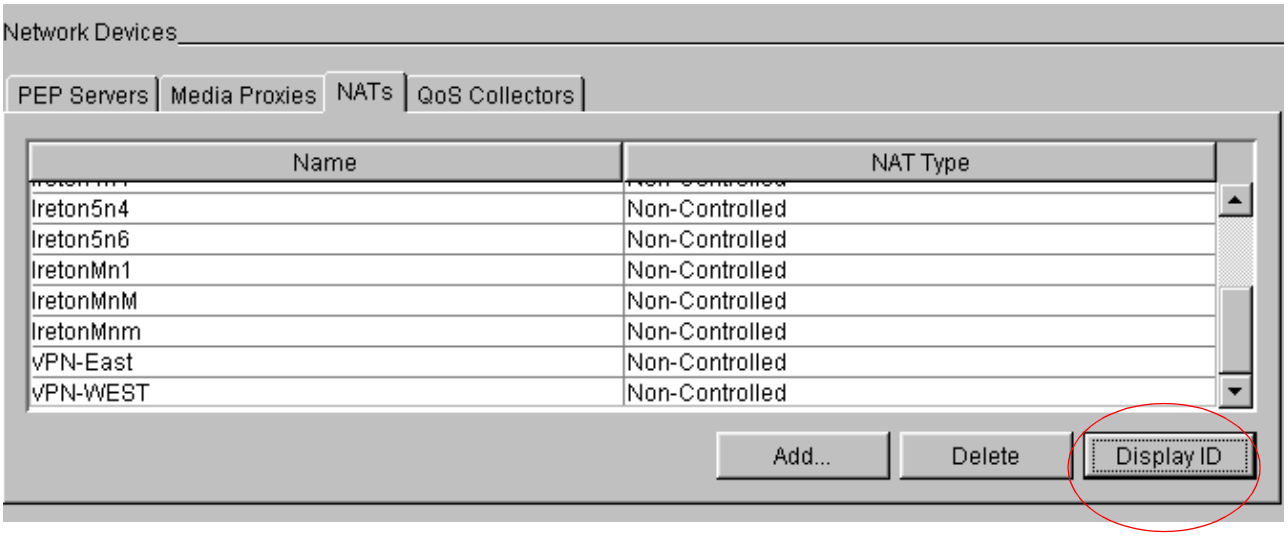
When the user provisions a NAT, the system will automatically allocate a NAT middlebox ID. However, some NATs are provisioned into multiple CS2k Mgrs. For these NATs, it is necessary for the user to override the automatic middlebox ID allocation when the NAT is provisioned into the second and subsequent CS2ks (see section 31.2). This is done by specifying the NAT middlebox ID during provisioning of the NAT. The middlebox ID must be a unique integer between 2 and 16777215

31.9.1 GUI Client

31.9.1.1 Display NAT middlebox ID

The middlebox ID for a NAT can be displayed via the ‘Display ID’ button on the NAT browser, which is a available on the GWC Network Devices tabbed Panel

Figure 12 NATs tab on Network Devices Panel



This brings up an information box displaying the NAT middlebox ID (Figure 13).

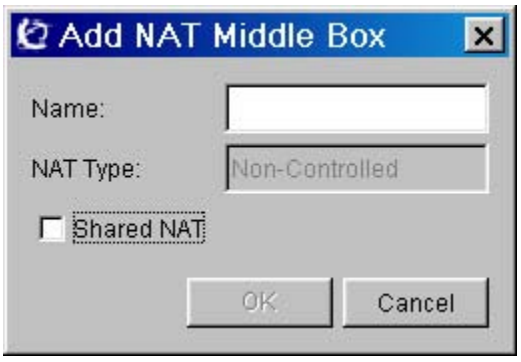
Figure 13 NAT middlebox ID display dialog

31.9.1.2 Specify NAT middlebox ID during NAT provisioning

The middlebox ID for a NAT may be specified during NAT provisioning as follows:

— Use the ‘Add’ button on the NAT browser (see Figure 12) to open the NAT provisioning dialog box (Figure 14).

Figure 14 Add NAT Middle Box dialog



— Check the box marked ‘Shared NAT’. This extends the dialog box to include the middlebox ID provisioning fields (Figure 15).

— Enter valid values for NAT name and NAT ID and press OK (Figure 16).

Figure 15 Add NAT Middle Box dialog with Shared NAT checked

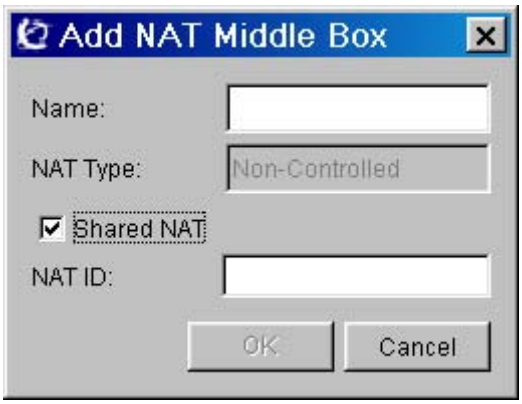
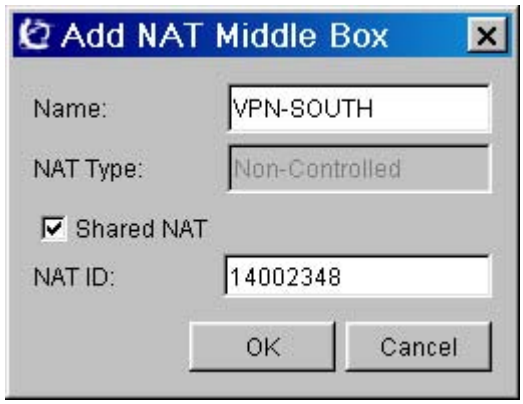
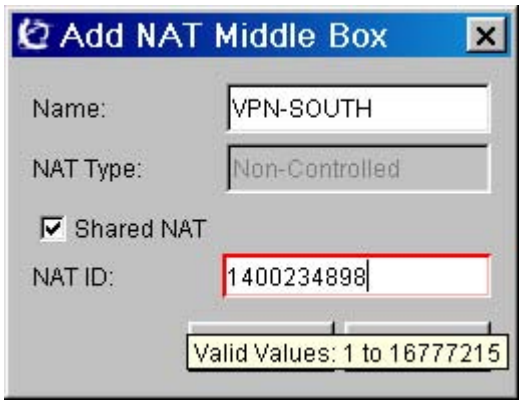


Figure 16 Add NAT Middle Box with valid entries & OK enabled.



Tool tips are displayed when the cursor is placed over each text field. If invalid values are entered, the text field with invalid data is outlined in red and the OK button is disabled (Figure 17).

Figure 17 Add NAT Middle Box dialog with invalid entry for NAT ID



31.9.2 XML Interface command

31.9.2.1 List NAT middlebox ID

The NAT middlebox ID can be listed as part of the information returned in the queryNAT request. This is done by including the <ListNATid> tag, set to ‘true’, in the XML command. If the tag is set to ‘false’, the NAT middlebox information is listed without the middlebox ID. If this tag is omitted, the NAT middlebox information again is listed without the middlebox ID, for backwards compatibility with previous releases.The XML for this command

is shown in Figure 9, Figure 20, Figure 22. Error messages returned are described in Appendix B.

Figure 18 XML command to query specified NAT, including middlebox ID

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITranslf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <Parameters>
        <NATname>NAT-A</NATname>
        <ListNATid>true</ListNATid>
      </Parameters>
     </queryNAT>
    </Methods>
  </Command>
 </CommandList>
```

Figure 19 XML response to query specified NAT, including middlebox ID

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITranslf</Interface>
    <Methods>
      <queryNAT usn="1" version="1.0">
       <ReturnData>
         <NATname>NAT-A</NATname>
         <NATType>1</NATType>
         <NATid>131080</NATid>
         <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </queryNAT>
    </Methods>
   </Response>
</CommandList>
```

Figure 20 XML command to query all NATs on a given GWC, with middlebox ID

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <Parameters>
       <GWCname>GWC-0</GWCname>
       <ListNATid>true</ListNATid>
      </Parameters>
     </queryNAT>
   </Methods>
  </Command>
 </CommandList>
```

Figure 21 XML response for query all NATs on a given GWC, with middlebox ID

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <ReturnData>
       <NATname>NAT-B</NATname>
       <NATid>131081</NATid>
       <NATname>NAT-D</NATname>
       <NATid>131083</NATid>
       <ReturnCode value="0" text="Successful result" />
      </ReturnData>
     </queryNAT>
    </Methods>
   </Response
  </CommandList>
```

Figure 22 XML Command: query all NATs, with middlebox id

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <Parameters>
       <ListNATid>true</ListNATid>
      </Parameters>
     </queryNAT>
    </Methods>
  </Command>
 </CommandList>
```

Figure 23 XML Response: query all NATs, with middlebox id

```
<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNAT usn="1" version="1.0">
      <ReturnData>
       <NATname>NAT-A</NATname>
       <NATid>131080</NATid>
       <NATname>NAT-B</NATname>
       <NATid>131081</NATid>
       <NATname>NAT-C</NATname>
       <NATid>131082</NATid>
       <NATname>NAT-D</NATname>
       <NATid>131083</NATid>
       <ReturnCode value="0" text="Successful result" />
      </ReturnData>
     </queryNAT>
    </Methods>
   </Response>
  </CommandList>
```

31.9.2.2 Specify NAT middlebox ID during NAT provisioning

The middlebox ID can be specified during NAT provisioning over the XML interface by including the <NATid> tag in the addNAT command, as shown in Figure 24. Valid values must be provided for all fields. Error codes are given in Appendix B.

Figure 24 XML Command: addNAT, including middlebox id:

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
   <Command>
     <Interface>ITransIf</Interface>
       <Methods>
         <addNAT usn="1" version="1.0">
           <Parameters>
            <NATname>nat1</NATname>
            <NATid>13378928</NATid>
           </Parameters>
          </addNAT>
         </Methods>
        </Command>
       </CommandList>
```

Figure 25 XML Response: addNAT, including middlebox id:

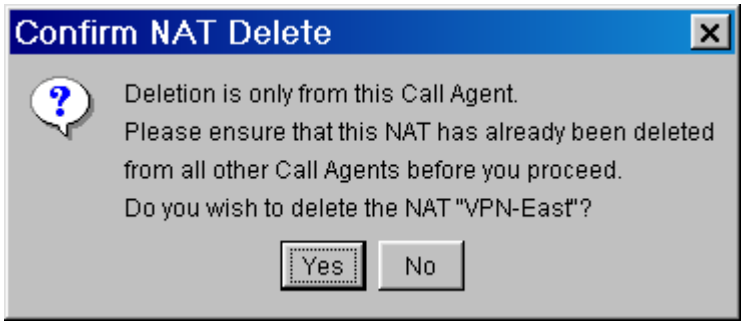
```
X<?xml version='1.0'?>
 <CommandList>
  <Response>
   <Interface>ITransIf</Interface>
    <Methods>
      <addNAT usn="1" version="1.0">
       <ReturnData>
        <ReturnCode value="0" text="Successful result" />
       </ReturnData>
      </addNAT>
    </Methods>
   </Response>
</CommandList>
```

31.10 NAT deletion

If the user has provisioned a NAT into multiple CS2ks, care should be taken when deleting the NAT. If the NAT middlebox ID used for the shared NAT has been automatically generated by one CS2k Mgr, the NAT should not be deleted

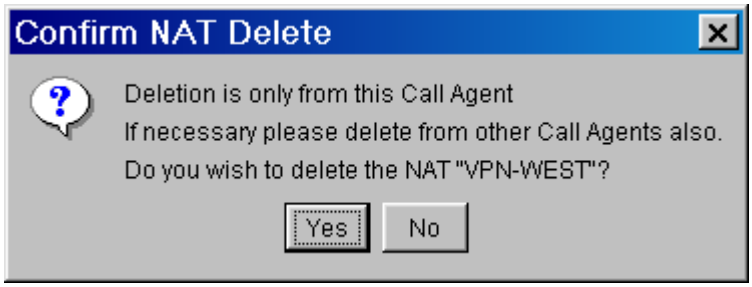
from that CS2k Mgr while it is still provisioned in other CS2ks. It must be deleted from all other CS2k Mgrs first. The GUI client displays a warning when deletion of a NAT whose middlebox id has been generated by this CS2k Mgr is requested, as shown in Figure 26.

Figure 26 Confirm NAT Delete dialog



For other NATs, a general reminder is given that the delete operation results in deletion of the NAT middlebox from this CS2k only.

Figure 27 Confirm NAT Delete dialog



31.11 Upgrade to SN07

During an upgrade to SN07, the need to upgrade the middlebox IDs of already provisioned NATs means that there is a possibility of temporary increase in usage of Media Proxies, depending on the exact network configuration. Hence if Media Proxy resources have been engineered so that this may cause problems, the period of time during which there are GWCs at different software versions should be minimised. It is suggested that one of the following sequences of operation, A or B, is used for upgrade. In steps A & B, ‘Upgrade the CS2k Mgr’ refers in particular to upgrade of the Node Provisioning and GWC EM applications.

A. Upgrade without soak test

1. Upgrade CS2k Mgr to SN07

2. Set a unique Call Agent ID. This causes the SN07 CS2k Mgr to generate new middlebox IDs for already provisioned NATs (and Pep Servers).

3. Upgrade all GWCs that will support internet transparency Media Endpoints to SN07. As part of this upgrade (in particular because of the busy/RTS/SWACT), the new middlebox IDs for already provisioned NATs will be downloaded to each GWC. During this step, GWCs with different versions of software may have different middlebox IDs for the same NAT and hence some additional Media Proxy usage may take place (depending on the exact network configuration and order in which GWCs are upgraded). Hence, if a temporary increase in Media Proxy usage is undesirable (e.g. for network engineering reasons), this step should be done within as short as possible a time window and during a low traffic period.

4. Repeat steps 1-3 for all other CS2ks in the network.

5. Intra-domain SIP-T trunks may now be configured.

B Upgrade with soak test

1. Upgrade CS2k Mgr to SN07

2. Upgrade a small number of GWCs that support internet transparency Media Endpoints to SN07 for soak test

3. Once soak test is complete, set a unique Call Agent ID. This causes the SN07 CS2k Mgr to generate new middlebox IDs for already provisioned NATs (and Pep Servers).

4. Carry out a busy/RTS/SWACT for the (SN07) GWCs that have been soak tested. This will cause the new middlebox IDs to be downloaded to boths sides of these GWCs.

5. Upgrade all other GWCs that will support internet transparency Media Endpoints to SN07. As part of this upgrade (in particular because of the busy/RTS/SWACT), the new middlebox IDs for already provisioned NATs will be downloaded to each GWC. During steps 4 & 5, GWCs with different versions of software may have different middlebox IDs for the same NAT and hence some additional Media Proxy usage may take place (depending on the exact network configuration and order in which GWCs are upgraded). Hence, if a temporary increase in Media Proxy usage is undesirable (e.g. for network engineering reasons), steps 4 & 5 should be done within as short as possible a time window and during a low traffic period.

6. Repeat steps 1-5 for all other CS2ks in the network.

7. Intra-domain SIP-T trunks may now be configured.

31.12 Authorization for Commands

The security for the GUI Client and OSSgate interface includes support for permission or ‘Authorization’ levels for commands. Each command is assoicated with one or more user groups. In order to execute a command, a user must belong to at least one of the assoicated user groups. The user groups assoicated with the new /modifed commands associated with this feature are specified in the table below.

Table 1 Internet Transparency Commands Authorization

Command	User Group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Display Call Agent ID (queryCallAgentId)	X	X	X	X	X
Change Call Agent ID (setCallAgentId)	X	X			
Display NAT ID (queryNAT)	X	X	X	X	X
Provision NAT (addNAT)	X	X			

31.13 Glossary

Term	Description
GUI	Graphical User Interface
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
ID	Identifier
ME	Media Endpoint
NAT	Network Address Translation

Term	Description
VPN	Virtual Private Network

31.14 Appendix A: XML validation schemas

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

<!-*************************************************************************-->
  <!-- * Define addNAT Method Parameters -->
<!-*************************************************************************-->

<xsd:complexType name="addNATmethodType">
   <xsd:all>
     <xsd:element name="Parameters" type="addNATparamsType" />
   </xsd:all>
   <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addNATparamsType">
   <xsd:sequence>
     <xsd:element name="NATname" type="NoSpaceNameType" />
     <xsd:sequence minOccurs="0">
       <xsd:element name="NATid" type="xsd:integer" />
     </xsd:sequence>
   </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<!-*************************************************************************-->
<!-- * Define queryNAT Method Parameters -->
<!-*************************************************************************-->

<xsd:complexType name="queryNATmethodType">
   <xsd:all>
     <xsd:element name="Parameters" type="queryNATparamsType" />
   </xsd:all>
   <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryNATparamsType">
   <xsd:sequence>
     <xsd:choice minOccurs="0">
```

```
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="GWCname" type="GWCNameType" />
    </xsd:choice>
    <xsd:choice minOccurs="0">
      <xsd:element name="ListNATid" type="NoSpaceNameType" />
    </xsd:choice>
   </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<!-*************************************************************************-->
<!-- * Define setCallAgentId Method Parameters -->
<!-*************************************************************************-->

  <xsd:complexType name="setCallAgentIdmethodType">
   <xsd:all>
    <xsd:element name="Parameters" type="setCallAgentIdparamsType" />
   </xsd:all>
   <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="setCallAgentIdparamsType">
   <xsd:sequence>
    <xsd:element name="CallAgentId" type="xsd:integer" />
   </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<!-*************************************************************************-->
<!-- * Define queryCallAgentId Method Parameters -->
<!-*************************************************************************-->

<xsd:complexType name="setCallAgentIdmethodType">
   <xsd:all>
   </xsd:all>
   <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
</xsd:schema>

<!-*************************************************************************-->
<!-- ** Global Attribute Groups Used by all schemas -->
<!-*************************************************************************-->

<!-*************************************************************************-->
<!-- * Define Common Usn_Version Attribute Group-->
<!-*************************************************************************-->

<xsd:attributeGroup name="Usn_VersionAttrbGroup" >
```

```
   <xsd:attribute name="usn" type="xsd:integer" use="required" />
   <xsd:attribute name="version" type="xsd:decimal" default="1.0" use="optional"/>
  </xsd:attributeGroup>

<!-************************************************************************-->
<!-- * Global Simple Types Used or Useable by all schemas follows: -->
<!-************************************************************************-->

<!-************************************************************************-->
<!-- * Define No Space Name Type -->
<!-************************************************************************-->

<xsd:simpleType name="NoSpaceNameType">
   <xsd:restriction base="xsd:token">
     <xsd:minLength value="1" />
     <xsd:pattern value="\S{1,32}" />
   </xsd:restriction>
  </xsd:simpleType>

<!-************************************************************************-->
<!-- * Define GWCNameType-->
<!-************************************************************************-->

<xsd:simpleType name="GWCNameType">
   <xsd:restriction base="xsd:string">
     <xsd:pattern value="GWC-\d\d?\d?" />
   </xsd:restriction>
  </xsd:simpleType>
```

31.15 Appendix B: Error codes and messages

Table 2 Return codes when command is unsuccessful

Cause of error	Return code	Example return messages
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error
Unable to provision requested NAT because a database error occurred	303	Database error occurred during setting of Call Agent Id.

Cause of error	Return code	Example return messages
Unable to provision requested NAT/Call Agent Id of problem with the GWCEM component of the CS2k Mgr.	304	Element Manager Initialisation in progress
No NAT data for this query. e.g. no NAT meets selection criteria or the NAT/GWC specified does not exist	305	NAT not found No NAT found for GWC
User is not a member of any of the user groups allowed to perform this action	501	Insufficient permissions to perform this operation

31.15.1 Example Error Message

```
<?xml version='1.0'?>
    <CommandList>
       <Response>
         <Interface>ITransIf</Interface>
           <Methods>
              <queryNAT usn="1.0" version="1.0">
               <ReturnData>
                  <NATname>nat1111</NATname>
                   <ReturnCode value= "305" text="NAT not found"/>
               </ReturnData>
              </queryNAT usn="1.0">
           </Methods>
       </Response>
    </CommandList>
```

31.16 Appendix C: XML Commands: description of method parameters

31.16.1 Parameter definitions

- **encoding??**
- **version** - The version refers to the version of the method or operation - e.g., the addNAT operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.

- **ReturnCode value**- A numeric value indicating the result of the attempted operation (see Table 3, for range and definitions of each possible value). TYPE *string*.
- **Return code text**- Appropriate text that describes the result of the operation. TYPE *string*.
- **CallAgentId** - The unique integer that has been assigned by the user ot this Call Agent (e.g. this CS2k). This must be a value between 1 and 255. TYPE *integer.*
- **ListNATid** - Indication of whether the NAT id should be included in the response to this command. Set to 'true' if the NATid is required and 'false' if not. TYPE *NoSpaceNameType*.
- **NATname** - The name of the NAT that this command applies to. TYPE *NoSpaceNameType* .(32 character token without spaces, see xsd definitions in Appendix A, section 25.12)
- **NATid** - The unique middlebox id for this NAT. This must be an integer between 2 and 16777215. TYPE *integer.*
- **NATType** - Indicates the type of NAT, in particular, NATType = 1 indicates an uncontrolled NAT. No other values are used in this release. TYPE *string*.
- **GWCname** - The name of the GWC that this command applies to. TYPE *GWCNameType* (string of form GWC-xxxx, see xsd definitions in Appendix A, section 25.12)

31.16.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **queryCallAgentId** - Method that gets the current value of the Call Agent Id for this Call Agent (CS2k). This method has the following parameters:

- Input data:
  - usn
  - version
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - CallAgentId **-** The value of the Call Agent Id for this Call Agent (CS2k).
  - ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

2. **setCallAgentId** - Method that sets to Call Agent Id for this Call Agent (CS2k) to the specified value. This method has the following parameters:

- Input data:

– usn

– version

– CallAgentId - The desired value for the Call Agent Id for this Call Agent (CS2k).

- Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

3. **queryNAT** - Method that gets the information regarding a NAT or set of NATs, depending on the parameters specified. If neither a NATname nor a GWCname is included, then information is returned for ALL NATs provisioned in this CS2k Mgr. This method has the following parameters:

- Input data:

– usn

– version

– NATname (optional, cannot be included as well as GWCname) - indicates the NAT for which information should be returned

– GWCname (optional, cannot be included as well as NATname) - returns information for all NATs associated with this GWC

– ListNATid (optional) - if set to true, this returns the NAT id as part information for each NAT, if set to false or if the parameter is omitted the NAT id is not returned.

- Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– NATname

– NATType (returned only when the NATname is specified)

– NATid (returned only when ListNATid is set to ‘true’ in the input data)

4. **addNAT** - Method that provsion a NAT into the CS2k Mgr. This method has the following parameters: If the NAT id is not specified then the CS2k Mgr generates a NAT middlebox id for the NAT.

- Input data:
  - usn
  - version
  - NATname - unique name for the NAT to be provisioned
  - NATid (optional) - indicates the middlebox id that should be allocated to this NAT.
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - ReturnCode

32: Functional Description (FN): A00002654

32.1 Feature name

CEPT AR (CLASS CALLBACK)

32.2 Description

The CEPT telephony service Call Back to Last Received Call enables a subscriber to inquire into the number of network origin of the last received call that was not answered, as well as the date and time in which the call took place, and to allow the subscriber to call back that number by pressing a single digit without the need to go on-hook.

This CEPT service is closely allied to the existing Automatic Recall (AR) service currently implemented in the MMP with the only major differences being that the CEPT service has a slightly different user interface and billing requirements. Thus, the CEPT Call Back to Last Received Call service will be assignable to subscribers as the current AR feature with modifications becoming active when the CEPT option is also provisioned on the line.

The first application of this feature will be for the Spanish market (Telefonica).

A summary of the modifications to the existing AR feature are as follows:

- Call processing - Current AR design only consists of invoking the feature using an access code. This activity will add the CEPT-defined capabilities of activation, deactivation, interrogation, and erasure to the AR feature. These capabilities will only apply to IBN lines with the CEPT line option.
- CEPT AR User Interface - Current AR design uses a telco-defined access code to enable the subscriber to invoke the feature. This activity will enable the subscriber to perform the following CEPT-defined capabilities for AR by using CEPT-defined dialing sequences: activation, deactivation, interrogation, invocation, erasure, and security key change.
- Security Key - Current AR design does not use a security key (i.e. PIN). This activity will add security key capabilities to the AR feature including the ability for both the subscriber and the telco to change the security key. These capabilities will only apply to IBN lines with the CEPT line option.
- Billing - Current AR design has an option to produce AMA billing records for feature use. However, the design uses the North American-defined Bellcore format. This activity will implement the ability for all

CEPT services to produce NAOC-defined billing records and NAOC meter counts for the following CEPT-defined capabilities: activation, deactivation, interrogation, invocation, erasure, and security key change.

32.2.1 CEPT AR Feature Controls

This activity introduces 4 new feature controls in addition to the existing ability to invoke the feature. They are activation, deactivation, interrrogation, and erasure. This activity also introduces a new dialing sequence for invoking the feature following the CEPT specification. NOTE: This new method not replace the existing method for invoking the feature, but will be used when the subscriber is a CEPT line.

With this activity, AR will no longer be activated once provisioned for CEPT lines. The subscriber will need to dial the CEPT-defined activation sequence to make the feature active. Once active, the subscriber may then invoke the feature. To prevent others from invoking the feature and thus incurring charges, the AR feature can be deactivated by dialing the CEPT-defined deactivation sequence. Activation and deactivation require the use of a PIN (Personal Identification Number) in order for the state of the feature to change.

For describing the dialing sequences of these feature contols, the following symbols will be used:

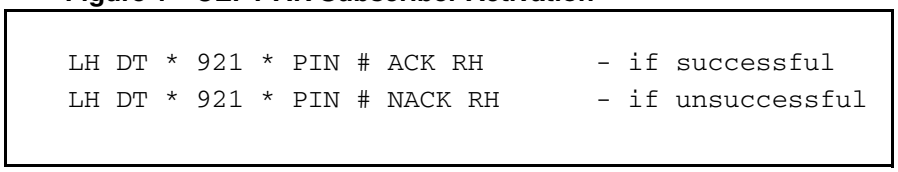
- LH - lift handset
- DT - receive dialtone
- PIN - Personal Identification Number (i.e. password, security key)
- ACK - a positve acknowledgement announcement or tone
- NACK - a negative acknowledement announcement or tone
- RH - replace handset

The ACK/NACK tone is used only if announcement resources are not available. Incomplete activation sequences will result in NACK treatment. (However, an implied octothorpe will be assumed upon digit time-out.).

32.2.1.1 Activation

The subscriber will have the ability to activate CEPT AR by using a special dialling sequence. To activate the CEPT AR feature, the subscriber must execute the sequence depicted in Figure 1.

Figure 1 CEPT AR Subscriber Activation

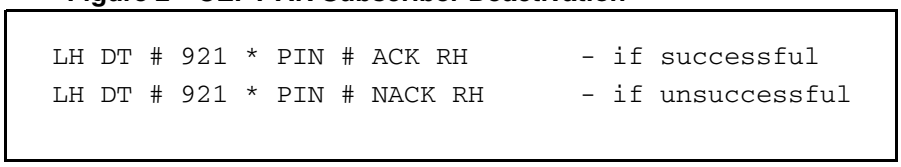


The CEPT AR becomes active immediately after execution of this sequence.

32.2.1.2 Deactivation

The subscriber will have the ability to deactivate CEPT AR by using a special dialling sequence. To deactivate the AR feature, the subscriber must execute the sequence depicted in Figure 2.

Figure 2 CEPT AR Subscriber Deactivation

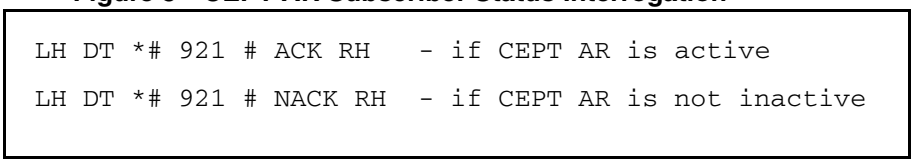


The CEPT AR is deactivated immediately after the execution of this sequence.

32.2.1.3 Interrogation

The subscriber will have the ability to interrogate (i.e. check) the status of the AR feature by using a special dialing sequence. To interrogate the status of the AR feature, the subscriber must execute the sequence depicted in Figure 3.

Figure 3 CEPT AR Subscriber Status Interrogation



32.2.1.4 Erasure

The AR feature stores information about the last incoming call into a register called the Incoming Call Memory Block (ICMB). The subscriber will have the ability to erase the information in the ICMB of the AR feature by using a special dialing sequence. To erase the information in the ICMB, the subscriber must execute the sequence depicted in Figure 4.

Figure 4 CEPT AR Erasure

```
LH DT # 92 # ACK RH   - if erasure is successful
LH DT # 92 # NACK RH  - if erasure is unsuccessful
```

32.2.1.5 Invocation

The subscriber will have the ability to invoke the CEPT AR feature by using a special dialing sequence. To invoke the CEPT AR feature, the subscriber must execute the sequence depicted in Figure 5.

Figure 5 CEPT AR Invocation

```
LH DT *92 # Feature Announcement - if invocation is successful
LH DT *92 # NACK RH              - if invocation is unsuccessful
```

32.2.1.6 Error situations when using AR Feature contols

The subscriber will receive re-order tone and a FTR138 log showing FNAL treatment when dialing an AR feature control sequence in the following situations:

— CEPT and AR options are not assigned on the line.

— Improper feature control is datafilled in table xxCODE for CEPT AR.

32.2.2 CEPT AR Translations

The CEPT AR feature controls must be datafilled using a feature translator in Universal Translations in any XLA xxCODE table, such as, ACCODE or PXCODE. There are five tuples which translations will need datafilled, they are (example Travers are provided in section “32.10 Appendix A - Translation Examples”):

- Activation & PIN change

  These will be handled by the existing xxCODE feature selector using the option feature AR (new FTR) and existing option function ACT. An example tuple in a xxCODE table would look like:

  ```
  AMBISTAR 921 921 FEAT ( FTR AR) ( PF 4) ( MM 3 15) (FUNC ACT)$
  ```

- Deactivation

This will be handled by the existing xxCODE feature selector using the option feature AR (new FTR) and existing option function DEACT. An example tuple in a xxCODE table would look like:

```
AMBIOCT 921 921 FEAT ( FTR AR) ( PF 4) ( MM 3 15) (FUNC DEACT)$
```

- Interrogation

  This will be handled by the existing xxCODE feature selector using the option feature AR (new FTR) and existing option function INTER. An example tuple in a xxCODE table would look like:

```
STARCEPT C921 C921 FEAT ( FTR AR) ( PF 5) ( MM 4 15) (FUNC INTER)$
```

- Erasure

  This will be handled by the existing xxCODE feature selector using the option feature AR (new FTR) and existing option function DELETE. An example tuple in a xxCODE table would look like:

```
OCT92XL 2 EQ FEAT ( FTR AR) ( PF 3) ( MM 2 15) (FUNC DELETE)$
```

- Invocation

  This will be handled by the existing xxCODE feature selector using the option feature AR (new FTR) and existing option function USAGE. An example tuple in a xxCODE table would look like:

```
STAR92XL 2 EQ FEAT ( FTR AR) ( PF 3) ( MM 2 15) (FUNC USAGE)$
```

32.2.3 Security Code (PIN) Assignment for Feature Act/Deactivation

The SEC (Security Code) option allows a common PIN to be assigned to specified services on that line. If a feature on a line is added to the SEC feature list, it becomes PIN protected. If a feature on a line is not in the SEC feature list, then it is not PIN-protected. Thus, there can be multiple features on a line, some PIN-protected and some not PIN-protected. Thus, a feature like CEPT AR which requires a PIN can co-exist on a line with a feature like CEPT ACRJ for which the PIN is optional (i.e. AR would be in the SEC feature list and ACRJ would not be.).

If none of the features on a line need PIN-protection, then, of course, the SEC option would not be added at all to the line. Thus if CEPT ACRJ is on a line with no other options and does not need to be PIN-protected, the SEC option need not be provisioned on that line.

32.2.3.1 CEPT AR PIN Assignment

As mentioned previously, PIN protection is required for the CEPT AR service. To associate PIN protection to the AR service, the craftsperson must use SERVORD to add the SEC option to the line provisioned with CEPT AR.

For example, if LEN 0 1 10 5 already has the CEPT AR option, then the following SERVORD sequence shown in Figure 6 should be used to add the SEC option. Figure 7 and Figure 8, respectively, show the resulting QLEN and IBNFEAT tuple.

Figure 6 Example of adding a PIN to CEPT AR using the SEC option

```
SO:
>ado
SONUMBER:    NOW   3  6 16 PM
>
DN_OR_LEN:
>0 1 10 5
OPTION:
>sec
FEATURES:
>ar <---------- The feature to which the SEC PIN applies
FEATURES:
>$
SEC_CODE:
>0000 <-------- The default PIN set by the TELCO (1 to 7 digits)
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 6 16 PM HOST 00 1 10 05 ( SEC ( AR) $ 0000 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Figure 7 Sample QLEN of CEPT AR and SEC

```
>qlen 0 1 10 5

----------------------------------------------------------------------------------------------

LEN:     HOST  00 1 10 05

TYPE: SINGLE PARTY LINE

SNPA: 613

DIRECTORY NUMBER:     6212064

LINE CLASS CODE:  IBN

IBN TYPE: STATION

CUSTGRP:         IBNTST     SUBGRP: 0  NCOS: 0

SIGNALLING TYPE:  DIGITONE

CARDCODE:  6X17AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N

PM NODE NUMBER     :    204

PM TERMINAL NUMBER :    326

OPTIONS:

CEPT AR NOAMA DGT SEC AR 0000

OFFICE OPTIONS:

AIN TIID

----------------------------------------------------------------------------------------------
```

Figure 8 Sample IBNFEAT tuple with SEC

```
TABLE: IBNFEAT

>format pack

>pos 0 1 10 5 0 sec

HOST 00 1 10 05 0 SEC SEC (AR) $ 0000
```

The reader should note the following regarding the PIN:

- The PIN specified with the SEC option applies to all features in the SEC feature list that are on that line. Thus, for example, if CEPT AR and CEPT ACRJ were both on the above LEN 0 1 10 5 and both features were included in the SEC feature list, both would share the same PIN of 0000.

- The PIN will be visible in Table IBNFEAT and also in the QLEN.
- The PIN length can range from 1 to 7 digits.

32.2.4 Security Code (PIN) Modification for Feature Act/Deactivation

To modify the shared PIN, the service subscriber should dial their designated PIN activation sequence. For example, the CEPT AR subscriber would change their CEPT AR PIN by dialling the following sequence:

* 921 * Current PIN * New PIN #

The CEPT ACRJ subscriber would change their CEPT ACRJ PIN by dialling the following sequence:

* 934 * Current PIN * New PIN #

After the service subscriber dials the '#' (octothorpe) terminating their particular PIN modification sequence (or if the user indicates digit termination by allowing the interdigit timer to expire after the last digit entered), (s)he will be guided by pre-recorded announcements to reenter the new PIN. Figure 9 illustrates the possible announcement sequences that could occur during a PIN change operation. The announcements will only start after the '#' has been entered and if there was successful validation of the *current* PIN.

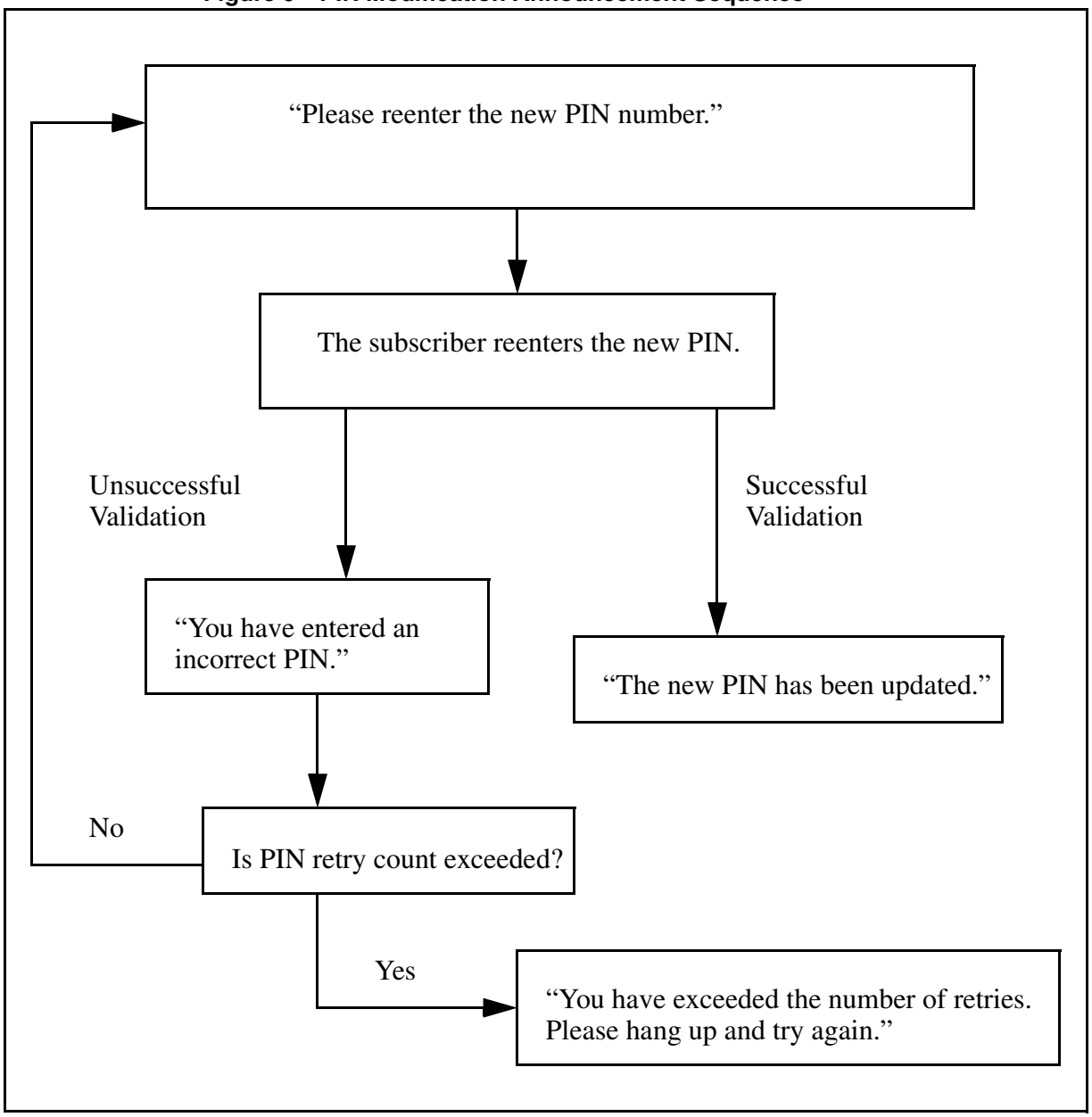
Successful validation of the *current* PIN implies that the entered current PIN matches the stored PIN.

Successful validation of the *new* PIN implies that the entered new PIN was the correct length (1 to 7 digits) and that it was different than the stored PIN.

Upon successful validation of the new PIN, note that the new PIN will be shared by ALL features on the line which are in the SEC feature list.

Note that the PIN can only be changed from the subscriber's phone. Also note that the subscriber will NOT be required to change their PIN from the default PIN upon first usage of the AR or ACRJ feature.

Figure 9 PIN Modification Announcement Sequence



To enable the PIN change capability, the customer group SPP (Station Programmable PIN) option must be datafilled in Table CUSTSTN. It is in this CUSTSTN tuple that the PIN retry count is set as well. The range for the PIN retry count is 1 to 3. See Figure 10 below for an example of an SPP CUSTSTN tuple.

Figure 10 Sample SPP Datafill

```
TABLE: CUSTSTN

IBNTST SPP SPP 3
```

SPP announcements also need to be configured. Refer to NTP 297-8001-350 "Call Forwarding Remote Activation" (CFRA) for more information about SPP as SPP was created as part of the CFRA feature. However, the reader should note that the SPP feature will be invoked automatically in the case of CEPT AR and ACRJ, and not explicitly by the subscriber as stated for CFRA.

32.2.5 NAOC Billing and Metering for CEPT Services

Currently, CEPT services only peg meter counts and produce billing records if World Metering is used. This activity in coordination with feature A00002638: PCA SW Metering Support for Billing **[1]** enhances CEPT services to peg meter counts and produce billing records based on a new table called NAOCFEAT and PCA Software Metering.

This activity introduces a new table, table NAOCFEAT, to be used to determine which feature controls for each CEPT feature will be metered and billed on a per Carrier/Carrier Reseller basis. The table also enables the telco to define what the charges will be for each feature control entered and to define a feature code to be used in the billing record for each feature on a per Carrier/Carrier Reseller basis. Refer to the CN section of this document for a complete description of this new table.

Please refer to the FN and CN sections of feature A00002638 **[1]** for examples and more details on the NAOC meter counts and billing records for CEPT Basic Call.

The NAOC feature billing will be recorded in an AMA record using the new module 612 extension as defined in A00002638 **[1]**. The information contained in the new AMA module is shown in Table 1, "Module 612 extension used for NAOC feature billing," on page 799.

Table 1 Module 612 extension used for NAOC feature billing

BCD Char	Length	Meaning
1 - 3	3	**Rating Class at the beginning of the Call** If the billing record is generated by basic call this field will contain the tariff index used for this call from Table TARFDATA, bound by an upper limit of 511 for the Spanish market. If the billing record is generated by a feature action this field will always be set to the value of “511”.
4 - 11	8	**Used Meter** The total number of meter pulses **used** for this call or feature action.
12 - 15	4	**Initial meter value MS** The 4 most significant digits of the initial meter pulse value.
16 - 19	4	**Initial meter value LS** The 4 least significant digits of the initial meter pulse value.
20 - 27	8	**Final Meter value** The final meter pulse value, i.e., initial value + used value.
28 - 29	2	**Call Type** This field describes if this is a **basic call** or a **feature action**. If the billing record is generated by basic call this field will be equal to “00”. If the billing record is generated by a feature action this field will be equal to a value based on the particular feature, i.e., the featcode, as it is provisioned in table NAOCFEAT (per the carrier/reseller).
30	1	**Feature Action** This field describes the type of feature action If the billing record is generated by basic call this field will be equal to “2”. If the billing record is generated by a feature action this field will be equal to one of 10 values based on the type of action as shown in Table 2, “Feature Actions,” on page 801.

An example (using calldump full) of the AMA billing record is shown in Figure 11, "AMA Record with Module 612 extension".

Figure 11 AMA Record with Module 612 extension

```
HEX ID:                                AA
STRUCTURE CODE:                        40511C
CALL CODE:                             006C        STATION PAID
SENSOR TYPE:                           036C        DMS 100F
SENSOR ID:                             0250250C
REC OFFICE TYPE:                       036C        DMS 100F
REC OFFICE ID:                         0250250C
DATE:                                  30909C      SEPTEMBER 09, 2003
TIMING IND:
    TIMING GUARD FLAG                  0           UNUSED
    SHORT CLD PARTY OFF-HOOK IND       0           UNUSED
    LONG DUR/SERV PTY CAPABILITY IND   0           UNUSED
    UNUSED                             0
    UNUSED                             0C
STUDY IND:
    STUDY TYPE A                       0           UNUSED
    STUDY TYPE B                       2           NETWORK COMPLETION
    STUDY TYPE C                       0           UNUSED
    TEST CALL IND                      0           UNUSED
    UNUSED                             0
    ORIG/TERM NANP NUM IND             0           UNUSED
    OPERATOR SERV IND                  0C          UNUSED
CLD PTY OFF-HK:                        0C          CLD OFF-HOOK DETECTED
SERVICE OBSERVED:                      0C          NONE
OPER ACTION:                           0C          ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:                       000C        OTHER
SIG DIGITS NEXT FIELD:                 010C
ORIG OPEN DIGITS 1:                    01418406301C
ORIG OPEN DIGITS 2:                    FFFFFFFFFF
ORIGINATING CHARGE INFO:               FFFF
DOMESTIC/INTL INDICATOR:               9C          UNKNOWN
SIG DIGITS NEXT FIELD:                 000C
TERM OPEN DIGITS 1:                    00000000000C
TERM OPEN DIGITS 2:                    FFFFFFFFFF
CONNECT TIME:                          1707136C    17:07:13.6
ELAPSED TIME:                          000000000C  000000:00.0
COMPLETION INDICATOR:                  001C        COMPLETED: ANSWERED
MODULE CODE:                           612C        GENERIC MOD: TWO DGT STR FMT
GENERIC CONTEXT ID:
    PARSE RULES                        80070       NAOC PCA CHARGING INFO
    SIGNIFICANT DIGITS                 00C         NIL
GENERIC DIGIT STRING ONE:
    RATING CLASS                       511
    USED METER                         00000015
    INITIAL_METER_MS                   0082
GENERIC DIGIT STRING TWO:
    INITIAL_METER_LS                   0000
    FINAL METER                        00820015
    CALL_TYPE                          27
    FEATURE ACTION                     8
MODULE CODE:                           000C        FINAL MODULE
```

Software feature metering relies on the datafill of Table NAOCFEAT. This table defines the charging per carrier/reseller, per feature, per action.

The carrier/reseller name **must** be defined in either Table CARNAME or Table RESNAME/DNSCRN (for resellers) prior to use in Table NAOCFEAT.

The CEPT features can be associated with software metering with any of the following actions defined in Table 2, “Feature Actions,” on page 801.

Table 2 Feature Actions

Action	Description	Value In Billing Record
assign	assignment	0
deassign	deassignment	1
admact	administrative activation	2
admdeact	administrative deactivation	3
admprog	administrative programming	4
subact	subscriber activation	5
subdeact	subscriber deactivation	6
subprog	subscriber programming	7
usage	usage	8
interrog	interrogation	9

If there is no entry for a particular carrier/feature/action combination, then no software metered billing will be created or used for that particular combination.

Figure 12, "Example entry in Table NAOCFEAT" contains an example of datafill in Table NAOCFEAT for carrier CAR100[1], feature AR.

Figure 12 Example entry in Table NAOCFEAT

```
CARRSNAM FEATNAME FEATCODE ACTIONS
-----------------------------------------------------------------
CAR100   AR       55       (USAGE 7) (ASSIGN 10) (DEASSIGN 10) $
```

To determine what the **used meter** value will be in module 612 for a particular feature action you will need to consider the following: **The provisioned unit value for each action in Table NAOCFEAT is 1/10 of a monetary unit, i.e., 0.10.** Therefore, if 1 metering pulse is equal to 0.06 monetary units per pulse then (based on the example in Figure 12):

- **usage** in meter pulses = `((0.1*7) / 0.06)= 11.67`

To determine what **call type** will appear in the module 612 (for AR usage), it's simply the feature code as provisioned in table NAOCFEAT, i.e., 55. The **feature action** field will be equal to the value 8 (see Table 2, "Feature Actions," on page 801 for details). Thus the module 612 would look like the example shown in Figure 13, "Module 612, for AR usage".

[1]As datafilled in Table CARNAME prior to being used in Table NAOCFEAT.

Figure 13 Module 612, for AR usage

```
MODULE CODE:                          612C       GENERIC MOD: TWO DGT STR FMT
GENERIC CONTEXT ID:
    PARSE RULES                       80070      NAOC PCA CHARGING INFO
    SIGNIFICANT DIGITS                00C        NIL
GENERIC DIGIT STRING ONE:
    RATING CLASS                      511
    USED METER                        00000012 <-- meter pulses based on usage
    INITIAL_METER_MS                  0082
GENERIC DIGIT STRING TWO:                        feature code
    INITIAL_METER_LS                  0000
    FINAL METER                       00820012
    CALL_TYPE                         55 <-------
    FEATURE ACTION                    8  <-------- usage feature action
MODULE CODE:                          000C       FINAL MODULE
```

NAOCFEAT billing is not supported for every feature/feature action combination, please refer to the matrix in Table 3 on page 802, to see which features support NAOCFEAT billing for which actions.

Table 3 Feature/Action Billing Matrix[a]

		Actions									
		Assign	Deassign	Admact	Admdeact	Admprog	Subact	Subdeact	Subprog	Usage	Interrog
Features	ACRJ	X	X	X	X		X	X	X		X
	AR	X	X	X	X		X	X	X	X	X
	AUL	X	X			X					
	CCBS	X	X		X		X	X		X	X
	CDND	X	X	X	X		X	X			X
	CDTA	X	X	X	X		X	X	X	X	X
	CDTO	X	X	X	X		X	X	X		X
	CFB	X	X		X		X	X	X	X	X
	CFD	X	X		X		X	X	X	X	X
	CFF	X	X		X		X	X		X	X
	CFRA	X	X		X						
	CFU	X	X		X		X	X	X	X	X
	CLF	X	X							X	
	CND	X	X	X	X		X	X	X	X	X
	CNDB	X	X						X		

Table 3 Feature/Action Billing Matrix[a]

		Actions									
		Assign	Deassign	Admact	Admdeact	Admprog	Subact	Subdeact	Subprog	Usage	Interrog
Features	CNDBO	X	X							X	
	ENQ	X	X								
	I3WC	X	X							X	
	I6WC	X	X							X	
	ICT	X	X							X	
	ICWT	X	X	X	X		X	X			X
	ILR	X	X	X	X		X	X			X
	IWUC	X	X		X		X	X	X	X	X
	LNR	X	X		X						
	RR									X	
	SCL[b]	X	X		X	X		X	X	X	X
	SCS	X	X					X	X	X	X
	SUPPRESS	X	X	X	X		X	X		X	X
	WML	X	X	X	X	X	X	X	X	X	X

a. “X” denotes a supported action. An empty block denotes an unsupported action.

b. Billing of ‘admprog’ for SCL pertains to the ability to change the size of the speed call list, not the contents of the list.

32.3 Hardware Requirements or Dependencies

none

32.4 Software Requirements or Dependencies

SN07 or ISN06 Activatable Patch for Telefonica

The NAOC feature billing portion of this feature requires the following feature to be activated by SOC:

- NSUP0023 - PCA SW Metering Support for Billing

  This requires the following SOC features:

  — NETK0019 - Network AOC

— NETK0024 - Network AOC Tariff

— NETK0028 - CGP Network AOC

— NSUP0017 - Payment Ceiling

— NSUP0020 - NAOC/PCA Supp Svcs

32.5 Limitations and restrictions

none

32.6 Interactions

none

32.7 Applicable customer facing sections

Fault Management	
Logs	__n/a____
Alarms	__n/a____
Configuration	
Data Schema	__x____
User Interface	__x____
Element Management	__n/a____
Security	__n/a____
Service Order	__n/a____
Office Parameters	__n/a____
Accounting (includes AMA billing)	__x____
Performance (includes operational measurements)	__n/a____

32.8 Glossary

Term	Description
ACK	positve ACKnowledgement announcement or tone
ACRJ	Automatic Call Rejection
AOC	Advice of Charge
AR	Automatic Recall
CEPT	European Conference Of Postal and Telecommunications
CS2K	Communication Server 2000
DT	receive Dial Tone
ETSI	European Telecommunication Standard Institute
IBN	Integrated Business Network
ICMB	Incoming Call Memory Block
LH	Lift Handset
MMP	Multi Market Platform
NACK	Negative ACKnowledement announcement or tone
NAOC	Network Advice of Charge
PCA	Payment Ceiling Advice
PIN	Personal Identification Number
PVG	Passport Voice Gateway
RH	Replace Handset
SEC	Security Code
XLA	Translations

32.9 References

REF #	Description of Reference
[1]	Feature 00002638, *PCA SW Metering Support for Billing* , Issue AA14, PLS FMDOC module: *a00002638.*

32.10 Appendix A - Translation Examples

Ambiguous translations tables AMHEAD & AMCODE are needed to handle the AR access codes in addition to table ACCODE. The following figures

contain example feature code translations for AR including the ambiguous translations.

Figure 14 Translation Example - AR Activation (no PIN)

```
 >traver l 8116666661 b921 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME STARCEPT
STARCEPT 9 NET N N 0 N NDGT N N DOD N 700 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
700 IBN NONE NT 0 0 NILSFC 0 PX STARCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
STARCEPT DFLT CONT ( XLT OFC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
STARCEPT DFLT CONT ( XLT AC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
STARCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE ACCODE
STARCEPT 92 92 CONT ( XLT AM STAR92XL)$
TABLE AMHEAD
STAR92XL SDFLT
THE TOTAL NUMBER OF DIGITS IS 3.
TABLE AMCODE
STAR92XL 3 GE CONT ( XLT AC AMBISTAR)$
TABLE ACHEAD
AMBISTAR SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE ACCODE
AMBISTAR 921 921 FEAT ( FTR AR) ( PF 4) ( MM 3 15) (FUNC ACT)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 15 Translation Example - AR Activation (with PIN)

```
 >traver l 8116666661 b921b1111 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME STARCEPT
STARCEPT 9 NET N N 0 N NDGT N N DOD N 700 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
700 IBN NONE NT 0 0 NILSFC 0 PX STARCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
STARCEPT DFLT CONT ( XLT OFC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        921B1111
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
STARCEPT DFLT CONT ( XLT AC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        921B1111
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
STARCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        921B1111
TABLE ACCODE
STARCEPT 92 92 CONT ( XLT AM STAR92XL)$
TABLE AMHEAD
STAR92XL SDFLT
THE TOTAL NUMBER OF DIGITS IS 8.
TABLE AMCODE
STAR92XL 3 GE CONT ( XLT AC AMBISTAR)$
TABLE ACHEAD
AMBISTAR SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        921B1111
TABLE ACCODE
AMBISTAR 921 921 FEAT ( FTR AR) ( PF 4) ( MM 3 15) (FUNC ACT)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 16 Translation Example - AR Deactivation

```
 >traver l 8116666661 c921 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME OCTCEPT
OCTCEPT 9 NET N N 0 N NDGT N N DOD N 701 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
701 IBN NONE NT 0 0 NILSFC 0 PX OCTCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
OCTCEPT DFLT CONT ( XLT OFC OCTCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
OCTCEPT DFLT CONT ( XLT AC OCTCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
OCTCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE ACCODE
OCTCEPT 92 92 CONT ( XLT AM OCT92XL)$
TABLE AMHEAD
OCT92XL SDFLT
THE TOTAL NUMBER OF DIGITS IS 3.
TABLE AMCODE
OCT92XL 3 GE CONT ( XLT AC AMBIOCT)$
TABLE ACHEAD
AMBIOCT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE ACCODE
AMBIOCT 921 921 FEAT ( FTR AR) ( PF 4) ( MM 3 15) (FUNC DEACT)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 17 Translation Example - AR Interrogation

```
 >traver l 8116666661 bc921 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME STARCEPT
STARCEPT C NET N N 0 N NDGT N N DOD N 700 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
700 IBN NONE NT 0 0 NILSFC 0 PX STARCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
STARCEPT DFLT CONT ( XLT OFC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                            C921
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
STARCEPT DFLT CONT ( XLT AC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                            C921
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
STARCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                            C921
TABLE ACCODE
STARCEPT C921 C921 FEAT ( FTR AR) ( PF 5) ( MM 4 15) (FUNC INTER)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 18 Translation Example - AR Erasure

```
 >traver l 8116666661 c92 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME OCTCEPT
OCTCEPT 9 NET N N 0 N NDGT N N DOD N 701 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
701 IBN NONE NT 0 0 NILSFC 0 PX OCTCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
OCTCEPT DFLT CONT ( XLT OFC OCTCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
OCTCEPT DFLT CONT ( XLT AC OCTCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
OCTCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE ACCODE
OCTCEPT 92 92 CONT ( XLT AM OCT92XL)$
TABLE AMHEAD
OCT92XL SDFLT
THE TOTAL NUMBER OF DIGITS IS 2.
TABLE AMCODE
OCT92XL 2 EQ FEAT ( FTR AR) ( PF 3) ( MM 2 15) (FUNC DELETE)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 19 Translation Example - AR Invocation

```
 >traver l 8116666661 b92 b
TABLE IBNLINES
LG 00 3 00 18 0 DT STN IBN 16666661 RUACEPT 0 21 81 (CWT) (CWI) (LNR) (CEPT)
    (I3WC) (CNDB) (CNAB) $
TABLE DNATTRS
81 $ 16666661
    (PUBLIC ( NAME RUA1_2_AAL2) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE NCOS
RUACEPT 21 0 0 ODP1 ( XLAS ODPXLA1 STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RUACEPT NXLA RUAXLA4 RUAFEAT 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME STARCEPT
STARCEPT 9 NET N N 0 N NDGT N N DOD N 700 NPRT_2 NLCA_NILLA_1 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
700 IBN NONE NT 0 0 NILSFC 0 PX STARCEPT NIL 00 NPRT_2 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
STARCEPT DFLT CONT ( XLT OFC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
STARCEPT DFLT CONT ( XLT AC STARCEPT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
STARCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              92
TABLE ACCODE
STARCEPT 92 92 CONT ( XLT AM STAR92XL)$
TABLE AMHEAD
STAR92XL SDFLT
THE TOTAL NUMBER OF DIGITS IS 2.
TABLE AMCODE
STAR92XL 2 EQ FEAT ( FTR AR) ( PF 3) ( MM 2 15) (FUNC USAGE)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

33: Functional description (FN): A00002655

33.1 Feature name

CEPT ACRJ (Rejection of Unidentified Calls)

33.2 Description

33.2.1 Background Information

ACRJ is an administration assigned feature, but the subscriber as well as administration has the ability of activating, deactivating, and interrogating the status of the feature. When activated, this service causes the switch to reject incoming calls to the line when the call is anonymous, i.e. when the calling name or number is not presented/presentable to the user. The calling party receives an announcement that the call is being rejected because it is anonymous.

33.2.2 CEPT ACRJ Feature Provisioning

CEPT ACRJ is essentially MMP ACRJ with the CEPT interface, PIN protection optionality, and CEPT billing. Accordingly, the feature is provisioned the same as MMP ACRJ except that the CEPT option is added to the line to give the service its CEPT character. In order to add CEPT to the line, CEPT must first be added to the applicable customer group in table CUSTSTN. CEPT ACRJ is available only for IBN lines.

Provisioning changes on the subscriber option can only be done via SO. For CEPT ACRJ both CEPT and ACRJ options should be assigned to the subscriber. There is no limitation or restriction to use together CEPT and ACRJ line options. Whenever CEPT line option is removed from the line ACRJ feature behaves as basic MMP feature instead of CEPT variant and so no CEPT subscriber interface and no CEPT billing will be available. Please refer to FN section of 59019274 CEPT Subscriber Control Functions Framework for CEPT line option.

Figure 1 Sample Feature Provisioning for CEPT ACRJ

```
>servord
SO:
>ado
SONUMBER:    NOW   3  6 19 PM
>
DN_OR_LEN:
>8406101
OPTION:
>acrj
STATUS:
>inact
OPTION:
>cept
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 6 19 PM 8406101 ( ACRJ INACT ) ( CEPT ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

33.2.3 CEPT Feature Control - Activation//Deactivation/Interrrogation

For describing activation, deactivation, and interrrogation (also known as status verification) sequences, it is useful to define several symbols:

- LH - lift handset
- DT - receive dialtone
- FC - the CEPT feature action code for ACRJ, specified as 934 by the CEPT specification.
- ACK - a positve acknowledgement announcement or tone
- NACK - a negative acknowledement announcement or tone
- RH - replace handset

The ACK/NACK tone is always used for interrogation. For activation/ deactivation, an ACRJ specific announcement exists and the tone is used only if announcement resources are not available. Incomplete activation sequences will result in NACK treatment. (However, an implied octothorpe will be assumed upon digit time-out.)

33.2.3.1 Activation

To activate the CEPT ACRJ feature, the subscriber must execute the sequence depicted in Figure 2.

Figure 2 CEPT ACRJ Subscriber Activation

```
LH DT * FC # ACK RH        - if successful
LH DT * FC # NACK RH       - if unsuccessful
```

The CEPT ACRJ becomes active immediately after execution of this sequence. The entry of a valid activation sequence when the feature is already active is treated as a success.

33.2.3.2 Deactivation

Subscriber has the ability to deactivate CEPT ACRJ by using special dialling sequence. To deactivate the ACRJ feature, the subscriber must execute the sequence depicted in Figure 3.

Figure 3 CEPT ACRJ Subscriber Deactivation

```
LH DT # FC # ACK RH        - if successful
LH DT # FC # NACK RH       - if unsuccessful
```

The CEPT ACRJ is deactivated immediately after the execution of this sequence. THe enty of a valid deactivation sequence when the feature is already deactivated is treated as a success.

33.2.3.3 Interrogation

Subscriber has the capability of interrogating the status of ACRJ by using special dialing sequence. To interrogate the status of ACRJ feature, subscriber must execute the sequence depicted in Figure 4.

Figure 4 CEPT ACRJ Subscriber Status Interrogation

```
LH DT *# FC # ACK RH   - if CEPT ACRJ is active
LH DT *# FC # NACK RH  - if CEPT ACRJ is inactive
```

Subscriber gets re-order tone and a FTR138 log with FNAL is generated for the following cases

— CEPT and ACRJ options are not assigned on the line.

— Improper feature action is datafilled in table ACCODE for CEPT ACRJ.

33.2.4 CEPT ACRJ Translations

The CEPT ACRJ feature must be invoked by a feature translator in Universal Translations in any XLA xxCODE table, such as, ACCODE or PXCODE. There are three tuples which translations will need datafilled, they are:

- Activation

  These will be handled by the existing xxCODE feature selector using the option feature ACRJ (new FTR) and existing option function ACT. An example tuple in a xxCODE table would look like:

```
starcept 934 934 FEAT (FTR ACRJ) (PF 4) (MM 3 15) (FUNC ACT) $
```

- Deactivation

  This will be handled by the existing xxCODE feature selector using the option feature ACRJ (new FTR) and existing option function DEACT. An example tuple in a xxCODE table would look like:

```
octcept 934 934 FEAT (FTR ACRJ) (PF 4) (MM 3 15) (FUNC DEACT) $
```

- Interrogation

  This will be handled by the existing xxCODE feature selector using the option feature ACRJ (new FTR) and existing option function INTER. An example tuple in a xxCODE table would look like:

```
starcept C934 C934 FEAT (FTR ACRJ) (PF 5) (MM 4 15) (FUNC INTER) $
```

33.2.5 PIN Protection Optionality

PIN protection is optionally available to users of CEPT ACRJ. PIN protectection is enabled via provisioning the SEC feature on the line -see AR FN for more information. If PIN protection is enabled for a line with ACRJ assigned, the activation and deactivation sequences are changed as follows (“PIN” represents the 4 digit PIN number).

Figure 5 CEPT ACRJ sequences with PIN Protection

Activation

```
LH DT * FC * PIN # ACK RH       - if successful
LH DT * FC * PIN # NACK RH      - if unsuccessful
```

Deactivation

```
LH DT # FC * PIN # ACK RH       - if successful
LH DT # FC * PIN # NACK RH      - if unsuccessful
```

PIN Modification

```
LH DT * FC * PIN * PIN # <voice prompting> RH
```

Details of the PIN protection option including its provisioning, impact on QLEN and QDN displays, and behavior during PIN modification are given in the PIN Protection Optionality section of the AR DSUM (A00002654). The material for AR applies in a straight-forward manner to the ACRJ feature as well.

33.2.6 Accounting/Billing

Billing records/meter pulses are generated for activation, deactivation, and interrogation. The FN for A00002654 documents the behavior of billing for both CEPT AR and CEPT ACRJ.

33.3 Hardware Requirements or Dependencies

N/A

33.4 Software Requirements or Dependencies

N/A

33.5 Limitations and restrictions

- This feature is only applicable on IBN lines with the CEPT option.
- If calling line information is unavailable (e.g. a trunk involved in the call does not propagate this information) then the call to the terminator will not be blocked due to action of this feature. An alternative mode of behavior - blocking all calls lacking calling line information (and called “Mode A” by CEPT specifications for rejection of unidentified calls) - is not supported.

33.6 Interactions

Same as MMP ACRJ

33.7 Applicable customer facing sections

Note: The Configuration and Accounting sections of A00002654 include information applicable to both the CEPT AR feature and this feature.

Fault Management

Logs	__N/A____
Alarms	__N/A____

Configuration

Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

33.8 Glossary

33.9 References

A00002654 CEPT AR (Call Back to Last Received Call) Service, FMDOC

AF2879 CLASS: Anonymous Caller Rejection, OLDOC3

A59019274 CEPT Subscriber Control Functions Framework, FMDOC

33: Functional Description (FN): A00002678

33.1 Feature name

Telefonica IN Enhancements

33.2 Description

33.2.1 Overview

This activity enhances the IN platform to meet Telefonica requirements. Some of the components are only relevant to Telefonica, others are more generic and would be available for use in other CS1-R networks. The following enhancements are provided:

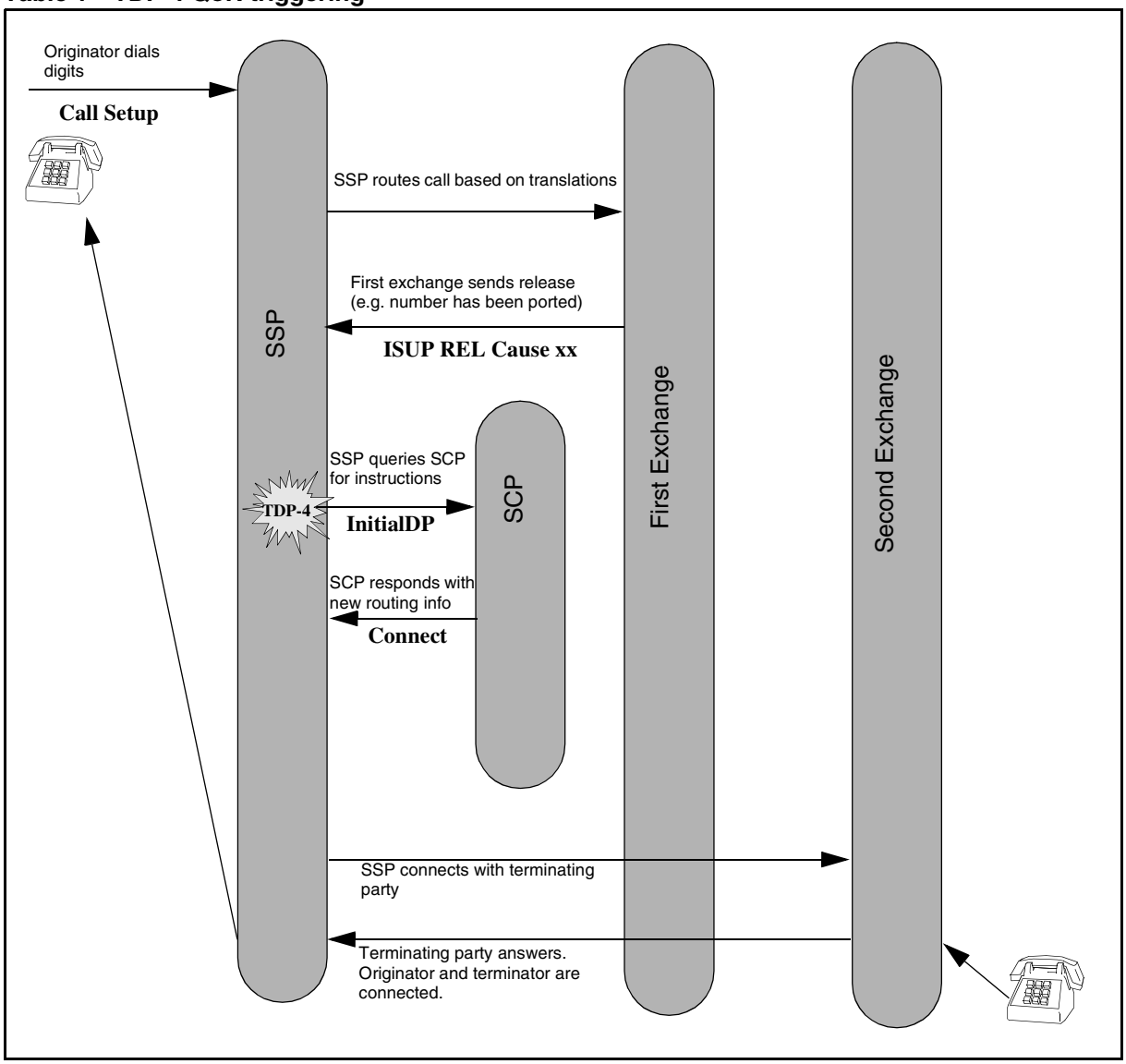
- TDP4 QoR triggering
- CPC Criteria triggering
- FCI handling
- ASF Enhancements
- Overdecadic digits in the CLI parm of the Connect message

For an overview of other IN functionality please refer to [1].

33.2.2 TDP4 Query on Release (QoR) Triggering

TDP4 occurs when a release indication is received from the network or internally within the switch. The feature partially implements TDP4, it only allows IN to be trigger on receipt of an ISUP REL message (from ETSI ISUP and national variants). It does not support releases from other trunk type, nor internal failures to route.

Table 1 TDP-4 QoR triggering



33.2.2.1 Configuration

The criteria for triggering TDP-4 is based on the cause value received in the ISUP message. The release cause value required to trigger TDP-4 is specified in a new criteria type CAUSE in table TRIGGRP. The CAUSE criteria can only be datafilled against NETBUSY triggers. Criteria matching will not be performed on digits at TDP-4, therefore an INFONAME must be datafilled in table TRIGINFO before using the CAUSE criteria.

Figure 1 Example datafill TRIGGRP

```
 KEY
                                                                      TRIGDATA
-------------------------------------------------------------------------------
         ETSIGRP NETBUSY
(GENTRIG ( CAUSE CSE_126) $ MDCKEY1)$
```

The following CAUSE value are supported (Note unsupported values may still be datafilled however they may not trigger.)

Supported Values : 1-5, 8,9, 17-22, 27-29, 34, 38, 41-44, 46,47,50,53,55,57,58,62,63,65,69,70,79,87,88,90,91,95,97,99,102,103,110,111,126

Upto 16 CAUSE values may be specified for a particular trigger group using either the same or different infonames.

Figure 2 Example datafill TRIGGRP

```
 KEY
                                                                      TRIGDATA
-------------------------------------------------------------------------------
TDP4  NETBUSY
(GENTRIG ( CAUSE CSE_126) $ MDCKEY1)
(GENTRIG ( CAUSE CSE_125) $ MDCKEY2)
(GENTRIG ( CAUSE CSE_124) $ MDCKEY2)$
```

The criteria ASSIGNED is also valid at TDP4, in this case all calls in which the originating trunk/line is subscribed to the TDP4 group, will trigger at TDP4 when released.

In addition to the criteria matching, TDP-4 triggering can be controlled on a per switch basis via a new office parm WTIN_TDP4_ACTIVE in table OFCENG. The default value for this parm is FALSE.

A new option CAUSE[1] has been added to the INITDP_PARMS options in table SERVINFO. If this option is present the cause value used to trigger at TDP-4, will be sent to the SCP in the InitDP.

Figure 3 Example datafill SERVINFO

```
SERVIDX                                                                OPTION
-------------------------------------------------------------------------------

4441    (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) (CAUSE) $)
           (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
           (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
```

[1]The CAUSE option is available from SN07 onwards

33.2.2.2 TRAVER support

The TRAVER tool can be used to verify TDP-4 functionality. If a TDP4 trigger is detected the user is prompted to input a cause value, this is then checked against the datafilled criteria.

Figure 4 Example TRAVER using CAUSE triggering at TDP-4

```
>traver l 8226034 743012345 b
TABLE IBNLINES
LG 01 2 00 34 0 DT STN IBN 8226034 CSLINES 0 0 141 (LNR) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
LG 01 2 00 34 0 AIN AIN TDP4GRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
CSLINES 0 0 0 DFLT ( XLAS K1TYPE NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSLINES NXLA K1PSTN CSFETXLA 0 CSACCDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME K1TYPE
K1TYPE 7 NET N N 0 N CSDIG N Y DOD N K1TYPE CS_NPRT CS_NIL NONE $
TABLE DIGCOL
CSDIG 7 COL L 7
TABLE LINEATTR
K1TYPE IBN NONE NT 0 0 NILSFC 0 PX TYPEPX NIL 00 CS_NPRT CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CS_NPRT NSCR 141 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
TABLE PXHEAD
TYPEPX DFLT CONT(XLT PX PUBAPSTN)$ DFOP(CLASS NATL)$NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:              743012345
TABLE PXCODE
TYPEPX 7 7 CONT ( PF 1) ( MM 6 18) ( XLT PX ATMEPX)$
TABLE PXHEAD
ATMEPX SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:              43012345
TABLE PXCODE
ATMEPX 430 430 RTE ( PF 3) ( DEST 430)$
TABLE: PXRTE
KEY:   ATMEPX  430
 . S K1197EISWBE
EXIT TABLE PXRTE
TABLE AMAXLAID
MANTEST DFLT (FLEXCTYP GENERIC 910 OVRDALL )$
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN K1197)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
 . GENTRIG ( CDPN SIMTOOL)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
```

```
TABLE TRIGGRP
TDP4GRP NETBUSY
 . GENTRIG ( CAUSE CSE_126)$ MDCKEY1
Trigger INAPV8 GENTRIG is applicable to individual line.
PLEASE ENTER VALUE FOR RELEASE CAUSE (0..127)
>126
 .  . TABLE TRIGINFO
 .  . MDCKEY1 EVENT TCAP INAPV8 SS7 EIN_NATL_GTT DFLT (SERVKEY 1111)
 .  .     (SERVINFO_INDEX 1111) $
 .  .  . TABLE SERVINFO
 .  .  . 1111
 .  .  .     (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) $)
 .  .  .     (BILL_INFO (FCI_OPT FREEFORM ) $)
 .  .  .     (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
 .  .  . EIN_NATL_GTT CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EIN_NATL_GTT 1111 1111 PCSSN (K1197RS1 EIN 50) $ SSN
INAP Route Select Failure TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


INAP Route Select Failure TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

33.2.2.3 TDP-4 Usage example: Local Number Portability

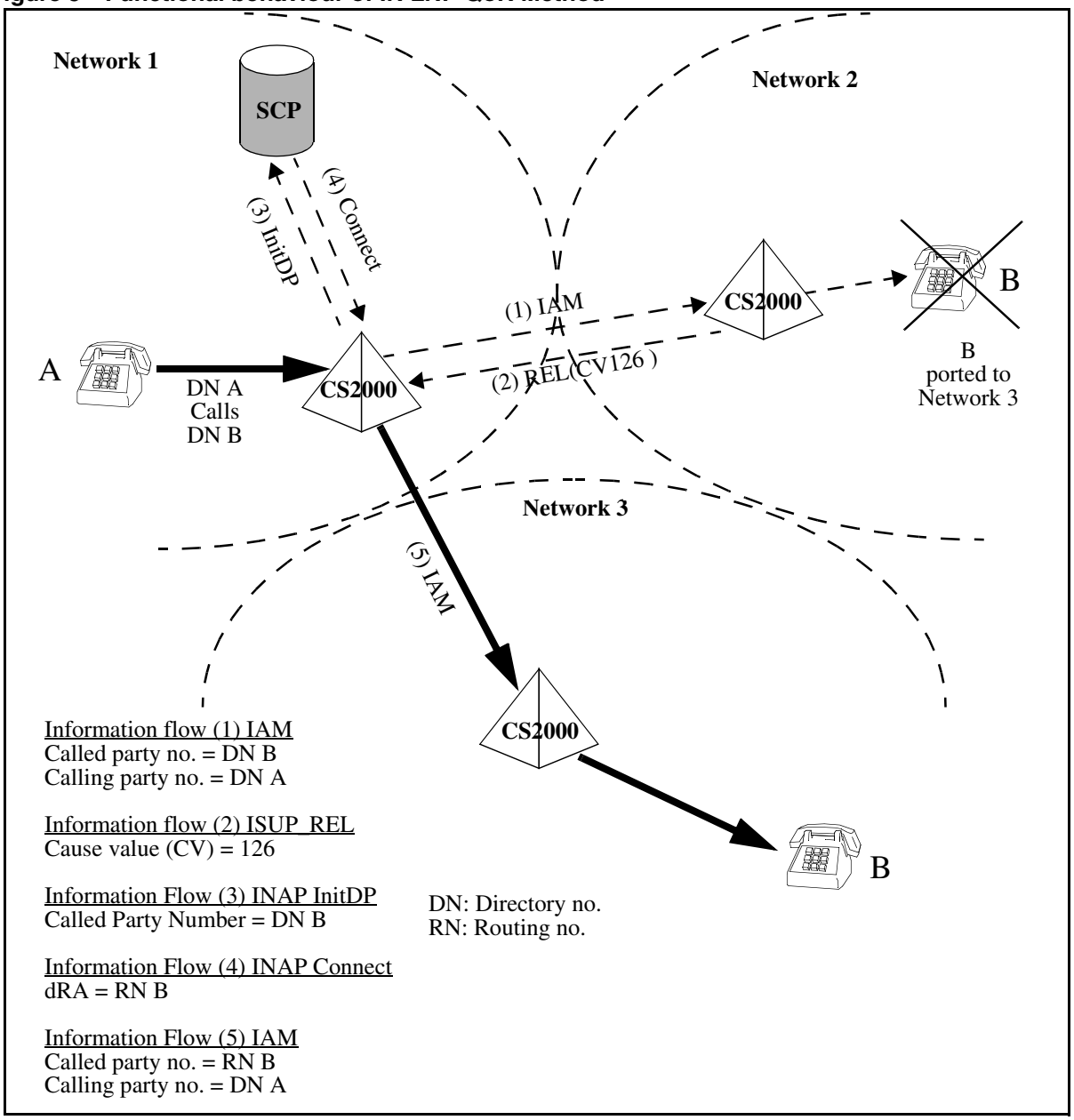
TDP-4 QoR functionality can be used for a variety of services, this example demonstrates an LNP service using TDP-4 triggering.

Local Number Portability (LNP) enables customers to switch from one service provider to another service provider in the same geographical location, without having to change their telephone number.

This feature supports the IN based Local Number Portability by the Query on Release (QoR) method. QoR allows a call to be routed over Spanish ISUP trunks to the donor exchange. If the called directory number is ported, the donor exchange will release the call by sending REL 126 (QoR: NUMBER PORTED) to the QoR serving exchange. The QoR serving exchange (the originating, or in some case an intermediate exchange) upon receiving REL 126 will trigger the IN service and a query will be sent to the SCP. The SCP will reply with the new routing number and the QoR serving exchange will route the call to the recipient exchange based on the new routing number provided by the SCP.

For more information on non-IN LNP please refer to [4].

Figure 5 Functional behaviour of IN LNP QoR Method



33.2.2.3.1 Configuring the CS2K for IN based QoR LNP

The following steps are required to configure the CS2K for IN based QoR LNP

1 Configure trunks to support QoR:

QoR Release sending and receiving is controlled by the LNP option in table ISUPSVC. For more information about the LNP option in table ISUPSVC see [4]. All outgoing trunks that need to support triggering at TDP-4 need to have either the FULL or RX options specified. If the

release should be propagated back to a previous exchange the originating trunk needs to have either the FULL or SEND options specified. If either of these options are datafilled on the originating trunk the call will not trigger at TDP-4 if a QoR specific cause value is used (e.g. 14 or 126), regardless of IN datafill.

To use the Spanish specific ported number release cause (126) rather than the default (14), the SPAIN NATL_LNP_QOR option must be specified in table ISUPSVC. For more information on the SPAIN ISUPSVC options please see [5].

Figure 6 Example datafill ISUPSVC

```
 KEY      SERVICE
-------------------------------------------------------------
LNPSEND   (LNP QOR (SEND) $) (SPAIN (NATL_LNP_QOR) $)$
LNPRX     (LNP QOR (RX)$)$
```

Figure 7 Example datafill TRKOPTS

```
 OPTKEY     OPTINFO
-------------------------------------------------------------------------------
K1S5040SP2A ISUPSVC ISUPSVC        LNPSEND
K1S5040SP2B ISUPSVC ISUPSVC        LNPRX
```

2 Configure TDP-4 trigger criteria:

For trunk originations the TDP-4 trigger criteria needs to be specified in table TRIGGRP and the originating trunk(s) subscribed to the trigger group, either on a per trunk basis in table TRKAIN or on an office wide basis with the AIN_OFFICE_TRIGGRP office parameter in table OFCVAR. For line originations the AIN line option needs to be added via SERVORD

Figure 8 Example datafill TRIGGRP

```
 KEY             TRIGDATA
-------------------------------------------------------------------------------
TDP4GRP NETBUSY   (GENTRIG ( CAUSE CSE_126) $ MDCKEY1)$
```

Figure 9 Example datafill TRKAIN

```
GRPKEY       AINGRP     AININFO
-------------------------------------------------------------------------------
K1S5020EI2B  TDP4GRP
```

Figure 10 Example datafill OFCVAR

```
 PARMNAME            PARMVAL
-------------------------------------------------------------------------------
AIN_OFFICE_TRIGGRP   ETSIGRP
```

Figure 11 Example Line datafill

```
>qdn 8226035
--------------------------------------------------------------------------------
DN:     8226035
TYPE: SINGLE PARTY LINE
SNPA: 141   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     LG    01 2 00 35
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CSLINES     SUBGRP: 0  NCOS: 0
CARDCODE:  GWLPOT    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    72
PM TERMINAL NUMBER :    36
OPTIONS:
LNR DGT AIN TDP4GRP

--------------------------------------------------------------------------------
```

3 Configure translations to modify the NOA post TDP-4:

If a specific NOA is required for Ported Calls (for Spain an NOA of 126 is required), translations needs to be set up to modify the NOA based on the new value specified by the SCP using the CDNRTE and SETCDN options. Example datafill for table CDNCHAR is shown in figure 12, and an example translations setup can be seen in figure 13. See reference [3] for more info on the CDNRTE and SETCDN options

Figure 12 Example datafill CDNCHAR

```
 CDNKEY     PROTLIST
--------------------------------------------------------------------------------
 NOA_126    (INAP (ALL 126) $ N N)
            (ETSIISUP (ALL 126) $ N 126)$
```

Figure 13 Example TRAVER for IN based LNP service using QoR

```
>traver tr K1S5020EI2B 5040508226034 ainres icsx connect 50208226034 in_cdnchar
1 126 b
TABLE TRKGRP
K1S5020EI2B IBNT2 0 NPDGP NCRT CSLINES 0 MIDL 0 N ANSDISC 0 N N N N N N N 0 0 N
    0 1 0 1 N N N N N N N N N NATL $
 .  . TABLE TRKAIN
 .  . K1S5020EI2B TDP4GRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CSLINES 0 0 0 DFLT ( XLAS K1TYPE NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSLINES NXLA K1PSTN CSFETXLA 0 CSACCDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME K1TYPE
K1TYPE 5 NET N N 0 N CSDIG N Y DOD N K1TYPE CS_NPRT CS_NIL NONE $
TABLE DIGCOL
CSDIG 5 COL L 7
TABLE LINEATTR
K1TYPE IBN NONE NT 0 0 NILSFC 0 PX TYPEPX NIL 00 CS_NPRT CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CS_NPRT NSCR 141 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
TABLE PXHEAD
TYPEPX DFLT CONT ( XLT PX PUBAPSTN)$ DFOP ( CLASS NATL)$ NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                  5040508226034
TABLE PXCODE
TYPEPX 5040 5040 RTE ( PF 4) ( MM 5 24) ( DEST 40) ( CLASS NATL)$
TABLE: PXRTE
KEY:   TYPEPX   40
 . S K1S5040SP2A
EXIT TABLE PXRTE
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN K1197)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
 . GENTRIG ( CDPN SIMTOOL)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
TABLE TRIGGRP
TDP4GRP NETBUSY
 . GENTRIG ( CAUSE CSE_126)$ MDCKEY1
Trigger INAPV8 GENTRIG is applicable to individual trunk.
PLEASE ENTER VALUE FOR RELEASE CAUSE (0..127)
>126
 .  . TABLE TRIGINFO
 .  . MDCKEY1 EVENT TCAP INAPV8 SS7 EIN_NATL_GTT DFLT (SERVKEY 1111)
 .  .     (SERVINFO_INDEX 1111) $
 .  .  . TABLE SERVINFO
 .  .  . 1111
 .  .  .     (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) (CAUSE) $)
 .  .  .      (BILL_INFO (FCI_OPT FREEFORM ) $)
 .  .  .      (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
```

```
 .  .  . EIN_NATL_GTT CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EIN_NATL_GTT 1111 1111 PCSSN (K1197RS1 EIN 50) $ SSN
INAP Route Select Failure TDP:  trigger criteria met, querying the database.
INAP Info Analyzed TDP:  AINRES CONNECT option specified
INAP Route Select Failure TDP:  CONNECT NPI = 1 NOA = 126
TABLE CDNCHAR
 . Matched on NOA_126
TABLE IBNXLA: XLANAME K1TYPE
K1TYPE 5 NET N N 0 N CSDIG N Y DOD N K1TYPE CS_NPRT CS_NIL NONE $
TABLE DIGCOL
CSDIG 5 COL L 7
TABLE LINEATTR
K1TYPE IBN NONE NT 0 0 NILSFC 0 PX TYPEPX NIL 00 CS_NPRT CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CS_NPRT NSCR 141 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
TABLE PXHEAD
TYPEPX DFLT CONT ( XLT PX PUBAPSTN)$ DFOP ( CLASS NATL)$ NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    50208226034
TABLE PXCODE
TYPEPX 5020 5020 RTE ( PF 4) ( MM 5 24) ( DEST 20) ( CLASS NATL) ( CDNRTE )$
TABLE CDNUXLA
 . NOA_126 PX TYPEPX XLA FT FANOA126
TABLE FTHEAD
FANOA126 DFLT RTE ( MM 1 24) ( DEST 20) ( SETCDN NOA_126)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                      8226034
TABLE FTCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE: FTRTE
KEY: FANOA126   20
 . S K1S5020EI2A
EXIT TABLE FTRTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 K1S5020EI2A    8226034                    ST
The called number characteristics set are NPI: Unchanged NOA: 126

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

33.2.1 CPC Triggering (only available from SN07 onwards)

This activity allows calls to be triggered based on the Calling Party Category (CPC) for incoming calls from supported protocol.

The CPC is mapped to a generic, protocol independent Calling Party Category Name (CPCNAME) in table CPCCHAR. A new criteria type, CPC, in table TRIGGRP, is then used to trigger calls based on the CPCNAME. The CPC option can be datafilled against the INFOCOL (TDP-2) and INFOANAL (TDP-3) TDPs.

33.2.1.1 Table CPCCHAR

Table CPCCHAR is used to convert the protocol's CPC value, into a generic, protocol independent CPCNAME. This CPCNAME is then used for routing the call.

Each tuple in table CPCCHAR comprises of a CPCNAME, followed by between one and eight protocols, of which four protocols are currently valid. Each protocol has a list of between one and sixteen CPC values to match. The CPC value is specified in decimal.

For more information on table CPCCHAR and CPC routing please refer to [2].

Figure 14 Example datafill for table CPCCHAR

```
TABLE: CPCCHAR
CPCKEY
                                                                        PROTLIST
-------------------------------------------------------------------------------
PUBLPAYP
(BTUP     3   8   $ )
(ETSIISUP 15  $   )
(FTUP     14  $   )
(REDBKTUP 15  $   ) $

OTHRPAYP
(BTUP     9   10  $ ) $

UNKNOWN
(BTUP     0   $   )
(ETSIISUP 0   $   )
(FTUP     0   $   )
(REDBKTUP 0   $   ) $
```

Figure 15 Example datafill TRIGGRP

```
 KEY
                                                                      TRIGDATA
-------------------------------------------------------------------------------
-
          ETSIGRP  INFOCOL
(GENTRIG ( CPC UNKNOWN) $ MDCKEY1)$

          ETSIGRP INFOANAL
(GENTRIG ( CPC PUBLPAYP) $ MDCKEY1)$
```

33.2.1.2 TRAVER support

The TRAVER tool can be used to verify CPC based triggering.

Figure 16 Example TRAVER using CPC triggering at TDP-2

```
 >traver tr pubm411eiswbe 01628430000 b
TABLE TRKGRP
PUBM411EISWBE IBNT2 0 NPDGP NCRT PUBLIC162MEL 0 MIDL 0 N ANSDISC 0 Y N N N N N
    0 0 N 0 1 0 1 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
PUBLIC162MEL 0 0 0 DFLT ( CPCRTE )$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
PUBLIC162MEL NXLA PUBMXLA PUBMFET 0 PUBMDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE TRIGGRP
ETSIGRP INFOCOL
 . GENTRIG (CPC UNKNOWN)$ MDCKEY1
Please enter a CPCCHAR protocol name or N
to specify CPC Routing not required
Protocol Name:
>etsiisup
ENTER CPC VALUE FOR ETSIISUP
CPC VALUE:
>0
TABLE CPCCHAR
 . Matched on UNKNOWN
Trigger INAPV8 GENTRIG is applicable to office.
 .  . TABLE TRIGINFO
 .  . MDCKEY1 EVENT TCAP INAPV8 SS7 EINJAZZ DFLT (SERVKEY 4441)
(SERVINFO_INDEX4441)
 .  .     $
 .  .  . TABLE SERVINFO
 .  .  . 4441
 .  .  .     (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) $)
 .  .  .     (BILL_INFO (FCI_OPT FREEFORM ) $)
 .  .  .     (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
 .  .  .     (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
 .  .  . EINJAZZ CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EINJAZZ 4441 4441 PCSSN (K1197RS1 EIN 50) $ SSN
INAP Info Collected TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


INAP Info Collected TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

33.2.2 Telefonica FCI

The FCI option in table SERVINFO has been expanded to include a new FCI format of TELEFONICA. If the TELEFONICA FCI option is present, the SSP will accept the FCI in an OCTET STRING with boundaries of 0 to 200 bytes of billing data. For more information on Multivendor FCI please refer to [6].

Figure 17 Example datafill SERVINFO

```
SERVIDX                                                                 OPTION
-------------------------------------------------------------------------------

4441    (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) $)
           (BILL_INFO (FCI_OPT TELEFONICA 127) $)
           (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
           (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
```

Figure 18 ASN.1 encoding for Telefonica FCI

```
Integer2 ::= INTEGER (0..32767)

Register ::= IA5 STRING (SIZE(1..20))

Item ::=        SEQUENCE {
   key          [0] Integer2,
   value        [1] Register
   }

SuplementaryService ::= SEQUENCE {
    serviceType              [0] Integer2,
    value                    [1] Integer2
    }

Feature ::=     SEQUENCE {
   key          [0] Integer2,
   value        [1] Integer4
   }

TESATariff ::= OCTET STRING (SIZE (5))

CorrelationID ::= OCTET STRING (SIZE (7))

FCIPartyToCharge ::= CHOICE {
    single   [0] ENUMERATED {
                        CallingParty(1),
                        Subscriber(2),
                        Account(3),
                        VPN-GN(4),
                        VPN-SGN(5),
                        ServiceProvider(6)
                        },
     legID   [1] LegID
     }

fCIBillingChargingCharacteristics ::= SEQUENCE{
   fCIRegisterClass          [0] ENUMERATED {
                                    first(0),
                                    intermediate(1),
                                    }                          OPTIONAL,
   fCIPartyToCharge          [17] FCIPartyToCharge            OPTIONAL,
   fCIServiceKey             [2] ServiceKey
   fCIChargeNumber           [7] Register                     OPTIONAL,
   correlationID             [1] CorrelationID                OPTIONAL,
   fCITariff                 [18] TESATariff
   fCIFeatures               [15] SET (SIZE (1-8) OF Feature  OPTIONAL,
   fCISuplementaryServices   [14] SET (SIZE (1-8) OF
                                    SuplementaryService
   fCIItems                  [16] SET (SIZE (1-8) OF Item
   }
```

The SSP will check the tag and length of the ASN.1 parameters received to ensure that they are contained in correct structure and then report the ASN.1 encoding in the module 199's appended to the AMA record.

The Parameters the fCIBillingChargingCharacteristics shall/may transport are:

1 First FCI Invocation

Scenario A - Before invoking a control connection operation: ETC, CONNECT and received after the opening of a AMA record on behalf of sending an InitialDP operation to the SCP. The following parameters are Mandatory:

fCIRegisterClass

fCIServiceKey

Scenario B - Before invoking a control connection operation ICA/ Continue and received after the opening of a AMA record on behalf of sending an InitiateCallAttempt operation to the SCP. The following parameters are Mandatory:

fCIRegisterClass

fCIServiceKey

fCITariff

In both cases if this first FCI Operation does not contain all of these mandatory parameters, the SSF shall abort the TCAP dialogue with the SCF and will initiate the release of the call.

The remaining Parameters are optional.

2 Second and subsequent FCI Invocation, which may be sent during the same connection configuration, only the additional information:

fCIFeatures

fCISupplementaryServices

fCIItems

can be sent to the SSP. In the case where EDPS are armed if the FCI contains any other parameters different from the ones mentioned, the SSP shall discard them.

33.2.2.1 NAOC support

If an fCITariff parameter is received, in addition to being it decoded and reported in the module 199's the charge information will be passed to the NAOC framework which is done by a separate activity.(See [7] A00002637 Network AOC support for spanish trunk metering). The CS2K will not generate ISUP TAR messages based on the received fCITariff.

33.2.3 ActivateService Filtering Enhancements

33.2.3.1 Network specific duration

A new office parm has been created called INAP_ASF_FILTERING_TIMEOUT_DUR in table OFCENG to specify the network specific ASF duration. The office parameter accepts values in the range -1 to 86,400 seconds, -1 represents an infinite duration. The default value of the office parm is 0. If the SSP receives a ASF operation with a duration of -2, this indicates the value is network specific and the value of the office parameter is used for the ASF operation. Changes to the office parm will only affect new ASF operations and not any that may currently be processing.

33.2.4 Multi-vendor ASF

This enables the SSP to accept sFBillingChargingCharacteristics that are not in the NortelFreeform format. This is similar to the way FCI can accept multi-vendor FCIBillingChargingCharachteristics.

Figure 19 ASN.1 encoding for Telefonica sFBillingChargingCharacteristics

```
SFBillingChargingCharacteristics::= SEQUENCE {
            sFServiceKey [0] ServiceKey OPTIONAL
            generateChargingInfo [1] TESATariff OPTIONAL
            generateAccountRecord [2] BOOL DEFAULT FALSE
            }
```

In order for the CS2K to accept Telefonica format sFBillingChargingCharacteristics the INAP_VARIANT office parameter in table OFCENG must be set to TELEFONICA

Figure 20 Example datafill INAP_VARIANT office parameter in table OFCENG

```
 PARMNAME                  PARMVAL
--------------------------------------------------------------------------------
INAP_VARIANT               TELEFONICA
```

33.2.5 Overdecadic digits in the CLI parm of the Connect message

This activity adds supports for overdecadic (B-F) digits in the CLI parm of the Connect message. Although the CS2K supports the reception of overdecadic digits, the protocol used for any subsequent routing may not. Therefore care should be taken that if overdecadic digits are used in the CLI parm of a connect message, all signalling protocols used to onward route the call must also support overdecadic CLI digits.

33.3 Hardware Requirements or Dependencies

None

33.4 Software Requirements or Dependencies

A00002713 Spanish ISUP Enhancements for Telefonica is required by this functionality.

33.5 Limitations and restrictions

33.5.1 General Limitations

In SN06.2 the CS2K IN platform has the following limitations:

33.5.1.1 Interactions with Explicit Call Transfer

The CS2K does not support IN service interactions with the Explicit Call transfer feature.

33.5.1.2 Call Forward denial per IN service

It is possible to prevent forwarded calls triggering all services but not on a per service basis

33.5.1.3 Call Waiting

If a Call Waiting signal is received during a call to a ASF (TeleVote service), the IN dialog will be aborted (as expected) and the TeleVote announcement (if applicable) may be cut short.

33.5.1.4 Telemetering

The CS2K does not support the generation of ISUP TAR messages from Tariff information received in an FCI or sFBillingChargingCharacteristics.

33.5.1.5 Three Way Call

It is not be possible for services that arm EDPs or CIRP to use the conference capability of 3WC.

33.5.1.6 Multiple Control Relationships per call

Multiple IN services are not possible in a single call (e.g. using a Calling card to access a TeleVote number). If multiple services are required looparounds are needed.

33.5.1.7 Omit missing ISUP parameters from InitDP

ISUP Parameters missing from ISUP signalling are not omitted from the InitDP, instead an unknown value is used. For example if Redirection info is required in the InitDP and a Redirection Parameter is not received from the ISUP signalling, a redirection parameter with a value of unknown will be sent to the SCP.

33.5.1.8 Filtering Criteria for callingAddressValue and location

The CS2K is not able to filter ASF (TeleVote) calls based on callingAddressValue or location.

33.5.1.9 ETC SCFId CorrelationID

The SCFId and CorrelationID ISUP parameters are not supported by the CS2K. These should be appended to the end of the assistingSSPIPRoutingAddress address

33.5.1.10 Telefonica Specific Extension Parameters

Telefonica specific Extension Parameters are not supported by the CS2K.

33.5.1.11 Cancel Operation

The CS2K does not support the cancel operation.

33.5.1.12 ASF (TeleVote) maximum counters = 20

The CS2K can support a maximum of 20 counters per ASF operation. If more TeleVote numbers are required, several ASF operations are required e.g. one for nbrs 0800000001 to 0800000020, one for 0800000021 to 0800000030 etc.

33.5.1.13 ICA in Begin Package

The CS2K does not currently support the ICA operation in a TCAP begin package.

33.5.2 TDP4 specific limitations

Only the following interworkings are supported. Where ETSI ISUP is listed below this includes all national variants.

- ETSI ISUP -> ETSI ISUP
- Line -> ETSI ISUP
- 3WC-> ETSI ISUP
- CFW -> ETSI ISUP
- PRI -> ETSI ISUP

TDP4 as a trigger point is only detectable from the Routing + Alerting PIC. It should not be possible to detect it post answer. However it is a possible for early ACM and ANM messages to be received from the network, and that these are indistinguishable from the real ACM and ANM. Therefore the SSP will trigger TDP4 even if an ANM or ACM has been received.

The originating line/trunk must be an IN capable agent and be subscribed to the TDP4 group datafilled in TRIGGRP. In the case of Lines, 3WC and CFW the relevant OFCPARMS (e.g WTIN_LINE_TRIGGERING_ACTIVE or INAP_3WC_INTERWORK) must also be datafilled.

33.6 Interactions

None

33.7 Applicable customer facing sections

Fault Management

- Logs _N/A__
- Alarms _N/A__

Configuration

- Data Schema __X___
- User Interface _N/A__
- Element Management _N/A__
- Security _N/A__
- Service Order _N/A__
- Office Parameters __X___

Accounting (includes AMA billing) _N/A__

Performance (includes operational measurements) _N/A__

33.8 Glossary

Term	Description
3WC	Three Way Call
ACM	Address Complete Message
AMA	Automatic Message Accounting
ANM	ANswer Message
ASF	ActivateService Filtering
ASN.1	Abstract Syntax Notation One
CDN	CalleD Number
CFW	Call Forward
CIRP	Call Information RePort
CPC	Calling Party Category
CPCCHAR	CPC Characteristics
CS1-R	Capability Set 1 - Refined
CS2000	CallServer 2000

Term	Description
CS2K	CallServer 2000
DN	Directory Number
EDP	Event Detection Point
ETC	Establish Temporary Connection
ETSI	European Telecommunications Standards Institute
FCI	Furnish Charging Information
IAM	Initial Address Message
ICA	Initiate Call Attempt
IN	Intelligent Network
InitDP	InitialDP
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LNP	Local Number Portability
NAOC	Network Advise of Charge
NOA	Nature of Address
NPI	Numbering Plan Indicator
PIC	Point In Call
PRI	Primary Rate Access
QoR	Query on Release
REL	RELease
RN	Redirecting Number
SCF	Service Control Function
SCFId	Service Control Function Id
SCP	Service Control Point
SSP	Service Switching Point
TAR	TARiff
TCAP	Transaction Capabilities Application Part
TDP	Trigger Detection Point
TRAVER	TRAnslations VERification

33.9 References

[1] ITU Intelligent Networks Systems Guide (INSYSGDE in PLS FMDOC)

[2] AJ5343 CPC Routing

[3] AJ4884 CDN Translations (enhanced by AJ5346, AT.59013196 & AT.59023654)

[4] AT.59027497 LNP Query on Release - Non IN

[5] ACT.A00002713 Spanish ISUP Enhancements for Telefonica

[6] AG5522 DMS SSP REL 6 (CUSTOMER FACING DOCUMENTATION)

[7] A00002637 Network AOC support for spanish trunk metering

34: Functional Description (FN): A00002680

34.1 Feature name

CEPT / Telefonica Spain Changed Number Indication

34.2 Description

This feature is intended for the Telefonica market to provide intercept service using the UAS platform for telco subscribers who dial directory numbers that are no longer in service. The service is known as AIS (Automatic Intercept System) or CNI (Changed Number Intercept). Note that this feature is not CEPT specific, despite the title.

Currently, the DMS supports AIS via a trunk interface to an external machine that provides all the necessary announcements and functionality. This activity will provide the same type of functionality via an on-switch application utilizing the UAS as the announcement platform.

Callers reaching an intercepted number will receive a customized announcement from the UAS which includes the number that has been dialled (base DN) and the new directory number (reference DN) of the subscriber they attempted to call. The reference DN will be associated with the base DN through datafill in the DMS.

Following is a description of how to provision and operate this service:

34.2.1 Routing a Directory Number to Intercept Service

When a subscriber requests a directory number change, their old number will be assigned to OPRT treatment via SERVORD. The intercept treatment OPRT can be assigned via any of the following SERVORD commands: CDN, CHDN, DEL, CICP_OUT, and EXBEST. In the case where only the generic notification is desired (number change notification without informing of the new number), the directory number should be routed to BLDN treatment instead of OPRT via SERVORD.

The OPRT tuples in TMTCNTL are modified to route to the CLLI corresponding to the AIS announcement. This can be accomplished by changing the individual instances (i.e. OPRT in subtable LNT for line terminations) or deleting the OPRT tuple from each TMTCNTL subtable and modifying the entry in OFFTREAT [The entry in OFFTREAT applies to the entire office, but is over-ridden by entries in the other TMTCNTL tuples].

Following is an example of the TMTCNTL datafill necessary to route to OPRT treatment:

Figure 1 TMTCNTL Datafill to Route to AIS

```
TABLE: TMTCNTL

EXTTMTNM   TREAT
----------
 OFFTREAT ( 234)

>SUB;POS OPRT

TREATMT LOG            FSTRTE
--------------------------------
  OPRT   Y  S        AIS_ANN
```

For software or virtual directory numbers (numbers not associated with physical circuits), the intercept service can be specified by routing to OPRT treatment via table DNROUTE as shown below:

Figure 2 DNROUTE Datafill to Route to AIS

```
AREACODE OFCCODE    STNCODE       DNRESULT
-------------------------------------------------------------------------------
   919     991       6100                              D OPRT
```

A list of all directory numbers routed to OPRT treatment can be obtained via the QDNSU command of SERVORD. This command can be used to generate either a numeric count of all numbers routed to OPRT or a listing of all individual directory numbers. Following is an example of the QDNSU command:

Figure 3 Servord QDNSU Command Output

```
>qdnsu
DIRECTORY_NUMBER_RANGE: ALL
>
TREATMENT: UNDT
>oprt
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QDNSU ALL  OPRT D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
WARNING : Queries of all DNs or a large range of DNs
        may run for 30 minutes or more before producing any output
Please confirm ("YES", "Y", "NO", or "N"):
>y
 REPORT ON UNASSIGNED DN
TREATMENT:OPRT
    9199911004 OPRT
    9199916100 OPRT
TOTAL COUNT OF UNASSIGNED DN:         2
TREATMENT:OPRT
```

A directory number that has been sent to OPRT treatment can be reused at any time by using the NEW command of SERVORD.

34.2.2 Datafill for AIS Announcement

34.2.2.1 Table CLLI

The Common Language Location Identifier (CLLI) or name for the AIS announcement must be defined in table CLLI. The value for field TRKGRSIZ must be set to specify how many individual members will exist for this announcement group.

34.2.2.2 Table ANNS

The AIS announcement must be datafilled in table ANNS with ANTYP of AIS and only one entry is permitted. Field MAXCON must be set to one (1) and field CYTIME must be set to zero (0) as the length of each individual announcement is variable and will be determined internally. Field MAXCYC

should be set to one (1) as the AIS announcement is a custom type announcement that ignores this field and is only played once.

The following figure depicts example datafill for the AIS announcement in table ANNS:

Figure 4 AIS Announcement Datafill for Table ANNS

```
TABLE: ANNS

      CLLI ANNARCH TRAFSNO   CYTIME MAXCYC                DATA
-------------------------------------------------------------------------------------
AIS_ANN   NETWK     5       0     1      AIS     1
```

34.2.2.3 Table ANNMEMS

Table ANNMEMS must be datafilled to specify all members of the AIS announcement. The HDWTYPE field must be UAS and the CARD field must be AUD. Since it is desired to provide the AIS announcement simultaneously to more than one user, additional members must be datafilled in this table. The following figure depicts example datafill for the AIS announcement in table ANNMEMS with two members defined:

Figure 5 AIS Announcement Datafill for Table ANNMEMS

```
TABLE: ANNMEMS

        ANNMEM
            HDWTYPE          CARD
                                        MEMINFO
-------------------------------------------------------------------------
    AIS_ANN    0
                UAS           AUD   1       AUD   0
    AIS_ANN    1
                UAS           AUD    1      AUD    0
```

34.2.2.4 Table ANNPHLST

Table ANNPHLST is used to create the AIS announcement from individual phrases. Two new external phrase names are introduced by this activity as valid entries for field PHSLIST. These phrase names are AISBASEDN and AISREFDN. The phrase AISBASEDN represents the digits of the subscriber's old directory number or base DN. The phrase AISREFDN represents the digits

of the subscriber's new directory number or reference DN. The following figure depicts example datafill for the AIS announcement in table ANNPHLST:

Figure 6 AIS Announcement Datafill for Table ANNPHLST

```
TABLE: ANNPHLST

        ANNPHKEY
                                        PHSLIST
-------------------------------------------------------------------------
      AIS_ANN   1
(      AUD_2014) (      AISBASEDN) (       AUD_2015) (       AISREFDN)$
```

All the phrases present in the phraselist must be assigned or recorded on the UAS. Exceptions to this are the phrases AISBASEDN and AISREFDN, which are manipulated internally to produce a phraselist composed of digits. In the above example, AUD_2014 and AUD_2015 are simple text phrases recorded by the Telco. They would be similar to the following: *AUD_2014-- "The number you have called"* and *AUD_2015-- "has been changed. The new number is"*. The result of the entire tuple in ANNPHLST would be *"The number you have called, OLDNUMBER has been changed. The new number is NEWNUMBER"*.

If multiple cycles of this announcement are desired, repeat the ANNPHLST datafill [in the above example, the tuple would be (AUD_2014) (AISBASEDN) (AUD_2015) (AISREFDN) (AUD_2014) (AISBASEDN) (AUD_2015) (AISREFDN)].

Also, if a tone or treatment is desired after the AIS announcement completes, add the phrase associated with the desired treatment to the end of the phraselist. In the above example, assuming AUD_2016 is T120 tone, a fifth phrase is added to the phraselist to provide T120 tone after the AIS announcement [(AUD_2014) (AISBASEDN) (AUD_2015) (AISREFDN) (AUD_2016)].

34.2.3 AIS Data Organization

There are three tables associated with AIS that were introduced previously via activity BV1522. These tables are also utilized by this activity, though some of the fields associated with them are not applicable to this design. These tables are presented below.

34.2.3.1 Table PAUSPATT

This table is intended to define the location of pauses during the speaking of the AIS base and reference directory numbers. This ability is required for the DRAM platform. Given that the Telefonica requirement is specific to the UAS, the functionality of this table is not relevant as the UAS has it's own pause formatting scheme. However, the key of table PAUSPATT is a required field in table AISDBS, so it is necessary to add datafill as shown in the following figure:

Figure 7 AIS Datafill for Table PAUSPATT

```
TABLE: PAUSPATT

      PAUSKEY PAUS1 PAUS2 PAUS3 PAUS4
   ------------------------------------------------------------
      UAS           NP   NP   NP   NP
```

34.2.3.2 Table ISCASSGN

This table introduces the Intercept Status Code (ISC), which is an organizational concept intended to simplify the association of an announcement and a number on intercept. [For example, a seven digit number may be routed to a different announcement than a ten digit number, so this table would have two entries (i.e. c7 and c10) and the appropriate announcements would be associated here. This key (i.e. c7, c10) would then be referenced in table AISDBS as a quick way to route to the desired announcement.] The ISC concept is not utilized by this activity. The only field of interest in this table is AISMSG, which is used to define the announcement CLLI and index. The entry for field AISMSG must correspond to a valid entry in table ANNPHLST for the desired AIS announcement.
The following figure depicts example datafill for this table:

Figure 8 AIS Datafill for Table ISCASSGN

```
TABLE: ISCASSGN

      ISCKEY          AISMSG          OVFLCHK
        TMOUTCHK
   ------------------------------------------------------------
      C7   AIS_TEST   1               NONE
          NONE
```

Fields OVFLCHK and TMOUTCHK dictate routes for overflow and time-out conditions and are not utilized in this design. The overflow condition can be addressed by adding additional members for the AIS announcement or using a T-selector in TMTCNTL to specify a routelist. The time-out condition can be addressed by adding the desired treatment to the end of the announcement in table ANNPHLST, as discussed in section 2.2.2.3 above.

34.2.3.3 Table AISDBS

The main function of table AISDBS is to allow the Telco to associate a reference DN with the base DN. This table also utilizes the key fields from tables PAUSPATT and ISCASSGN. The following figure depicts example datafill for this table:

Figure 9 AIS Datafill for Table AISDBS

```
TABLE: AISDBS

        AISKEY AISPATT ISC    YR    MT    DY LOCAL
                  REFREQ
  ------------------------------------------------------------
     9199911004     UAS  C7   2003     6     3    Y
 DN             9199915555  UAS
```

The date field can be used as a reference by the Telco to identify how long the number has been or should be on intercept treatment; However, it is not used by this feature to provide any functionality. The pause information in fields AISPATT and PAUSREF is not needed by the UAS since it does it's own audio formatting. The field ISC provides an association to the phraselist index in table ANNPHLST for the AIS announcement. Field LOCAL is not utilized by this activity and field REFREQ must be set to DN.

The index into table AISDBS is derived from the dialled digits of the originator. Any prefix digits dialled will be removed and the resulting digits will be used as the index into table AISDBS. This may result in the need to datafill multiple entries of a subscriber's old directory number in table AISDBS to address varied dialling plans of the originator (i.e. An example for the North American dialling plan might be to add a seven digit instance of the base DN for line terminations and a ten digit instance of the base DN for trunk terminations).

34.3 Hardware Requirements or Dependencies

This activity supports the AIS announcement on the UAS platform only. Therefore, AIS announcement members should not be defined on a MTM as this is not supported.

34.4 Software Requirements or Dependencies

None.

34.5 Limitations and restrictions

If the AIS announcement cannot be terminated upon during call processing (i.e. due to a problem in the UAS), the originator will be routed to GNCT treatment. If a problem is encountered providing the AIS announcement, the originator will be routed to BLDN treatment.

The index into table AISDBS is derived from the dialled digits of the originator. Any prefix digits dialled will be removed and the resulting digits will be used as the index into table AISDBS. This may result in the need to datafill multiple entries of a subscriber's old directory number in table AISDBS to address varied dialling plans of the originator (i.e. An example for the North American dialling plan might be to add a seven digit instance of the base DN for line terminations and a ten digit instance of the base DN for trunk terminations).

34.6 Interactions

For ISUP and PRI terminations into the switch providing the AIS service, the OPRT treatment must be mapped as local via table TMTMAP for the AIS announcement to be provided. If OPRT is mapped remotely, the remote office will provide whatever treatment is datafilled there for OPRT treatment.

A flash attempt will be denied from a line connected to the AIS announcement. The flash capability and operation of a trunk terminating to the AIS announcement will be dictated by the switch associated with the trunk. Also, since flashing is denied, features that require flash for activation (such as CWT) will be denied when an agent is connected to an AIS announcement.

Call forwarding from a line to a number on AIS intercept is not supported. In the case of CFU, an attempt to forward to a number on AIS intercept will result in BLDN treatment given to the originator. In the case of CFB, the originator will receive BUSY treatment. In the case of CFD, the forward will not be attempted and the originator will continue to ring the base station. Call forwarding to a number on AIS intercept via trunk will function like a trunk termination to the AIS announcement. That is, the originator will receive the AIS announcement stating the old and new numbers associated with the

forward-to number once the forwarding trigger is reached (i.e. busy condition for CFB or timer expiration for CFD).

No billing or AIS specific OM pegging is performed upon termination to the AIS announcement. The generic OMs associated with announcements are supported.

If the caller does not exit after the completion of the AIS announcement, the call will be routed to DISC (disconnect) treatment.

This feature supports the Primary and Secondary languages associated with the UAS through the assignment of the external pharseIDs LANGUAGE1 or LANGUAGE2 in table ANNPHLST. Specifying LANGUAGE1 will notify the UAS to play the announcement in it's primary language and LANGUAGE2 will notify the UAS to play the announcement in it's secondary language. The SL (Secondary Language) line option is not supported nor is the ability to specify a language directly via ANNPHLST datafill.

34.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	_Y_
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

34.8 Glossary

Term	Description
AIS	Automatic Intercept System
AUD	Audio Node
BLDN	Blank Directory Number
CEPT	Conference of European Posts and Telecommunications Administrations
CLLI	Common Language Location Identifier
CNI	Changed Number Intercept
DN	Directory Number
DRAM	Digital Recorded Announcement Machine
GNCT	General No Circuit Treatment
ISC	Intercept Status Code
OPRT	Operator Treatment
SERVORD	Service Order System
UAS	Universal Audio Server

35: Functional Description (FN): A00002702

35.1 Feature name

No Line Origination Without Charging

35.2 Description

The purpose of this activity is to provide optionality for restricting line origination of the calls which does not have appropriate charging options. Required line options to originate a call when this functionality is enabled are:

- MOG option for IBN subscribers having CEPT option.
- SMDR line option for non-CEPT IBN subscribers
- SMDR line option for P-phone subscribers
- MOG or SMDR line option for ISDN (ISDNKSET) subscribers

For the cases where the originator line does not comply the above conditions, the call is sent to treatment at origination phase.

In addition, call origination is not allowed and sent to treatment for the below condition to avoid duplicate charging if this functionality is enabled:

- MOG and SMDR line options on the same IBN or ISDNKSET subscriber

Table 1 Functional behavior during call origination when NCW_CHG is set to DISALLOWED

Line type	Has CEPT option	Has MOG option	Has SMDR option	SMDR datafill in XLA tables	Call origination	Charging method
IBN line	Y	Y	Y	N	**Not allowed**	**N/A**
IBN line	Y	Y	Y	Y	**Not allowed**	**N/A**
IBN line	Y	Y	N	N	**Allowed**	**Metering**
IBN line	Y	Y	N	Y	**Not allowed**	**N/A**
IBN line	Y	N	Y	N	**Not allowed**	**N/A**
IBN line	Y	N	Y	Y	**Not allowed**	**N/A**
IBN line	Y	N	N	N	**Not allowed**	**N/A**
IBN line	Y	N	N	Y	**Not allowed**	**N/A**
IBN line	N	N	Y	N	**Allowed**	**SMDR**

Table 1 Functional behavior during call origination when NCW_CHG is set to DISALLOWED

Line type	Has CEPT option	Has MOG option	Has SMDR option	SMDR datafill in XLA tables	Call origination	Charging method
IBN line	N	N	Y	Y	**Allowed**	**SMDR**
IBN line	N	N	N	N	**Not Allowed**	**N/A**
IBN line	N	N	N	Y	**Not Allowed**	**N/A**
IBN line	N	Y	Y	N	**Not Allowed**	**N/A**
IBN line	N	Y	Y	Y	**Not Allowed**	**N/A**
IBN line	N	Y	N	N	**Not Allowed**	**N/A**
IBN line	N	Y	N	Y	**Not Allowed**	**N/A**
P-Phone	N/A	N/A	Y	N	**Allowed**	**SMDR**
P-Phone	N/A	N/A	Y	Y	**Allowed**	**SMDR**
P-Phone	N/A	N/A	N	N	**Not allowed**	**N/A**
P-Phone	N/A	N/A	N	Y	**Not allowed**	**N/A**
BRI line	N/A	Y	Y	N	**Not allowed**	**N/A**
BRI line	N/A	Y	Y	Y	**Not allowed**	**N/A**
BRI line	N/A	Y	N	N	**Allowed**	**Metering**
BRI line	N/A	Y	N	Y	**Not allowed**	**N/A**
BRI line	N/A	N	Y	N	**Allowed**	**SMDR**
BRI line	N/A	N	Y	Y	**Allowed**	**SMDR**
BRI line	N/A	N	N	N	**Not allowed**	**N/A**
BRI line	N/A	N	N	Y	**Not allowed**	**N/A**

In addition to usage of SMDR line option, SMDR may be activated during translation by setting the SMDR field to Y at the appropriate table IBNXLA tuple.

If SMDR is activated via translation option for an originator IBN or BRI line with MOG option during the call, then the call is sent to treatment to avoid duplicate charging. For this case, the call is sent to treatment after the digits were dialed.

For all mentioned cases where the call is sent to treatment because of using illegal charging method, an MTR 158 log is generated.Treatment type is “No_software_resource” NOSR. The existing treatment in DMS100 MMP is used.

The functionality is enabled by setting the metering system parameter NCW_CHG in table MTRSYSPM to DISALLOWED. This parameter is renamed from the existing metering system parameter NCW_MOG with no change in it's existing functionality.

Note that this activity does not cover successful generation of SMDR records or increasing of meter counts at the end of the call for the allowed calls.

35.2.1 Changes in MTR 158 log format

For supporting the additional SMDR and MOG &SMDR interaction restrictions, existing MTR158 log text is enhanced. Also called DR field is added to log data text for SMDR activation from translation cases. For other log creation cases, there's no dialed digits since the call is sent to treatment during origination.

The new log output is given in Figure 1.

Figure 1 Sample log report for MTR 158 log

```
RSNW4E07 MTR158 JUN12 15:17:50 9600 INFO INVALID CHARGING METHOD

    HOST 02 0 00 06    DN 1027835476
    CALLED DR 0
    CALL RESULT: TRMT- No MOG option
```

Other possible call result texts printed within the log are:

- TRMT-MOG & SMDR on line
- TRMT- No MOG or SMDR on line
- TRMT- MOG option on a line without CEPT
- TRMT-SMDR activation during XLA

Table 2 Possible call result texts in MTR 158 log

Reason	CALL RESULT:
No MOG option on a line with CEPT	TRMT- No MOG option
No SMDR or MOG option on a line without CEPT option	TRMT- No MOG or SMDR on line
MOG option on a line without CEPT	TRMT- MOG option on a line without CEPT
SMDR and MOG options both exists on the line	TRMT- MOG & SMDR on line

Table 2 Possible call result texts in MTR 158 log

Reason	CALL RESULT:
SMDR activated during translation for a line with MOG option	TRMT-SMDR activation during XLA

35.2.2 Renaming of metering system parameter NCW_MOG to NCW_CHG

Existing metering system parameter NCW_MOG defined in table MTRSYSPM is renamed to NCW_CHG within this activity.

NCW_CHG has the same activation/ deactivation, ONP behavior with the old NCW_MOG parameter. For the upgrades to ISN07 from older releases, the value of the NCW_MOG parameter value will be transferred to NCW_CHG.

35.2.3 Complex call interactions for the feature

Complex call interactions of this functionality is as below:

- For call forwarding scenarios, call diversion to another agent will not be allowed if diverting agent has no charging option.
- For conference calls (3WC, 6WC), when this feature is active, a call will not be originated after flash/add on leg of the complex call members without charging option. Agent will not get special dial tone after flash/ add on leg and an MTR 158 log is generated.
- During enquiry call setup, flashing/ add on leg of an agent without charging option in the enquiry call is not allowed. The flash/ addon leg is ignored and the agent will not get special dial tone, also an MTR 158 log is generated.
- An IBN line with call waiting option and without charging option can get the call waiting tone during a call and use the feature.(Mentioned line is included in the first call as terminator).The restriction introduced for this case with the prior activity, ‘No Line Origination Call Without Line Metering Option’ (ACT.A59033820) is removed.

35.2.4 SMDR Restrictions when NCW_CHG is set to DISALLOWED

In case an agent with SMDR option in IDLE state is involved in an active complex call (call diversion, call transfer) and an SMDR record generation for this agent is expected for that call, following operations are restricted:

- Usage of OUT, CLN, CDN, DEL SERVORD commands on the agent
- Removing of SMDR option from the agent via DEO SERVORD command or via table control operations.
- Removing of the agent from IBNLINES/KSETLINE tables via table control operations.

- Adding SUS, DOR, RESL options to the agent via SERVORD and table control operations.

Note that these restrictions are applicable if NCW_CHG parameter in table MTRSYSPM is set to DISALLOWED.

35.2.5 MOG option restrictions when NCW_CHG is set to DISALLOWED

If a line with MOG option has active call forwarding or is not idle, then below operations are restricted:

- Addition of DOR SUS RESL options to the line via SERVORD.
- Deleting of MOG option from the line via servord or via table control operations.
- Removing the line with OUT command or via table control operations.

Note that these restrictions are applicable if NCW_CHG parameter in table MTRSYSPM is set to DISALLOWED.

35.2.6 ICMOG option restriction on IC PRI trunks when NTOW_CHG is set to DISALLOWED

If an incoming (IC) PRI trunk has no ICMOG datafill in table TRKOPTS then call origination from this trunk is restricted.

In case of restriction, new MTR log MTR163 is generated for the IC PRI trunk and the call is sent to “No_software_resource” NOSR treatment.

This restriction is applicable to ETSI PRI trunks if NTOW_CHG value in table MTRSYSPM is set to DISALLOWED.

The details for the new MTR 163 and MTRSYSPM parameter NTOW_CHG are given in Fault management and Configuration sections.

35.3 Hardware Requirements or Dependencies

None

35.4 Software Requirements or Dependencies

None

35.5 Limitations and restrictions

- This feature is not activated if ENABLE_METERING office parm in table OFCENG is set to N
- This function is available only for line origination types which are IBN, ISDNKSET or P-phone.

- For MLH and DLH hunt groups, call origination is not allowed for members that have SMDR option if the pilot DN has MOG option assigned.
- No trunk origination without charging functionality activated by MTRSYSPM NTOW_CHG parameter is only available for ETSI PRI trunks.

35.6 Interactions

This feature is the enhancement of the existing ISN04 activity 'No Line Origination Call Without Line Metering Option' (ACT.A59033820). Except for the points stated in this document, 'No Line Origination Without Charging' feature provides the same functionality with the mentioned A59033820 feature.

QLT command for a MLH or DLH hunt group member BRI line does not display the MOG option assigned to the huntgroup pilot. This is a general behavior for QLT and pilot DN of the huntgroup should be checked for detecting MOG option existence on the hunt group.

35.7 Applicable customer facing sections

Fault Management

Logs	___X___
Alarms	___N/A___

Configuration

Data Schema	___X___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	__N/A____

35.8 Glossary

Term	Description
ONP	One Night Process
MOG	Meter Origination Group
ISDNKSET	Class of agents for BRI line type
IBN	Integrated Business Network
NCW_MOG	No call without MOG
NCW_CHG	No call without charging
ICR	International Call Recording
P-phone	Proprietary Phone
CENTREX	Centralized Exchange
CEPT	Conference of European Postal and Telecommunications
SMDR	Station Message Detail Recording

36: Functional Description (FN): A00002713

36.1 Feature name

Spanish ISUP enhancements for Telefonica

36.2 Description

36.2.1 Overview

This feature extends the capabilities of the CS2000 Spanish ISUP V2 (PUSI 4/2) trunk interface to support additional capabilities used within the Telefonica Espania (TESA) network.

The existing CS2000 Spanish ISUP V2 (PUSI 4/2) interface is compliant to Telefonica specifications EG.S3.003 4th ed. + appendices 1 and 2 with some minor limitations. It satisfies Spanish national network interconnect requirements.

This feature enhances the Spanish ISUP V2 (PUSI 4/2) interface to provide optional support for additional capabilities used within the Telefonica Espania (TESA) network, and specified in Telefonica specification Gt.EG.s3.403 sections 5 & 6.

The main additional capabilities introduced by this feature are:

- A TESA defined “Call Stamp” in the IAM of all calls- comprising a Call Reference parameter to uniquely identify the call within the network.
- Support of Charge (#TAR) message enhanced at the call originating node.
- Number Portability support is enhanced to support use of Query on Release mode Local Network Portability within the Telefonica network.
- Transit Network Selection support.
- Barring of Reverse Charge Calls to certain (non-billable) lines.

Each capability will be individually controlled by datafill options and will only be supported on Spanish ISUP V2 trunks. Spanish ISUP V2 trunks are configured by the following set of field values in table TRKSGRP.

- Exernal Protocol = ‘**Q767**’

  ITU/ETSI ISUP variants in the CS2000 ISN load.

- Version=‘**100_WHITE**’

  indicates that the variant is based on ITU White Book/ETSI ISUP V2 and

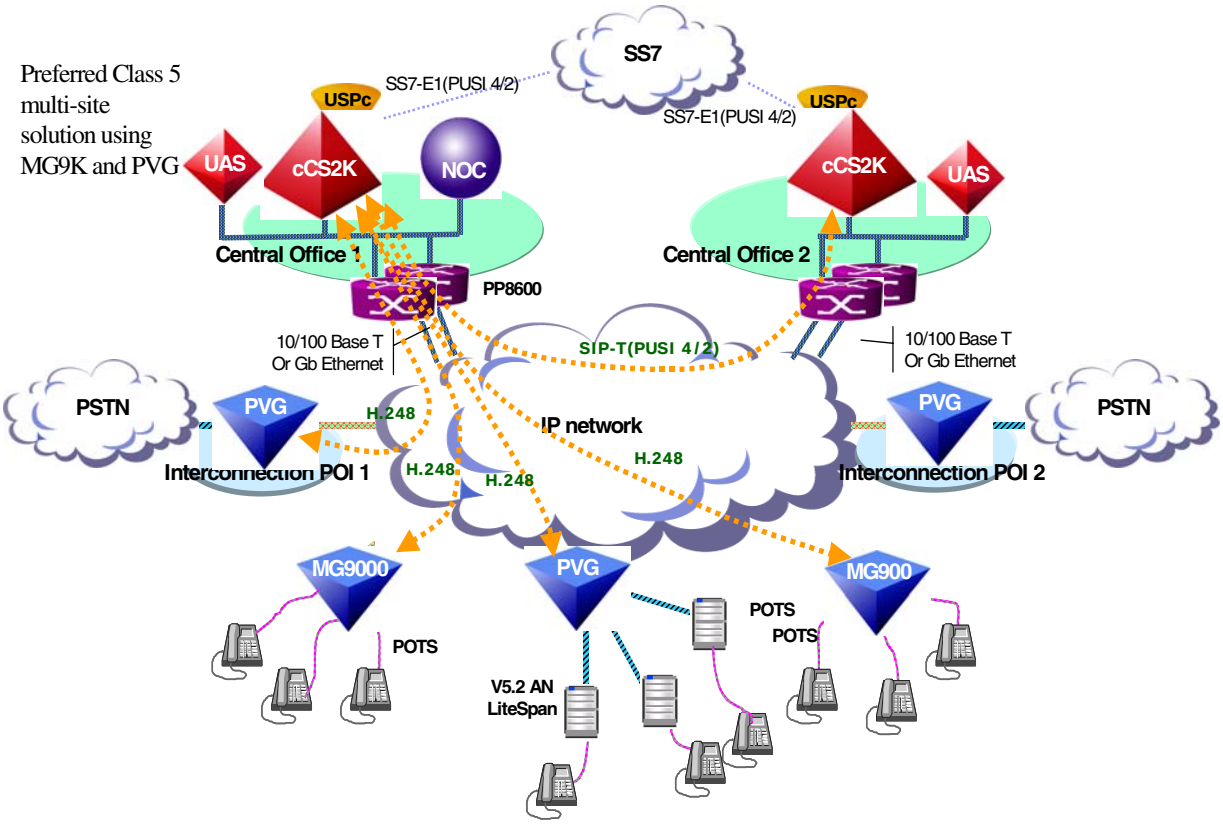
- Variant='**SPAIN**'

  marks the country specific variant as Spain

eg:
2W N N UNEQ NONE **Q767** THRL 0 DMSNODE N N **SPAIN 100_WHITE** $ ETSI CIC

Unless stated otherwise in the body of this document support for the features described in this document is limited to the scenario of PUSI 4/2 trunks interworking to Analog Lines - hosted on an MG9000 Gateway or connected via a PVG V5.2 Gateway as shown in Figure 1.

Figure 1 Supported configuration



36.2.2 Telefonica defined PUSI requirements common to all Operating Companies as defined in GT.EG.S3.403 Section 5

This section describes the CS2000 implementation of Telefonica defined ISUP capabilities that are intended to be common across all Telefonica networks in all countries. These are specified in GT.EG.S3.403 Section 5.

36.2.2.1 BACKWARD COMPATIBILITY (GT.EG.S3.403 Section 5.1)

The CS2000 implementation of PUSI 4/2 fully complies to this requirement for compatibility with the previous and future versions of PUSI, by compliance to Point 2.4. of Rec. Q.761 of the White Book.

36.2.2.2 TIMERS (GT.EG.S3.403 Section 5.2)

The PUSI timer values agreed upon for all the Grupo Telefónica, are contained in the following table. The column on the left contains the timers; the 2nd column shows the values (0 range of values) allocated in Rec. Q.764 of the White Book ITU-T. The values that have been agreed upon by the Grupo Telefónica, can be seen in the 3rd column and the range configurable on the CS2000 in the 4th column..

Timers which are configurable on CS2000 are generally datafilled in table C7UPTMR. One or more tuples should be created in table C7UPTMR with the values required by the Telefonica network and associated to PUSI trunkgroups.

Table 1 PUSI Timer Value

Timer	Q.764 range	EG.S3.403 requirement	CS2000 range in C7UPTMR
T1	15 - 60 s	30 s	1 to 60
T2	3 m	3 m	1 to 240
T3	2 m	2 m	N/A
T4[a]	5 - 15 m	10 m	1 to 326s
T5	5 - 15 m	10 m	1 to 900s
T6	Q.118	60 s	1 to 240s
T7	20 - 30 s	20 s	1 to 60s
T8	10 - 15 s	15 s	1 to 60s
T9	Q.118	60 s	1 to 300s
T10	4 - 6 s	6 s	1 to 30s
T11	15 - 20 s	15 s	1 to 60s
T12	15 - 60 s	30 s	1 to 60s
T13	5 - 15 m	10 m	1 to 900s
T14	15 - 60 s	30 s	1 to 60s
T15	5 - 15 m	10 m	1 to 900s

Table 1 PUSI Timer Value

Timer	Q.764 range	EG.S3.403 requirement	CS2000 range in C7UPTMR
T16	15 - 60 s	30 s	1 to 60s
T17	5 - 15 m	10 m	1 to 900s
T18	15 - 60 s	30 s	1 to 60s
T19	5 - 15 m	10 m	1 to 900s
T20	15 - 60 s	30 s	1 to 60s
T21	5 - 15 m	10 m	1 to 900s
T22	15 - 60 s	30 s	1 to 60s
T23	5 - 15 m	10 m	1 to 900s
T24	< 2 s	1.5 s	100 to 2000ms
T25	1 - 10 s	10 s	1 to 30s
T26	1 - 3 m	2 m	1 to 240s
T27	4 m	4 m	1 to 300s
T28	10 s	10 s	1 to 30s
T29	300 - 600 ms	500 ms	
T30	5 - 10 s	8 s	
T31	> 6 m	(*)	
T32	3 - 5 s	(*)	
T33	12 - 15 s	15 s	
T34	2 - 4 s	2 s	
T35	15 - 20 s	15 s	
T36	10 - 15 s	15 s	
T37	2 - 4 s	(*)	
T38	Q.118	(*)	
T39	Q.730	(*)	
NortelT35 = initial interdigit timer	-	-	1 to 60
NortelT37 = subsequent interdigit timer	-	-	1 to 30

a. Not required by Telefonica ISUP - Call Modification not supported

36.2.2.2.1 Call Stamp (GT.EG.S3.403 Section 5.3.1)

Overview

The aim is to identify all the calls that enter the network in an unequivocal way, whether this be at the originating local exchange or the frontier exchange with other operators (national or international). There are basically two applications: to be able to use this information when providing services (whether they be on the Intelligent Network or not), and to be able to relate the various records, for rating, statistics, or of another kind, that can be carried out at different nodes on the network.

This service is supported by the CS2000 for calls originating from and Terminating to Lines on the CS2000.

Encoding

"Call reference" and "Generic Digits" are the two parameters that carry this information.

- "Call reference":

  The "call reference" parameter is as specified in Q.763 [3]. The increasing send interpretation will be applied in both fields of this parameter, that is, the least significant bit in the "call identity" field, is bit 1 of octet 1, and the most significant one is bit 8 of octet 3, whereas bit 1 of octet 4 is the least significant one in the "point code" field and bit 6 of octet 5 is the most significant one.

"Generic Digits" - Generic digits implementation is backed out as it is not required by Telefonica.

Procedure

The procedure to be followed at the originating exchanges, will be the same for local exchanges and for frontier exchanges. The originating exchange will carry out the following actions, whether the call is generated from the network itself, or whether it comes from another network:

It will generate the "call reference". It will make a note of all the parameters in the respective register: the rating register at the local exchanges and the accountancy register at the frontier exchanges.

It will include call reference in the PUSI initial address message

The pure transit exchanges that do not have to make any note, will pass this parameter without making any modification at all.

Note: CS2000 does not support this SSP related functionality at present.

The destination exchanges, will discard and will carry on as if they had not received them, if they do not have any specific procedure enabled.

The network outlet exchanges will make a note of this information in the accountancy registers, and will remove the parameters, unless they have a specific agreement with the next network.

CS2000 Datafill Control of Call Stamp

a) Call Reference Parameter:

This feature meets the Telefonica requirements for the Call Reference parameter for calls originating and terminating to analog lines on the CS2000 and entering or leaving the Telefonica network on Spanish ISUP V1 & V2 or Base ETSI ISUP V2 trunks.

It extends the generic ETSI ISUP Call Reference capability implemented by A59023264.

Calls that enter the Telefonica Spanish ISUP V2 network on Spanish ISUP V1 or V2 or ETSI ISUP V2 will be handled as described in feature A59023264.

To control generation of the Call Reference parameter in the IAM for calls from Lines to Spanish ISUP V2 trunks a new service “CALLREF” is introduced to table ISUPSVC. The CALLREF service will have a vector of options to control which scenarios the trunks should add a Call Reference parameter for. In this release only one option value will be available

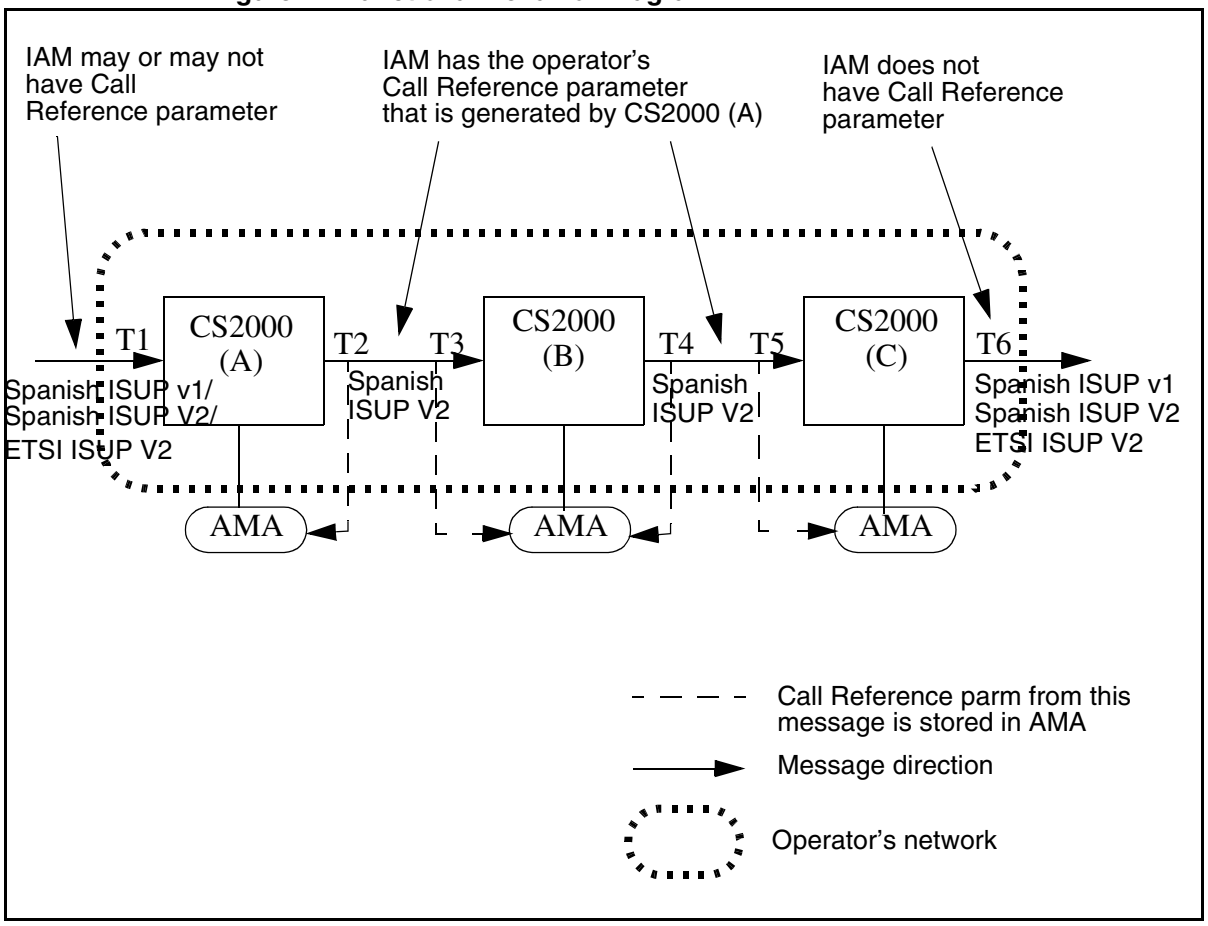
— “LINE” - to indicate that the call reference parameter is required to be generated for Line originated calls.

CALLREF LINE

This option will only take effect on trunkgroups that also have the TRKOPTS option CALLREF datafilled with no suboptions.

The Call Reference paramater may be optionally captured in the AMA billing record as described in A59023264. This capability is extended to the Line origination and termination scenario by the CALLREF LINE option. This option needs to be datafilled for generating AMA records for Call reference in line origination and termination scenario.

Figure 1 Functional Behavior Diagram



:

Table 1 Setting of TRKOPTS and ISUPSVC options for Telefonica network to generate Call Reference for all Line originations

Trunk	TRKOPT CALLREF Datafill	ISUPSVC CALLREF Datafill
Internal trunks within Telefonica network - T2, T3, T4, and T5	`CALLREF $`	CALLREF LINE
T1 and T6 if two-way trunks	`CALLREF (ADD_OVERWRITE )(DELETE ) $`	dont care
T1 if it is a one-way incoming trunk	`CALLREF (ADD_OVERWRITE ) $`	dont care
T6 if it is a one-way outgoing trunk	`CALLREF (DELETE ) $`	dont care

Refer to A59023264 for full details of the Call Reference support on CS2000.

SAMPLE DATAFILL FOR CALLSTAMP

1 . CALLREFERENCE PARAMETER

TABLE: TRKSGRP

ETSIV2IC 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMSETSI N Y **SPAIN 100_WHITE** $ ETSI2W CIC

ETSIV2OG 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMSETSI N Y **SPAIN 100_WHITE** $ ETSI2W CIC

ETSIV2OG and ETSIV2IC ,the outgoing and incoming trunks are configured as Spain variants .

TABLE ISUPSVC:

EIV2_SPAIN (SPAIN $) (CALLREF LINE $)

Define a key " EIV2_SPAIN" in ISUPSVC with option SPAIN .This will be used to configure a trunk as a telefonica trunk when used in table TRKOPTS .Also add option CALLREF with suboption LINE.This option controls the CALL REFERENCE parameter generation for calls originated from line to TELEFONICA trunk.This option also controls AMA billing record generation

for line origination and termination within telefonica network along with the existing option “STORE_CALLREF” in table AMAOPTS.

TABLE TRKOPTS

ETSIV2OG ISUPSVC ISUPSVC EIV2_SPAIN

TABLE AMAOPTS

STORE_CALLREF ON

Call Reference parameter is captured in AMA record in module code .

e.g “calldump full “ command after the call, check for

MODULE CODE: 611C GENERIC MOD: ONE DGT STR FMT

GENERIC CONTEXT ID:

PARSE RULES 80035 CALL REFERENCE

SIGNIFICANT DIGITS 00C NIL

GENERIC DIGIT STRING ONE:

CALL ID 590029

POINT CODE 0FA3

SPARE 00000C

The non full version (i.e. Just “calldump” command on CI) look for

Subrecord data:

MODULE_CODE_ID 611C

GENERIC_CONTEXT_ID 8003500C

GENERIC_DIGIT_STRING DF007F958000000C

To control Call Reference for transit scenaio follow the TRKOPTS datafill as mentioned in table 1 in page 161.An example is shown below, note that this is not the complete datafill in table TRKOPTS for call reference, derive the

datafill required from the above mentioned table or refer to feature A59023264 in fmdoc for the exhaustive list.

TABLE TRKOPTS

ETSIV2IC CALLREF CALLREF ADD_OVERWRITE

36.2.2.2.2 Services in IN (GT.EG.S3.403 Section 5.3.2

The CS2000 does not support this service. If the generic digits parameters related to this service are received by CS2000 they will be handled according to their corresponding PCI instructions.

The generic digits parameters related to this service are encoded:

"correlationID" would be as follows: the "encoding scheme" must be 011 (binary) and code 11100 (correlationID) would be used as "type of digits".

"SCFID" would be as follows: the "encoding scheme" must be 011 (binary) and code 11011 (SCFID) would be used as "type of digits". The digits" field would be encoded as the parameter "call party address" of the SCCP.

36.2.2.2.3 Authorisation and account codes (GT.EG.S3.403 Section 5.3.3)

The CS2000 does not support this service. If the generic digits parameters related to this service are received by CS2000 they will be handled according to their corresponding PCI instructions.

The generic digits parameters related to this service are encoded as follows:

The encoding details depend on the specific application. For example, if the local originating exchange receives these codes and cryptographs, which increases the safety of these procedures, then the "encoding scheme" must be 011 (binary encoded). The relevant code would be used as "type of digits", 00000 for the account code or 00001 for the authorisation code.

This service may be implemented on CS2000 by inband transmission over ISUP trunks of the Authorisation and account codes as DTMF digits.

36.2.2.2.4 Corporate networks (GT.EG.S3.403 Section 5.3.4)

The CS2000 does not support this service. It will not generate the format of generic digits parameter used by this service. If the generic digits parameter related to this service are received by CS2000 they will be handled according to their corresponding PCI instructions.

The generic digits parameters related to this service are encoded as follows:

The "encoding scheme" must be 011 (binary), and code 00011 (company communications) would be used as "type of digits". The corporate network code in "digits" would go in 2 octets (65536 possibilities).

36.2.2.3 PARAMETERS CONFIGURABLE BY ROUTE (GT.EG.S3.403 Section 5.3.4)

Telefonica requires that frontier exchanges must be able to restrict sending certain parameters out of the network on the basis of the incoming or outgoing route of the call. These parameters will only go to those other routes with which an agreement exists to that effect.

The list of parameters that have to be able to be configurable by route, is defined below.

- Calling number
- Connected number
- Generic number
- Generic digits
- User-to-user information

CS2000 supports this requirement for parameters in the IAM by use of existing table ISPARM. This table allows the network operator to specify one or more parameter(s) to be blocked/removed from an outgoing IAM on a set of trunkgroups that are associated to a particular entry in table ISPARM. Any optional parameter can be removed using this table. Refer to feature A59028040.[10]

Certain parameters in the IAM and other messages may also be blocked by specific datafill that controls the use of messages and parameters on a per service basis.eg: Controls for the User-to-user Service and Call Reference capability.

36.2.3 NETWORK SPECIFIC REQUIREMENTS (GT.EG.S3.403 Section 6)

36.2.3.1 (GT.EG.S3.403 Section 6.1) CTC REQUIREMENTS

Not Applicable

36.2.3.2 (GT.EG.S3.403 Section 6.2)TASA REQUIREMENTS

Not Applicable

36.2.3.3 (GT.EG.S3.403 Section 6.3) TDP + TESA REQUIREMENTS

The following subsections follow the **GT.EG.S3.403 Section** numbering

36.2.3.3.1 (GT.EG.S3.403 Section 6.3.1) Caller categories (TDP requirement)

Not Applicable

36.2.3.3.2 (GT.EG.S3.403 Section 6.3.2) Malicious call. (TESA requirement)

If the destination local exchange does not have the complete calling number. It will make use of the information request procedure to request it. Q.764 xxx2.1.6

The bits for the parameter "information request indicators" that are encoded to 1, are as follows: / "a calling party request indicator") and H ("malicious call identification request indicator"). The rest will go to 0.

36.2.3.4 (GT.EG.S3.403 Section 6.3.3) Rating (TESA requirement)

The following subsections follow the **GT.EG.S3.403 Section** numbering

6.3.3.1General

Telefónica de España requires the following rating procedure, which makes use of the rating information message #TAR and a parameter referred to as &TFA.

Table 2

Rating information message (#TAR) (national use)			
Parameter	Type	Length	

Table 2

Rating information message (#TAR) (national use)			
Type of message	F	1	
&TFA	F	5	

6.3.3.2Encoding.

The rating information message (#TAR) has only two parameters, both compulsory and of fixed length: message type and rate.

The code 1111 1000 has been allocated to the rate parameter (&TFA), but it is never used, given that it is only used in the message #TAR, where it is compulsory. It occupies 5 octets and is compulsory in the message #TAR. The least significant bit in octet 1, indicates whether octets 2 and 3, which contain rating information, are relevant or not; the following less significant bit, indicates whether octets 4 and 5, which contain charging information, are relevant or not; the rest of the bits in the octet are reserved. Octets 2 and 3, indicate the type of rate. Octets 4 and 5 indicate a number of monetary units to charge to the call.

The name and code of the parameter used, is indicated in the following table.

Table 3

ACRONYM	NAME	REF	CODE	notes
&TFA	Rate		1111 1000	@

@ = national use parameter.

The format ¬TFA can be seen in the figure:

ReserveInPInT

Type of rate

Monetary units

The fields for this parameter are as follows:

InT (rate indicator): indicates whether the rating information (the type of rate) included in the parameter is relevant or not.

0: the rating information (octets 2 and 3) is not relevant

1: the rating information (octets 2 and 3) is relevant

InP (call price indicator): indicates whether the charging information (the monetary units) included in the parameter is relevant or not.

0: the charging information (octets 4 and 5) is not relevant

1: the charging information (octets 4 and 5) is relevant

The type of rate: a code that expresses the number for the type of rate that is to be applied (0-65535) in pure binary form (the most significant bit is 8 from octet 3, and the least significant bit is 1 from octet 2).

d) Monetary units: a code that indicates the number of units to be added to the call, expressed in pure binary form (the most significant bit is 8 from octet 5, and the least significant bit is 1 from octet 4).

6.3.3.3Procedure.

The rating procedure that determines the use of the rating message #TAR, together with the use of the various rating indicators (such as those that appear in the "backward call indicators"), is explained in the rating Specification that is in force. The procedures that are followed by default, are explained below.

Criterion for determining whether a call is subject to a rate being applied: all calls will be rated except in the following circumstances:

- If the rate to be applied is zero
- If the final value received for the "backward call indicators" in the "charge indicator", is "no charge" (01), and none of the values received beforehand, if any had been received beforehand, came with the "charge" (10) meaning.

Call rate determination criterion: the originating local exchange will determine the rate to be applied to the call. If a #TAR is received with relevant rating information prior to the address complete message (#MDC) (or the connection message, #COX), then it will apply that rate, and not the one calculated previously. Furthermore, of a #TAR is received at any time, with relevant charging information, it will add to the caller's meter, the value concerned to the price of the call indicated in the message.

The CS2000 will not generate the TAR message in this release.

In transit, the #TAR message will pass without any modifications at all.

In an originating office, no action is taken upon receiving the Charge message and it is ignored .

36.2.3.5 (GT.EG.S3.403 Section 6.3.4) Number Portability (TESA requirement)

This requirement is replaced by that in Addendum A.

This activity implements Numbering Portability by the method of Query on release.Number Portability by IN is covered by a separate activity A00002678

LNP QoR functionality is enabled by existing options in table ISUPSVC which was implemented by feature A59027497.

Additionally , a release cause indicator #126 is supported on spanish trunks for ported numbers.This is controlled by an option in table ISUPSVC in SPAIN service , “NATL_LNP_QOR”.This is a symbolic option , if this option is datafilled along with LNP service datafill, then a cause value of #126 will be sent for ported numbers otherwise the default cause value 14 will be sent on ported number.

Additionally, accepting NOA value #126 is supported on Spanish ISUP variant having SPAIN service datafilled in table ISUPSVC.

SAMPLE DATAFILL for LNP QoR

Datafills as mentioned in Activity A59027497 is required in addition to the following datafills.

TABLE: TRKSGRP

ETSIV2IC 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMSETSI N Y **SPAIN 100_WHITE** $ ETSI2W CIC

TABLE: ISUPSVC

EIV2_SPAIN (SPAIN NATL_LNP_QOR $)

TABLE: TRKOPTS

ETSIV2IC ISUPSVC ISUPSVC EIV2_SPAIN

36.2.3.6 (GT.EG.S3.403 Section 6.3.6) Selection of the Transit Network (TESA requirement)

This requirement is amended by that in Addendum A.

It is necessary to prepare the network to allow the user to select the transit network that each call should use. The issue that concerns the PUSI is how to transport this information and - keeping in mind that in Spain we will soon have other basic telephony service local operators besides Telefónica - indicate to the transit network if the call is offered by subscriber / user selection or through the choice of the operator that provides the access.

It is necessary to note that the existence of several local operators and several transit networks in a same country requires an agreed national network signaling (PUSI) that must be used between frontier exchanges of different networks.

The future anticipates the possibility of selecting a transit network by pre-assignment for all calls of a certain type; in this case, when a user uses the generic dialing (without explicit selection), the calls will be offered to the pre-assigned transit network. Otherwise, the local operator will choose the transit network to which to offer the call.

Whenever the call is offered to a transit network, it must be informed that this call has been offered by user selection (explicit selection or pre-subscription); keeping in mind the existence of local operators other than Telefónica, there will be calls established between subscribers of different local operators that, even without selecting the transit network, must cross the frontier exchanges of these operators and must be discriminated from the former for statistical and accounting purposes.

The origin local exchange will include the Transit Network Selection parameter in the Initial Address Message. This parameter will also be included in the Initial Address Message when the transit network selection is carried out by pre-assignment. This parameter will contain the digits that identify the selected transit network. The transit exchanges will analyze the content of the Transit Network Selection parameter received in the Initial Address Message to route the call to the frontier exchange with the Operator selected by the user.In the frontier exchanges, the initial address messages that do not contain the Transit Network Selection parameter will correspond to calls that do not require the transit network selection.

The following strategy will be used to introduce this parameter:

The update process will take some time during which the prefixes method will be used. In other words, the CSO (Operator Selection Code) will be used as prefix in the Called Party Number parameter. First, the transit network will be updated so that it supports the Transit Network Selection parameter; then, the entire access network will be updated, and when all the network exchanges support the Transit Network Selection parameter (even if they are not using it), it will be necessary to determine a point in time in which to carry out the change.The exchanges will have both logics implemented (prefix and use of

the Transit Network Selection parameter), and at the time determined, the change will be made from one logic to another. At this time, the exchanges will begin to send the Transit Network Selection parameter, as well as the Called Party Number parameter without the prefix. The Transit Network will already be prepared to handle it.

The coding of the transit network selection parameter will be made according to Recommendation Q.763, as shown in the figure:

Even /odd Type of network identifier Network identification plan.Network identifier

a) Odd / even indicator: 0 = even number of digits. 1 = odd number of digits.

a) Odd / even indicator: 0 = even number of digits. 1 = odd number of digits.

b) Type of network identifier: 010 = national code.

c) Network identification plan: 0000 = default value.

d) Network identifier: BCD coding of the digits that identify the selected transit network.

The possible user dialing that will allow the transit network selection for each call will of the type indicated next:

05Y

1050 1070T1T2 (Six figures)

1051 1071

1052 1072

1053 1073

1054 1074

1055 1075

1056 1076

1057 1077

1058T1 (Five figures) 1078T1 (Five figures)

1059T1 (Five figures) 1079T1 (Five figures)

CS200 Implementation

TNS implemented by activity A59017057 will be reused for this feature.

This feature ensures CDPN format requirements for telefonica can be selected due to Spanish ISUP variant and existing Carrier Selection/Preselection datafill. Note that TNS parameter is not supported by this activity.

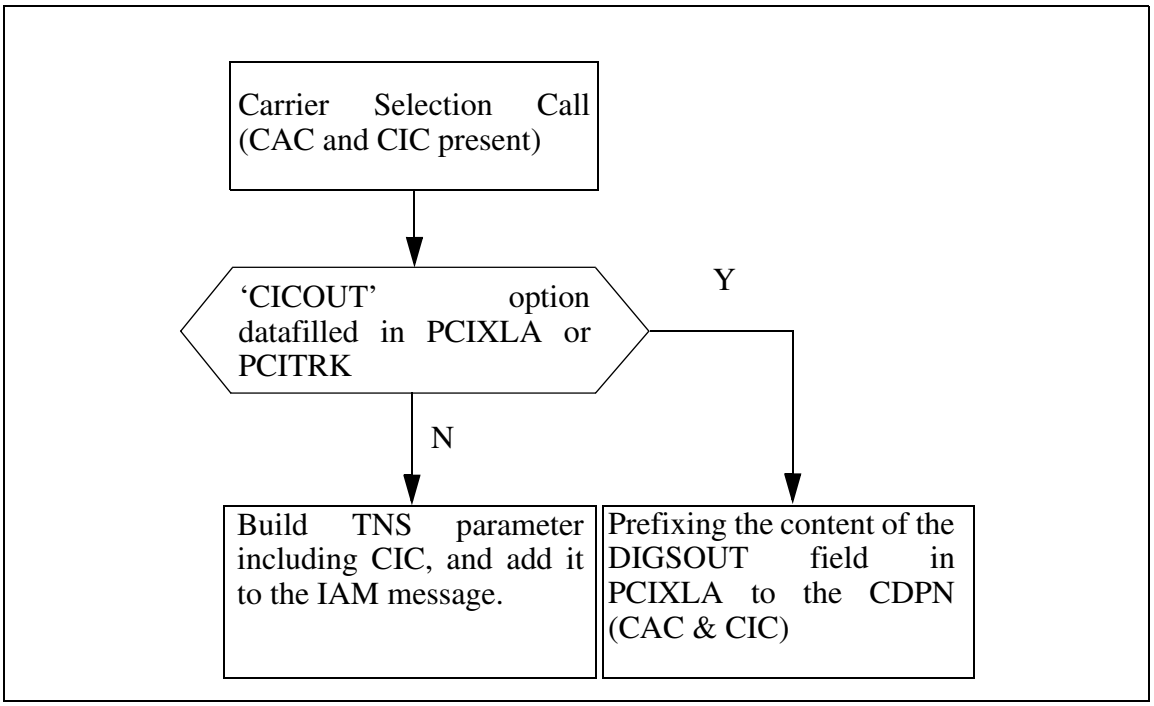
The carrier selection related information can be sent out either in the Transit Network Selection (TNS) parameter or to the called party number (CDPN) parameter.This is controlled by an option in on the outgoing trunk group or the route.

The Carrier Selection related information, the Carrier Access Code (CAC) and the Carrier Identification Code (CIC) can either be transported in the Transit Network Selection Parameter (TNS) or the Called Party Number plus (CDPN+). The Called Party Number plus consists of a prefix (‘10xx’, ‘10’ = CAC and ‘xx’ = CIC) and the regular Called Party Number.

The decision which parameter will be used will be done by the CICOUT option in table PCIXLA or PCITRK. This option was implemented under “[2] A59012694.AA, Carrier Preselection and charge category based routing.” This implementation adds the content of the field DIGSOUT in table PCIXLA as a prefix to the Called Party Number. Therefore this field has to be datafilled with the CAC and CIC information (e.g. ‘10xx’).

In case the CICOUT option is not present in tables PCIXLA or PCITRK, the CIC information will be sent in the Transit Network Selection parameter (TNS). The mechanism for routing according to this information is covered in “[1] A19008748.AA, Austrian ISUP - TNS parameter invoked routing and CLI screening.”

Decision either TNS or CDPN+ is used to transport CS information



36.2.3.7 (GT.EG.S3.403 Section 6.3.7) Vacant Lines (TESA requirements)

CS2000 does not support this requirement. It is not possible to initiate a call from a vacant line on CS2000.

36.2.3.8 (GT.EG.S3.403 Section 6.3.8) Compatibility Information (TESA requirement)

CS2000 is compliant to the following requirements, with no datafill control required.

6.3.8.1Minimum value of message

This edition does not use any message defined by Telefónica de España.

6.3.8.2Minimum value of a parameter

The minimum value of the compatibility information value for a parameter, is the following encoding: "transit interpretation", "do not release call", "do not send notification", "do not discard message (pass it on)" and in the "pass indicator not possible" field, "discard parameter".

This is the one that will be used by default in the parameters defined by Telefónica de España.

36.2.3.9 (GT.EG.S3.403 Section 6.3.9) Reverse charge tagging (TESA requirement)

With respect to reverse charge calls through the operator, it is possible that the person who picks up the telephone and informs the operator that he or she is willing to pay for the call, will not necessarily be the person who eventually does pay for it. As a result, frauds could take place in public places, such as hospitals and hotels, which are provided with direct dialling from extensions.

If this situation is to be prevented, it is necessary to tag the reverse charge calls. With a view to this, bit N from the parameter "forward call indicators" will be used to mean "indicated: reverse charge call", and will be encoded in the following way: if N = 0: ordinary call, if N = 1: reverse charge call. Certain exchanges will generate it, it will pass transparently through transit, and the relevant procedure will be applied at the destination (it will be ignored by default). The frontier exchanges will either set it at 0 or let it pass through transparently, depending on the route.

Note : Cs2k does not set Bit N to 0 or 1 i.e. the frontier exchange capability is not supported.The functionality supported by this activity is just as described in the following paragraph..

Reverse charge tagged calls indicated by the N bit set to 1 in “forward call indicators” will not be allowed to terminate on a line with ACCB (Automatic collect call blocking) option enabled.This will be controlled by an option **REV_CHG** in table ISUPSVC on the incoming trunk.Calls will be checked for reverse charge(bit N) only if this option is datafilled on the incoming spanish ISUP trunk.

SAMPLE DATAFILL

TABLE: TRKSGRP

ETSIV2IC 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMSETSI N Y **SPAIN 100_WHITE** $ ETSI2W CIC

TABLE: ISUPSVC

EIV2_SPAIN (SPAIN REV_CHG $)

TABLE: TRKOPTS

ETSIV2IC ISUPSVC ISUPSVC EIV2_SPAIN

36.3 Accounting

36.4 Hardware Requirements or Dependencies

None

36.5 Software Requirements or Dependencies

This feature is an increment to the Spanish ISUP V2 functionality in NSUP0001. Feature reference 59027768: SPANISH ISUP - V2 VARIANT'

36.6 Limitations and restrictions

36.6.1 Agent Interworking

This capabilities introduced by this feature are only supported for the agent interworkings given below. The feature should not be activated on Spanish ISUP v2 trunks that will have any other interworkings as the behavior in other scenarios is undefined.

Figure 2 Agent interworking for the current feature

Platform	Originator	Terminating agents			
CS2K		IBN lines (POTS)	V5.2 IBN (POTS)	PUSI 4/2 (Spanish ISUP V2)	SIP-T(Spanish ISUP V2)
	IBN (POTS)			X	X
	V5.2 IBN (POTS)			X	X
	PUSI 4/2 (Spanish ISUP V2)	X	X	X	X
	SIP-T(Spanish ISUP V2)	X	X	X	X

36.7 Interactions

The current activity interacts with the features listed below and their dependencies to support Line HW Metering and Software Metering and Billing when the charge determination point for the call is not the originating office and the call tariff and/or incremental charges are signalled across the ISUP network:

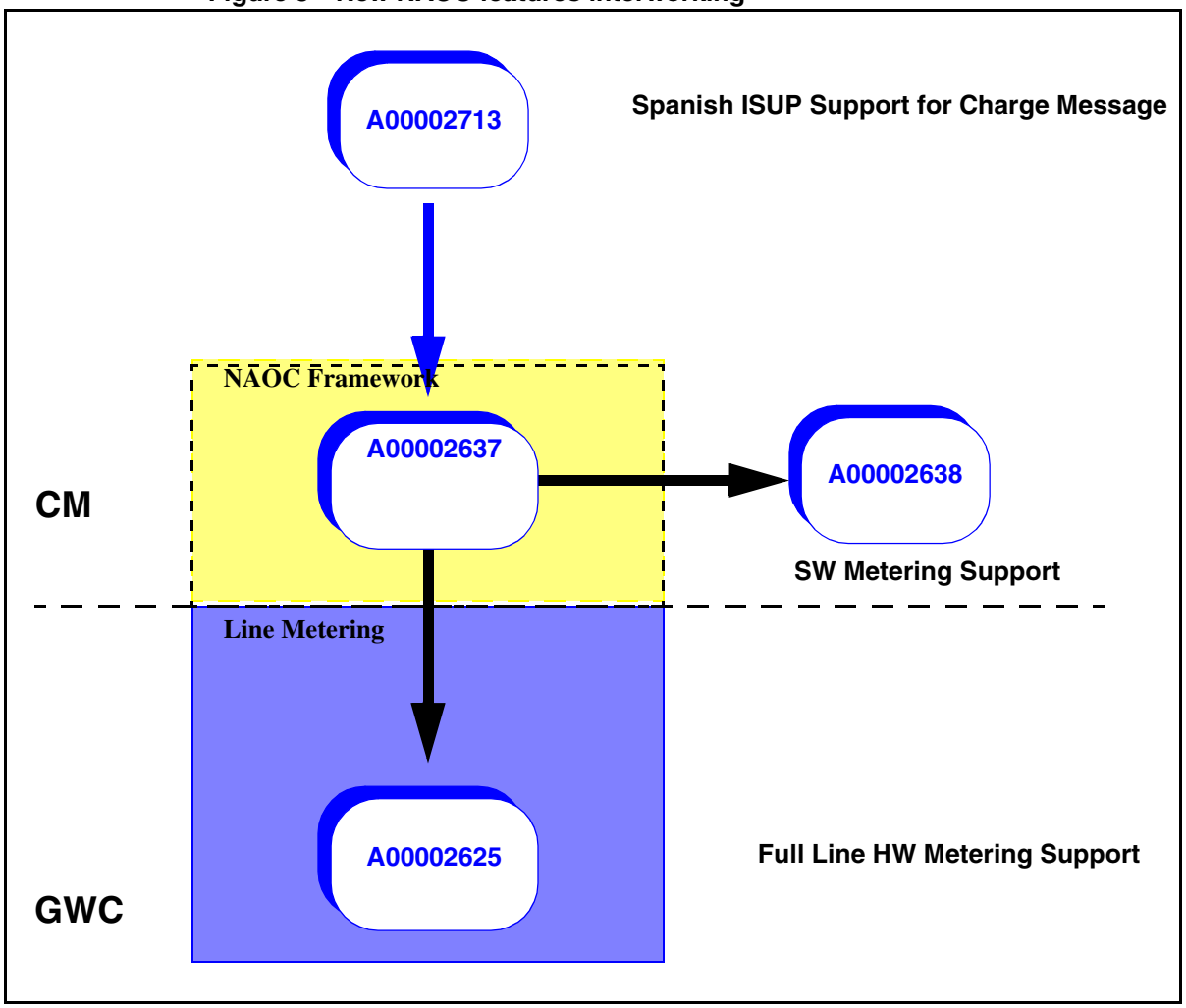
i. NAOC for Spanish Trunk Metering Enhancements [7]

ii. Software Metering Billing support [8}

iii. Full Line HW Metering Billing compliance [9]

A brief overview of the feature interworkings is depicted in Figure 3, "New NAOC features interworking" Refer to A00002637, NAOC for Spanish Trunk Metering Enhancements for further details.

Figure 3 New NAOC features interworking



36.8 Hardware Requirements or Dependencies

No new hardware requirements or dependencies specifically for this feature.

36.9 Applicable customer facing sections

Fault Management	
Logs	_____N/A
Alarms	_____N/A
Configuration	
Data Schema	_____X
User Interface	_____N/A
Element Management	_____N/A
Security	_____N/A
Service Order	_____N/A
Office Parameters	_____X
Accounting (includes AMA billing)	_____X
Performance (includes operational measurements)	_____N/A

36.10 Glossary

Term	Description
AOC	Advice of Charge
AOCRG	Add-On Charge
APM	Application Transport Message
APP	Application Transport Parameter
BCD	Binary Coded Digit
BRI	Basic Rate Interface
CCB	Call Condense Block
CCS7	Common Channel Signalling System No. 7
CDN	Called Party Directory Number
CDP	Charge Determination Point
CGN	Calling Party Directory Number
CGP	Charge Generation Point
CFBP	Call Forward Busy Programmable
CFBF	Call Forward Busy Fix
CFDP	Call Forward Don’t Answer Programmable
CFDF	Call Forward Don’t Answer Fix
CFF	Call Forward Fix
CFU	Call Forward Universal Programmable
CIC	Carrier Identification Code
CLF	Calling Line Identification with Flash
CLID	Calling Line Identification
CONT	Translation Option - Continue
CRGA	Charging Acknowledgment
CRGT	Charging Tariff
CRP	Charge Registration Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000

CSP	Carrier Selection Parameter
ECT	Explicit Call Transfer
ELN	Essential Line
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
MEB	Metering Extension Block
MMP	Multi Market Platform
NAOC	Network Advice of Charge
NDC	National Destination Code
NLO	New Licensed Operator
NP	Number Portability
ODP	Open Dial Plan
OLE	Originating Local Exchange
PCA	Payment Ceiling Advice
PVG	Passport Voice Gateway
PRI	Primary Rate Interface
RTE	Translation Option - Route
SIE	Service Interaction Environment
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol - Telephony
SNP	Service Number Portability
UXLA	Universal Translations
VBD	Voice Band Data
XLA	Translations

36.11 References

REF #	Description of Reference
[1]	Telefonica specification GT.EG.S3.003 Ed 4: Common Channel Signalling System (SCC) Integrated Services User Part (PUSI 4)
[2]	Telefonica specification GT.EG.S3.003 Ed 4 App.1
[3]	Telefonica specification GT.EG.S3.003 Ed 4 App.2
[4]	Telefonica specification GT.EG.S3.403 1st Edition 1997: Unified Specifications for the User Part of the Integrated Services Digital Network (PUSI)
[5]	Telefonica specification GT.EG.S3.403 1st Edition Addendum 1 June1998:
[6]	Rating in the digital switching exchanges, GT.ER.d4.463 (Spanish Metering specification)
[7]	Feature A00002637, NAOC for Spanish Trunk Metering Enhancements, PLS FMDOC module: *A00002713*
[8]	Feature A00002638, *Software Metering support for Billing*, PLS FMDOC module: *A00002638*
[9]	Feature A00002625, *Full Line HW Metering / Billing Compliance* , PLS FMDOC module: *A00002625*
[10]	*Feature A59028040:* SS7 Attributes Equivalence*,* PLS FMDOC module: *A59028040*
[11]	Feature A00002678, NAOC Trunk Metering Enhancements, PLS FMDOC module: *A00002678*
[12]	Feature A59027497 , LNP-Query On Release (Non-IN), PLS FMDOC module A59027497:

37: Functional Description (FN): A00002751

37.1 Feature name

A00002751 - China BRI Supplementary Services using Keypad protocol

37.2 Description

The feature provides ISN07 with the support of BRI Supplementary Services using Keypad protocol according to "YDN 065- 1997 - China MPT/MII standards".

37.2.1 The services on BRI line using keypad protocol

Table 1 The services using keypad protocol for China market supported in ISN07.

Supplementary Service	Implementation in DMS SN07
Hot Line Service With time out (**WML**)	Yes
WakeUp Call Request(**WUCR**)	Yes
Call Forwarding on No Reply (**CFNR**)	Yes
Call Forwarding Unconditional (**CFU**)	Yes
Call Forwarding on Busy (**CFB**)	Yes
Make Set Busy(**MSB**)	Yes
Calling Line Identification presentation Restriction (**CLIR**)	Partial [a]
Connected Line Identification Restriction(**COLR**)	Yes
Outgoing Call Barring (**OCB**)	Yes
Call Waiting Activation/Deactivation (**CWACT**)	Yes

a. Refer to 2.2.3.4 Restriction and limitation.

The service being shaded will be developed in ISN07

37.2.2 Make Set Busy(MSB)

MSB service provides the same function as Do not Disturb (DnD) which is defined in China Spec. It provides a subscriber with the ability to control the termination of calls.

The function is provided by adding MSB line option to subscriber by means of SERVORD. After being assigned this feature, the default status of MSB is inactive. Subscriber can activate or deactivate this service by dialing access

code. For example, to dial access code “*33#”, the feature is activated, and to dial access code “#33#”, the feature is deactivated.

When the feature is active, any call terminated at this DN will receive busy tone or announcement. At the same time, no notification is sent to terminator.

37.2.2.1 Assignment and Unassignment of the service

The MSB line option is assigned or unassigned by means of SERVORD command as the following example:

Figure 1 The assignment example of MSB option

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1 (this field specify which DN key the feature is assigned
to)
OPTION:
>MSB
OPTKEY
>$
COMMAND AS ENTERED :
ADO MAY 95 6 46 PM ISDN 400(1 MSB) $
Enter Y to confirm, N to reject or E to edit
>Y
```

Figure 2 The unassignment example of MSB option

```
>SERVORD
SO:
>DEO
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>MSB
OPTKEY
>$
COMMAND AS ENTERED:
DEO MAY 95 6 46 PM ISDN 400(1 MSB) $
Enter Y to confirm, N to reject or E to edit
>Y
```

37.2.2.2 Provisioning of Feature Access Codes

The MSB feature access code is defined in table IBNXLA. The provision is as the following example.

Figure 3 Access codes datafill example for MSB

```
Featxla 33 feat N N MSBA
DeFeatxla 33 feat N N MSBD
```

37.2.2.3 Working with multi Key

For a BRI line, only one ETSI BRI Logic terminator Id(Ltid) can be assigned to it. For a BRI Ltid, many DNs can be assigned to it, each DN has an individual key. The MSB is a per DN option, and works on the specified DN only, i.e. it does not affect the other DNs which are assigned to the same BRI Ltid. The MSB is assigned to specified DN using field OPTKEY.

37.2.2.4 Interaction with WUCR service

According to China Spec, the MSB can not coexist with WUCR. In this feature, MSB and WUCR can be assigned to a subscriber simultaneously. MSB has higher priority than WUCR. When MSB is active, any WUC request fail and the corresponding wakeup call can not be established, just like the line is busy. When a request fails, an attempt request will be created automatically according to the office parameter WAKEUP_REQUEST_DELAY. When the attempt request reaches and the MSB is still active, the attempt request fails also and WUCBLCK OM is pegged. If the MSB is inactive, the attempt request will work normally.

37.2.2.5 Interaction with CFX service

The MSB feature has higher priority than CFX. Here the CFX means various call forward services, includes CFU, CFNR, and CFB. When a subscriber has CFX and MSB activated at the same time and a call terminated at the DN, the MSB will work instead of forwarding the call.

37.2.3 Calling Line Identification Restriction(CLIR)

The BRI Calling Line Identification Restriction (CLIR) supplementary service provides the calling party with the ability to prevent presentation of its number to the called party.

To implement CLIR service on BRI line, two services are involved, SUPPRESS and CNDB service. SUPPRESS option is assigned to subscriber, and gives a default status of CLIR. It has been provided in previously release. The CNDB option is provided for BRI line in this feature to give subscriber the ability to control the status of CLIR using keypad protocol.

The CNDB on BRI is independent of SUPPRESS. It works only per call and does not affect SUPPRESS configuration. And the 2nd dial tone will be heard after CNDB access code is dialed. The combination of two services can provide various functions(see following table).

Table 2 Combination of SUPPRESS and CNDB

Status of suppress	Status of CNDB	Function description
Not add the option	Active[a]	The number of calling party can not present to called party
	Not active	The number of calling party can present to called party
Unsuppress[b]	Active	The number of calling party can not present to called party
	Not active	The number of calling party can present to called party
Suppress[c]	Active	The number of calling party can present to called party
	Not active	The number of calling party can not present to called party
Suppress	Not add the option	The number of calling party can not present to called party

a. Assigning CNDB option and dialling access code when initial a call, the CNDB will be activated.For example dial "*62 + called number" (In enbloc mode, dial "*62#called number").It is activated per call.
b. Datafill "SUPPRESS N N/Y" to provision Unsuppress.It corresponds with fields "Option, SUPPRESSDN, SUPPRESSNAME"
c. Datafill "SUPPRESS Y N/Y" to provision Suppress.

37.2.3.1 Assignment and Unassignment of the service

CNDB option and SUPPRESS option are assigned independently. The two options are assigned or unassigned to a BRI line by means of SERVORD command as the following example.

Figure 4 The assignment example of CNDB option

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 45 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>CNDB
BILLING_OPTION:NOAMA
>[ENTER]
KEYLIST:
>1
KEYLIST:
>$
COMMAND AS ENTERED:
ADO MAY 95 6 45 PM 4001 ( CNDB NOAMA 1 $)$
Enter Y to confirm, N to reject or E to edit
>Y
```

Figure 5 The assignment example of SUPPRESS option

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 45 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>SUPPRESS
NETNAME
>PUBLIC
SUPPRESS_DN
>Y
SUPPRESS_NAME
>Y
NETNAME
>$
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 45 PM 4001 (1 SUPPRESS (PUBLIC Y Y) $ )$
Enter Y to confirm, N to reject or E to edit
>Y
```

37.2.3.2 Provisioning of Feature Access Codes

The CNDB feature access code is defined in table IBNXLA. As a per-call feature, only one access code is provided. The provision is as the following example:

Figure 6 Access codes datafill example for CNDB

```
Featxla 62 feat N N CNDB
```

37.2.3.3 Working with multi Key

Both two options are per DN options, so both do not affect the other DNs' status, which are assigned to the same BRI Ltid.

There is a difference in the method of specifying the DN key of the service between the two options. The SUPPRESS options is specified the DN key using OPTKEY field; The CNDB is specified the DN key using KeyList field.

37.2.3.4 Restriction and limitation

The implementation of CLIR in this feature is not fully compliant with China BRI Spec. It is compliant with China PSTN Spec. In China BRI Spec the CLIR is not a per-call function. That means after setting the CLIR to restricted, any calling number can not present to called party until the CLIR access code is dialed to toggle the status of CLIR. But in this feature the CLIR is a per-call function as mentioned in above description.

37.2.4 COnnected Line identification Restriction (COLR)

The BRI COnnected Line identification Restriction (COLR) supplementary service enables the connected party to prevent the presentation of its number to the calling party.

The function is provided by adding COLR line option to subscriber by means of SERVORD. It provides subscriber with the ability to control the default value of COLR. There are two modes for COLR: temporary and permanent. See following table for difference of the function between two modes:

Table 3 Contrast of temporary and permanent mode of COLR

Mode of COLR	Default value of COLR	Function description
Permanent	RESTRICT	PI equals PI_restricted. The number of connected party can not be presented to the calling party.
	ALLOW	PI equals PI_allowed. The number of connected party can be presented to the calling party.
Temporary	RESTRICT	If the CONNECT message sent by terminator includes CNN IE, PI equals the PI of CNN IE. Otherwise, the PI equals default value PI_restricted.
	ALLOW	If the CONNECT message sent by terminator includes CNN IE, PI equals the PI of CNN IE. Otherwise, the PI equals default value PI_allowed.

When office parameter MARKET_OF_OFFICE in table OFCENG is set to CHINA, the default value of permanent mode can be set to ALLOW, and in both modes subscriber can change the default value of COLR by dialing feature access code. For example, “*34#” makes the default status as restrict; “#34#” makes the default status as allow.

37.2.4.1 Assignment and Unassignment of this service

The COLR option is assigned and unassigned to BRI line by means of SERVORD command as the following example.

Figure 7 The assignment example of COLR option for permanent mode

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>COLR
MODE
>PERM
DFLT:
>allow
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 46 PM ISDN 400(1 COLR PERM ALLOW) $
Enter Y to confirm, N to reject or E to edit
>Y
```

Figure 8 The assignment example of COLR option for temporary mode

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>COLR
MODE
>TEMP
DEFAULT
>ALLOW
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 46 PM ISDN 400(1 COLR TEMP ALLOW) $
Enter Y to confirm, N to reject or E to edit
>Y
```

37.2.4.2 Provisioning of Feature Access Codes

The COLR feature access code is defined in table IBNXLA. The provision is as the following example:

Figure 9 Access codes datafill example for COLR

```
Featxla 34 feat N N COLRA
DeFeatxla 34 feat N N COLRD
```

37.2.4.3 Working with multi Key

The COLR is a per DN service. It does not affect the other DNs' status which are assigned to the same BRI Ltid. The DN is specified by the field OPTKEY.

37.2.5 Outgoing Call Baring - User Define(OCB_UD)(need to discuss)

The Outgoing Call Barring enables calls belonging to certain types to be rejected when they are originated by the served user. The served user can choose one of the following three barring programs according to China Spec.

1. DABE code-1: Deny all but emergency calls. All calls are restricted except emergency calls like police, fire department, ambulance, etc.
2. DIND code-2: Deny national and international direct dial calls. All calls except local and international operator assisted calls are restricted.
3. DIDD code-3: Deny international direct dial calls. All international except international operator assisted calls are restricted.

The function is provided by adding OCB line option to subscriber by means of SERVORD. There are two types of OCB, OCBF and OCB-UD. OCBF is assigned by operator, and subscriber can not modify its configuration, which is not required in China market. OCB-UD is assigned by operator also, but subscriber can modify its configuration by access code. When office parameter MARKET_OF_OFFICE in table OFCENG is set to CHINA, the access code sequence is compliant with China Spec as below.

- Activate: *AC*KSSSS#, K is barring program code, SSSS is password;
- Deactivate: #AC*KSSSS#, K is barring program code, SSSS is password;

In OCB-UD, when the feature is active, any call will be checked by the activated bar program. If the call is forbidden, busy tone will be received. The password is needed when activating/deactivating action is taking. This service does not affect any incoming call.

After assigning this feature to subscriber, the password can not be changed directly by subscriber or operator. If operator must change the password, he can delete the service and add the service again by means of SERVORD.

37.2.5.1 Assignment and Unassignment of this service

The OCB option is assigned or unassigned by means of SERVORD. The operator has to enter three fields, BPROG, OCBPW and OCBACTIVE, within the OCB option.

- BPROG is a barring program which restricts origination of a call.Values are defined in table ISERVOPT, but the value will be ignored in China market. The value NIL is default.
- OCBPW is a password which will be used by the served user for activation /deactivation of the feature in OCB-UD. OCBPW can be entered as either ‘NNNN’ or four digits from 0 to 9.
- OCBACTIVE field shows the status of the OCB option indicating if it is activated or deactivated. Values are Y or N. If the value is N, the assignment is OCB-UD; If the value is Y and OCBPW is datafilled as ‘NNNN’, the assignment is OCB-F.

OCB-UD is assigned as the following example.

Figure 10 The assignment example of OCB-UD

```
>SERVORD
SO:
>ADO
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>OCB
BPROG
>NIL
OCBPW
>1111(this is password)
OCBACTIVE
>N
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 46 PM ISDN 400(1 NIL 1111 N) $
Enter Y to confirm, N to reject or E to edit
>Y
```

37.2.5.2 Provisioning of Feature Access Codes

The OCB_UD feature access codes is defined in table IBNXLA, as the following example:

Figure 11 Access codes datafill example for OCB

```
Featxla 45 feat N N OCBA
DeFeatxla 45 feat N N OCBD
```

37.2.5.3 Working with multi Key

The OCB is a per DN option, so it does not affect the other DNs' status which are assigned to the same BRI Ltid. The DN is specified by the field OPTKEY.

37.2.6 Call Waiting Activation/Deactivation (CWACT)

This Call Waiting Activation/Deactivation(CWACT) allows the subscriber to activate and deactivate call waiting via feature access codes (i.e. *74, #74).

The function is provided by assigning CWACT line option to subscriber by means of SERVORD command. It works with CW service. The CWACT can only be assigned to a BRI DN that already has CW (Call Waiting), therefore the removal of CW from the DN with CWACT will not be allowed.

There is only one boolean field CW_ACTIVE of the CWACT option. When it is set to 'Y', means that the CW (Call Waiting) is allowed. The 'N' means that the CW (Call Waiting) is not allowed. To set the field to 'Y', "*74#" will be dialed; To set the field to 'N', "#74#" will be dialed .

37.2.6.1 Assignment and Unassignment of this service

The CWACT option is assigned or unassigned to a BRI line by means of SERVORD command. To assign the option to a BRI DN, the CW option must exist on this DN. To delete CW option, CWACT option must be deleted firstly. The assignment is as the following example.

Figure 12 The assignment example of CWACT option

```
>SERVORD
SO:
>ado
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>CWACT
CW_ACTIVE:
>Y
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 46 PM ISDN 400(1 CWACT Y) $
Enter Y to confirm, N to reject or E to edit
>Y
```

37.2.6.2 Provisioning Of access codes

The CWACT feature access codes is defined in table IBNXLA. The provision is as following example.

Figure 13 Access codes datafill example for CWACT

```
Featxla 74 feat N N CWACT
DeFeatxla 74 feat N N CWDEACT
```

37.2.6.3 Working with multi Key

The CWACT is a per DN service, so it does not affect the other DNs' status which are assigned to the same BRI Ltid. The DN is specified by the field OPTKEY.

37.3 Hardware Requirements or Dependencies

N/A

37.4 Software Requirements or Dependencies

N/A

37.5 Limitations and restrictions

- Interrogating CFX provision by keypad is not supported.

- Interrogating OCB provision by keypad is not supported.
- Interrogating CLIR provision by keypad is not supported.
- Interrogating COLR provision by keypad is not supported.
- Interrogating CWACT provision by keypad is not supported.
- Interrogating MSB provision by keypad is not supported.
- When activating CFX, Specifying bearer service is not supported.
- When activating CFX, Specifying sub-address is not supported.
- The CLIR is not fully compliant with China Spec, please refer to 2.2.3.4.
- WUCR can coexist with MSB, which does not comply with China Spec, please refer to 2.2.2.4.
- WUCR can coexist with CFX, which does not comply with China Spec.
- When OCB is activated with bar program DABE, WML can coexist with it, which does not comply with China Spec.
- When OCB is activated with bar program DABE, 3PTY can coexist with it, which does not comply with China Spec.
- OCB is not affected by CEPTPW in China market.
- 2nd dial tone will be heard after access code is dialed for CFX.
- 2nd dial tone will be heard after access code is dialed for CNDB.

37.6 Interactions

N/A

37.7 Applicable customer facing sections

Fault Management	
Log s	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A

Performance (includes operational measurements) N/A

37.8 Glossary

Term	Description
BRI	Basic Rate Interface
CFX	Call Forwarding Function, Include CFB, CFU, CFNR
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CM	Computing Module
CNDB	Call Number Deliver Block
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
DN	Directory Number
DnD	Do not Disturb
ETSI	European Telecommunications Standards Institute
FA	Facility
GW	Gateway
GWC	Gateway Controller
ISDN	Integrated Services Digital Network
ISN	International Succession Network
ISUP V2	ISDN User Part Version Two
ITU	International Telecommunication Union
MMP	Multi-Market Platform
MS	Message Switch
MSB	Make Set Busy
MSN	Multiple Subscriber Number
OCB	Outgoing Call Bar
PDTC	PCM-30 Digital Trunk Controller
PLGC	PCM-30 Line Group Controller
SUB	Sub addressing
TDM	Time Division Multiplex
WUCR	Wake Up Call Request

Term	Description
DnD	Do not Disturb

37.9 Reference

1. YDN 065- 1997 - China MPT/MII standards

2. NIS-S223-1 - ETSI BRI Specification.

3. Q.931 - ISDN User-Network Interface Layer 3 Specification for Basic Call Control.

4. Q.932 - General Procedures for the Control of ISDN Supplementary Services.

5. A59032661 - Outgoing Call Barring - User Defined (OCB-UD)

6. A59027720 - ETSI ISDN BRI WUC (Wake-Up Call) SERVICE

7. A59016672-MMP14 ETSI-PRI CLIP/CLIR Enhancement.

8. A59039647 - Support China PRI on CS2000 Product.

9. AD8729 - CLIP and CLIR.

10. TA0584 - Calling Number Delivery for China

11. AF6585- BRI point-to-point support.

38: Functional Description (FN): A00002754

38.1 Feature name

A00002754 - China INAP Compliance Enhancement Part 1

38.2 Description

This feature is to improve Nortel SSP's INAP functionality to comply with China INAP requirement.

38.2.1 Functional Overview

The enhancement is based on the China INAP specification and China INAP test specification (see reference 1, 2). Following enhancement is provided:

- CallGap(CG) parameter support enhancement: gapInterval.
- Multiple CallGaps support enhancement.
- ResetTimer parameter support enhancement: timerValue.
- CallInformationRequest/Report parameter support enhancement: legID, calledAddress & releaseCause.
- ActiveServiceFiltering parameter support enhancement: sfBillingRecordCharacteristics.
- ApplicationContextName negotiation support.
- ApplyChargingReport enhancement: conversation time measurement
- Support CS-1R ICA.

This feature is developed for both TDM and IP platform.

These functions are not agent specific, they are supported on the originating agents with the condition: the originating agent <-> INAP interworking is ALREADY supported. For example, China ISUP, IBN lines, SIP-T (no ISUP), China PRI.

The office parameter: INAP_Variant is used for China INAP specific enhancement: only when INAP_Variant = Chinese, the China INAP specific enhancement will take effect.

Following sections give detail of this feature:

38.2.1.1 CG parameter Support Enhancement: gapInterval

This enhancement is general for all INAP market.

This enhancement is to enhance the processing for gapInterval value ‘0’.

The CG parameter gapInterval specifies the minimum time between calls being allowed through. A CG with gapInterval = 0 indicates that calls matching the CG’s gapCriteria are not to be rejected. An InitialDP is sent to SCP, with cGEncountered set to the value of this CG’s controlType.

Note: InitialDP will carry the cGEncountered when ‘CGE’ is datafilled in INITDP_PARMS of table SERVINFO.

38.2.1.2 Multiple CGs Support Enhancement

This enhancement is to comply with China INAP specific rules for multiple CGs scenarios (please refer to reference 2):

Suppose: CG2 is received after CG1, within CG1’s duration.

1. Two CGs with same gapCriteria but different controlType

This enhancement is China INAP specific.

In this scenario:

— CG1’s data should be overwritten by CG2 EXCEPT the controlType: the gapIndicator in CG1 is replaced by CG2’s gapIndicator, gapTreatment in CG1 is replaced(or appended) by CG2’s gapTreatment if it exists in CG2.

— The controlType is set to manuallyInitiated because its priority is higher.

As a result, there won’t be a new CG data saved for CG2 but CG1’s parameters are updated. For example: Following two CGs are received,

Table 1 CG1 and CG2 with Same gapCriteria But Different controlType

```
CG1{
    gapCriteria {gapOnService 200}
    gapIndicator {duration=30000sec, gapInterval=30sec}
    controlType=manuallyInitiated
   }
```

```
CG2{
    gapCriteria {gapOnService 200}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType= sCPOverloaded
    gapTreatment {toneID=1, duration=10}
   }
```

Then CG1 will be updated to:

Table 2 Updated CG1

```
CG1{
    gapCriteria {gapOnService 200}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=manuallyInitiated
    gapTreatment {toneID=1, duration=10}
   }
```

When next INAP calls comes in, the above CG data will be used.

In the above example, if CG1's controlType is sCPOverloaded and CG2's controlType is manuallyInitiated, the updated CG1 will be the same with that is shown in Table 2 because manuallyInitiated has higher priority.

2. Two CGs with different gapCriteria

This enhancement is general for all INAP market.

In this scenario, these two CGs co-exist in SSP. If an IN service is to be triggered and it meets both of these two CG's criterias, then the CG to be activated should be the one whose criteria is more specific.

"More specific" means: first, gapCriteria has a higher priority. Following list shows gapCriteria from high priority to low priority:

- calledAddressValueAndService
- calledAddressValue
- callingAddressValueAndService
- gapOnService

Second, if two CGs have a gapCriteria with same priority, "More specific" means the gapCriteria is more detail. Following are examples:

a. For gapCriteria calledAddressValueAndService, calledAddressValue and callingAddressValueAndService, if two CGs are found in both control types(manuallyInitiated and sCPOverloaded), the CG, whose gapCriteria has higher priority, takes effect.

   For example: Following two CGs are received,

Table 3 CG1 and CG2 with gapCriteria: calledAddressValue

```
CG1{
    gapCriteria{calledAddressValue, 8765}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=manuallyInitiated
   }
```

Table 3 CG1 and CG2 with gapCriteria: calledAddressValue

```
CG2{
    gapCriteria{calledAddressValue, 87654}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=sCPOverloaded
   }
```

when an IN service with calledAddressValue is 876543 is to be triggered, CG2 should be activated because its matched address value is longer, in another word, it's more specific.

b. For gapCriteria gapOnService, the one has an exact match takes effect. For example: Following two CGs are received,

Table 4 CG1 and CG2 with gapCriteria: gapOnService

```
CG1{
    gapCriteria{gapOnService, 1}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=manuallyInitiated
   }
```

```
CG2{
    gapCriteira{gapOnService, 10}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=sCPOverloaded
   }
```

When an IN service is to be triggered and

- if the service key is 1, CG1 should be activated;
- if the service key is 10, CG2 should be activated;
- if the service key is 101, no CG should be activated.

c. If the criteria is met in both control types and they are the same specific, the CG whose controlType is manuallyInitiated takes effect because its priority is higher. For example: the incoming call matches the criteria of two CGs (Table 5), in this case CG1 should take effect if both of them meet the gap criteria.

Table 5 CG1 and CG2 have the same gapCriteria but different controlType

```
CG1{
    gapCriteria{calledAddressValue, 8765}
    gapIndicator {duration=60000sec, gapInterval=60sec}
    controlType=manuallyInitiated
 }
```

```
CG2{
    gapCriteria{calledAddressValue, 8765}
    gapIndicator {duration=30000sec, gapInterval=60sec}
    controlType=sCPOverloaded
 }
```

Note: This won't happen in China INAP because these two CGs can not coexist, see requirement (1).

38.2.1.3 RT Parameter Support Enhancement: timerValue

This enhancement is to extend the supported timerValue value.

In INAP call, timer Tssf is used to prevent the call from suspending too long, protect the dialogue between SSF and SCF. ResetTimer operation is sent from SCF to SSF, to restart Tssf timer using the timerValue, so that Tssf will not time out. It only takes effect in the following 3 states:

— waiting for instruction (WFI)

— waiting for end of user interaction (WFEOUI)

— waiting for end of temporary connection (WFEOTC)

This feature performs the following enhancement:

1. report UnexpectedDataValue error when the timerValue exceed 0-2047.

This enhancement is China INAP specific.

2. extend the supported timer values between 10 seconds & 60 seconds: 15, 20, 25, 30, 35, 40, 45, 50, 55 seconds support is added. For in-range value other than one of the above values, it is rounded up to the next supported value.

This enhancement is general for all INAP market.

3. extend the supported range for timerValue in WFI state to 1-60 seconds.

This enhancement is general for all INAP market.

38.2.1.4 CIRQ/CIRP Parameter Support Enhancement: legID, calledAddress & releaseCause

This enhancement is general for all INAP market.

This enhancement is to:

1. support CS-1R CIRP: if CIRP is datafilled in the CS1R option of table SERVINFO, the outgoing CIRP will use the CS-1R format, the legID will not be included:

Table 6 Table SERVINFO

```
SERVIDX                                                                  OPTION
-------------------------------------------------------------------------------
200    (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) $)
           (TCAP_INFO ( INAP_OPT (AUTO_CONTINUE) $)(TCAP_VERSION CCITT_V1)$)
           (CS1R ( CIRP) $)$
```

2. add support for calledAddress and releaseCause parameters in CIRQ/ CIRP:

— calledAddress indicates the incoming called party address that was received by the SSF (i.e. before translation by the SCF) and is as available on the UNI or NNI and interpreted as per the numbering plan. The format is shown in Table 7.

— releaseCause is defined the same as Q.762, which is applied to the indicated or default party.The format is shown in Table 8. The diagnostics is not included in the releaseCauseValue of CIRP.

Note: for release cause, if the incoming release message is not in Q.762 format, then default value: 'normal clearing' is used.

Table 7 calledAddressValue Format (it uses the format of ISUP parameter: GenericNumber)

8	7	6	5	4	3	2	1
Number qualifier indicator							
Odd/even	Nature of address indicator						
NI Ind.	Numbering plan Ind.			Presentation Ind.		Screening Ind.	
2nd address signal				1st address signal			
.....				.....			
Filler(if necessary)				nth address signal			

Table 8 releaseCauseValue Format (same as ISUP parm: CauseIndicators)

8	7	6	5	4	3	2	1
Ext.	Coding standard		spare	Location ...			
Ext.	Cause Value						
Diagnostics (if any)							
.....							
Diagnostics (if any)							

38.2.1.5 ASF Parameter Support Enhancement: sfBillingRecordCharacteristics

This enhancement is general for all INAP market.

This enhancement is to provide support the sFBillingChargingCharacteristics. Whatever received, this parameter and sub-parameter is treated as: noINCharging.

The following functions are provided for sFBillingChargingCharacteristics subparameter:

— noINCharging

— iNCharging

— sendChargeInformation

Note: the decoding of sFBillingChargingCharacteristics is not supported. When received correct sFBillingChargingCharacteristics, no handling, no reject or return error. When recevied sFBillingChargingCharacteristics with problems, no handling, no reject or return error.

Following table gives the definition of SFBCC (highlighted in bold):

Table 9 China INAP ActiveServiceFiltering Definition:

```
ActiveServiceFiltering::= SEQUENCE {
      filteredCallTreatment [0] IMPLICIT SEQUENCE {
        sFBillingChargingCharacteristics [0] CHOICE {
          noINCharging [0] IMPLICIT NULL,
          iNCharging [1] IMPLICIT SEQUENCE {
            ......} OPTIONAL },
          sendChargeInformation [2] IMPLICIT SEQUENCE {...}} OPTIONAL,
        informationToSend [1] CHOICE {
        maximumNumberOfCounters [2] IMPLICIT INTEGER (1..100) OPTIONAL,
        releaseCause [3] IMPLICIT OCTET STRING (SIZE (2..20)) OPTIONAL},
      ......
      }
```

38.2.1.6 ACN Negotiation Support

This enhancement is to provide the following functions:

1. Support China INAP ACNs

This enhancement is China INAP specific.

The ACN definition of China INAP is shown in the following table:

Table 10 China INAP Specific Application Context Name (Based on ISO/IEC DIS 8824-1)

```
ACN pattern:
D'00 - CCITT(ITU-TS)
D'03 - Network Operator
D'xxxx - DNIC (market based)
D'01 - INAP field
D'01 - INAP
D'01 - Application Context
D'xx - specific AC value (see below)
D'00 - market based version
```

Table 10 China INAP Specific Application Context Name (Based on ISO/IEC DIS 8824-1)

ACN Values: DNIC = D'4605 Specific AC values: xx = H'00 - H'07 00 - SSP uses InitialDP to initiate dialogue 01 - SSP uses AssistRequestInstruction to initiate dialogue 03 - SCP uses InitiateCallAttempt to initiate dialogue 04 - SCP uses CallGap to initiate dialogue 05 - SCP uses ActivateServiceFiltering to initiate dialogue 06 - SSP uses ServiceFilteringResponse to initiate dialogue
ACN coding: H'(03 a3 7d 01 01 01 xx 00)

2. Support ACN negotiation

This enhancement is general for all INAP market.

Following ACN negotiation rules for SSP are supported:

a. when SSP sends TC-BEGIN package:

— encode the correct ACN into the package and store the ACN value.

b. when SSP receives TC-BEGIN package:

— if the ACN is supported, go on processing the TC component.

— else, response SCP with TC-U-ABORT. Abort reason is 'application context name not supported'.

— when processing component, if the component contains a China INAP operation, verify the application context according to the operation code (please refer to Table 10). If fails, response SCP with TC-U-ABORT, abort reason is 'application context name not supported'. Else, go on processing the component.

c. when SSP receives the first response from SCP in TC-CONTINUE/ TC-END:

— if the ACN match the ACN value of previous TC-BEGIN, go on processing the TC component.

— else, response SCP with TC-U-ABORT. Abort reason is 'application context name not supported'.

d. when SSP receives the first response from SCP in TC-U-ABORT:

— release the current dialogue.

38.2.1.7 ACR Enhancement: Conversation Time Measurement

This enhancement is China INAP specific.

This enhancement is to fix the following problem: For INAP call being charged using AC operation, when the conversation is longer than 255 seconds, the duration value in ACR will go incorrect. This problem exists in max conversation time, duration, report interval measurement.

38.2.1.8 Support CS-1R ICA

This enhancement is general for all INAP market.

This enhancement is to:

- support ICA in TC-BEGIN package
- support multiple components in TC-BEGIN package

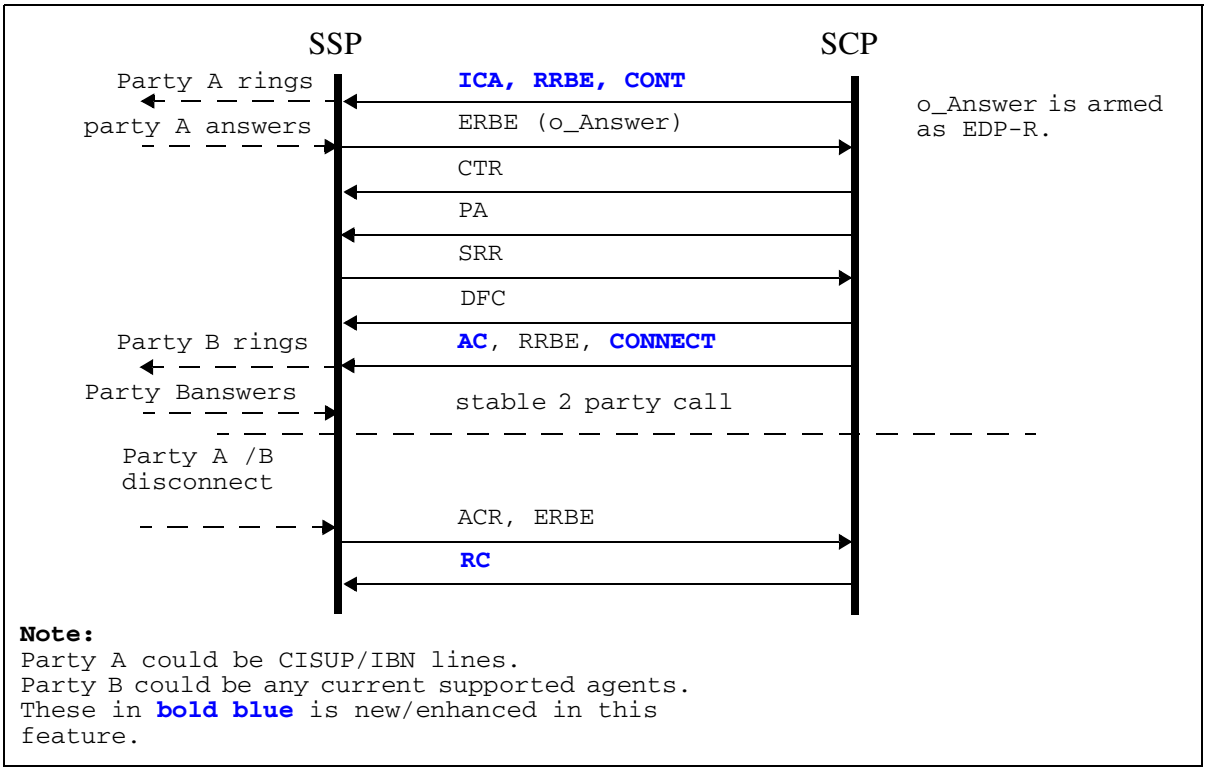
  The operation sequence must be: the first operation is ICA; the subsequence call processing operations could be RRBE, CONT, CWA, FCI, AC; the last operation must be CONT or CWA.

  If the operations in the BEGIN package does not obey the rule, the package will be aborted.

  If the package match the above rules but has logic conflict in the operations it carries, then it is out of this feature's scope. The existing handling will be used. Also the imply and handling of each operation except ICA is out of this feature's scope.
- support CS-1R ICA
- support virtual agent -> IBN line interworking
  No line features is supported in the interworking.
- enhance the AC, CONNECT handling for extended dialogue.

Following figure shows an example for ICA usage:

Figure 1 China ICA Implementation Example



As different markets may have different configuration on ICA in BEGIN package, some general rules is defined for what call related operation can be in BEGIN package:

- If the first operation is callp related, it must be ICA
- If the first operation is ICA, RRBE must be in the same package and the last operation must be CONT (CONTINUE) or CWA (ContinueWithArgument)
- The following callp operations are supported in BEGIN package if the first operation is ICA: RRBE, CWA, CONT, FCI, AC.

38.2.2 Data Requirement

Standard datafill for IN will be used.

38.3 Hardware Requirements or Dependencies

N/A.

38.4 Software Requirements or Dependencies

N/A.

38.5 Limitations and restrictions

- This feature does not support the following ACN negotiation scenario: when SSP receives the first response from SCP in TC-U-ABORT, with abort reason is ‘application context name not supported’, then verify its ACN value, if it is valid, initiate a new dialogue using the new ACN, and release the current dialogue.
- This feature only accepts the Chinese ASF SfBillingChargeCharacteristics, does not handle it. In EINTRACE, this parms is displayed. There is no any handling on this parameter.
- For parameters not mentioned in this document, their implementation exceeds this feature’s range.
- In the scenario that SCP originates a call to IBN lines, only the IBN lines use DGT are supported.

38.6 Interactions

N/A.

38.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

38.8 Glossary

Term	Description
AC	ApplyCharging
ACN	Application Context Name
ACR	ApplyChargingReport
ASF	ActiveServiceFilting
CIRP	CallInformationReport
CIRQ	CallInformationRequest
CG	CallCap
CON	Connect
CONT	Continue
CTR	ConnectToResource
CWA	ContinueWithArgument
DFC	DisconnectForwardConnection
DGT	Digit Tone
ERBE	EventReportBCSMEvent
ICA	InitialCallAttempt
IN	Intelligent Network
INAP	Intelligent Network Application Part
ISUP	ISDN User Part
PA	PlayAnnouncement
PCUI	PromptAndCollectUserInformation
RC	ReleaseCall
RRBE	RequestReportBCSMEvent
RT	ResetTimer
SCP	Service Control Point
SRR	SpecialResourceReport
SSP	Service Switching Point

38.9 Recommended Reading/References

1. GF017-1995 China INAP Specification
2. YDN107.2-1999, INAP test spec - SSP part
3. A59039729 - CS1R China ISUP Calling Card Service
4. A89008388 - China IN SSP capability
5. DMS Implementation of CS-n INAP (ITU-T Recommendations Q.12 n8), release PRE 10.0

39: Functional Description (FN): A00002755

39.1 Feature name

A00002755 - CHINA PSTN LINE SERVICE COMPLIANCE

39.2 Description

This activity enhances IBN line services to comply with the China PSTN line service requirements in the China specification YDN065 and YDT1128 (partial) for DMS-Hybrid TDM solution and CS2Kc-IAD IP solution.

Table 1 below shows the IBN line services which are chosen to achieve the corresponding China PSTN line service requirements.

Table 1 Line Services Required By China Market

IBN Line Service	Requirement
CEPT SC	YDN065: Abbreviated Dialling
CEPT WML	YDN065: Hot Line Service with Time-Out
CEPT ILR	YDN065: Outgoing Call Barring
CEPT CDND	YDN065: Don't Disturb Service
CLF	YDN065: Malicious Call Tracing
CEPT IWUC	YDN065: Alarm-Call Service
CEPT CFU	YDN065: Call Forwarding Unconditional
CEPT CFD	YDN065: Call Forwarding on No Answer
CEPT CFB	YDN065: Call Forwarding on Busy
CEPT CDTA	YDN065: Absent-Subscriber Service
CEPT ICWT, CEPT SCWID	YDN065: Call Waiting
CEPT CCBS	YDN065: Call Back
CEPT I3WC	YDN065: Three Party Services
CEPT I6WC	YDN065: Conference Service
CND	YDN065: Calling Identity Delivery
CNDB, SUPRESS	YDN065: Calling Identity Delivery Restriction
AUL	YDT1128: Hot Line
CEPTPW	YDT1128: Password

IBN Line Service	Requirement
CEPTRA	YDT1128: Call Forwarding Remote Access
	YDT1128: Outgoing Call Barring Remote Access

This activity is divided into following components:

- Identification of China line service usage
- CEPT line service on the IBN line without CEPT option
- China line service's interaction compliance
- China line service's operation and administration compliance
- New downloadable China toneset CHINALGC

39.2.1 Identification of China line service usage

In order to identify in which market the line services are working, this activity introduce a new field MARKET into the tuple CEPTONCENTREX. At present, two values are available for this field. One is DEFAULT and another is CHINA. For the chinese office, this field must be set to CHINA.

Refer to following datafill example of tuple CEPTONCENTREX:

Figure 1 Datafill example of tuple CEPTONCENTREX

```
TABLE ISERVOPT
==============
CEPTONCENTREX CEPTONCENTREX CHINA (SC) (WML) (ILR) $
```

39.2.2 CEPT line service on the IBN line without CEPT option

For the CEPT line services in Table 1, "Line Services Required By China Market," on page 913, this activity allows them to work on the IBN line without CEPT option. In addition, this activity also allows the following CEPT line services to work on the IBN lines without CEPT option, which are not stated in the China Specification, but are used by China Market on DMS100I:

- CEPT CDTO
- CEPT CFF
- CEPT ICT

In order to allow all CEPT line services mentioned above on the IBN line without CEPT option, the corresponding service options must be present in tuple CEPTONCENTREX in table ISERVOPT. Table 2 below shows the available options in tuple CEPTONCENTREX, and the associated CEPT line services:

***Note**: The CEPTONCENTREX options with **bold** font are introduced by this activity.*

Table 2 CEPTONCENTREX Options and CEPT Line Services

CEPTONCENTREX OPTION	Associated CEPT Line Service
SC	SCL, SCS
WML	WML
ILR	ILR
CDIV	CDND, CFU, CFB, CFD, CFF, CDTA, CDTO, CFRA
ICT	ICT
ICWT	ICWT
IWUC	IWUC
ICWT	ICWT
CCBS	CCBS
I3WC	I3WC
I6WC	I6WC
CEPTPW	CEPTPW
CEPTRA	CEPTRA

Refer to the following datafill example of tuple CEPTONCENTREX:

Figure 2 Datafill example of tuple CEPTONCENTREX

```
TABLE ISERVOPT
==============
CEPTONCENTREX CEPTONCENTREX CHINA (SC) (WML) (ILR) (IWUC) (CDIV)
(ICT) (ICWT) (CCBS) (I3WC) (I6WC) (CEPTPW) (CEPTRA) $
```

39.2.3 China line service's interaction compliance

For the chinese market, the line services in Table 1, “Line Services Required By China Market,” on page 913 have following interactions (Note: this activity does not cover the interaction with the line services out of Table 1):

Table 3 IBN Line Services Interaction according to China requirement

IBN Line Service	Interaction
CEPT SC	The option SCS/SCL can not be assigned together with AUL. No precedence interactions with other line services.
CEPT WML	The option WML can not be assigned together with AUL. CEPT WML can not be activated when the ILR is registered to the class which restricts all calls.
CEPT ILR	The option ILR can not be assigned together with AUL. The ILR can not be registered to the class which restricts all calls when CEPT WML or CEPT I3WC is activated.

IBN Line Service	Interaction
CEPT CDND	The option CDND can not be assigned together with AUL, CDTA, CCBS or IWUC. The CEPT CDND takes precedence of CEPT CFU, CEPT CFD and CEPT CFB. The CEPT CDND takes precedence of the CEPT IWCT, no waiting calls can be established if the CEPT CDND is activated. The CLF can not be performed if the CEPT CDND is activated.
CLF	The option CLF is compatible with other line options. The CLF functionality can not be invoked if the CEPT CDND or CEPT CDTA is activated. When the CLF functionality is invoked, the CLI must be provided if it is available, even the CLI delivery is restricted. For the diverted calls, the original calling party number should be traced if possible.
CEPT IWUC	The option IWUC can not be assigned together with AUL, CDND or CDTA. The CEPT IWUC can not be activated if CEPT CFU, CEPT CFD or CEPT CFB is activated.
CEPT CFU	The option CFU can not be assigned together with AUL, CDTA or CCBS. The CEPT CFU can not be activated if CE PT IWUC is activated. The CEPT CDND takes precedence of CEPT CFU, no calls can be diverted to the destination number if the CEPT CDND is activated. The CEPT CFU takes precedence of CEPT ICWT, CEPT CFD and CEPT CFB. The party who has the CFU is not aware of the occurrence of the unconditional call diversion, and CND is not allowed to invoke on the party who diverting the CFU call. For the diverted call, the original calling party number is provided if possible.
CEPT CFD	The option CFD can not be assigned together with AUL, CDTA or CCBS. The CEPT CDND takes precedence of CE PT CFD, no calls can be diverted to the destination number if the CEPT CDND is activated. The CEPT CFD can not be activated if CEPT IWUC is activated. When the call is diverted, the CND is allowed to invoke on the party who diverting the CFD call. For the diverted call, the original calling party number is provided if possible.
CEPT CFB	The option CFB can not be assigned together with AUL or CDTA. The CEPT CDND takes precedence of CEPT CFB, no calls can be diverted to the destination number if the CE PT CDND is activated. The CEPT CFB can not be activated if CEPT IWUC is activated. The CEPT CFB takes precedence of CEPT ICWT. The party who has the CFB is not aware of the occurrence of the call diversion on busy, and CND is not allowed to invoke on the party who diverting the CFB call. For the diverted call, the original calling party number is provided if possible.

IBN Line Service	Interaction
CEPT CDTA	The option CDTA can not be assigned together with AUL, CCBS, CDND, IWUC, CFU, CFD or CFB. The CEPT CDTA takes precedence of the CEPT ICWT, no waiting calls can be established if the CEPT CDTA is activated. The CLF can not be performed if the CEPT CDTA is activated.
CEPT ICWT, CEPT SCWID	The option ICWT can not be assigned together with AUL. The CEPT CFU and CEPT CFB take precedence of CEPT ICWT, and for the CFU or CFB calls, the SCWID is not allowed.
CEPT CCBS	The option CCBS can not be assigned together with AUL, CDND, CDTA, CFU or CFD. No precedence interactions with other line services.
CEPT I3WC	The option I3WC can not be assigned together with AUL. The CEPT I3WC functionality can no be invoked when the ILR is registered to the class which restricts all calls.
CEPT I6WC	As Nortel provision. There are not detailed requirement according to the China specification YDN065.
CND	The option CND is compatible with other line options. The CND is not allowed to invoke on the party who diverting CFU or CFB calls.
CNDB, SUPRESS	The option CNDB can not be assigned together with AUL. No precedence interactions with other line services.
AUL	The option AUL can not be assigned together with SCS, SCL, WML, ILR, CDND, IWUC, CFU, CFD, CFB, CDTA, ICWT, CCBS, I3WC, I6WC or CNDB. The AUL has the highest precedence against other line services.
CEPTPW	The option CEPTPW is compatible with other line options. No precedence interactions with other line services.

***Note**: Refer to Section 39.10.9.6, 39.10.10.6, 39.10.11.6, Alarm-Call Service is incompatible with call diversion service (Call Forward Unconditional, Call Forward on No answer or Call Forward on Busy), however, refer to Section 39.11.1.1.6, Alarm-Call Service is compatible with call diversion service. After confirmed with the specification YDT1128 drafter, the interaction is that Alarm-Call Service can be assigned together with the call diversion service to the same subscriber, but both service can not be activated at the same time.*

The customer can achieve the China specific line options compatibilities/ incompatibilities by changing the table OPTOPT manually. Regarding the current release, the following changes are required to perform into table OPTOPT according to the China requirement:

— Remove ICWT, I3WC and I6WC options from the CLF tuple;

— Remove CLF option from the ICWT tuple;

— Remove CLF option from the I3WC tuple;

— Remove CLF option from the I6WC tuple;

— Add AUL, CCBS, CDTA and IWUC options to the CDND tuple;

— Add AUL, CDND and CDTA options to the IWUC tuple;

— Add CDTA and CCBS options to the CFU tuple;

— Add CDTA and CCBS options to the CFD tuple;

— Add CDTA option to the CFB tuple;

— Add CDND, IWUC, CFU, CFD, CFB and CCBS options to the CDTA tuple;

— Add CDND, CFU, CFD and CDTA options to the CCBS tuples,

— Add CDND and IWUC options to the AUL tuples.

The changes in table OPTOPT can be done by deleting the existing tuple, and adding a new tuple. Please note that, during the ONP, the table OPTOPT can not be transferred to the inactive side automatically, so the operator has to change the table OPTOPT according to the China requirement manually after the ONP.

The field MARKET of tuple CEPTONCENTREX in table ISERVOPT must set to CHINA to achieve the China line service's interaction compliance.

39.2.4 China line service's operation and administration compliance

39.2.4.1 ILR Password: Display and Change

Prior to this activity, the ILR password can not be displayed by using QDN command (it is masked with "NNNN"), and the password can not be changed by using CHF command. This activity introduces a new field SHOW_CHG_PSWD into the tuple ILRCLS in table ISERVOPT. If this field is set to Y, the ILR password allows to be displayed and changed.

Refer to following datafill example of tuple ILRCLS:

Figure 3 Datafill example of tuple ILRCLS

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ILRCLS
OPTION:
>ILRCLS
ILR_PROG:
>N
SDT:
>N
CR_PSWD: N
>Y
SHOW_CHG_PSWD: N
>Y
TUPLE TO BE ADDED:
ILRCLS ILRCLS N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

39.2.4.2 IWUC: Abort wakeup request if line is in use

The existing implementation of IWUC service, if the line is in use at the scheduled time, the wakeup request may retry after a given time delay. However, according to the China specification, the wakeup request should be aborted automatically if the line is in use.

This activity introduces a new field ABORT_IF_IN_USE into the tuple IWUC in table ISERVOPT. If this field is set to Y, the wakeup request is aborted automatically when the line is in use at the scheduled time, and the IWUC102 log with the reason ‘LINE IN USER’ will be generated to indicate the abortion of the wakeup request.

Refer to following datafill example of tuple IWUC:

Figure 4 Datafill example of tuple IWUC

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>IWUC
OPTION:
>IWUC
MIN_AHEAD_TIME:
>1
REPEAT_NEXT_DAYS: N
>
ABORT_IF_IN_USE: N
>Y
REPEAT_PER_REQUEST:
>1
NUMBER_OF_REQUEST:
>ONE
OVERWRITE: N
>Y
TUPLE TO BE ADDED:
IWUC IWUC 1 N Y 1 ONE Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

39.2.4.3 ICWT: Datafillable Timer for "Called Party Ignores Waiting Call"

In the existing implementation of ICWT service, the time-out of timer "Called Party Ignores Waiting Call" is hardcoded as 30 seconds, however, according to China Specification YDN065, this time-out should be set to 15 seconds.

This activity introduces a new field ICWT_IGNORE_WAITING_TMO into tuple ICWT in table ISERVOPT. The operator can specify a value from 10 to 45 seconds for the timer "Called Party Ignores Waiting Call" of ICWT service. If the tuple ICWT is not present in table ISEROVPT, by default, the time-out of 30 seconds is used.

Refer to following datafill example of tuple ICWT:

Figure 5 Datafill example of tuple ICWT

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>icwt
OPTION:
>icwt
ICWT_IGNORE_WAITING_TMO:
>15
ICWT_ANN_ACTIVE: N
>N
ICWT_TMO_ANN_ACTIVE: N
>N
ICWT_TIMEOUT_TREATMENT:
>NOSC
TUPLE TO BE ADDED:
ICWT ICWT 15 N N NOSC
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

39.2.4.4 CEPTRA: Collect DN and PIN in Different Stages

According to China Specification YDN1128, the service CEPTRA is required to collect DN and PIN in different stages, that is, the subscriber should input DN firstly, and receive prompt, then input PIN.

This activity introduces a new field COLLECT_DNPIN_IN_DIFF_STAGES into tuple CEPTPW in table ISERVOPT, if this field is set to Y, the CEPTRA will collect DN and PIN in different stages.

Moreover, in order to support to play announcements to prompt the subscriber to input DN and PIN, two new announcements (COLLECT_DN_ONLY and COLLECT_PIN_ONLY) are introduced to the service CEPTRA, the operator can datafill tuple CEPTPW in table ISERVOPT to assign the corresponding announcement trunks which are connected for the new announcement names.

When provisioning the announcements for the service CEPTRA, if the field COLLECT_DNPIN_IN_DIFF_STAGES is set to Y, the announcement IDs COLLECT_DN_ONLY and COLLECT_PIN_ONLY are required to provision, and the announcement ID DNPIN is useless, and the datafill is not required. If the field COLLECT_DNPIN_IN_DIFF_STAGES is set to N, the announcement ID DNPIN is required to provision, and the announcement IDs COLLECT_DN_ONLY and COLLECT_PIN_ONLY are useless.

Refer to following datafill examples of tuple CEPTPW and announcement provision when the field COLLECT_DNPIN_IN_DIFF_STAGES is set to Y:

Figure 6 Datafill example of tuple CEPTPW

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>3333
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>y
ANNOUNCE:
>y
ANNC_STATE:
>SILENCE
CEPT_ANNCS:
>chgpin ceptpw_chgpin
CEPT_ANNCS:
>vldpin ceptpw_vldpin
CEPT_ANNCS:
>collect_dn_only ceptra_coll_dn
CEPT_ANNCS:
>collect_pin_only ceptra_coll_pin
CEPT_ANNCS:
>$
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1234 Y Y AUD_RNG (CHGPIN CEPTPW_CHGPIN)
(VLDPIN CEPTPW_VLDPIN) (COLLECT_DN_ONLY CEPTRA_COLL_DN)
(COLLECT_PIN_ONLY CEPTRA_COLL_PIN)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Figure 7 Announcement Provision when the field COLLECT_DNPIN_IN_DIFF_STAGES is set to Y

```
TABLE CLLI
CLLI ADNUM TRKGRSIZ ADMININF
-----------------------------------------------------------------
CEPTPW_CHGPIN   991 5    CEPTPW_ANNOUNCEMENT
CEPTPW_LOCKED    992 5    CEPTPW_ANNOUNCEMENT
CEPTPW_VLDPIN    993 5    CEPTPW_ANNOUNCEMENT
CEPTRA_COLL_DN   994 5    CEPTRA_ANNOUNCEMENT
CEPTRA_COLL_PIN  995 5    CEPTRA_ANNOUNCEMENT
CEPTRA_SCODE     996 5    CEPTRA_ANNOUNCEMENT

TABLE: ANNS
CLLI  ANNTYP TRAFSNO MAXCONN CYTIME MAXCYC
-----------------------------------------------------------------
CEPTPW_CHGPIN     ALL 1 3 1 STND N 255 1
CEPTPW_LOCKED     ALL 1 3 1 STND N 255 1
CEPTPW_VLDPIN     ALL 1 3 1 STND N 255 1
CEPTRA_COLL_DN    ALL 1 3 1 STND N 255 1
CEPTRA_COLL_PIN   ALL 1 3 1 STND N 255 1
CEPTRA_SCODE      ALL 1 3 1 STND N 255 1


TABLE: ANNMEMS
ANNMEM HDWTYPE CARD MEMINFO
-----------------------------------------------------------------
CEPTPW_CHGPIN   0 DRAM DRA (0 DTM 0 5)$
CEPTPW_LOCKED   0 DRAM DRA (0 DTM 0 6)$
CEPTPW_VLDPIN   0 DRAM DRA (0 DTM 0 7)$
CEPTRA_COLL_DN  0 DRAM DRA (0 DTM 0 8)$
CEPTRA_COLL_PIN 0 DRAM DRA (0 DTM 0 9)$
CEPTRA_SCODE    0 DRAM DRA (0 DTM 0 10)$

TABLE: ANNPHLST
ANNPHKEYPHSLIST
-----------------------------------------------------------------
CEPTPW_CHGPIN   0 (CEPTPW_CHGPIN) $
CEPTPW_LOCKED   0 (CEPTPW_LOCKED) $
CEPTPW_VLDPIN   0 (CEPTPW_VLDPIN) $
CEPTRA_COLL_DN  0 (CEPTRA_COLL_DN) $
CEPTRA_COLL_PIN 0 (CEPTRA_COLL_PIN) $
CEPTRA_SCODE    0 (CEPTRA_SCODE) $
```

On the above announcements provisioning example, the announcements CEPTRA_COLL_DN and CEPTRA_COLL_PIN for the announcement IDs COLLECT_DN_ONLY and COLLECT_PIN_ONLY should be recorded as:

- **CEPTRA_COLL_DN**: “Please enter your telephone number”

  This is an interruptible announcement and applied to the subscriber when he/she dials DISA DN in order to use CEPTRA. It is datafilled as CEPTRA_COLL_DN 0 in the datafill example in the figure 7.

- **CEPTRA_COLL_PIN**: “Please enter your password of the telephone number which you entered just now”

  This is an interruptible announcement and applied to the subscriber when he/she dials a valid telephone number. It is datafilled as CEPTRA_COLL_PIN 0 in the datafill example in the figure 7.

For provisioning other announcements, please refer to the FN of activity A00001919.

39.2.4.5 SCU on CEPT SCL

When the telecom operating company sets up a Centrex group, some fixed abbreviated codes may request to be defined on per Centrex group basis. This requirement can be fulfilled by using SCU and SCL services in the Centrex group.

Prior to this feature, the SCU service can not be supported on CEPT SCL service. This feature allows the SCU service to be used on the CEPT SCL service if the option SC is datafilled in the tuple CEPTONCENTREX.

Following feature metering charges for SCU on CEPT SCL are introduced:

- ASSIGN - The option SCU is assigned to the line via SERVORD.
- DEASSIGN - The option SCU is de-assigned from the line via SERVORD.
- ADMPROG - The option SCU of the line is changed via SERVORD.
- USAGE - The line which SCU service dials a valid abbreviated code.

The SCU metering is charged only when the option SC is datafilled in the tuple CEPTONCENTREX.

In order to supply feature metering the table MTRFEAT should be datafilled properly for seven meterable activities.In addition the MOG option should have been provisioned against the subscriber. Please refer to FN section of A59017349 feature metering provisioning.

39.2.5 New downloadable China toneset CHINALGC

This activity introduces a downloadable China toneset CHINALGC, which can be specified for the PLGC in table LTCINV to support the ADSI CAS tone.

The toneset CHINALGC has the following tones definitions:

— Test and Diagnostic Tones

— DTMF Tones

— Simple Supervisory Tones

— Periodic Supervisory Tones

The operating company can change the field TONESET of the PLCG datafill in table LTCINV to specify the toneset CHINALGC. For the toneset change, the PLGC is requested to perform BSY and RTS manipulation in the MAPCI interface to take it effect, the toneset parameters can then be downloaded from the CM as part of XPM's static data upon RTS.

Please refer to section “39.12 Tone Specifications” on page 953 for more information.

The following datafills are required for activating feature tones in the existing parameters and tables:

- For all feature tones, in OFCENG table,

  FEATURE_TONE_SET CHINALGC

- For CWT in OFCVAR table,

  CWT_TONE_LENGTH 4

  CWT_TONE_CYCLE_TIME 5

  CWT_NO_OF_ALERTS 3

39.3 Hardware Requirements or Dependencies

N/A.

39.4 Software Requirements or Dependencies

N/A.

39.5 Limitations and restrictions

- According to the existing handling, during the ONP, the table OPTOPT can not be transferred to the inactive side automatically, so the operator has to change the table OPTOPT according to the China requirement manually after the ONP.
- For the line services that Centrex and CEPT are sharing the same line options (such as CFU, CFD and CFB), if the corresponding service options are present in tuple CEPTONCENTEX in table ISERVOPT, then only the CEPT line services can be available in the office.
- Regarding the China requirement of the service “Hot Line Service with Time-Out” in section 39.10.2, the CEPT WML service can not be activated by the subscriber when the CEPT ILR service has been activated as restriction class K=1 on the line. However, the CEPT WML service can be activated by the operator via SERVORD when the CEPT ILR service has been activated as restriction class K=1 on the line.
- Regarding the China requirement of the service “Outgoing Call Barring” in section 39.10.3, the CEPT ILR service can not be activated as restriction class K=1 by the subscriber when the CEPT WML service has been activated or the CEPT I3WC service has been assigned on the line. However, the CEPT ILR service can be activated as restriction class K=1 by the operator via SERVORD when the CEPT WML service has been activated or the CEPT I3WC service has been assigned on the line.

- Regarding the China requirements of the service “Call Forwarding Unconditional” in section 39.10.9, “Call Forwarding on No Answer” in section 39.10.10 and “Call Forwarding on Busy” in section 39.10.11, the CEPT CFU, CFD and CFB services can not be activated by the subscriber when the subscriber has activated a wake-up request. However, the CEPT CFU, CFD and CFB services can be activated by the operator via SERVORD when the subscriber has activated a wake-up request.
- Regarding the China requirement of the service “Three Party Service” in section 39.10.15, the line option I3WC can be assigned to the line by the operator via SERVORD even when the CEPT ILR service is activated as restriction class K=1 on the line.
- Regarding the China requirement of the service “Call Waiting” in section 39.10.13, the CEPT ICWT service can not support the permanent activation. The operator can activate the ICWT service when assigning it to the subscriber, however, the subscriber can deactivate the ICWT by dialing corresponding access code.
- For the subscriber assigned with the CEPT services such as ICWT, I3WC, I6WC and ICT, in order to invoke the corresponding functionalities (such as: toggle, disconnect talking party or establish conference) of these services, the subscriber must to dial the R-Code after flashing. The R-Code is one digit code of 1~9 or 0. This implicitly means only one digit is allowed to input when the subscriber goes flash, and the digit * and # is illegal. It is not allowed to activate/deactivate/program/interrogate other services when these services require the subscriber to dial the R-Code.
- According to the feature A00001919, the R1 loopback trunks are required to perform digit collection for CEPTRA calls incoming from ISUP/TUP/FDCP R2 trunks. However, if UTR (Universal Tone Receiver) card exists on the XPM, the digit collection is supported on incoming ISUP/TUP/FDCP R2 trunks directly, no R1 loopback trunks are required. This feature is responsible to verify this functionality on the China variant trunks (CISUP/CTUP/FDCP C1) only. For the other markets request this functionality, the further verification is required accordingly.
- Refer to existing restrictions of the related line services.

39.6 Interactions

Please refer to Section “39.2.3 China line service's interaction compliance” on page 915.

39.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	X
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

39.8 Glossary

Term	Description
ADSI	Analogue Display Services Interface
AUL	Automatic Line
CAS	CPE Alerting Signal
CCBS	Call Completion to Busy Subscriber
CDND	CEPT Do Not Disturb
CDTA	Call Diversion To Announcement
CDTO	Call Diversion to Operator
CEPT	European Conference of Post and Telecommunications Administrations
CEPTPW	CEPT Features' Password
CEPTRA	CEPT Features Remote Access
CFB	Call Forward on Busy
CFD	Call Forward on Don’t Answer
CFF	Call Forward Fixed
CFU	Call Forward Unconditional
CLF	Calling Line Identification with Flash
CND	Calling Number Delivery
CNDB	Calling Number Delivery Blocking
I3WC	International Three Way Call
I6WC	International Six Way Call
ICT	International Call Transfer
ICW	International Call Waiting
ILR	International Line Restriction
IWUC	International Wake-Up Call
SC	Speed Call
SCWID	Spontaneous Call Waiting ID
WML	Warm Line

39.9 References

REF	Description of Reference
A59012835 (FMDOC)	POTS CLF for German
A59011976 (FMDOC)	Call Completion to Busy Subscriber, CCBS, (public) to analog lines (incl. V5.2)
A59018575 (FMDOC)	Warm Line Interaction With Octothorpe Translation
A59019083 (FMDOC)	CEPT Call Diversion and CEPT Do Not Disturb
A59019097 (FMDOC)	CEPT WAKEUP CALL AND LAST NUMBER REDIAL
A59019274 (FMDOC)	CEPT Subscriber Control Functions Framework
A59019281 (FMDOC)	CEPT I3WC and ICT
A59019288 (FMDOC)	CEPT Call Waiting
A59019295 (FMDOC)	CEPT International Line Restriction
A59019302 (FMDOC)	CEPT HOT LINE AND WARM LINE
A59019572 (FMDOC)	CEPT CCBS-Call Completion to Busy Subscriber
A59019579 (FMDOC)	CEPT Speed Call Enhancement
A59022203 (FMDOC)	CEPT Six Way Call (I6WC)
A59039130 (FMDOC)	CEPT Call Forward Enhancements
A59040478 (FMDOC)	SCWID (spontaneous call waiting identification) on CE PT lines
CEPTONIBN (FMDOC)	CR.Q00638696, China Line Services in SN06
A00001919 (FMDOC)	CEPT SERVICES PASSWORD ENHANCEMENT

39.10 Appendix 1: China PSTN Line supplementary Services (YDN065)

39.10.1 Abbreviated Dialling

39.10.1.1 Service Description

Subscriber can specify a list of target numbers (local, national or international numbers), and assign a one- or two-digit code (abbreviated code) to each number.

When the subscriber dials the abbreviated code, the switch associates it with the assigned TN and attempts to complete the call.

39.10.1.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *51*MN*TN#,

— Receives confirmation tone,

— Goes on-hook.

where, the code MN stands for the abbreviated code, the code TN stands for the target number, which can be a local, national or international number.

39.10.1.3 Service Usage

The subscriber can use this service through the following steps:

— Subscriber goes off-hook,

— Receives dial tone

— Dials **MN

where, the code MN stands for abbreviated code.

39.10.1.4 Service Cancellation

This service can be cancelled on the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *51*MN#,

— Receives confirmation tone,

— Goes on-hook.

where, the code MN stands for the abbreviated code.

39.10.1.5 Interaction with other services

a. No collision with other PSTN line services.

39.10.2 Hot Line Service with Time-Out

39.10.2.1 Service Description

If the subscriber lifts the handset and dials no digit during a given time, the switch will set up a call to a predetermined destination number after the timer expires. The subscriber can program the predetermined destination number.

39.10.2.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *52*TN#,

— Receives confirmation tone,

— Goes on-hook.

where, the code TN stands for the target number.

39.10.2.3 Service Usage

If the subscriber wants to call a predetermined destination number, the call can be established automatically by switch if the subscriber lifts the handsets and dials no digit within 5 seconds.

If the subscriber wants to call the subscriber other than the predetermined destination number, the subscriber can start dialing within 5 seconds, and the call is processed as a regular call.

39.10.2.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #52#,

— Receives confirmation tone,

— Goes on-hook.

39.10.2.5 Interaction with other services

a. Outgoing Call Barring

Hot Line Service with Time-Out can not be activated when Outgoing Call Barring Service is activated and its restriction class (K) is

registered to 1. On the other hand, Outgoing Call Barring Service can not set its restriction Class (K) to 1 when Hot Line Service with Time-Out Service is activated.

b. No collision with other PSTN line services.

39.10.3 Outgoing Call Barring

39.10.3.1 Service Description

This service restricts the outgoing calls according to the restriction class (K):

— Deny all outgoing calls (K=1), includes the local calls.

— Deny the national and international direct dial calls (K=2).

— Deny the international direct dial calls (K=3)

39.10.3.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *54*KSSSS#,

— Receives confirmation tone,

— Goes on-hook.

where, the code K stands for the restriction class (K=1/2/3), the code SSSS stands for 4 digits password, which is preassigned by the administrator when the user subscribes this service.

39.10.3.3 Service Usage

If the restriction class is set, all restricted outgoing calls from the phone are routed to a busy tone.

39.10.3.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #54*KSSSS#,

— Receives confirmation tone,

— Goes on-hook.

where, the code K stands for the restriction class, which must be identical with the registered restriction class; The code SSSS stands for 4-digits password, which is preassigned by the administrator when the subscriber applies this service.

39.10.3.5 Service Interrogation

The subscriber can interrogate service status through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *#54#,

— Receives confirmation tone,

— Goes on-hook.

39.10.3.6 Interaction with other services

a. Hot Line Service with Time-Out

Refer to Section 39.10.2.5, item a.

b. Three Party Services

The subscriber can not apply Three Party Service when Outgoing Call Barring Service is activated and its restriction class (K) is registered to 1, on the other hand, Outgoing Call Barring Service can not set its restriction Class (K) to 1 when Three Party Service is assigned to the subscriber.

c. No collision with other PSTN line services.

39.10.4 Don’t Disturb Service

39.10.4.1 Service Description

This service can be used when the subscriber does not want to receive any incoming calls in a period. The switch will route all incoming calls to an announcement. This service does not impact the outgoing calls of this subscriber.

39.10.4.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *56#,

— Receives confirmation tone,

— Goes on-hook.

39.10.4.3 Service Usage

If this service is activated, all incoming calls to the subscriber are routed to an announcement.

39.10.4.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #56#,

— Receives confirmation tone,

— Goes on-hook.

39.10.4.5 Interaction with other services

a. Call Diversion (including: Call Forwarding Unconditional, Call Forwarding on No Answer and Call Forwarding on Busy)

When the subscriber has registered both Call Diversion and Don't Disturb Service at the same time, Don't Disturb Service takes precedence of Call Diversion.

b. Absent-Subscriber Service

Absent-Subscriber Service and Don't Disturb Service are incompatible. The subscriber can not apply Absent-Subscriber Service and Don't Disturb Service at the same time.

c. Call Back

Call Back and Don't Disturb Service are incompatible. The subscriber can not apply Call Back and Don't Disturb Service at the same time.

d. Call Waiting

It is impossible that the subscriber has the waiting call when Don't Disturb Service is activated.

e. Malicious Call Tracing

The malicious call can not be traced when Don't Disturb Service is activated.

f. Alarm-Call Service

Alarm-Call Service and Don't Disturb Service are incompatible. The subscriber can not apply Alarm-Call Service and Don't Disturb Service at the same time.

g. No collision with other PSTN line services.

39.10.5 Malicious Call Tracing

39.10.5.1 Service Description

The subscriber can apply this service to trace the calling number of the malicious call.

39.10.5.2 Service Registration

This service is assigned by the operator per request from the subscriber.

39.10.5.3 Service Usage

The subscriber can use this service through the following steps:

— Subscriber receives a malicious call,

— Goes flash and receives dial tone,

— Dials *32#,

— Receives confirmation tone,

— Goes on-hook.

39.10.5.4 Service Cancellation

This service is cancelled by the operator per request from the subscriber.

39.10.5.5 Interaction with other services

a. Call Diversion (including: Call Forwarding Unconditional, Call Forwarding on No Answer and Call Forwarding on Busy)

   For the call scenario that subscriber A calls subscriber B, and this call is diverted to subscriber C (A->B->C), if the subscriber C requests Malicious Call Tracing service, the switch should provide the number of subscriber A if possible. For some reason or restriction, for example, subscriber A and B belong to the same local network, but subscriber B and C belong to different network, and subscriber B and C are connected via R2 MFC trunk (C1), then the subscriber C only can get the number of subscriber B.

b. Calling Identity Delivery Restriction

   Even when the calling party has Calling Identity Delivery Restricting Service (in this case, the calling number can not be allowed to be displayed on the called party), the operating company must provide the calling number to the subscriber.

c. Don’t Disturb Service

   Refer to Section 39.10.4.5, item e.

d. Absent-Subscriber Service

   The malicious call can not be traced if Absent-Subscriber Service is activated. The subscriber can not apply Absent-Subscriber Service and Malicious Call Tracing at the same time.

e. No collision with other PSTN line services.

39.10.6 Alarm-Call Service

39.10.6.1 Service Description

The switch can ring the phone automatically at the subscriber specified time to remind the subscriber.

39.10.6.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *55*$H_1H_2M_1M_2$#,

— Receives confirmation tone,

— Goes on-hook.

where, the code H_1H_2 stands for the hour (00-23), M_1M_2 stands for the minute (00-59).

39.10.6.3 Service Usage

At the subscriber specified time, the switch will ring the subscriber's phone. If the subscriber goes off-hook, he/she can receive the reminder announcement, and this service is cancelled automatically. If the call is not answered, the ring will last 1 minute. Five minutes later, the switch will ring the phone again. If the second attempt is also not answered, this service will be cancelled after 1 minute ring. Moreover, at the subscriber specified time, if the phone is in use, this Alarm-Call Service will be cancelled automatically.

39.10.6.4 Service Cancellation

This service can be cancelled on the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #55#,

— Receives confirmation tone,

— Goes on-hook.

39.10.6.5 Interaction with other services

a. Don't Disturb Service

   Refer to Section 39.10.4.5, item f.

b. Absent-Subscriber Service

   Absent-Subscriber Service and Alarm-Call Service are incompatible. The subscriber can not apply Absent-Subscriber Service and Alarm-Call Service at the same time.

c. Call Diversion

Call Diversion and Alarm-Call Service are incompatible. The subscriber can not apply Call Diversion and Alarm-Call Service at the same time.

d. No collision with other PSTN line services.

39.10.7 Interception Calls

The switch should have the capability to intercept the calls that can not be established successfully (for instance, vacant number or the blocked route), and route these calls to the announcement.

39.10.8 Registered Call

This service is not used at present. Omitted here.

39.10.9 Call Forwarding Unconditional

39.10.9.1 Service Description

This service allows the subscriber to divert all incoming calls to a predetermined destination number (including the voice mail box), regardless of the subscriber's state.

39.10.9.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *57*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for the predetermined destination number (the number in this example is 6 digits).

39.10.9.3 Service Usage

After this service is activated, all incoming calls to the subscriber will be diverted to the predetermined destination number automatically.

39.10.9.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #57#,

— Receives confirmation tone,

— Goes on-hook.

39.10.9.5 Service Interrogation

The subscriber can interrogate service status through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *#57*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for predetermined destination number (the number in this example is 6 digits).

39.10.9.6 Interaction with other services

a. Absent-Subscriber Service

Absent-Subscriber Service and Call Forward Unconditional are incompatible. The subscriber can not apply Absent-Subscriber Service and Call Forward Unconditional at the same time.

b. Don't Disturb Service

Refer to Section 39.10.4.5, item a.

c. Call Waiting

Call Forwarding Unconditional takes precedence of Call Waiting if both services are activated.

d. Alarm-Call Service

Refer to Section 39.10.6.5, item b.

e. Malicious Call Tracing

Refer to Section 39.10.5.5, item a.

f. Call Back

Call Back and Call Forwarding Unconditional are incompatible. The subscriber can not apply Call Back and Call Forward Unconditional at the same time.

g. Call Forwarding on Busy

Call Forward Unconditional Service takes precedence of Call Forwarding on Busy Service if both services are activated.

h. Call Forwarding on No Answer

Call Forwarding Unconditional takes precedence of Call Forwarding on No Answer if both services are activated.

i. Calling Identity Delivery

If subscriber A makes call to subscriber B, and this call is diverted to subscriber C (that is, A->B->C), in case that both subscriber B and C have Calling Identity Delivery Services, only the subscriber C can display the subscriber A's number.

j. No collision with other PSTN line services.

39.10.10 Call Forwarding on No Answer

39.10.10.1 Service Description

This service allows the subscriber to divert the incoming calls to a predetermined destination number if the called party does not answer within a prescribed time.

39.10.10.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *41*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for the predetermined destination number (the number in this example is 6 digits).

39.10.10.3 Service Usage

After this service is activated, all incoming calls which are not answered within a prescribed time will be diverted to the predetermined destination number automatically.

39.10.10.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #41#,

— Receives confirmation tone,

— Goes on-hook.

39.10.10.5 Service Interrogation

The subscriber can interrogate service status through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *#41*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for predetermined destination number (the number in this example is 6 digits).

39.10.10.6 Interaction with other services

a. Absent-Subscriber Service

Absent-Subscriber Service and Call Forward on No Answer are incompatible. The subscriber can not apply Absent-Subscriber Service and Call Forward on No Answer at the same time.

b. Don't Disturb Service

Refer to Section 39.10.4.5, item a.

c. Alarm-Call Service

Refer to Section 39.10.6.5, item b.

d. Malicious Call Tracing

Refer to Section 39.10.5.5, item a.

e. Call Back

Call Back and Call Forward on No Answer are incompatible. The subscriber can not apply Call Back and Call Forward on No Answer at the same time.

f. Calling Identity Delivery

If subscriber A makes call to subscriber B, and the unanswered call is diverted to subscriber C (that is, A->B->C), in case that both subscriber B and C have Calling Identity Delivery Service, the subscriber A's number can be displayed on both phones of subscriber B and C.

g. No collision with other PSTN line services.

39.10.11 Call Forwarding on Busy

39.10.11.1 Service Description

This service allows the subscriber to divert the incoming calls to a predetermined destination number if the called party is in busy state.

39.10.11.2 Service Registration

This service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *40*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for predetermined destination number (the number in this example is 6 digits).

39.10.11.3 Service Usage

After this service is activated, if the called line is in use, all incoming calls to the subscriber will be diverted to the predetermined destination number automatically.

39.10.11.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #40#,

— Receives confirmation tone,

— Goes on-hook.

39.10.11.5 Service Interrogation

The subscriber can interrogate service status through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *#40*PQABCD#,

— Receives confirmation tone,

— Goes on-hook.

where, the code PQABCD stands for predetermined destination number (the number in this example is 6 digits).

39.10.11.6 Interaction with other services

a. Absent-Subscriber Service

   Absent-Subscriber Service and Call Forward on Busy are incompatible. The subscriber can not apply Absent-Subscriber Service and Call Forward on Busy at the same time.

b. Don’t Disturb Service

   Refer to Section 39.10.4.5, item a.

c. Call Waiting

Call Forward on Bust takes precedence of Call Waiting if both services are activated.

d. Alarm-Call Service

Refer to Section 39.10.6.5, item b.

e. Malicious Call Tracing

Refer to Section 39.10.5.5, item a.

f. Calling Identity Delivery

If subscriber A makes call to subscriber B in busy state, and the call is diverted to subscriber C (that is, A->B->C), in case that both subscriber B and C have Calling Identity Delivery Service, only the subscriber C can display the subscriber A's number.

g. No collision with other PSTN line services.

39.10.12 Absent-Subscriber Service

39.10.12.1 Service Description

The subscriber can activate this service when he/she is absent. The operating company will respond to all incoming calls on behalf of the subscriber.

39.10.12.2 Service Registration

This service can be registered through following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *50#,

— Receives confirmation tone,

— Goes on-hook.

39.10.12.3 Service Usage

When this service is activated, all incoming calls are routed to an announcement to inform the calling party that the called party is absent at present.

39.10.12.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #50#,

— Receives confirmation tone,

— Goes on-hook.

39.10.12.5 Interaction with other services

a. Call Back

Call Back and Absent-Subscriber Service are incompatible. The subscriber can not apply Call Back and Absent-Subscriber Service at the same time.

b. Malicious Call Tracing

Refer to Section 39.10.5.5, item d.

c. Call Waiting

Absent-Subscriber Service takes precedence of Call Waiting. If Absent-Subscriber Service is activated, no waiting calls can be established.

d. Alarm-Call Service

Refer to Section 39.10.6.5, item b.

e. Call Diversion

Refer to Section 39.10.9.6, item a; Section 39.10.10.6, item a; Section 39.10.11.6, item a.

f. Don’t Disturb Service

Refer to Section 39.10.4.5, item b.

g. No collision with other PSTN line services.

39.10.13 Call Waiting

39.10.13.1 Service Description

When the subscriber A is talking with subscriber B, if the subscriber C attempts to make a call to subscriber A, A will get a call waiting indication to know someone else is waiting for a call connection.

39.10.13.2 Service Registration

For the permanent service of Call Waiting, it is assigned by the operator per the request from the subscriber. No special registration action is required when using this service.

If the subscriber only uses this service casually, this service can be registered through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *58#,

— Receives confirmation tone,

— Goes on-hook.

39.10.13.3 Service Usage

When the subscriber A is talking with B, and the subscriber C calls subscriber A, the subscriber A will receive the waiting tone, and the subscriber C will receives ring back tone, the subscriber has three options:

1 Reject the connection request of the waiting subscriber

Do nothing, the waiting call will be dropped after 15 seconds.

2 Hold the active connection and talk with the waiting subscriber

— Subscriber goes flash,

— Receives dial tone,

— Dials 2

3 Terminate the active connection and talk with the waiting subscriber

— Subscriber goes flash,

— Receives dial tone,

— Dials 1

39.10.13.4 Service Cancellation (For casual using)

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #58#,

— Receives confirmation tone,

— Goes on-hook.

39.10.13.5 Interaction with other services

a. Calling Identity Delivery

When both services of Calling Identity Delivery and Call Waiting are activated, the calling number should be displayed on the phone when the subscriber receives the call waiting tone.

b. Call Diversion

Refer to Section 39.10.9.6, item c and Section 39.10.11.6, item c.

c. No collision with other PSTN line services.

39.10.14 Call Back

39.10.14.1 Service Description

This service provides the subscriber with ability to set up an automatic call back in the switch when he/she encounters a busy called party.

39.10.14.2 Service Registration

In case that the called party is busy, the calling party can register a call back request in switch through following steps:

— Subscriber goes flash,

— Receives dial tone,

— Dials *59#,

— Receives confirmation tone,

— Goes on-hook.

39.10.14.3 Service Usage

If this service is registered, when both parties are idle, the calling party is given ring when the calling party answers, the call is set up and called party is given ring.

The call back request is cancelled if the calling party is not answered at the first call back attempt.

39.10.14.4 Service Cancellation

This service can be cancelled by the subscriber through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials #59#,

— Receives confirmation tone,

— Goes on-hook.

39.10.14.5 Interaction with other services

a. Absent-Subscriber Service

   Refer to Section 39.10.12.5, item a.

b. Don’t Disturb Service

   Refer to Section 39.10.4.5, item c.

c. Call Diversion

   Refer to Section 39.10.9.6, item f; Section 39.10.10.6, item e.

d. No collision with other PSTN line services.

39.10.15 Three Party Services

39.10.15.1 Service Description

This service provides a subscriber with the ability to place an existing call on hold and set up a call to another subscriber. The controller can put three parties into a conference, or toggle and drop the active party when the three-way call is in progress.

39.10.15.2 Service Registration

This service is assigned by the operator per request from the subscriber. No special registration action is required when using this service.

39.10.15.3 Service Usage

1 When subscriber A is talking with subscriber B, if subscriber A wants to talk with subscriber C, A can go flash to hold the connection with B and dial the number of C after receiving dial tone, A can talk with C after the connection is created. In case that A can not connect C, A can go flash again to resume the conversation of B.

2 When A is talking with C, if A wants to talk with B again and remain the connection of C, A can go flash and dial digit 2 after receiving dial tone. If A doesn't want to remain the connection of C, A can go flash and dial digit 1 after receiving dial tone, the connection of C will be dropped and the connection is switched to B.

3 When A is talking with C, if A wants B to join in this conversation, A can go flash and dial digit 3 after receiving dial tone, then the three party conference can be established.

4 During the three party conference, if the controller A wants to talk with one party privately and hold another party, A can go flash and dial digit 2.

39.10.15.4 Interaction with other services

a. Outgoing Calling Barring

   Refer to Section 39.10.3.6, item b.

b. No collision with other PSTN line services.

39.10.16 Conference Service

39.10.16.1 Service Description

This service provides more than three ports connection during a call. The conference must be established by the operator.

39.10.17 Calling Identity Delivery

39.10.17.1 Service Description

This service can deliver the calling number to the called party, and display the calling number on the called party's phone.

This service is applicable to the called subscriber only.

This service is assigned by the operator per request from the subscriber. No special registration action is required when the subscriber uses this service.

39.10.17.2 Interaction with other services

a. Call Diversion

   Refer to Section 39.10.9.6, item i; Section 39.10.10.6, item f; Section 39.10.11.6, item f.

b. Malicious Call Tracing

   Refer to Section 39.10.5.5, item b.

c. Call Waiting

   Refer to Section 39.10.13.5, item a.

d. Calling Identity Delivery Restriction

   If the calling number is restricted to the called party, the calling number can not be displayed on the called party even though the called party applies Calling Identity Delivery Service.

e. No collision with other PSTN line services.

39.10.18 Calling Identity Delivery Restriction

39.10.18.1 Service Description

The subscriber can use this service to restrict the display of the calling number on the called party's phone.

39.10.18.2 Service Registration

The subscriber must specify which category he/she belongs to when applying this service from the operator:

— Category A subscriber, who can restrict the calling number delivery through the certain operation on an individual call basis. By default, the calling number is allowed to be displayed on the called party.

— Category B subscriber, who can allow the calling number delivery through the certain operation on an individual call basis. By default, the calling number is restricted to be displayed on the called party.

— Category C subscriber, who never allows the calling number delivery to the called party.

39.10.18.3 Service Usage

1 For the category A subscriber, in this particular call, the calling number is allowed to be delivered to the called party through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *62, following with the called number.

2 For the category B subscriber, the calling number is not allowed to be delivered to the called party through the following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *68, following with the called number,

39.10.18.4 Interaction with other services

a. Malicious Call Trace

Refer to Section 39.10.5.5, item b.

b. No collision with other PSTN line services.

39.11 Appendix 2: Additional China PSTN Line supplementary Services (YDT1128, Partial)

39.11.1 Enhanced Remote Access Services

39.11.1.1 Call Forwarding Remote Access

39.11.1.1.1 Service Registration

This service is assigned by the operator per request from the subscriber.

39.11.1.1.2 Service Activation

The subscriber A can activate the call diversion from the remote location through following steps:

a. Subscriber A goes off-hook and receives dial tone. A dials "$0X_1X_2$PQRYYYY" if the remote phone and the subscriber A's base station do not belong to the same local network, or dials "PQRYYYY" if the remote phone and the subscriber A's base station belong to the same local network.

In the above dialing, "$0X_1X_2PQR$" stands for the area code and the office code of the subscriber A's base station, "YYYY" stands for the access code of this service.

b. Subscriber A receives the announcement which prompts to input the base station number. A dials "PQRABCD", which is the number.

c. Subscriber A receives the announcement which prompts to input the subscriber A's password. A dials "$S_1S_2S_3S_4$", which is the password.

d. Subscriber A receives the prompt announcement. A dials *SC*FTN#, receives the announcement to inform that the operation is successful. A goes on-hook.

In the above dialing, "SC" stands for the access code of call diversion (Unconditional/Busy/No Answer, SC=57/40/41), "FTN" stands for the forwarded target number.

39.11.1.1.3 Service Usage

If the corresponding call diversion of the subscriber A is activated, the call to subscriber A will be diverted to the target number according to the state of the line and the activated type of call diversion.

39.11.1.1.4 Service Deactivation

The subscriber A can deactivate the call diversion from the remote location through the following steps:

a. Subscriber A goes off-hook and receives dial tone. A dials "$0X_1X_2PQRYYYY$" if the remote phone and the subscriber A's base station do not belong to the same local network, or dials "PQRYYYY" if the remote phone and the subscriber A's base station belong to the same local network.

In the above dialing, "$0X_1X_2PQR$" stands for the area code and the office code of the subscriber A's base station, "YYYY" stands for the access code of this service.

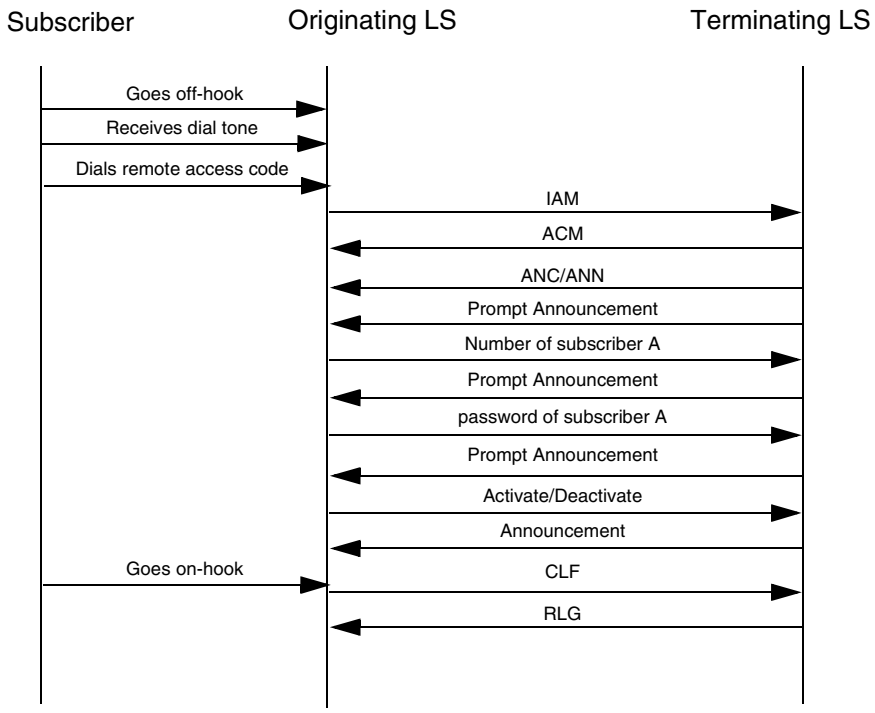
b. Subscriber A receives the announcement which prompts to input the base station number. A dials "PQRABCD", which is the number.

c. Subscriber A receives the announcement which prompts to input the remote subscriber A's password. A dials "$S_1S_2S_3S_4$", which is the password.

d. Subscriber A receives the prompt announcement. A dial #SC#. A receives the announcement to inform that the operation is successful, goes on-hook.

In the above dialing, "SC" stands for the access code of call diversion (Unconditional/Busy/No Answer, SC=57/40/41).

39.11.1.1.5 Signalling Flow



39.11.1.1.6 Interaction with other services

a. Alarm-Call Service

   Both services can be used on the same subscriber.

b. Refer to Section 39.10.10.6, 39.10.11.6 and 39.10.12.5 for the interaction with other services

39.11.1.2 Outgoing Call Barring Remote Access

39.11.1.2.1 Service Registration

This service is assigned by the operator per request from the subscriber.

39.11.1.2.2 Service Activation

The subscriber A can activate the Outgoing Call Barring service from the remote location through the following steps:

a. Subscriber A goes off-hook and receives dial tone. A dials "$0X_1X_2$PQRYYYY" if the remote phone and the subscriber A's base station do not belong to the same local network, or dials "PQRYYYY" if the remote phone and the subscriber A's base station belong to the same local network.

In the above dialing, "$0X_1X_2PQR$" stands for the area code and the office code of the subscriber A's base station, "YYYY" stands for the access code of this service.

b. Subscriber A receives the announcement which prompts to input the base station number. A dials "PQRABCD", which is the number.

c. Subscriber A receives the announcement which prompts to input the subscriber A's password. A dials "$S_1S_2S_3S_4$", which is the password.

d. Subscriber A receives the prompt announcement. A dials *54*$KS_1S_2S_3S_4$#. A receives the announcement to inform the subscriber the operation is successful. A goes on-hook.

In the above dialing, the code K stands for the restriction class:

K=1: Deny all outgoing calls, includes the local calls.

K=2: Deny the national and international direct dial calls.

K=3: Deny the international direct dial calls.

39.11.1.2.3 Service Usage

If Outgoing Call Barring of the subscriber A is activated, all restricted outgoing calls from this phone is routed to a busy tone or an announcement.

39.11.1.2.4 Service Deactivation

The subscriber A can deactivate the Outgoing Call Barring service from the remote location through following steps:

a. Subscriber A goes off-hook and receives dial tone. A dials "$0X_1X_2PQRYYYY$" if the remote phone and the subscriber A's base station do not belong to the same local network, or dials "PQRYYYY" if the remote phone and the subscriber A's base station belong to the same local network.

In the above dialing, "$0X_1X_2PQR$" stands for the area code and the office code of the subscriber A's base station, "YYYY" stands for the access code of this service.

b. Subscriber A receives the announcement which prompts to input the base station number. A dials "PQRABCD", which is the number.

c. Subscriber A receives the announcement which prompts to input the remote subscriber A's password. A dials "$S_1S_2S_3S_4$", which is the password.

d. Subscriber A receives the prompt announcement. A dials "#54*$KS_1S_2S_3S_4$". A receives the announcement to inform the subscriber the operation is successful. A goes on-hook.

39.11.1.2.5 Signalling Flow

Refer to Section 39.11.1.1.5.

39.11.1.2.6 Interaction with other services

a. Refer to Section 39.10.3.6 for the interaction with other services.

39.11.2 Hot Line

39.11.2.1 Service Registration

This service is assigned and programmed by the operator. The subscriber must predetermine the target number when applying this service.

39.11.2.2 Service Usage

When the subscriber goes off-hook, the switch immediately sets up the call to the predetermined terminating target number.

39.11.2.3 Interaction with other services

Hot line can not be compatible with the line services which require the operations via phone.

39.11.3 Password

39.11.3.1 Service Registration

The subscriber must apply this service and provide the password when applying the other line services require password (Such as: Outgoing Call Barring or Remote Access Services).

This service is assigned by the operator.

39.11.3.2 Service Usage

This service only can be used for other PSTN line services which require password.

39.11.3.3 Password Modification

The subscriber only can change the password at his/her own phone station via following steps:

— Subscriber goes off-hook,

— Receives dial tone,

— Dials *77*old_pw*$S_1S_2S_3S_4$*$S_1S_2S_3S_4$#

— Receives confirmation tone,

— Goes on-hook.

where, “old_pw” stands for the old password, “$S_1S_2S_3S_4$” stands for the new password.

39.12 Tone Specifications

39.12.1 DTMF Tones

The DTMF tones specified for China market are contained in the table below:

Tone	Frequency (Hz)	Level (dBm)
DTMF Digit 1	697 + 1209 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 2	697 + 1336 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 3	697 + 1477 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 4	770 + 1209 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 5	770 + 1336 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 6	770 + 1477 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 7	852 + 1209 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 8	852 + 1336 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 9	852 + 1477 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit 0	941 + 1336 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit *	941 + 1209 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit #	941 + 1477 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit A	697 + 1633 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit B	770 + 1633 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit C	852 + 1633 (+/-2.0%)	-7/-9 (+/-3)
DTMF Digit D	941 + 1633 (+/-2.0%)	-7/-9 (+/-3)

Note, according to the China specification YDN065, section 8, for the DTMF tones, the allowed levels of low frequency and high frequency can be -4 ~ -23dBm, and the distinction of the levels of low frequency and high frequency can not exceed 6dBm. This activity sets -7dBm for the low frequency, and -9dBm for the high frequency.

39.12.2 Audible Tones

The following sections provide the tables that describe the audible tones in the CHINALGC toneset specified for the China market. For each tone, a format is provided to include the meaning, frequency, level and cadence information.

39.12.2.1 Idle Tone

Meaning	Silence
Frequency (Hz)	300
Level (dBm)	-
Cadence	Continuous

Note: this tone is cloned from toneset CHINA100.

39.12.2.2 Dial Tone

Meaning	A tone advising that the exchange is ready to receive call information and inviting the user to start sending call information.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	Continuous

39.12.2.3 Special Dial Tone

Meaning	A tone advising that the exchange is ready to receive call information and inviting the user to start sending call information, at the same time reminding the caller that special conditions (such as CFU is activated). are encountered.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	400 ms ON 40 ms OFF Repeated pattern

39.12.2.4 Busy Tone

Meaning	A tone advising the caller that the called party is busy.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	350 ms ON 350 ms OFF Repeated pattern

39.12.2.5 Congestion Tone

Meaning	A tone advising the caller that the groups of lines or switching equipment necessary for the setting up of the required call or for the user of a specific service are temporarily engaged.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	700 ms ON 700 ms OFF Repeated pattern

39.12.2.6 Ring Back Tone

Meaning	A tone advising the caller that the connection has been made and that a calling signal is being applied to the telephone number or service point.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	1000 ms ON 4000 ms OFF Repeated pattern

39.12.2.7 Vacant Number Tone

Meaning	A tone advising the party during a call that a toll call is waiting
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Condense	100 ms ON 100 ms OFF 100 ms ON 100 ms OFF 100 ms ON 100 ms OFF 400 ms ON 400 ms OFF Repeated pattern

39.12.2.8 Toll Break In

Meaning	A tone advising the party during a local call that the operator wants to establish a toll call to the party.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-20 (+/-3)
Cadence	200 ms ON 200 ms OFF 200 ms ON 600 ms OFF Repeated pattern

39.12.2.9 Call Waiting Tone

Meaning	A tone advising the user of the call waiting service who engaged on a talking call that another call is attempting to connect to this user.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	400 ms ON 4000 ms OFF Repeated pattern

39.12.2.10 Holding Tone (Reminder Tone)

Meaning	The subscriber on hold receives holding tone during the conference or enquiry call.
Frequency (Hz)	950 (+/-10%)
Level (dBm)	-20 (+/-3)
Cadence	400 ms ON 10000 ms OFF Repeated pattern

39.12.2.11 Howler Tone (Receiver Offhook Tone)

Meaning	Prompts the subscriber to place the receiver on-hook.
Frequency (Hz)	1400 / 2060 / 2460 / 2600 (+/-5%)
Level (dBm)	-6

Meaning	Prompts the subscriber to place the receiver on-hook.
Cadence	100 ms ON 100 ms OFF Repeated pattern

39.12.2.12 Confirmation Tone

Meaning	Indication to a subscriber controlling a supplementary service that the control procedure for access to that service or a service feature has been successfully completed and accepted.
Frequency (Hz)	450 (+/-10%)
Level (dBm)	-10 (+/-3)
Cadence	160 ms OFF 160 ms ON 160 ms OFF 320 ms ON 640 ms OFF Nonrepeated pattern

39.12.3 ADSI CAS Tone

The ADSI CAS tone specified for China market is shown in the table below:

Tone	Frequency (Hz)	Level (dBm)
ADSI CAS tone	2130 + 2750 (+/-0.5%)	-15/-15 (+/-1)

39.12.4 Test and Diagnostic Tones

The test and diagnostic tones are cloned from the toneset CHINA100:

Tone	Frequency (Hz)	Level (dBm)
Low Tone	450	-20
1004Hz Tone	1004	0
950Hz Tone	950	-20
Milliwatt	950	0

39.13 Appendix - Q00869086 FN

This is the documentation for CR: Q00869086 - CI tool for line services auto update.

Notes: In this document, both ‘option’ and ‘service’ are referring to the services that can be provided on lines through SERVORD tool.

39.13.1 Function Description

The SN07 feature “A00002755 China Line Service Compliance” introduces line services that compliant to China line services spec (YDN065). While on SN06, some lines are using non China compliance services.

So the requirement rises: in an SN06 -> SN07 upgrade, update the non China compliance services to compliance services. The CI tool is designed to achieve this.

The CI tool is named “SERVUPD”, it does not require parameters.

The SERVUPD tool uses the datafill in CEPTONCENTREX to decide which services need update. Following table list the decision logic: if the option in ‘CEPTONCENTREX option’ column is datafilled, the service listed in ‘From Service’ column is updated to those listed in ‘To Service’ column. The “Update Description” column describes the update action.

Table 4 Service Update Decision Logic

CEPTONCE NTREX option	From Service	To Service	Update Description
IWUC	WUCR	CEPT IWUC	Wake up call. - The wake up timer setting in WUCR will be transferred to IWUC.
CDIV	MSB	CEPT CDND	Make set busy. - The MSB state will be transferred to CDND.
	CFO	CEPT CDTA/ CDTO	Call forward to operator. - Since CFO can be mapped to CDTA or CDTO, according to the CFO route, it will not be updated by SERVUPD. The operator can update it manually. No update action.
	CFF	CEPT CFF	Call forward fix. - No update action.
ICT	CXR	CEPT ICT	Call transfer.

Table 4 Service Update Decision Logic

CEPTONCE NTREX option	From Service	To Service	Update Description
ICWT	CWT	CEPT ICWT	Call waiting. - Before updating, if the line has CWI, CCW, CWTACT & SCWID, they will be deleted first: the CWTACT state will be transferred to ICWT, the SCWID will be added back after ICWT added. - The ICWT_ACTIVE field will be set to default 'Y' if there was no CWTACT.
CCBS	RAG	CEPT CCBS	Ring back (call complete to busy subscriber). - If RAG is activated on a line, its setting will NOT be transferred to CCBS.
I3WC	3WC	CEPT I3WC	Three way call.
I6WC	CNF(C06)	CEPT I6WC	Six way call. - Only CNF(C06) will be updated to I6WC.

When the operator types ‘SERVUPD’, following actions will be taken:

1. Read the CEPTONCENTREX tuple of ISERVOPT, first check the MARKET field. If it is not China, prompt the error message and abort.

Following is the intended error message.

Table 5 ERROR Message

```
>ServUpd
Error:
ServUpd is for China market usage only.
If the market is China, please set the following field to CHINA, then retry:
table ISERVOPT, tuple CEPTONCENTREX, field MARKET
ServUpd not started.
```

2. If the MARKET is China, get the datafilled options in it.

Following is an example of CEPTONCENTREX.

Table 6 Datafill Example of CEPTONCENTREX in table ISERVOPT

```
SOPTSKEY SOPTSVAR
-----------------
CEPTONCENTREX CEPTONCENTREX China (SC) (WML) (ILR) (CCBS) (I3WC) (CDIV) $
```

3. Prompts to list the services that will be updated one by one, ask for the confirm from operator. (refer to Table 7 on page 960)
4. Then list all services that will be updated, also list the services that can be updated but not datafilled in CEPTONCENTREX, and wait for the confirm from operator.

Following is the intended prompt.

Table 7 Prompt Example of ServUpd

```
>SERVUPD
Update: From 3WC to CEPT I3WC, agree?
Type 'y' or 'n'
>Y
Update: From  CFO to CEPT CDTA/CDTO, agree?
Type 'y' or 'n'
>Y
Update: From  MSB to CEPT CDND, agree?
Type 'y' or 'n'
>Y
Update: From  RAG to CEPT CCBS, agree?
Type 'y' or 'n'
>Y
-----------------------------------------------------------------
Following line service update will be performed:
From 3WC  TO  CEPT I3WC
From MSB  TO  CEPT CDND
From RAG  TO  CEPT CCBS
-----------------------------------------------------------------
Warning:
Following line services can be updated but not required by user:
From 6WC  TO  CEPT 6WC
From CWT  TO  CEPT ICWT
From CXR  TO  CEPT ICT
From WUCR TO  CEPT IWUC
They will not be updated.
-----------------------------------------------------------------
Type 'Y' to start, type 'N' to abort.
>Y
```

5. If the operator types 'N', just abort the command. If the operator types 'Y', perform the service update.

The SERVORD DEO/ADO utilities will be used to perform the update. The SERVORD requirement on line state applies, lines will not be updated if the state is invalid(eg: SB).

6. During update, the result will be printed to the screen. When update finishes, report the summary.

There are four kinds of result:

— success. It is counted in the 'number of success' in summary.

— error occurred. Some options may have been deleted before error occurs, the deleted option will be printed. It is counted in the 'number of not updated' in summary.

— line state not proper. It is counted in the 'number of not updated' in summary.

— partly success: the option is updated successfully, but the option setting before update lost. It is counted in the ‘number of partly success’ in summary.

Following is the result and summary example. Could use the existing CI tool ‘RECORD’ to record the logs into a file on disk.

Table 8 Logs/Report Example of ServUpd

```
Type 'Y' to confirm, type 'N' to abort.
>Y
Services being updated:
-----------------------
LG 0 0 0 0: From 3WC TO CEPT I3WC ... success.
LG 0 0 0 1: From MSB TO CEPT CDND ... success.
......

LG 0 1 0 0: From RAG TO CEPT CCBS ... Line state is not proper, no update. Please
retry later.
LG 0 1 0 1: From RAG TO CEPT CCBS ... success.
......
LG 0 2 0 1: From MSB TO CEPT CDND ... Partly success, the service setting before
update lost.
LG 0 2 0 2: From MSB TO CEPT CDND ... Error occurred. Not updated.
            Deleted Options:
            MSB
......
```

```
ServUpd completed,
Following line services are updated:
------------------------------------------------
3WC  ->  CEPT I3WC
Total number of success lines:       300
Total number of partly success lines:0
Total number of not updated lines:   3
------------------------------------------------
MSB  ->  CEPT CDND
Total number of success lines:       125
Total number of partly success lines:0
Total number of not updated lines:   0
------------------------------------------------
RAG  ->  CEPT CCBS
Total number of success lines:       200
Total number of partly success lines:0
Total number of not updated lines:   2
```

39.13.2 Limitation

- The SERVUPD tool will be used for ONP only, it will be put in no context. The ONP team can bring it to site on tape for usage.
- Only one-way update is supported. This means, when an option is removed from the CEPTONCENTREX tuple in table ISERVOPT, the lines using this option can not be updated using ‘ServUpd’ command. For example:

ServUpd can change the RAG to CEPT CCBS, but can not change CEPT CCBS to RAG.

- The tool only uses SERVORD utilities to delete/add services on line. The service related translations, office parameters, etc. has to be deleted/added by the operator.
- When adding CEPT options to line, if the ‘assign’ action option is datafilled to be metered in table MTRFEAT, and the line has MOG option, the metering of ‘Assign’ will increase.
- When update RAG to CEPT CCBS, if the RAG is activated on the line, SERVUPD will only update RAG to CEPT CCBS, the RAG setting will NOT be transferred to CCBS to reduce the risk.

40: Functional Description (FN): A00002756

40.1 Feature name

A00002756 JAPAN TRUNK SERVICES

40.2 Description

40.2.1 Introduction

This activity migrates Japan trunk services “Notification of Time and Charge” (NTC), “Carrier Name Notification” (CNN) and “Account Code” (ACCT) from the legacy MMP product to CS2K Hybrid product IP side in ISN07. It transparently ports the functionality implemented under these MMP features onto the CS2K Hybrid IP side. “Hybrid” always means “CS2K Hybrid” within this document.

If these services are triggered by incoming IP side in hybrid, they are provided by IP side directly. On the contrary, if triggered by incoming TDM side, they are provided by legacy MMP features.

About the services provided by TDM side in hybrid, it is not the scope of this activity and please read the original MMP activities listed below.

The existing MMP NTC service was implemented by following activities:

- AR0480 Notification Of Time & Charge
- AR1344 NTC
- AR1599 Enhancement to NTC
- AR1816 Multilingual NTC
- A59017299 Japan Interconnect ISUP

The service of “Carrier Name Notification for Japan” has been provided on MMP under following activities:

- A59027517 Equal Access Carrier Name Notification
- A59034248 Carrier Name Notification for Carrier Designation Service

The “Account Code” service on MMP was originally done under following activities:

- AR2028 Account Code
- A59017299 Japan Interconnect ISUP

Also, this feature provides the following interworkings on CS2K Hybrid product IP side in ISN07:

- JI-ISUP to ETSI ISUP V1
- ETSI ISUP V1 to JI-ISUP

40.2.2 Notification of Time and Charge (NTC)

40.2.2.1 Functional Overview

Notification of Time and Charge is a service provided over JI-ISUP trunks to the Japanese domestic market.

The subscriber activates this service by using the NTC service code prior to the destination address digits. A call is registered as requesting NTC service when traversing a tuple in universal translation that has the NTC feature assigned to it. The NTC service contains two calls: original NTC call and NTC callback.

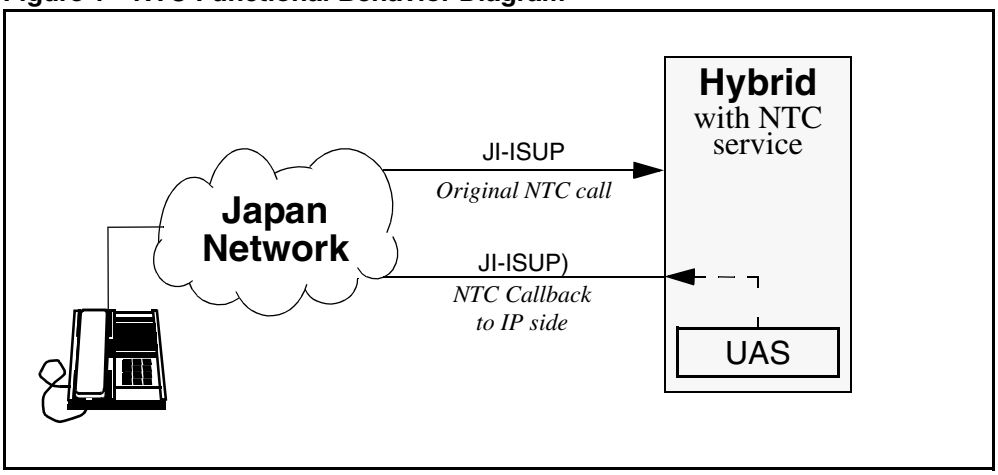
The original NTC call proceeds normally. After a successful call is answered, released and an AMA billing record is produced, NTC service calls the subscriber back using the Calling Line IDentifier (CLID) and provides an announcement indicating such information as the destination address digits, the duration of the original call and the charge amount for this service. The NTC announcement is delivered from EDRAM hardware on Hybrid TDM side. As a Hybrid switch IP side is unlikely to use EDRAM hardware, this activity will rework the feature to use the newer UAS hardware in IP side.

The NTC announcement is a custom announcement that consists of a number of simple and compound phrases. Each simple phrase has a corresponding recording on UAS. Each compound phrase is composed of 1 or simpler phrases.

NTC service is not affected by the out going agent of the original NTC call. The service works providing the interworking from JI-ISUP to the outgoing agent is available and AMA record is used for the call.

Please refer to Figure 1 ”NTC Functional Behavior Diagram”.

Figure 1 NTC Functional Behavior Diagram



40.2.2.2 Linguistic Logic

In this feature, the linguistic logic supports all of the nine languages, Japanese, English, Tagalog, Portuguese, Chinese, Korean, Thai, Spanish and Malay, supported by legacy MMP features.

Following shows the English version NTC announcement.

*This is IDC. The international call you have just made to **A** the number **B** was **C** hours **D** minutes **E** seconds long and cost **F** yen. Repeat, **C** hours, **D** minutes, **E** seconds long and cost **F** yen. Thank you for using IDC. This is a recording.*

Here:

A = Area Name

B = the number recorded by hybrid during the original call.

C = Hours quantity, range is from 1 to 277.

D = Minutes quantity, range is from 0 to 59.

E = Seconds quantity, range is from 0 to 59.

F = Yen quantity, range is from 1 to 10 065 533 yen.

40.2.2.3 Repeating/Skipping a Language during Cyclic Announcement

NTC service provides announcement in a cyclic fashion. In order to provide the subscriber with some control over NTC announcement playing, this feature

supports '*' key for repeating a language in the same cycle and '#' key for skipping to the next language.

— *skipping:* the received '#' keys are used for skipping.

Skipping does not change the playing sequence of the selected languages. This means that a '#' key stops the language currently being played immediately and starts the *next language* right after. The next language here may be the next one on the current cycle, or the first language of the next cycle if the stopped language is the last one of this cycle.

If a '#' key is received while the last language is being played during the last cycle, skipping is ignored. This is so for providing an explicit ending of the NTC service, i.e. either by a complete announcement in the last language or by subscriber disconnect.

— *repeating:* the received '*' keys are used for repeating.

A received '*' key stops the language currently being played immediately and starts to repeat the *same* language on the current cycle.

The maximal number of repeats allowed per cycle of NTC announcement is datafillable via an office parameter. If '*' keys are received beyond the maximum datafilled, the '*' keys are ignored.

Office parameter NTC_ANNC_CONTROL in table OFCVAR has two fields.

1. The first field sets the total number of cycles for NTC service. This field has a range from 1 to 8 with a default value of 2.
2. The second field sets the maximal number of repeats (i.e. '*' keys) allowed per cycle of the announcement. This field has a range from 0 to 7 with a default value of 2.

Let's say there are three languages: A, B and C. One cycle is defined as (A B C) and NTC_ANNC_CONTROL is set to (4 2), i.e. four cycles and maximum of two repeats per cycle. The entire announcement without repeating (note, skipping may be happening) is:

```
(A B C) (A B C) (A B C) (A B C)
```

If skipping occurs during the above announcement, the language sequence would still be the same. The only difference is the skipped language would be stopped (except for *C* in the last cycle above) once the '#' key is received by hybrid and the next language, which may be the next language on the current cycle or the first language on the next cycle, starts playing right after. Without skipping, each language would be played completely.

With repeating, the actual announcement may be:

```
(A A A B C) (A B B C C) (A B C) (A B B C)
```

Note that during the first cycle above, language B or C cannot be repeated any more since the only two repeats allowed per cycle is used up for language A. This means that all the '*' keys received during the playing time of B and C in this cycle are ignored.

40.2.3 Carrier Name Notification (CNN)

40.2.3.1 Functional Overview

When a JI-ISUP IAM reaches hybrid IP side, the IAM is analyzed for a number of parameters as to whether the announcement is to be played. Once hybrid decides to provide Carrier Name Notification announcement (The conditions please refer to A59034248 FN section 3.2.2 "Conditions for Feature activation"), an early ACM is sent to the calling party that serves to open a backward speech path and then the announcement is played.

Please refer to Figure 2 "CNN Call Flow for Interworking with ISUP" and Figure 3 "CNN Call Flow for interworking with SIP-T".

This service is supported in the following interworking scenarios by this activity:

- JI-ISUP -> JI-ISUP
- JI-ISUP -> IBN7 ISUP
- JI-ISUP -> ETSI ISUP V1
- JI-ISUP -> ETSI ISUP V2
- JI-ISUP -> SIP-T (JI-ISUP)
- JI-ISUP -> SIP-T (No ISUP to IMS)

Figure 2 CNN Call Flow for Interworking with ISUP

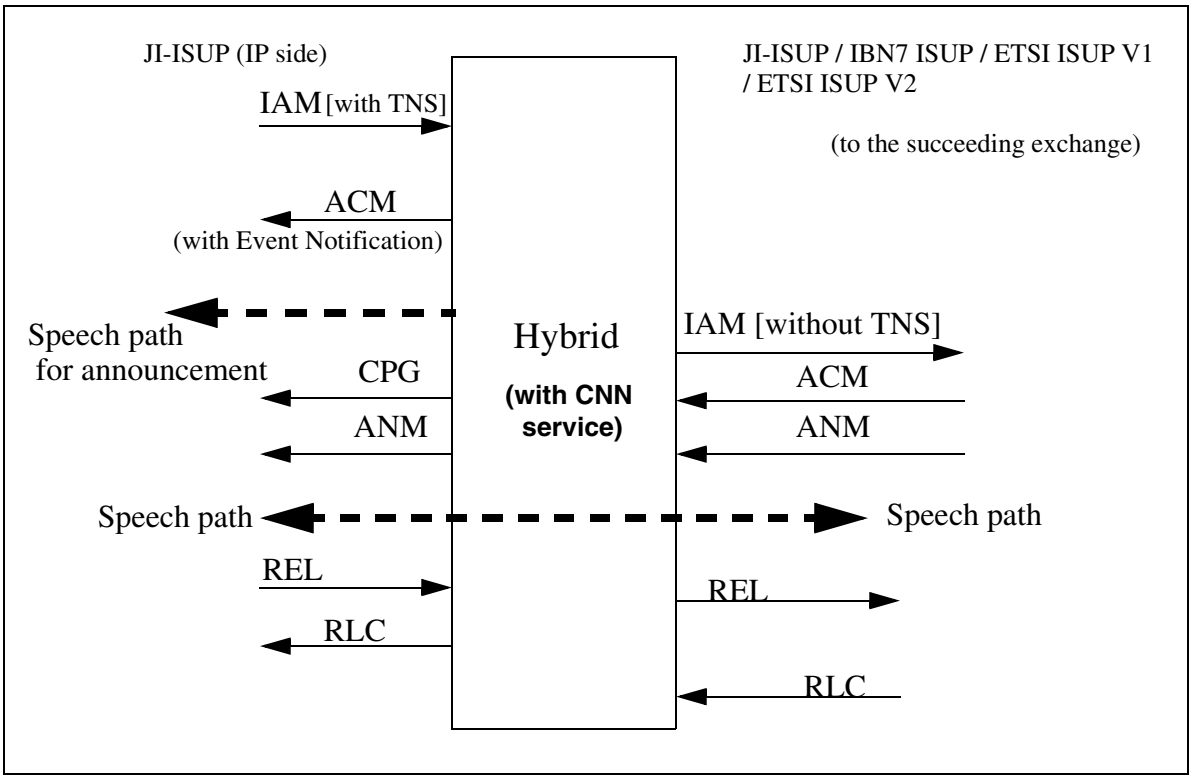
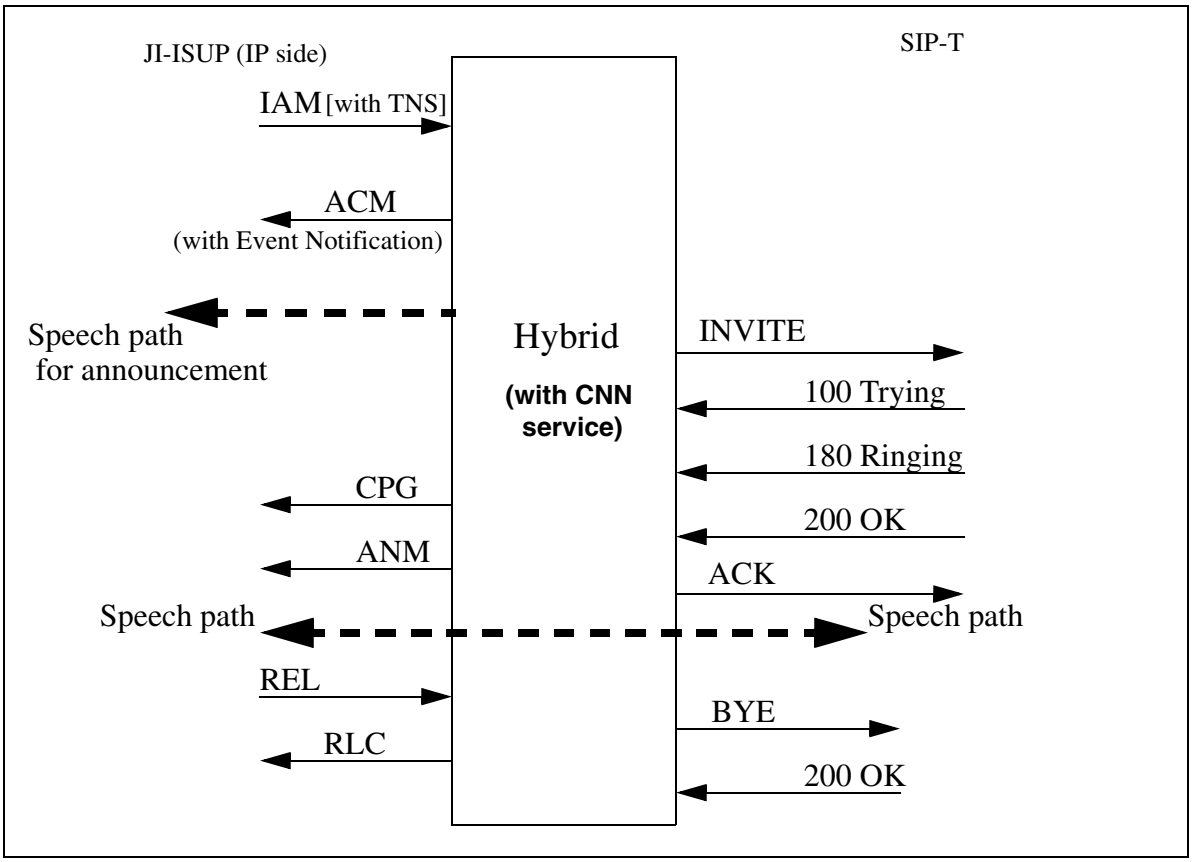


Figure 3 CNN Call Flow for interworking with SIP-T



40.2.3.2 Announcement Handling

If all conditions for feature activation are satisfied and the Network Identification Code in the TNS parameter matches with the CARRID datafill in table CARRNAME, then the announcement recorded corresponding to the announcement CLLI is played. Samples for CNN announcement datafill in ANNS & CARRNAME are shown in Figure 4 "Example datafill in table ANNS" and Figure 5 "Example datafill in table CARRNAME". In this sample, the announcement CLLI is “ANNCLLI1” and CARRID is “111111”.

Figure 4 Example datafill in table ANNS

```
ANNCLLI1 NETWK 0 0 1 STND Y 10
```

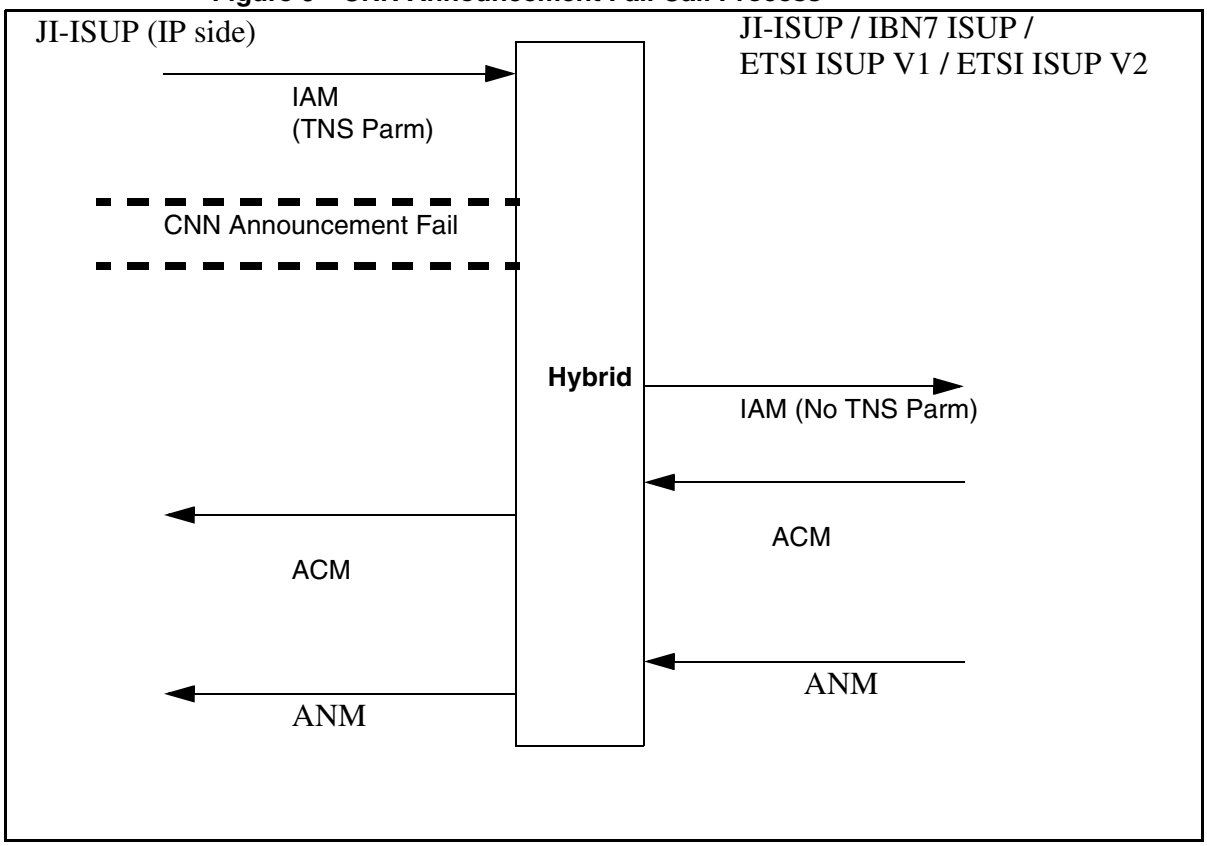
Figure 5 Example datafill in table CARRNAME

```
111111 ANNCLLLI1
```

If CNN announces fail, e.g. all ANNCLLI1 trunks are busy, the call is tandemed as a normal tandem call and the outgoing IAM doesn't contain TNS parameter. At the same time, CNN101 log is generated. For more information about CNN log, please refer to activity A59034248 FN section 3.7 "Logs". The call process of this case please refer to Figure 6 "CNN Announcement Fail Call Process".

Service → i2001

Figure 6 CNN Announcement Fail Call Process



40.2.3.3 Handling of Charge Indicator in BCI of CPG

When CNN feature is triggered, the charge indicator in the CPG is modified according to the CHGIND datafill or the CPGCGIND datafill in table XXCODE / XXHEAD.

The rule of it is shown in Table 1 ”Handling of CPGCGIND in CPG”

Table 1 Handling of CPGCGIND in CPG

CHGIND datafilled	Freedial (NOCHARGE) datafilled	CPGCGIND datafilled	Charge Indicator in CPG
Y / N	N	Y	datafilled value of CPGCGIND
Y	N	N	Datafilled value of CHGIND

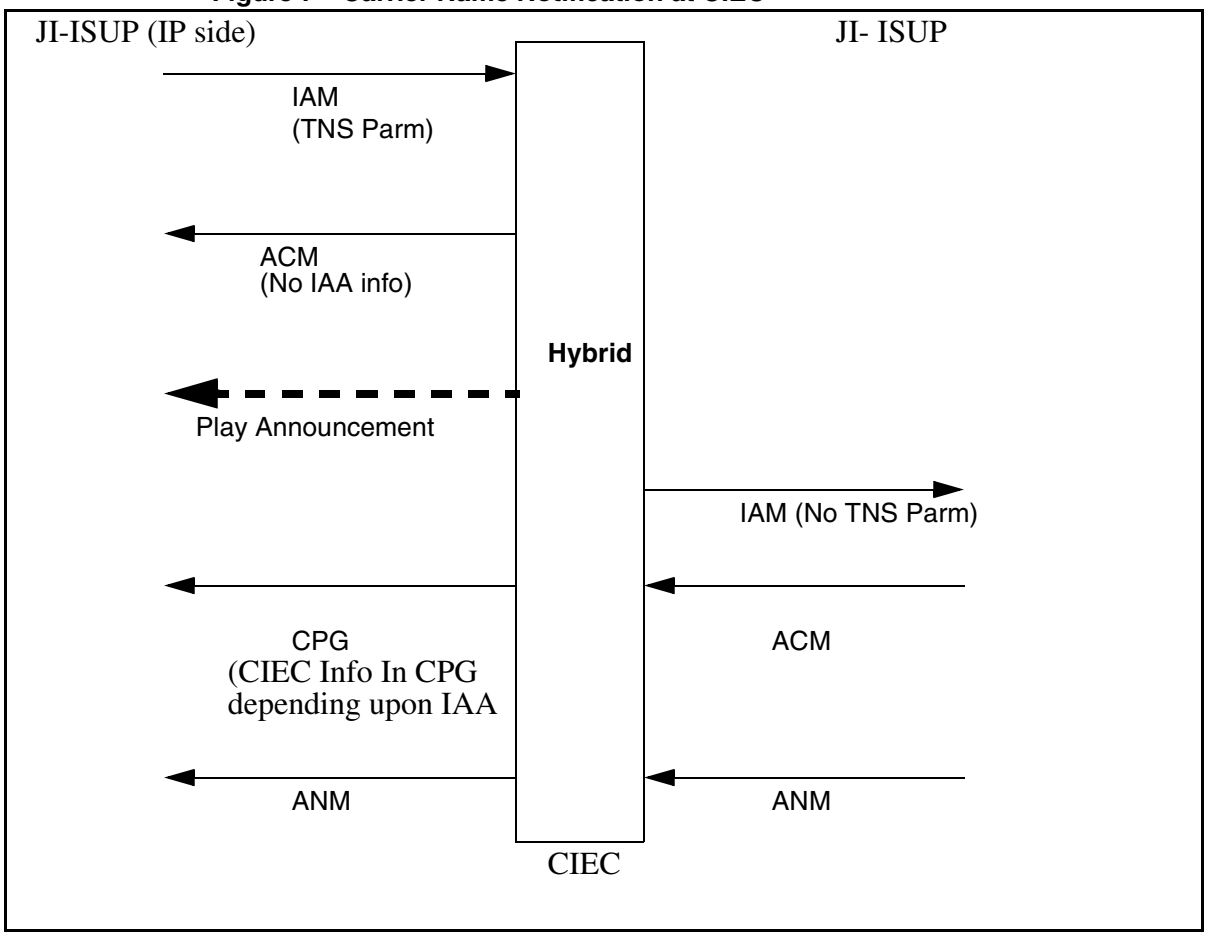
CHGIND datafilled	Freedial (NOCHARGE) datafilled	CPGCGIND datafilled	Charge Indicator in CPG
Y/N	N/Y	Y	Datafilled value of CPGCGIND
Y	N/Y	N	Datafilled value of CHGIND

40.2.3.4 Handling of IAA parameters

IAA is the abbreviation of Inter-Administration Accounting. For more information about IAA, please refer to AU2343 FN section APPENDIX A.

40.2.3.4.1 Carrier Name Notification at CIEC

Figure 7 Carrier Name Notification at CIEC



Please refer to Figure 7 ”Carrier Name Notification at CIEC”.

At hybrid that behaves as a CIEC, if an early ACM for the feature is generated, it will not contain the IAA parameters.

The IAA parameters in the incoming ACM are mapped to the CPG. The IAA parameters of the CIEC are appended to the CPG depending on the IAA logic.

The hybrid will append the CIEC info to the CPG only if all the following conditions are met: -

- the interworking is JI-ISUP to JI-ISUP,
- CIEC datafill in table IAACTRL is encountered during translation;
- all conditions for generating CIEC in IAM are met;
- the incoming ACM must contain the Carrier Info parm (#F1).
- the received TCIT indicator in the incoming IAM must be Backwards (10) or Bothways (11)

If all the above conditions are met, then the behavior depends on which of the following two conditions are met:

(1) if the last sub-block inside the received Carrier Info Parameter in the ACM is CIEC, and the received CIEC Carrier ID is NOT the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then CIEC is not updated by hybrid. On the contrary, if it is the same as TELCO_ID or SUB_TELCO_ID, then the behavior is like: -

Table 2

CarrierID sub-parm	no change
POI-CA sub-parm	no change (even if EXIT_POI_CA is datafilled)
POI-CAT sub-parm	if received, the ENTRY_POI_CAT overwrites the received one when EXIT_POI_CAT is datafilled. And the received EXIT_POI_CAT is not changed; if not received, this sub-parm is added if EXIT_POI_CAT is datafilled;

(2) if the last sub-block inside the received Carrier Info parameter in the ACM is not CIEC, then the Carrier ID in it is not be the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then the behavior is like: -

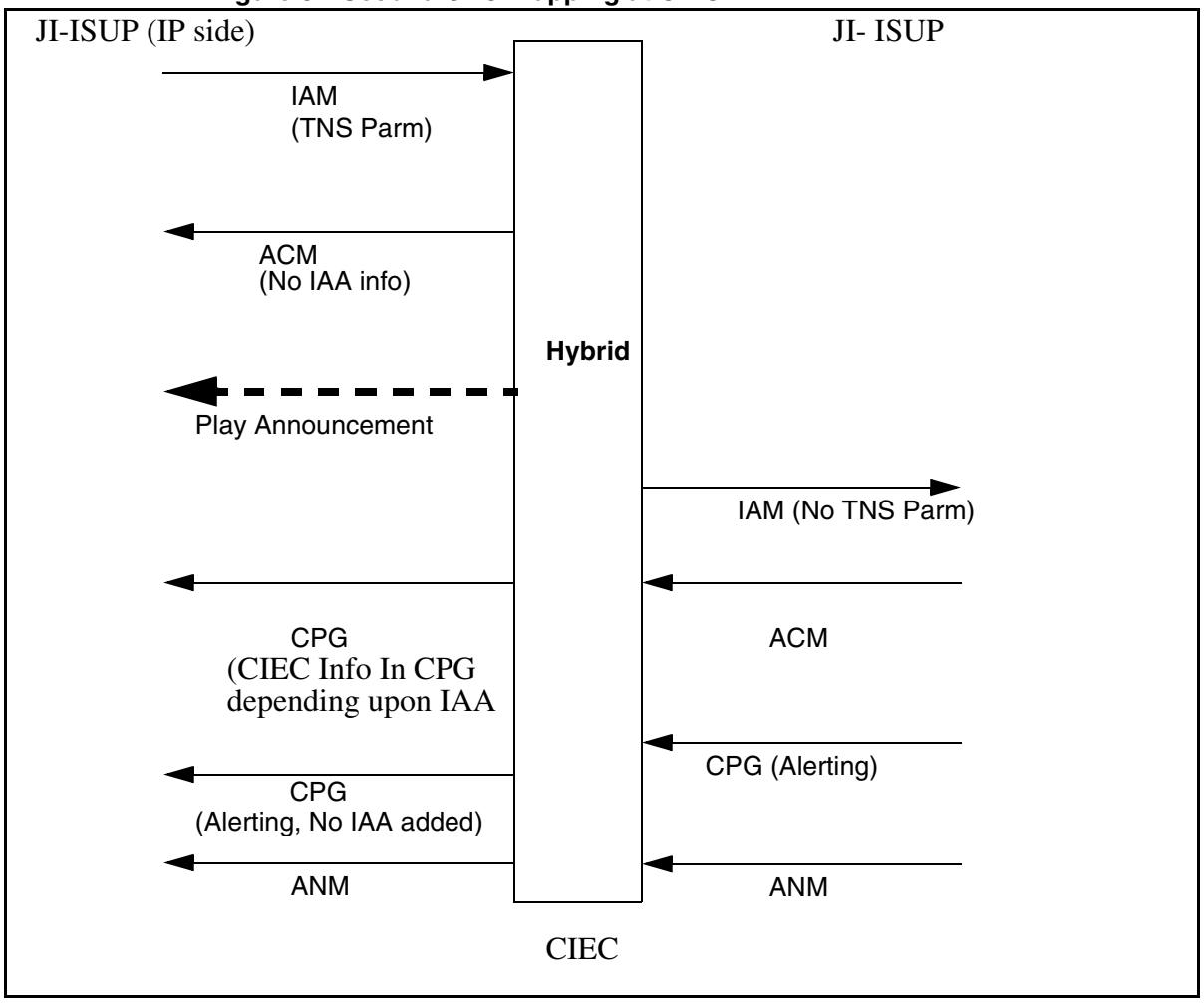
Table 3

CarrierID sub-parm	taken from ofcparm TELCO_ID or SUB_TELCO_ID datafill in table IAACTRL

POI-CA sub-parm	added only if EXIT_POI_CA is datafilled
POI-CAT sub-parm	added if (EXIT_POI_CAT) OR (EXIT_POI_CAT and E NTRY_POI_CAT) is datafilled

After the CPG with IAA is sent out, if there is an alerting CPG coming from outgoing JI-ISUP side, it is just tandemed out to incoming JI-ISUP side and no IAA is added. Please refer to Figure 8 "Second CPG mapping at CIEC".

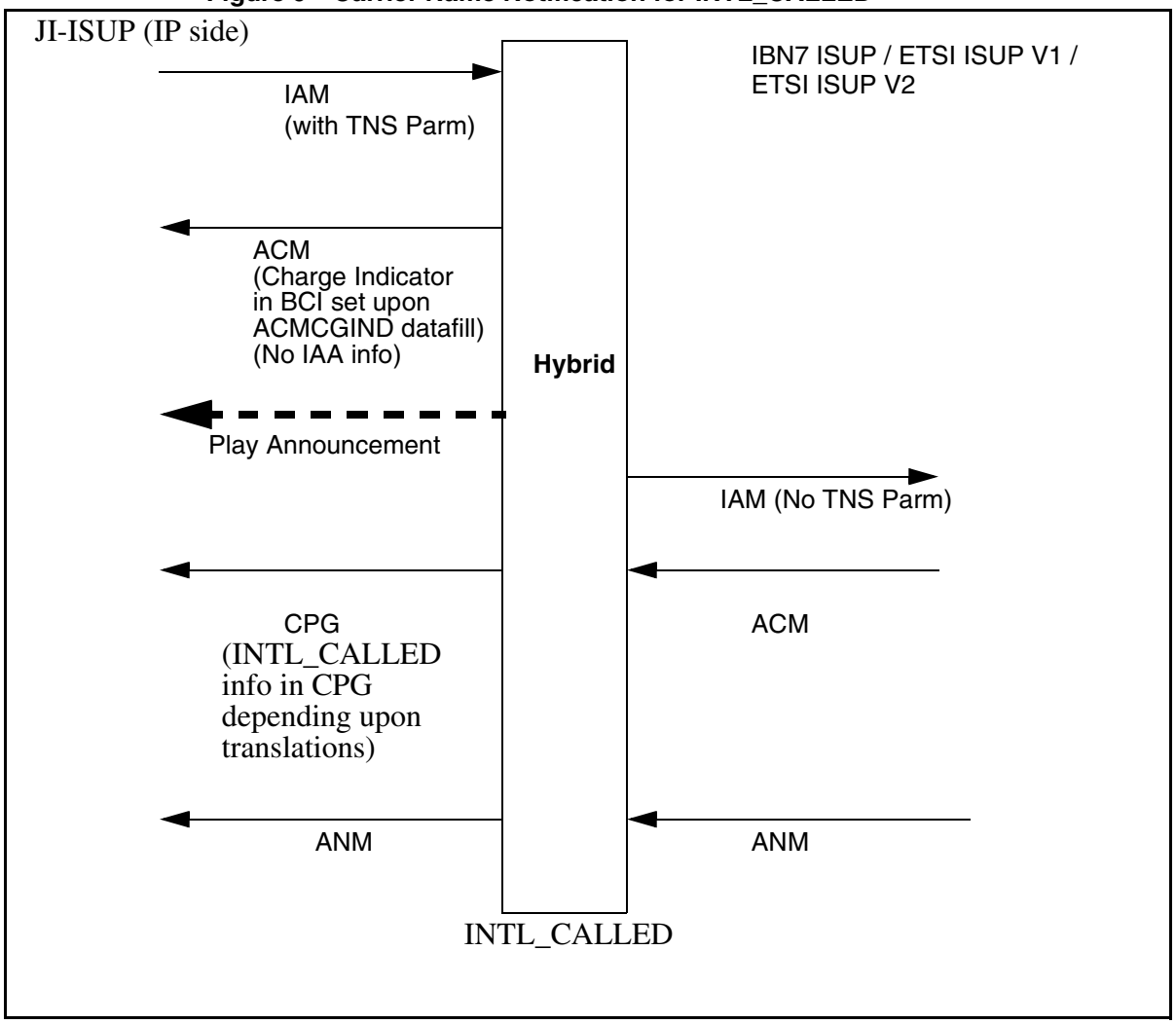
Figure 8 Second CPG mapping at CIEC



40.2.3.4.2 Carrier Name Notification at INTL_CALLED (Outbound International Calls)

Please refer to Figure 9 ”Carrier Name Notification for INTL_CALLED”.

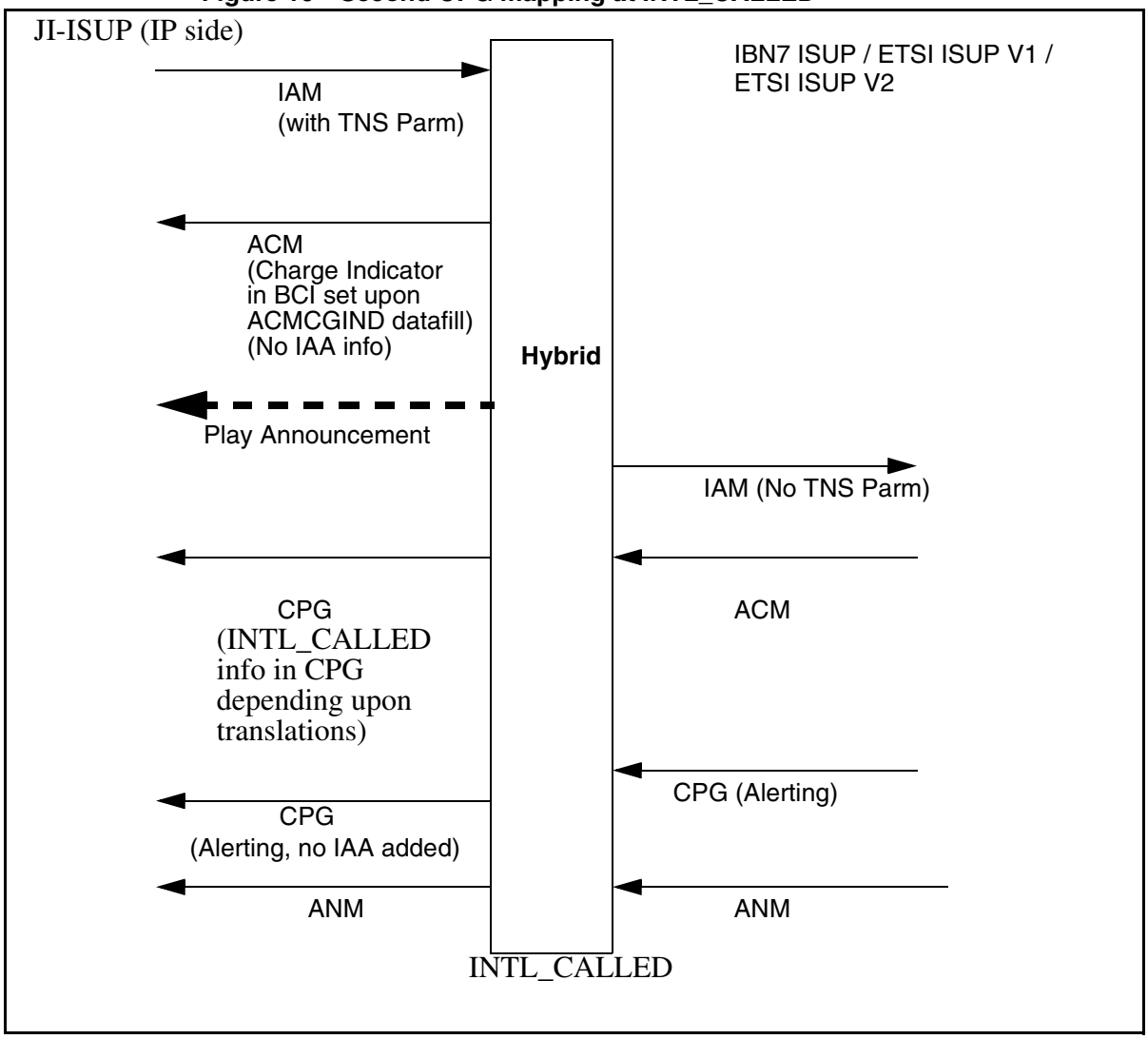
Figure 9 Carrier Name Notification for INTL_CALLED



At hybrid that behaves as an INTL_CALLED (for an international outbound call), if an early ACM for the feature is generated, it will not contain the IAA parameters. So the IAA parameters of the INTL_CALLED will be added to the CPG, i.e. the Carrier Information Parameter containing the Carrier ID.

After the CPG with IAA is sent out, if there is an alerting CPG coming from outgoing IBN7 ISUP side, it is just tandemed out to incoming JI-ISUP side and no IAA is added. Please refer to Figure 10 "Second CPG mapping at INTL_CALLED".

Figure 10 Second CPG mapping at INTL_CALLED



40.2.3.4.3 Carrier Name Notification at IEC

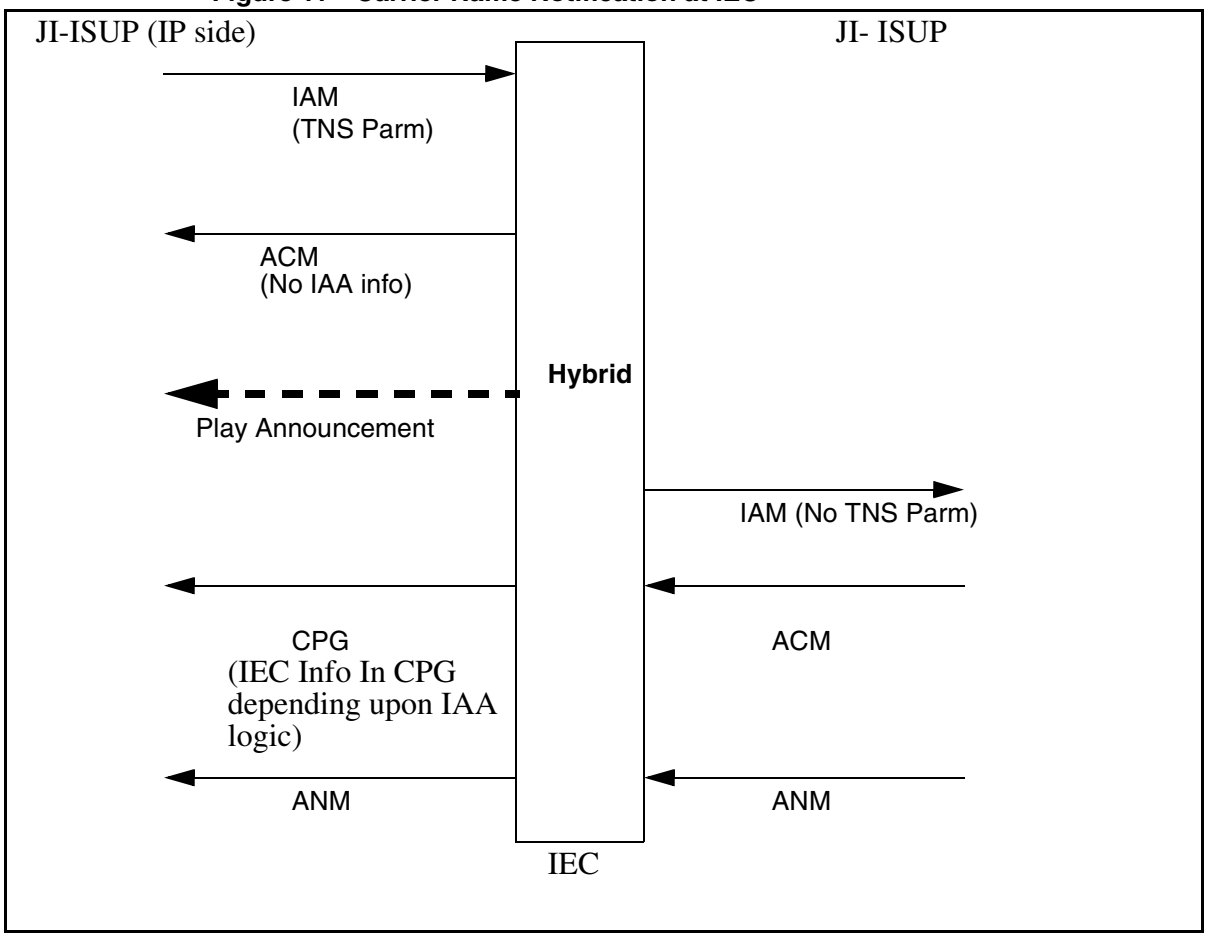
The activation of Carrier Name Notification announcement doesn't differentiate between IEC, CIEC or INTL_CALLED.

If the announcement is played at an IEC, the early ACM generated will not contain the IAA parameters.

The IAA parameters in the incoming ACM are mapped to the CPG. The IAA parameters of the IEC are appended to the CPG depending on the IAA logic.

Please refer to Figure 11 "Carrier Name Notification at IEC".

Figure 11 Carrier Name Notification at IEC



The hybrid updates the IEC carrier info parm to the CPG only if all the following conditions are met:

- the interworking is JI-ISUP to JI-ISUP;
- IEC datafill in table IAACTRL is encountered during translation;
- all conditions for generating IEC in IAM, except the condition regarding the received TCIT value, are met;
- the incoming ACM must contain the Carrier Info parm (#F1);
- the received TCIT indicator in the incoming IAM must be Backward (10) or Bothways (11);

If all the above conditions are met, then the behavior depends on which of the following two conditions are met: -

(1) if the last sub-block of the received #F1 parm is IEC, and this received IEC Carrier ID is NOT the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then IEC is not updated by hybrid. On the contrary, if it is the same as TELCO_ID or SUB_TELCO_ID, then the behavior is like:

Table 4

CarrierID sub-parm	No Change
POI-CA sub-parm	no change (even if EXIT_POI_CA is datafilled)
POI-CAT sub-parm	if received, the ENTRY_POI_CAT overwrites the received one when EXIT_POI_CAT is datafilled. And the received EXIT_POI_CAT is not changed; if not received, this sub-parm is added if EXIT_POI_CAT is datafilled;

(2) if the Carrier ID in the last sub-block of the received #F1 parm is not the same as the datafill in ofcparm TELCO_ID or the SUB_TELCO_ID datafill in table IAACTRL, then the behavior is like: -

Table 5

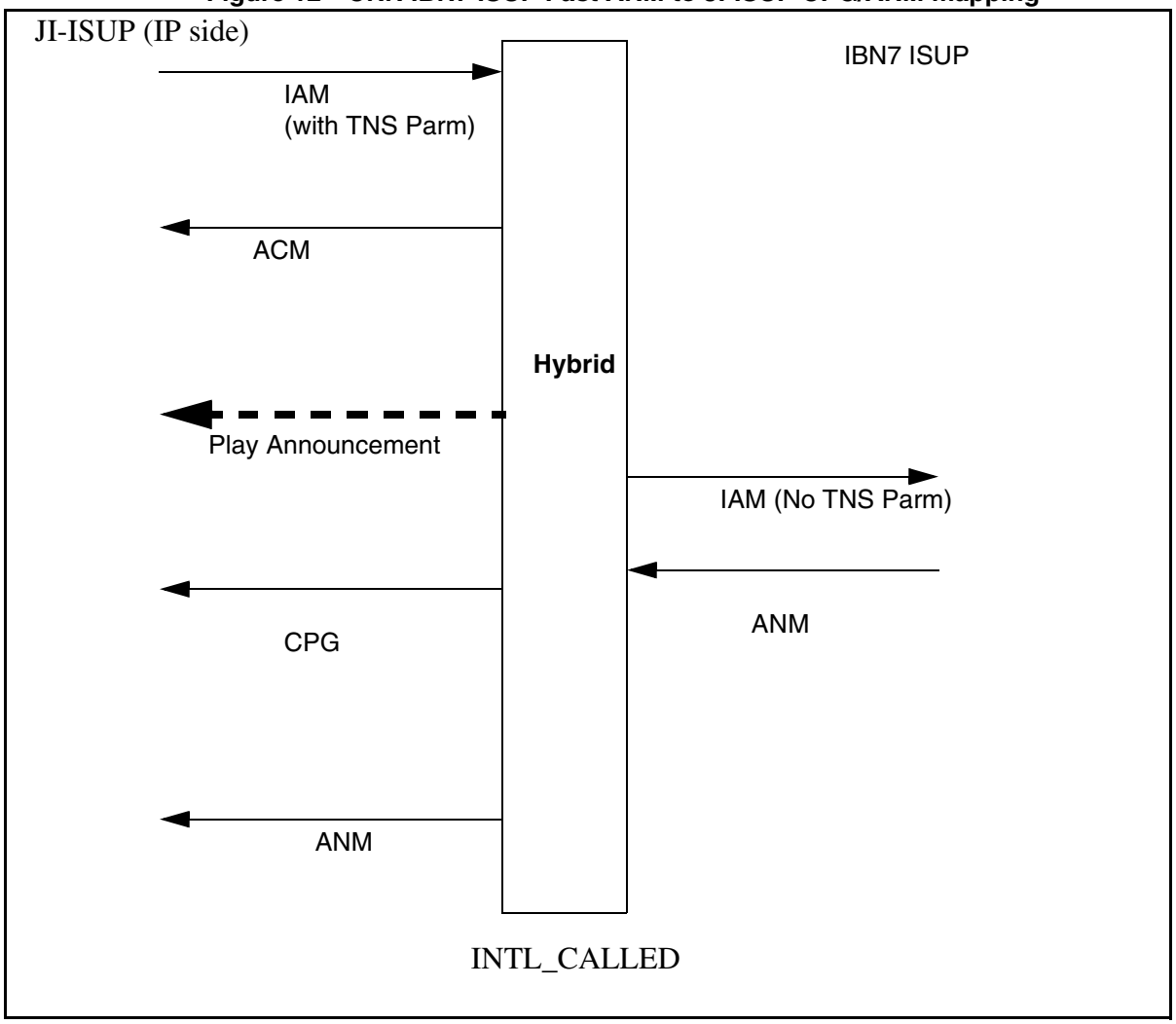
CarrierID sub-parm	taken from ofcparm TELCO_ID or SUB_TELCO_ID datafill in table IAACTRL
POI-CA sub-parm	added only if EXIT_POI_CA is datafilled
POI-CAT sub-parm	added if (EXIT_POI_CAT) OR (EXIT_POI_CAT and E NTRY_POI_CAT) is datafilled

40.2.3.5 Handling IBN7 ISUP Fast ANM

IBN7 ISUP fast ANM to JI-ISUP ACM/ANM mapping is enhanced to JI-ISUP CPG/ANM mapping. The call flow please refers to Figure 12 ”CNN IBN7 ISUP Fast ANM to JI-ISUP CPG/ANM mapping” .

If the fast ANM with no charge and ANM (NOCHG) mapping feature is turned off, ANM is just mapped to CPG and no ANM is sent out. The IAA parameters of the INTL_CALLED exchange will be added to CPG. Except this, the mapping is not impacted.

Figure 12 CNN IBN7 ISUP Fast ANM to JI-ISUP CPG/ANM mapping

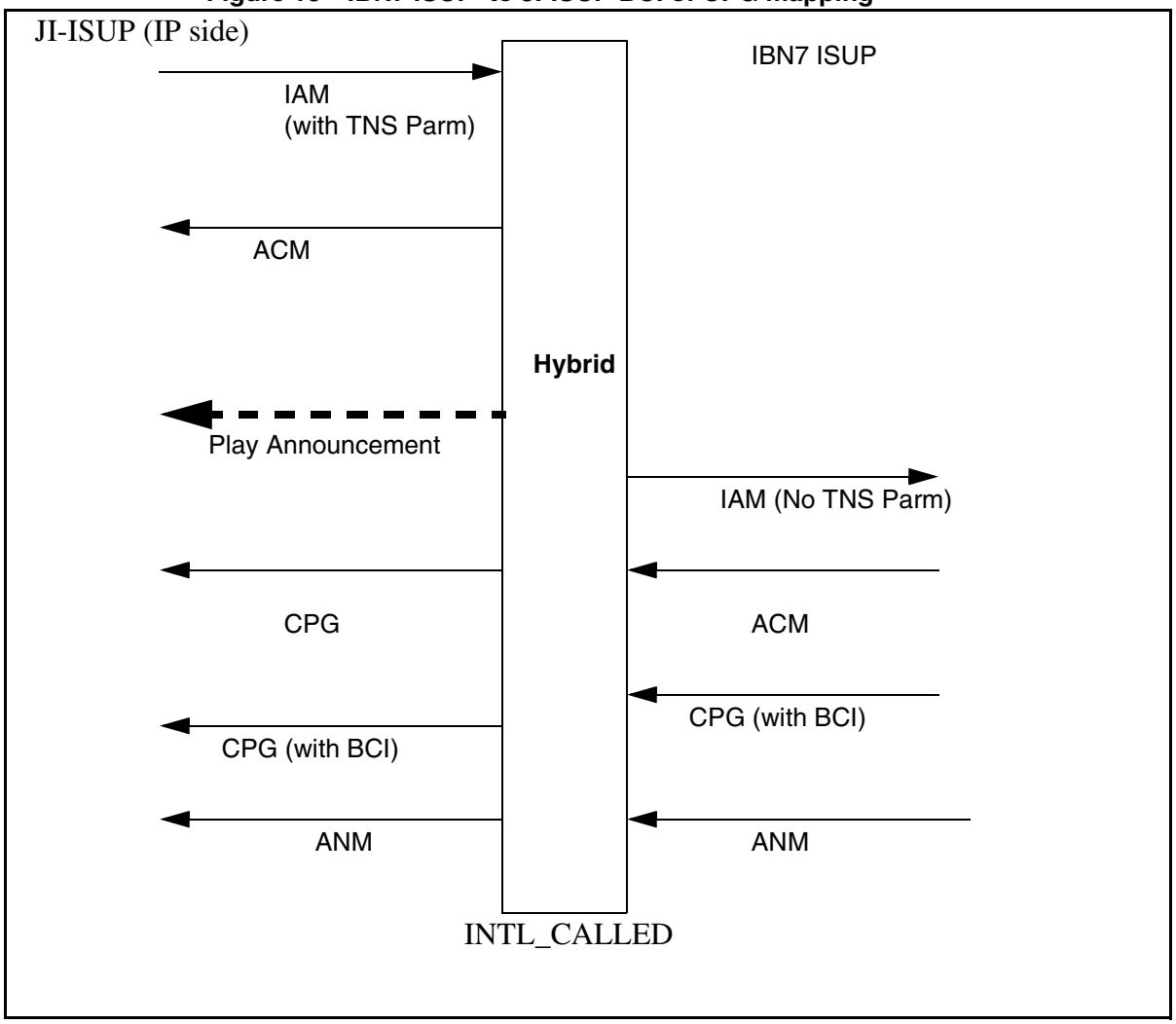


40.2.3.6 IBN7 ISUP to JI-ISUP BCI of CPG Mapping

After the first CPG is sent back to JI-ISUP side, if there is a CPG with BCI is received from IBN7 ISUP side, it is mapped to CPG which has BCI in JI-ISUP side. The BCI mapping rule is the same as BCI of ACM to BCI of CPG mapping. The rule please refers to RS section of A59017299 table 52 “Parameter Mapping - ANSI7+ ISUP ACM to JI-ISUP ACM”.

Please refer to Figure 13 "IBN7 ISUP to JI-ISUP BCI of CPG mapping".

Figure 13 IBN7 ISUP to JI-ISUP BCI of CPG mapping



40.2.4 Account Code (ACCT)

40.2.4.1 Functional Overview

"Account Code" service enables the subscriber to enter an account code during the call setup in order to classify the call on the customer's bill.

The hybrid checks the customer group (CUSTGRP) and the network class of service (NCOS) to see if an account code is required on this call. If it is, the hybrid sends back second dial tone or announcement to prompt the subscriber to enter an account code. The hybrid receives the account code digits as DTMF tones over the voice path.

When entering the account code, the subscriber has the option to enter the reset digit (*). This causes all account code digits entered by the subscriber during the present stage of dialing to be ignored. Accompanying the '*' is a reset tone, ~~of datafillable duration,~~ to prompt the subscriber to begin re-entering the required digits where the first digit dialed breaks the reset tone.

Once the account code digits are entered, the hybrid checks to see if the required number of digits has been entered and the call continues. The entered account code digits will be contained in the AMA billing record.

If the subscriber enters the hash (#) during the dialing phase it is treated as end of dialing. At this point, if the minimum required number of digits has been collected, the call proceeds to the next phase of call processing.

ACCT is supported in following interworking scenarios on hybrid by this activity:

- JI-ISUP -> JI-ISUP
- JI-ISUP -> IBN7 ISUP
- JI-ISUP -> ETSI ISUP V1
- JI-ISUP -> ETSI ISUP V2
- JI-ISUP -> SIP-T (JI-ISUP)
- JI-ISUP -> SIP-T (No ISUP to IMS)

Please refers to Figure 14 "ACCT Interworking with ISUP Functional Behavior Diagram" and Figure 15 "ACCT Interworking with SIP-T Functional Behavior Diagram".

Figure 14 ACCT Interworking with ISUP Functional Behavior Diagram

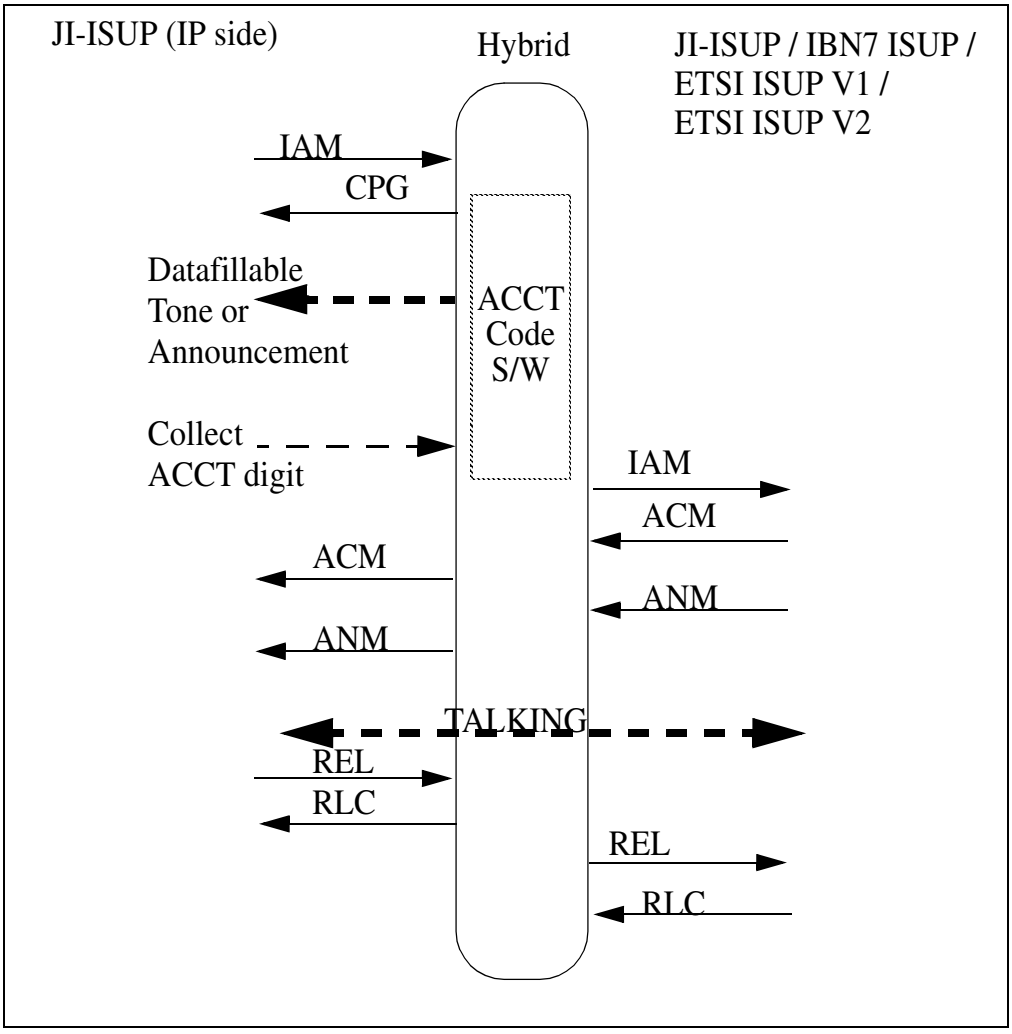
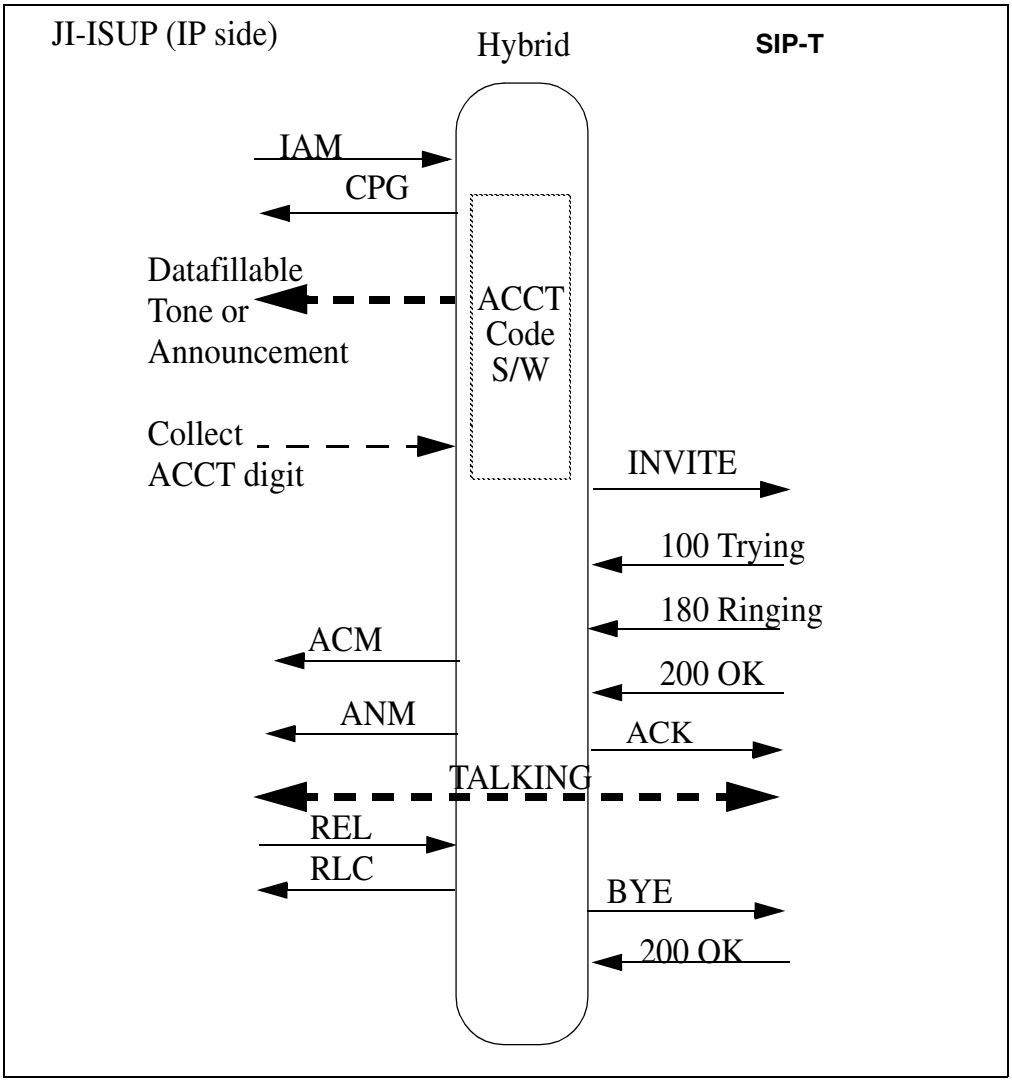


Figure 15 ACCT Interworking with SIP-T Functional Behavior Diagram



40.2.4.2 Reset Tone

When entering the account code, the subscriber has the option to enter the reset digit (*). This causes all account code digits entered by the subscriber during the present stage of dialing to be ignored and “Reset tone” is played. This tone is stopped when first digit is received or reset tone duration is time out.

~~The reset tone duration is controlled by the office parameter RESET_TONE_DURATION_160MS in table OFCVAR.~~

~~For JI-ISUP or IBN7 ISUP to account code calls, the maximum reset tone duration is 24 seconds, even if datafill represents a larger value.~~

The specification of reset tone is shown in Table 6 ”Specification of Reset tone”.

Table 6 Specification of Reset tone

Tone	Single Frequency	Cadence	Duration	Level
Reset Tone (for reset of the digit collection)	400 Hz	Constant	~~Datafillable~~ (0.5 second)	-16 dBmO +/-0.5 dB

40.2.4.3 Tone/Announcement Handling

The JI-ISUP agent, on receipt of the first digit, handles the tone/announcement in the following fashion:

- 0 - 9, ‘*’ - Tone/Announcement stopped
- ‘#’ - Tone stopped/Announcement continues

40.2.4.4 Effect On Permanent Signal Timer

If digit 0 through 9 is entered as a first digit then the permanent signal timer is stopped, and the interdigit timer is used to collect the remaining digits.

If `*' or `#' is entered as the first digit the handling of the permanent signal timer is shown in Table 7 ”Account Code Handling of First Digit” .

Table 7 Account Code Handling of First Digit

Digit Entered	Perm Signal Timer
* (asterisk)	restarted
#(octothorpe)	restarted

40.2.5 Interworking between JI-ISUP and ETSI ISUP V1

Following interworkings are provided in this feature:

- JI-ISUP (NATL) to ETSI ISUP V1 (INTL)
- ETSI ISUP V1 (INTL) to JI-ISUP (NATL)

Because ETSI ISUP V1 trunk is an international trunk which is datafilled as INTL in table TRKGRP, and JI-ISUP trunk is a national trunk which is datafilled as NATL in table TRKGRP, the gateway supporting the interworking is regarded as an international gateway.

In this feature, the message and parameter mappings for above interworkings in the international gateway is handled based on the Q.767 specification (Application of CCITT ISUP for international ISDN interconnectios). All of messages and parameters which are not supported in Q.767 are not supported in this feature.

Detail mappings are described in Appendix B.

40.3 Hardware Requirements or Dependencies

Announcement hardware UAS needs to be present in Hybrid.

40.4 Software Requirements or Dependencies

. N/A

40.5 Limitations and restrictions

. N/A

40.6 Interactions

Due to this activity is a migration, we don’t change any code about interaction. So all the interactions are the same as the legacy MMP features.

For more information about NTC, please refer to original documents in AR0480, AR1344, AR1599, AR1816 and A59017299.

For more information about CNN, please refer to original documents in A59027517 and A59034248.

For a detailed description about ACCT, please refer to activities AR2028 and A59017299.

40.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	N/A

User Interface N/A

Element Management N/A

Security N/A

Service Order N/A

Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with "N/A" if these sections do not apply to this functionality.

Realtime N/A

Engineering Information N/A

40.8 Glossary

Term	Description
ACCT	Account Code
ACM	Address Complete Message
ANM	Answer Message
BLO	Blocking Message
BLA	Blocking Acknowledgement Message
CIEC	Chosen Intermediate Exchange Carrier
CNN	Carrier Name Notification
CPG	Call Progress Message
CSM	Channel Supervision Message (CallP)
DMS	Digital Multiplex System
DT	Dial Tone
ENTRY_POI_CA	Entry Point of Interconnect - Charge Area
ENTRY_POI_CAT	Entry Point of Interconnect - Category
EXIT_POI_CA	Exit Point of Interconnect - Charge Area

Term	Description
EXIT_POI_CAT	Exit Point of Interconnect - Category
IAA	Inter Administration Accounting
IAM	Initial Address Message
IEC	Intermediate Exchange Carrier
INTL_CALLED	International Called Carrier
JI-ISUP	Japan Interconnect ISUP
MCMP	Media Controller Messaging Protocol
MGCP	Media Gateway Controller Protocol
MMP	Multiple Market Platform
MTM	Maintenance Trunk Module
NCCI ISUP	New Common Carrier Interface ISUP
NTC	Notification of Time and Charge
OLEC	Originating Local Exchange Carrier
POI	Point of Interconnect
PVG	Passport Voice Gateway
RBT	Ring Back Tone
REL	Release Message
RLC	Release Complete
TCIT	Transit Carrier Indicator
TLEC	Terminating Local Exchange Carrier
TLC	Test Line Call
TMR	Transmission Medium Requirement
TNS	Transit Network Selection
TPT	Terminal Processing Task (CallP)
UAS	Universal Audio Server
UBL	Unblocking Message

Term	Description
UBA	Unblocking Acknowledgement Message
UUI	User to User Information
UUInd	User to User Indicator

40.9 Reference

[1] AR0480 Notification Of Time & Charge

[2] AR1344 NTC

[3] AR1599 Enhancement to NTC

[4] AR1816 Multilingual NTC

[5] A19013546 Announcement Provisioning

[6] A59017299 Japan Interconnect ISUP

[7] Simcoe, Chris. International Succession Japan NTC. Nov 2001. http://snarch.us.nortel.com/files/Architecture%20Areas/Solutions/VToIP/Solution%20Checklist/SN05/International/Information/Japan%20NTC%20on%20CS2000%20v0.1.zip

[8] A59027517 Equal Access Carrier Name Notification

[9] A59034248 Japan Interconnect ISUP Carrier Name Notification Feature for Carrier Designation

[10] A59040192 Carrier Name Notification for Japan

[11] AR2028 original account code feature documentation.

[12] A59017299 Japan Interconnect ISUP

[13] A59040239 Japan Account Code service.

[14] AU2343 Inter-Administration Accounting for International Carriers

40.10 Appendix A: Datafill Sample

```
%% Notification of Time and Charge (NTC)
%% For detail datafill of NTC, firstly please refer to features AR1344, AR1599,
```

```
%% AR1816, A59017299 and A19013564.

%% UAS must be provisioned to support variable announcements for 9 languages used
%% by NTC service

%% For AMA billing

TABLE OFCENG
CDR_FORMAT                CDR_NIL_FORMAT
CDR_ENABLE_LOG_ALL        N
UNIVERSAL_AMA_BILLING     Y
ALLOC_UNIV_EXT_BLK        Y


TABLE OFCOPT
LAMA_OFFICE               Y
SMDR_OFFICE               N


TABLE AMAOPTS
LOGAMA   ON


TABLE CRSFMT
AMA     BCFMT         N   NIL_FM      N        N        0
SMDR   SMDRFMT        N   NIL_FM      N        N        0


SOC -> select group rbil
    -> assign state idle to RBIL0014
    -> quit



%% For announcement

TABLE CLLI
NTCCHN   195       10                      NTC_CHINESE


TABLE ANNS
NTCCHN    ALL      25        0      1        NTC    10  NTC_CHN


TABLE ANNMEMS
NTCCHN    0      UAS AUD 0 AUD 11


TABLE ANNPHLST
NTCCHN 5 NTCCHMAN1 $


TABLE ANNAUDID
NTCCHMAN1 6000



%% For Japan Market
TABLE OFCENG
MARKET_OF_OFFICE JAPAN
```

```
%% For NTC feature triggering

TABLE OFCVAR
NTC_XLATIONS FA NTCFTR
NTC_REATTEMPTS   0
NTC_ANNC_CONTROL 2 2


TABLE PXCODE
GDNTLXLA  062 062 FEATINFO NTC DUR_ADJ 1 $ 3 7 17 PX GDNTLXLA


TABLE NTCLANGS
DFLT1       5          CHINESE_NTC_ANNOUCEMENT


TABLE DNSCRN


TABLE AREANAME


TABLE FAHEAD
NTCFTR SDFLT NODFOP NOCON F
NTCRTE SDFLT NODFOP NOCON F


TABLE FACODE
NTCFTR 0 9 DMOD INSRT 062 XLT FA NTCRTE $
NTCRTE 062 062 RTE PF 3 DEST 2 $


TABLE FARTE
NTCRTE 2 S JIISUP2K


TABLE CCGROUPS
CHN


TABLE CC2GROUP
602 CHN
9 CHN
8 CHN
7 CHN
6 CHN


TABLE DAYOFWK
MON WD
TUE WD
WED WD
THU WD
FRI WD
SAT WD
SUN WD


TABLE TODCHG
CHN WD D D D
```

```
CHN D 30 20 50 40 60 0 $


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% Carrier Name Notification (CNN)

TABLE ANNS
JIANNS NETWK 0 0 1 STND Y 10


TABLE ANNMEMS
JIANNS 0 UAS AUD 0 AUD 1


TABLE ANNPHLST
CNN 0 (ANN1) $


TABLE OFCENG
CARRNAME_ANNC Y


TABLE OFCVAR
ACTIVATE_OMEF N


TABLE CARRNAME
111111 JIANNS


TABLE IAACTRL
60 INTL_CALLED $
50 TLEC $
40 IEC (TCIT NOTSENT) (ENTRY_POI_CAT LEVEL_2) (EXIT_POI_CAT LEVEL_1) (ENTRY_POI_CA
VALUE 1234) (EXIT_POI_CA VALUE 5555) $
30 CIEC (SUB_TELCO_ID 6666) $


TABLE PXCODE
GDNTXLA2 872 872 RTE (PF 3) (MM 3 19) (DEST 870) (CARRANNC) (IAA 30) $


TABLE PXHEAD
GDNTXLA2 DFLT FEATINFO CALLCHAR (CPGCGIND CI_CHARGE)$ 0 6 22 PX GDNTXLA2 NODFOP
NOCON STD


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% Account Code (ACCT)

TABLE CUSTHEAD
PRADEFAULT PRAXLA NDGT NIL (VACTRMT 0) (EXTNCOS 0) (ACCT 4 N N N N) (SUPERCNF )
(ACR ACCT 1) (ACRANN ACCTANNC) $


TABLE NCOS
PRADEFAULT 0 PRAD 0 0 (ACR N) $


TABLE IBNXLA
PRAXLA 441 NET Y Y 0 N CSDIG N Y DOD N CSIDXA CSGRPA CS_NIL NONE $


TABLE ISERVOPT
```

```
ACCTCODE ACCTCODE Y


TABLE OFCVAR
DIG_COL_MAX_RESETS 3
RESET_TONE_DURATION_160MS 3


TABLE: OFCENG
LN_PERM_SIG_TIME 125
LN_SHORT_PARTIAL_DIAL_TIME 25


TABLE IBNTREAT
PRADEFAULT 1 N S FAILACCT


TABLE AMAOPTS
CDAR ON
TRMTID_CAPTURE ON
```

40.11 Appendix B: Mappings between JI-ISUP and ETSI ISUP V1

40.11.1 JI-ISUP to ETSI ISUP V1 Interworking

Table 8 JI-ISUP to ETSI ISUP V1 Message Mappings

JI-ISUP Messages	Trigger Direction (Table reference)	ETSI ISUP V1 Messages
IAM	=> (Table 9)	IAM
ACM	<= (Table 11)	ACM
ANM	<= (Table 13)	ANM
ACM ANM	<= (Table 13)	CON
REL	=> (Table 14)	REL
RLC	<=	No trigger
SUS/RES	<=	SUS/RES

Table 8 JI-ISUP to ETSI ISUP V1 Message Mappings

JI-ISUP Messages	Trigger Direction (Table reference)	ETSI ISUP V1 Messages
REL	<= (Table 15)	REL
No trigger	=>	RLC
CPG	<= (Table 16)	CPG

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Nature of Connection	**Satellite Indicator**	0 0: No satellite cct. in connection	=>	0 0: No Satellite cct.	**Satellite Indicator[a]**	**Nature of Connection**
		0 1: One satellite cct. in connection.		0 1: One satellite cct.		
		1 0: Two satellite cct. in connection.		1 0: Two satellite cct.		
		1 1: Spare				
	Continuity Check Indicator	00 - continuity check not required	=>	00 - continuity check not required	**Continuity Check Indicator[a]**	
		01 - continuity check required		10 - continuity check performed on a previous circuit		
		10 - continuity check performed on a previous circuit				
		11 - spare		00 - continuity check not required		
	Echo Control Device Indicator	0 - outgoing half echo control device not included	=>	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**Echo Control Device Indicator**	
		1 - outgoing half echo control device included	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Forward Call Indicator	**National/ International Call Indicator**	0 - call to be treated as a national call	=>	Value based on the settings of CLASS field in translations	**National/ International Call Indicator**	**Forward Call Indicator**
		1 - call to be treated as an international call	=>	1 - call to be treated as an international call		
	End-to-End Method Indicator	00 - no end-to-end method available	=>	00 - no end-to-end method available	**End-to-End Method Indicator**	
		01-11 spare	=>			
	Interworking Indicator	0 - no interworking encountered	=>	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	=>	1 - interworking encountered		
	End-to-End Information Indicator	0 - no end-to-end information available	=>	0 - no end-to-end information available	**End-to-End Information Indicator**	
		1 - spare	=>			
	ISDN User Part Indicator	0 - ISDN user part not used all the way	=>	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	
		1 - ISDN user part used all the way	=>	1 - ISDN user part used all the way		
	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	=>	Please refer to "Table 10 ISUP Preference Indicator Parameter Coding" on page 1002.	**ISDN User Part Preference Indicator[a]**	
		01 - ISDN user part not required all the way	=>			
		10 - ISDN user part required all the way	=>			
		11 - spare	=>	Release the call.		
	ISDN Access Indicator	0 - origination access non-ISDN	=>	0 - origination access non-ISDN	**ISDN Access Indicator**	
		1 - origination access ISDN	=>	1 - origination access ISDN		
	SCCP Method Indicator	00 - no indication	=>	00 - no indication	**SCCP Method Indicator**	
		01-11 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party category		00000000 - CPC unknown		00001010 - ordinary calling subscriber	**Calling Party category**	
		00000001 - spare 00000010 - spare 00000011 - spare 00000100 - spare 00000101 - spare	=>	00000000 - CPC unknown		
		0000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement 00001001 - national operator desk	=>	00001010 - ordinary calling subscriber		
		00001010 - ordinary calling subscriber	=>	00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority	=>	00000000 - CPC unknown		
		00001100 - data call	=>	00000000 - CPC unknown		
		00001101 - test call	=>	00001101 - test call		
		00001111 - payphone	=>	00001111 - payphone		
		00010000-11110000 spare	=>	00001010 - ordinary calling subscriber		
		11110001-11111110 reserved for national use 11111111 - spare	=>	00001010 - ordinary calling subscriber		

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Transmission Medium Requirement		00000000 - Speech	=>	00000000 - speech	**User Services Information**	
		00000001 - spare	=>	Call is released.		
		00000010 - 64kbit/s Unrestricted	=>	00000010 - 64kbit/s Unrestricted		
		00000011 - 3.1 kHz Audio	=>	00000011 - 3.1 kHz Audio		
		00000100 - Alt speech	=>	Call is released.		
		00000101 - Alt 64K	=>			
		00000110 - 64K pref	=>			
		00000111 - spare	=>			
		00001000 - 384kbit/s unrestricted	=>			
		00001001-11111111 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	0 - even number of address signals	**Odd/Even Indicator**	**Called Party Number**[b]
		1 - odd number of address signals	=>	1 - odd number of address signals		
	Nature of Address Indicator	0000000 - spare	=>	Release the call	**Nature of Address Indicator**	
		0000001 - subscriber's number	=>			
		0000010 - reserved for national use	=>			
		0000011 - National number	=>	0000011 - National number		
		0000100 - International number	=>	Release the call		
		0000101-1101111 spare	=>			
		1110000-1111101 reserved for national use	=>			
		1111110 - peculiar number of network	=>	0000011 - National number		
		1111111 - spare	=>	Release the call		
	Internal Network Number Indicator	0 - routing to an internal network number allowed	=>	0 - routing to an internal network number allowed	**Internal Network Number Indicator**	
		1 - routing to an internal network number not allowed	=>			
	Numbering Plan Indicator	000 - spare	=>	001 - ISDN numbering plan (default) (datafilled as ALL_NPI in table TRKSGRP of both trks)	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>			
		010-111 spare	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Called Party Number**
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1111 - ST	=>	Treatment is set and call is released if these values are received.		
		1010 - spare	=>			
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	Set as required	**Odd/Even Indicator**	**Calling Party Number**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000000 - spare	=>	0000011 - National number	**Nature of Address Indicator**	
		0000001 - subscriber's number	=>			
		0000010 - reserved for national use	=>			
		0000011 - National number	=>			
		0000100 - International number	=>			
		0000101-1101111 spare	=>			
		1110000-1111101 reserved for national use	=>			
		1111110 - peculiar number of network	=>			
		1111111 - spare	=>			
	Calling Party Number Incomplete Indicator	0 - complete	=>	0 - complete	**Calling Party Number Incomplete Indicator**	
		1 - incomplete	=>			

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Numbering Plan Indicator**	000 - spare	=>	CGPN is discarded	**Numbering Plan Indicator**	**Calling Party Number**
		001 - ISDN numbering plan	=>	001 - ISDN numbering plan		
		010-111 spare	=>	CGPN is discarded		
	Address Presentation Restricted Indicator	00 - presentation allowed	=>	00 - presentation allowed	**Address Presentation Restricted Indicator**	
		01 - presentation restricted	=>	01 - presentation restricted		
		10 - address not available	=>	00 - presentation allowed		
		11 - spare	=>			
	Screening Indicator	00 - spare	=>	01 - user provided, verified and passed	**Screening Indicator**	
		01 - user provided, verified and passed	=>			
		10 - reserved	=>			
		11 - network provided	=>	11 - network provided		

Table 9 Parameter Mapping - JI-ISUP IAM to ETSI ISUP V1 IAM

		JI-ISUP IAM	dir	ETSI ISUP V1 IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Calling Party Number**[b]
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1010 - spare	=>	Treatment is set and call is released if these values are received.		
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
		1111 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	
Access Transport			=>	**Access Transport**		
Generic Number			=>	**Discarded**		
All other parameters			=>	Discarded		

a. This value is encoded based on incoming information and existing datafill. Datafill may result in values other than those shown.

b. Fields within this parameter will be set based on translations unless there is only one possible value for that field.

Table 10 ISUP Preference Indicator Parameter Coding

Information Field	JI-ISUP -->	ETSI ISUP V1	JI-ISUP -->	ETSI ISUP V1
Supplementary Service	**None (No UUI, ATP or CLIP present in the IAM)**		**Any (UUI, ATP and/or CLIP present in the IAM)**	
(Applies to messages: IAM)	**Bits**	**Bits**	**Bits**	**Bits**
ISUP Preferred	HG	HG	HG	HG
For Bearer Service = Speech	00	01	00	00
For Bearer Service = 3.1 kHz Aud.	00	01	00	00
For Bearer Service = 64k Unres.	00	00	00	00
ISUP Not Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	01	01	01	00
For Bearer Service = 3.1 kHz Aud.	01	01	01	00
For Bearer Service = 64k Unres.	01	00	01	00
ISUP Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	10	01	10	00
For Bearer Service = 3.1 kHz Aud.	10	01	10	00
For Bearer Service = 64k Unres.	10	00	10	00

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	00 - No Indication	**<=**	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	**<=**	01 - No Charge		
		10 - Charge	**<=**	10 - Charge		
		10 - Charge	**<=**	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	**<=**	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	**<=**	01 - subscriber free		
		00 - no indication	**<=**	10 - connect when free		
		00 - no indication (default)	**<=**	11 - spare		
	Called Party's Category Indicator	00 - no indication	**<=**	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	**<=**	01 - ordinary subscriber		
		10 - payphone	**<=**	10 - payphone		
		00 - no indication (default)	**<=**	11 - spare		
	End-to-End Method Indicator	00 - no end-to-end method available	**<=**	00 - no end-to-end method available	**End-to-End Method Indicator**	
				01 - pass along method available		
				10 - SCCP method available		
				11 - SCCP and Pass along methods available		
	Inter-working Indicator	0 - no interworking encountered	**<=**	0 - no interworking encountered	**Inter-working Indicator**	
		1 - interworking encountered	**<=**	1 - interworking encountered		
	End-to-End Info Indicator	0 - no end-to-end information available	**<=**	0 - no end-to-end information available	**End-to-End Info Indicator**	
			<=	1 - end-to-end information available		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**ISDN User Part Indicator**	0 - ISDN user part not used all the way	**<=**	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	**Backward Call Indicators**
		1 - ISDN user part used all the way	**<=**	1 - ISDN user part used all the way		
	Holding Indicator	0 - holding not requested	**<=**	0 - holding not required	**Holding Indicator**	
				1 - holding required		
	SCCP Method Indicator	00 - no indication	**<=**	00 to 11 - any value	**SCCP Method Indicator**	
	ISDN Access Indicator	0 - terminating access non-ISDN	**<=**	0 - terminating access non-ISDN	**ISDN Access Indicator**	
		1 - terminating access ISDN	**<=**	1 - terminating access ISDN		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**<=**	0 - incoming half echo control device not included	**Echo Control Device Indicator**	
			<=	1 - incoming half echo control device included		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	00 - CCITT	**Coding Standard**	**Cause Indicators**
			<=	All other values		
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0100 - public network serving the remote user	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		1010 - network beyond interworking point	**<=**	1010 - network beyond interworking point		
		0111 - international network	**<=**	All other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	0 - octet continues thru the next octet	**Extension Indicator**	
			<=	1 - Last Octet		
	Recommedation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommedation(Octet 1a)**	
Access Transport		transit without alteration	**<=**	**Access Transport**		
discarded			**<=**	**User to User Information**		

Table 11 Parameter Mapping - ETSI ISUP V1 ACM to JI-ISUP ACM

		JI-ISUP ACM	dir	ETSI ISUP V1 ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Optional Backward Call Indicators	**In-band Information indicator**	1 - in band information or an appropriate pattern is now available	**<=**	0 - no indication	**In-band Information indicator**	**Optional Backward Call Indicators**
			<=	1 - in band information or an appropriate pattern is now available		
	Call Forwarding May Occur indicator	0 - no indication	**<=**	0 - no indication	**Call Forwarding May Occur indicator**	
			<=	1 - call diversion may occur		
	Simple Segmentation Indicator	0 - No Additional Information will be sent	**<=**	0 - No Additional Information will be sent	**Simple Segmentation Indicator**	
			<=	1 - Additional Information will be sent in the segmentation message		
discarded			**<=**	**Call Reference**		
discarded			**<=**	**Connection Request**		
discarded			**<=**	**Information Indicator**		
discarded			**<=**	**Redirection Information**		
Carrier Information Transport			**<=**	No equivalent		
Charge Area Information			**<=**	No equivalent		
Charge Information Type			**<=**	No equivalent		
Charge Information			**<=**	No equivalent		

Table 12 Cause Value Parameter Coding

Information Field	**JI-ISUP -> ETSI V1**		**ETSI V1 -> JI-ISUP**	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Normal Event	**00X XXXX**	**00X XXXX**	**00X XXXX**	**00X XXXX**
Unallocated Number	000 0001	000 0001	000 0001	000 0001
No route to destination	000 0011	000 0011	000 0011	000 0011
Send Special Information Tone	000 0100	000 0100	000 0100	000 0100
Qor ported	000 1110	0001110	000 1110	000 1110
Normal Call Clearing	001 0000	001 0000	001 0000	001 0000
User Busy	001 0001	001 0001	001 0001	001 0001
No Response From Called User	001 0010	001 0010	001 0010	001 0010
No ans. from user (user alerted)	001 0011	001 0011	001 0011	001 0011
Subscriber Absent	001 0100	001 0100	0010100	001 0100
Call Rejected	001 0101	001 0101	001 0101	001 0101
Number changed	001 0110	001 0110	001 0110	001 0110
Destination out of order	001 1011	001 1011	001 1011	001 1011
Address Incomplete	001 1100	001 1100	001 1100	001 1100
Facility Reject	001 1101	001 1101	001 1101	001 1101
Apply locally			001 1110	001 1111
Normal, Unspecified	001 1111	001 1111	001 1111	001 1111
All other values in this category	Other values	001 1111	Other Values	Tandem

Table 12 Cause Value Parameter Coding

Information Field	**JI-ISUP -> ETSI V1**		**ETSI V1 -> JI-ISUP**	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Resource unavailable	**010 XXXX**	**010 XXXX**	**010 XXXX**	**010 XXXX**
Circuit Congestion	010 0010	010 0010	010 0010	010 0010
Network out of order	010 0110	010 0110	010 0110	010 0110
Temporary Failure	010 1001	010 1001	010 1001	010 1001
Switching Equipment Failure	010 1010	010 1010	010 1010	010 1010
Requested channel not avail.	010 1100	010 1100	010 1100	010 1100
Preemption			010 1101	111 1111
No preemption ckt avail			010 1110	111 1111
Resource unavailable	010 1111	010 1111	010 1111	010 1111
All Other values in this category	Other Values	010 1111	Other values	Tandem
Service or option not available	**011 XXXX**	**011 XXXX**	**011 XXXX**	**011 XXXX**
Req'sted facility, not subscribed	011 0010	011 1111		
Bearer capability not authorized	011 1001	011 1001	011 1001	011 1001
Bearer Cap. not presently avail.	011 1010	011 1010	011 1010	011 1010
Serv./opt. not avail - unspec	011 1111	011 1111	011 1111	011 1111
All Other values in this category	Other Values	011 1111	Other Values	Tandem
Service option not implemented	**100 XXXX**	**100 XXXX**	**100 XXXX**	**100 XXXX**
Bearer Capability Not Implmtd	100 0001	100 0001	100 0001	100 0001
Chnl type not impl			100 0010	100 1111
Svc./opt. not avail - unspec'd	100 1111	100 1111	100 1111	100 1111
All Other values in this category	Other Values	100 1111	Other Values	Tandem

Table 12 Cause Value Parameter Coding

Information Field	**JI-ISUP -> ETSI V1**		**ETSI V1 -> JI-ISUP**	
(Applies to ACM, REL)	**Bits**	**Bits**	**Bits**	**Bits**
Cause Values	**G-A**	**G-A**	**G-A**	**G-A**
Invalid message	**101 XXXX**	**101 XXXX**	**101 XXXX**	**101 XXXX**
Inv call ref value			101 0001	101 1111
Bearer capability not authorized	101 0111	101 0111		
Incompatible destination	101 1000	101 1000	101 1000	101 1000
Invalid message - unspecified	101 1111	101 1111	101 1111	101 1111
All Other values in this category	Other Values	101 1111	Other Values	Tandem
Protocol error	**110 XXXX**	**110 XXXX**	**110 XXXX**	**110 XXXX**
Inv parm contents			110 0100	110 1111
Recovery on Timer Expiry	110 0110	110 0110	110 0110	110 0110
Protocol error - unspecified	110 1111	110 1111	110 1111	110 1111
All Other values in this category	Other Values	110 1111	Other Values	Tandem
Interworking	**111 XXXX**	**111 XXXX**	**111 XXXX**	**111 XXXX**
Interworking Unspecified	111 1111	111 1111	111 1111	111 1111
All Other values in this category	Other Values	111 1111	Other Values	Tandem

Table 13 Parameter Mapping - ETSI ISUP V1 ANM/CON[a] to JI-ISUP ANM

		JI-ISUP ANM	dir	ETSI ISUP V1 ANM/CON		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	10 - Charge	<=	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	<=	01 - No Charge		
		10 - Charge	<=	10 - Charge		
		10 - Charge	<=	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	<=	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	<=	01 - subscriber free		
		00 - no indication	<=	other values		
	Called Party's Category Indicator	01 - ordinary subscriber	<=	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	<=	01 - ordinary subscriber		
		10 - payphone	<=	10 - payphone		
		01 - ordinary subscriber	<=	11 - spare		
	End-to-End Method Indicator	00 - no end-to-end method available	<=	00 - no end-to-end method available	**End-to-End Method Indicator**	
				01 - pass along method available		
				10 - SCCP method available		
				11 - SCCP and Pass along methods available		
	Inter-working Indicator	0 - no interworking encountered	<=	0 - no interworking encountered	**Inter-working Indicator**	
		1 - interworking encountered	<=	1 - interworking encountered		
	End-to-End Info Indicator	0 - no end-to-end information available	<=	0 - no end-to-end information available	**End-to-End Info Indicator**	
			<=	1 - end-to-end information available		

Table 13 Parameter Mapping - ETSI ISUP V1 ANM/CON[a] to JI-ISUP ANM

		JI-ISUP ANM	dir	ETSI ISUP V1 ANM/CON		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**ISDN User Part Indicator**	0 - ISDN user part not used all the way	**<=**	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	**Backward Call Indicators**
		1 - ISDN user part used all the way	**<=**	1 - ISDN user part used all the way		
	Holding Indicator	0 - holding not requested	**<=**	0 - holding not required	**Holding Indicator**	
				1 - holding required		
	SCCP Method Indicator	00 - no indication	**<=**	00 to 11 - any value	**SCCP Method Indicator**	
	ISDN Access Indicator	0 - terminating access non-ISDN	**<=**	0 - terminating access non-ISDN	**ISDN Access Indicator**	
		1 - terminating access ISDN	**<=**	1 - terminating access ISDN		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**<=**	0 - incoming half echo control device not included	**Echo Control Device Indicator**	
			<=	1 - incoming half echo control device included		
Access Transport		transit without alteration	**<=**	**Access Transport**		
discarded			**<=**	**User to User Information**		
discarded			**<=**	**Call Reference**		
discarded			**<=**	**Connection Request**		
discarded			**<=**	**Information Indicator**		
discarded			**<=**	**all other parameters**		

a. CON is mapped to a ACM and a ANM message. The ACM has the same BCI parameter as ANM.

Table 14 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	All values	=>	00 - CCITT	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	=>	0000 - user	**Location**	
		0001 - private network serving the local user	=>	0101 - private network serving the remote user		
		0010 - public network serving the local user	=>	0111 - international network		
		0011 - transit network	=>	0011 - transit network		
		0100 - public network serving the remote user	=>	0100 - public network serving the remote user		
		0101 - private network serving the remote user	=>	0101 - private network serving the remote user		
		0111 - international network	=>	0111 - international network		
		1010 - network beyond interworking point	=>	1010 - network beyond interworking point		
		All other values	=>	1010 - network beyond interworking point		
	Cause Value	value	=>	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	**Cause Value**	
	Extension Indicator	All Values	=>	1 - Last Octet	**Extension Indicator**	
	Recommedation(Octet 1a)	All Values	=>	Octet Discarded	**Recommedation(Octet 1a)**	
	Extension Indicator(Octet 1a)	All Values	=>	Octet Discarded	**Extension Indicator(Octet 1a)**	
User to User Information			=>	No mapping		

Table 14 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Parameter	Field	Field Value	=>	Field Value	Field	Parameter
Redirection Number			=>	No mapping		
Domestic Redirection Reason			=>	No mapping		

Table 15 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		JI-ISUP REL	dir	ETSI ISUP V1 REL		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	All Values	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0100 - public network serving the remote user	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		0111 - international network	**<=**	all other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	All Values	**Extension Indicator**	
	Recommedation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommedation(Octet 1a)**	
	Extension Indicator(Octet 1a)	Octet Discarded	**<=**	All Values	**Extension Indicator(Octet 1a)**	
Discarded			**<=**	**Access Transport**		
no mapping			**<=**	**User to User Information**		
no mapping			**<=**	**Automatic congestion level**		
no mapping			**<=**	**All other parameters**		

Table 16 Parameter Mapping - JI-ISUP CPG to ETSI ISUP V1 CPG

		JI-ISUP CPG	dir	ETSI ISUP V1 CPG		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Event Information	**Event Indication**	0000010 - PROGress	**<=**	0000000 - spare	**Event Indication**	**Event Information**
		0000001 - ALERTing		0000001 - ALERTing		
		0000010 - PROGress		0000010 - PROGress		
		0000011 - In-band information or appropriate pattern is now available		0000011 - In-band information or appropriate pattern is now available		
		0000100 - call forwarded on busy		0000100 - call forwarded on busy		
		0000101 - call forwarded on no reply		0000101 - call forwarded on no reply		
		0000110 - call forwarded unconditional		0000110 - call forwarded unconditional		
		0000010 - PROGress		0000111 to 1111111 - spare		
	Event presentation restricted indicator	0 - no indication	**<=**	0 - no indication	**Event presentation restricted indicator**	
				1 - presentation restricted		
Access Transport			**<=**	**Access Transport**		
User to User Information			**<=**	**User to User Information**		

40.11.2 ETSI ISUP V1 to JI-ISUP Interworking

Table 17 ETSI ISUP V1 to JI-ISUP Message Mappings

ETSI ISUP V1 Messages	Trigger Direction (Ref Table)	JI-ISUP Messages
IAM	=> (Table 18)	IAM
ACM	<= (Table 19)	ACM
ANM	<= (Table 20)	ANM
REL	=> (Table 21)	REL
RLC	<=	No trigger
REL	<= (Table 22)	REL
No trigger	=>	RLC
SUS/RES	<= (Table 23)	SUS/RES
CPG	<= (Table 24)	CPG

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Nature of Connection	**Satellite Indicator**	0 0: No satellite cct. in connection	=>	0 0: No Satellite cct.	**Satellite Indicator** [a]	**Nature of Connection**
		0 1: One satellite cct. in connection.	=>	0 1: One satellite cct.		
		1 0: Two satellite cct. in connection.	=>	0 1: One satellite cct.		
		1 1: Spare	=>	0 1: One satellite cct.		
	Continuity Check Indicator	00 - continuity check not required	=>	00 - continuity check not required	**Continuity Check Indicator** [a]	
		01 - continuity check required	=>			
		10 - continuity check performed on a previous circuit	=>			
		11 - spare	=>			
	Echo Control Device Indicator	0 outgoing half echo control device not included	=>	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**Echo Control Device Indicator**	
		1 outgoing half echo control device included	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Forward Call Indicator	**National/ International Call Indicator**	0 - call to be treated as a national call	=>	change based on the settings of CLASS field in translations	**National/ International Call Indicator**	**Forward Call Indicator**
		1 - call to be treated as an international call	=>			
	End-to-End Method Indicator	00 - no end-to-end method available	=>	00 - no end-to-end method available	**End-to-End Method Indicator**	
		01-11 spare	=>			
	Interworking Indicator	0 - no interworking encountered	=>	0 - no interworking encountered	**Interworking Indicator**	
		1 - interworking encountered	=>	1 - interworking encountered		
	End-to-End Information Indicator	0 - no end-to-end information available	=>	0 - no end-to-end information available	**End-to-End Information Indicator**	
		1 - spare	=>			
	ISDN User Part Indicator	0 - ISDN user part not used all the way	=>	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	
		1 - ISDN user part used all the way	=>	1 - ISDN user part used all the way		
	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	=>	00 - ISDN user part preferred all the way	**ISDN User Part Preference Indicator**	
		01 - ISDN user part not required all the way	=>	01 - ISDN user part not required all the way		
		10 - ISDN user part required all the way	=>	10 - ISDN user part required all the way		
		11 - spare	=>	Release the call		
	ISDN Access Indicator	0 - origination access non-ISDN	=>	0 - origination access non-ISDN	**ISDN Access Indicator**	
		1 - origination access ISDN	=>	1 - origination access ISDN		
	SCCP Method Indicator	00 - no indication	=>	00 - no indication	**SCCP Method Indicator**	
		01-11 spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party category		00001010 - ordinary calling subscriber	=>	00001010 - ordinary calling subscriber	**Calling Party category**	
		00001011 - calling subscriber with priority	=>	00001010 - ordinary calling subscriber		
		00001101 - test call	=>	00001101 - test call		
		00001111 - payphone	=>	00001111 - payphone		
		All other values	=>	00001010 - ordinary calling subscriber		
Transmission Medium Requirement		00000000 - Speech	=>	00000 - speech	**Transmission Medium Requirement**	
		00000010 - 64kbit/s Unrestricted	=>	00000010 - 64kbit/s Unrestricted		
		00000011 - 3.1 kHz Audio	=>	00000011 - 3.1 kHz Audio		
		00000100 - Alt speech	=>	Release the call		
		00000101 - Alt 64K	=>			
		00000110 - 64K pref	=>			
		All other values	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	set as required	**Odd/Even Indicator**	**Called Party Number (set according to table CDNCHAR data fill)**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000011 - National number	=>	0000011 - National number	**Nature of Address Indicator**	
		1111110 - peculiar number of network	=>			
		all other values	=>			
	Internal Network Number Indicator	0 - routing to an internal network number allowed	=>	0 - routing to an internal network number allowed	**Internal Network Number Indicator**	
		1 - routing to an internal network number not allowed	=>			
	Numbering Plan Indicator	000 - spare	=>	001 - ISDN numbering plan (default)	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>			
		010-111 spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Called Party Number	**Address Signals**	0000 - digit 0	=>	map as it is	**Address Signals**	**Called Party Number**
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1111 - ST	=>	Treatment is set and call is released if these values are received.		
		1010 - spare	=>			
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Odd/Even Indicator**	0 - even number of address signals	=>	Set as required	**Odd/Even Indicator**	**Calling Party Number**
		1 - odd number of address signals	=>			
	Nature of Address Indicator	0000011 - national number	=>	Set by hard-coded default logic (if CLASS selector during translation is set to INTL, then NOA is set to Peculiar; otherwise, NOA is set to National. This setting can be overwritten by table TRKCGPN datafill)	**Nature of Address Indicator**	
		1111110 - peculiar number of network	=>			
		any other value	=>			
	Calling Party Number Incomplete Indicator	0 - complete	=>	0 - complete	**Calling Party Number Incomplete Indicator**	
		1 - incomplete	=>			
	Numbering Plan Indicator	000 - spare	=>	CGPN is discarded	**Numbering Plan Indicator**	
		001 - ISDN numbering plan	=>	001 - ISDN numbering plan		
		010-111 spare	=>	CGPN is discarded		
	Address Presentation Restricted Indicator	00 - presentation allowed	=>	00 - presentation allowed	**Address Presentation Restricted Indicator**	
		01 - presentation restricted	=>	01 - presentation restricted		
		10 - address not available	=>	01 - presentation restricted		
		11 - spare	=>			

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Calling Party Number	**Screening Indicator**	00 - spare	=>	Discard CGPN	**Screening Indicator**	**Calling Party Number**
		01 - user provided, verified and passed	=>	01 - user provided, verified and passed		
		10 - reserved	=>	Discard CGPN		
		11 - network provided	=>	11 - network provided		
	Address Signals	0000 - digit 0	=>	map as it is	**Address Signals**	
		0001 - digit 1	=>			
		0010 - digit 2	=>			
		0011 - digit 3	=>			
		0100 - digit 4	=>			
		0101 - digit 5	=>			
		0110 - digit 6	=>			
		0111 - digit 7	=>			
		1000 - digit 8	=>			
		1001 - digit 9	=>			
		1010 - spare	=>	Treatment is set and call is released if these values are received.		
		1011 - code 11	=>			
		1100 - code 12	=>			
		1101 - spare	=>			
		1110 - spare	=>			
		1111 - spare	=>			
	Filter		=>	In case of an odd number of address signals, the filler code 0000 is inserted after the last address signal	**Filter**	
Access Transport			=>	**Access Transport**		
User Service Information			=>	**User Service Information**		
All other parameters			=>	discarded		

Table 18 Parameter Mapping - ETSI ISUP V1 IAM to JI-ISUP IAM

		ETSI ISUP V1 IAM	dir	JI-ISUP IAM		
Parameter	Field	Field Value	=>	Field Value	Field	Parameter
No equivalent			=>	Carrier Information Transport		
No equivalent			=>	Charge Area Information		

a. This value is encoded based on incoming information and existing datafill. Datafill may result in values other than those shown.

Table 19 Parameter Mapping JI-ISUP ACM to ETSI ISUP V1 ACM

		ETSI ISUP V1 ACM	dir	JI-ISUP ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	00 - No Indication	**<=**	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	**<=**	01 - No Charge		
		10 - Charge	**<=**	10 - Charge		
		10 - Charge (default)	**<=**	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	**<=**	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	**<=**	01 - subscriber free		
		00 - no indication	**<=**	10 - connect when free		
		00 - no indication (default)	**<=**	11 - spare		
	Called Party's Category Indicator	00 - no indication	**<=**	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	**<=**	01 - ordinary subscriber		
		10 - payphone	**<=**	10 - payphone		
		00 - no indication (default)	**<=**	11 - spare		
	End-to-End Method Indicator	00 - no end-to-end method available (default)	**<=**	00 - no end-to-end method available	**End-to-End Method Indicator**	
			<=	01 - pass along method available		
			<=	10 - SCCP method available		
			<=	11 - SCCP and Pass along methods available		
	Inter-working Indicator	0 - no interworking encountered	**<=**	0 - no interworking encountered	**Inter-working Indicator**	
		1 - interworking encountered	**<=**	1 - interworking encountered		
	End-to-End Info Indicator	0 - no end-to-end information available	**<=**	0 - no end-to-end information available	**End-to-End Info Indicator**	
			<=	1 - end-to-end information available		
	ISDN User Part Indicator	0 - ISDN user part not used all the way	**<=**	0 - ISDN user part not used all the way	**ISDN User Part Indicator**	
		1 - ISDN user part used all the way	**<=**	1 - ISDN user part used all the way		

Table 19 Parameter Mapping JI-ISUP ACM to ETSI ISUP V1 ACM

		ETSI ISUP V1 ACM	dir	JI-ISUP ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Holding Indicator**	0 - holding not requested	<=	0 - holding not required	**Holding Indicator**	**Backward Call Indicators**
			<=	1 - holding required		
	SCCP Method Indicator	00 - no indication	<=	00 to 11 - any value	**SCCP Method Indicator**	
			<=			
	ISDN Access Indicator	0 - terminating access non-ISDN	<=	0 - terminating access non-ISDN	**ISDN Access Indicator**	
		1 - terminating access ISDN	<=	1 - terminating access ISDN		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	<=	0 - incoming half echo control device not included	**Echo Control Device Indicator**	
			<=	1 - incoming half echo control device included		
Cause Indicators	**Coding Standard**	00 - CCITT	<=	00 - CCITT	**Coding Standard**	**Cause Indicators**
			<=	All other values		
	Location	0000 - user	<=	0000 - user	**Location**	
		0101 - private network serving the remote user	<=	0001 - private network serving the local user		
		0111 - international network	<=	0010 - public network serving the local user		
		0011 - transit network	<=	0011 - transit network		
		0100 - public network serving the remote user	<=	0100 - public network serving the remote user		
		0101 - private network serving the remote user	<=	0101 - private network serving the remote user		
		0111 - international network	<=	0111 - international network		
		1010 - network beyond interworking point	<=	1010 - network beyond interworking point		
		0111 - international network	<=	All other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	<=	value	**Cause Value**	

Table 19 Parameter Mapping JI-ISUP ACM to ETSI ISUP V1 ACM

		ETSI ISUP V1 ACM	dir	JI-ISUP ACM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Access Transport		transit without alteration	**<=**	**Access Transport**		
Optional Backward Call Indicators	**In-band Information indicator**	1 - in band information or an appropriate pattern is now available	**<=**	0 - no indication	**In-band Information indicator**	**Optional Backward Call Indicators**
			<=	1 - in band information or an appropriate pattern is now available		
	Call Forwarding May Occur indicator	0 - no indication	**<=**	0 - no indication	**Call Forwarding May Occur indicator**	
			<=	1 - call diversion may occur		
discarded			**<=**	**User to User Information**		
discarded			**<=**	**User-to-User Indicator**		
discarded			**<=**	**Charge Information**		
discarded			**<=**	**Charge Information Identification**		
discarded			**<=**	**Charge Information Delay Indicator**		
discarded			**<=**	**Additional Party's Category**		
discarded			**<=**	**Carrier Information Transport**		
discarded			**<=**	**Charge Area Information**		

Table 20 Parameter Mapping - JI-ISUP ANM to ETSI ISUP V1 ANM

		ETSI ISUP V1 ANM	dir	JI-ISUP ANM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Backward Call Indicators	**Charge Indicator**	00 - No Indication	**<=**	00 - No Indication	**Charge Indicator**	**Backward Call Indicators**
		01 - No Charge	**<=**	01 - No Charge		
		10 - Charge	**<=**	10 - Charge		
		10 - Charge	**<=**	11 - Spare		
	Called Party's Status Indicator	00 - no Indication	**<=**	00 - no Indication	**Called Party's Status Indicator**	
		01 - subscriber free	**<=**	01 - subscriber free		
		00	**<=**	10		
		00	**<=**	11		
	Called Party's Category Indicator	00 - no indication	**<=**	00 - no indication	**Called Party's Category Indicator**	
		01 - ordinary subscriber	**<=**	01 - ordinary subscriber		
		10 - payphone	**<=**	10 - payphone		
		00 - no indication	**<=**	11 - spare		
	End to End Method Indicator	00 - No end to end method available	**<=**	all values	**End to End Method Indicator**	
	Interworking Indicator		**<=**	**Interworking Indicator**		
	End to End Info available	0 - No end to end info available	**<=**	all values	**End to End Info available**	
	ISDN User Part Indicator		**<=**	**ISDN User Part Indicator**		
	Holding Indicator	0 - holding not requested		0 - holding not required	**Holding Indicator**	
				1 - holding required		
	ISDN Access Indicator		**<=**	**ISDN Access Indicator**		
	Echo Control Device Indicator	If TMR is set to 00 or 03, it will be mapped to 1. If TMR is set to 02, it will be mapped to 0.	**<=**	all values	**Echo Control Device Indicator**	
	SCCP Method Available	00 - No Indicator	**<=**	All values	**SCCP Method Available**	

Table 20 Parameter Mapping - JI-ISUP ANM to ETSI ISUP V1 ANM

		ETSI ISUP V1 ANM	dir	JI-ISUP ANM		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Access Transport			**<=**	**Access Transport**		
discarded			**<=**	**User to User Information**		
discarded			**<=**	**Charge Area Information**		
discarded			**<=**	**Additional Party's Category**		

Table 21 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	**Field**	**Field Value**	**=>**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	All values	=>	00 - CCITT	**Coding Standard**	**Cause Indicators**
			=>			
	Location	0000 - user	=>	0000 - user	**Location**	
		0001 - private network serving the local user	=>	0101 - private network serving the remote user		
		0010 - public network serving the local user	=>	0100 - public network serving the remote user		
		0011 - transit network	=>	0011 - transit network		
		0100 - public network serving the remote user	=>	0100 - public network serving the remote user		
		0101 - private network serving the remote user	=>	0101 - private network serving the remote user		
		0111 - international network	=>	0111 - international network		
		1010 - network beyond interworking point	=>	1010 - network beyond interworking point		
		All other values	=>	0111 - international network		
	Cause Value	value	=>	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	**Cause Value**	
	Extension Indicator	All Values	=>	1 - Last Octet	**Extension Indicator**	
	Recommedation(Octet 1a)	All Values	=>	Octet Discarded	**Recommedation(Octet 1a)**	
	Extension Indicator(Octet 1a)	All Values	=>	Octet Discarded	**Extension Indicator(Octet 1a)**	
Access Transport			=>	discarded		

Table 21 Parameter Mapping - ETSI ISUP V1 REL to JI-ISUP REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	Field	Field Value	=>	Field Value	Field	Parameter
User to User Information			=>	discarded		
Automatic congestion level			=>	discarded		

Table 22 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Cause Indicators	**Coding Standard**	00 - CCITT	**<=**	All Values	**Coding Standard**	**Cause Indicators**
	Location	0000 - user	**<=**	0000 - user	**Location**	
		0101 - private network serving the remote user	**<=**	0001 - private network serving the local user		
		0111 - international network	**<=**	0010 - public network serving the local user		
		0011 - transit network	**<=**	0011 - transit network		
		0100 - public network serving the remote user	**<=**	0100 - public network serving the remote user		
		0101 - private network serving the remote user	**<=**	0101 - private network serving the remote user		
		0111 - international network	**<=**	0111 - international network		
		1010 - Beyond an interworking point	**<=**	1010 - Beyond an interworking point		
		1010 - Beyond an interworking point	**<=**	all other values		
	Cause Value	Please refer to “Table 12 Cause Value Parameter Coding” on page 1007.	**<=**	value	**Cause Value**	
	Extension Indicator	1 - Last Octet	**<=**	All Values	**Extension Indicator**	
	Recommedation(Octet 1a)	Octet Discarded	**<=**	All Values	**Recommedation(Octet 1a)**	
	Extension Indicator(Octet 1a)	Octet Discarded	**<=**	All Values	**Extension Indicator(Octet 1a)**	
discarded			**<=**	**User to User Information**		

Table 22 Parameter Mapping - JI-ISUP REL to ETSI ISUP V1 REL

		ETSI ISUP V1 REL	dir	JI-ISUP REL		
Parameter	Field	Field Value	<=	Field Value	Field	Parameter
discarded			<=	Redirection Number		
discarded			<=	Domestic Redirecting Reason		

Table 23 Parameter Mapping - JI-ISUP SUS/RES to ETSI ISUP V1 SUS/RES

		ETSI ISUP V1 SUS/RES	dir	JI-ISUP SUS/RES		
Parameter	Field	Field Value	<=	Field Value	Field	Parameter
Suspend/ Resume Indicators	Suspend/ Resume Indicator	0 - subscriber initiated	<=	0 - subscriber initiated	Suspend/ Resume Indicator	Suspend/ Resume Indicators
		1 - network initiated	<=	1 - network initiated		
	spare	0000000 - Hard code	<=	0000000 - Hard code	spare	

Table 24 Parameter Mapping - JI-ISUP CPG to ETSI ISUP V1 CPG

		ETSI ISUP V1 CPG	dir	JI-ISUP CPG		
Parameter	**Field**	**Field Value**	**<=**	**Field Value**	**Field**	**Parameter**
Event Information	**Event Indication**	Discard CPG	**<=**	0000000 - spare	**Event Indication**	**Event Information**
		0000001 - ALERTing		0000001 - ALERTing		
		0000010 - PROGress		0000010 - PROGress		
		0000011 - In-band information or appropriate pattern is now available		0000011 - In-band information or appropriate pattern is now available		
		Discard CPG		0000100 - call forwarded on busy		
				0000101 - call forwarded on reply		
				0000110 - call forwarded unconditional		
				0000111 - generic notification to terminating user		
				0001000 to 1111111 - spare		
	Event presentation restricted indicator	0 - no indication	**<=**	0 - no indication	**Event presentation restricted indicator**	
				1 - presentation restricted		
Discarded			**<=**	**Cause Indicator**		
Access Transport			**<=**	**Access Transport**		
Discarded			**<=**	**User to User Information**		

41: Functional Description (FN): A00002844

41.1 Feature name

Excessive Metering Detection (EMD) Support for Metered Trunks

41.2 Description

EMD detects and reports the lines and trunks whose meter counts reach a threshold value. The activation, start time, period and threshold values are provided by provisioning.

EMD funtionality is enhanced for metered trunks with this ISN07 activity.

When the feature is activated, a process is scheduled to wake up at certain times defined by the start time and period. This process runs periodically and compares the current meters of trunks agents with the previously copied ones. The meter delta values obtained from the comparison are compared with a threshold value provisioned prior to the feature activation. The agents whose meter counts reach the threshold value are reported with a new log. After all meters of trunk agents are checked, these values are copied to be used by the next run of the process.

Any desired metered trunk agent can be excluded from EMD process by assigning NEMD (No Excessive Metering Detection) option to that agent in TRKOPTS table.

When the feature is deactivated, EMD process is disabled and allocated data store for the previous meter counts is freed.

This feature can be divided into 6 parts in terms of behavior:

- Provisioning
- Activation/deactivation
- Trunk option
- Log format
- Detection process
- Robustness
- ONP

41.2.1 Provisioning

Existing EMD tuple in MTRSYSPM table is enhanced to include a separate threshold value for trunks. All other fields are common for both line and trunk agents. Changed form of EMD tuple includes the following fields:

- ACTIVATION
  Identifies whether the feature is activated or not.
- START_TIME (Hour and Minute)
  Indicates the start time of EMD process in terms of hour and minute.
- PERIOD
  Indicates running interval of EMD process in terms of days.
- **LINE_THRESHOLD** *(renamed)*
  Indicates the expected maximum value of total delta between previous and current meter counts of a line.
- **TRUNK_THRESHOLD** *(new)*
  Indicates the expected maximum value of total delta between previous and current meter counts of a trunk. If range of turnk threshold is calculated in the same logic with line, it is found as 0..7,999,999,999,992. But this value can not be supported in terms of coding/compile issues. The maximum value that can be supported is 2,147,483,647. According to this maximum value of trunk threshold is decided as 2,100,000,000.

Ranges of parameters of EMD tuple are as follows:

Table 1 EMD tuple with ranges

Field name	Range
ACTIVATION	NO, YES
HOUR	0 TO 23
MINUTE	0 TO 59
PERIOD	1 TO 30 (day)
LINE_THRESHOLD	0 TO 799,999,992
TRUNK_THRESHOLD	0 TO 2,100,000,000

The default values of these fields are as follows:

Table 2 EMD tuple with default values

Field name	Default Value
ACTIVATION	NO
HOUR	4

Table 2 EMD tuple with default values

Field name	Default Value
MINUTE	15
PERIOD	1
LINE_THRESHOLD	20,000
TRUNK_THRESHOLD	200,000

With these default values, EMD process will start at 4:15 am and will be repeated every day.

It is restricted to add or delete a tuple to/from MTRSYSPM table. So EMD tuple can only be changed. The following is a change example of EMD tuple:

Table 3 Change example for EMD tuple in table MTRSYSPM

```
>pos EMD
   EMD     EMD NO 10 30 2 300
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
MTRSEL: EMD
>EMD
ACTIVATION: NO
>yes
HOUR: 10
>4
MINUTE: 30
>15
PERIOD: 2
>1
LINE THRESHOLD: 300
>500
TRUNK THRESHOLD: 200
>400
TUPLE TO BE CHANGED:
   EMD     EMD YES 4 15  1       500 400
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Store allocation is running.
Please wait...
EXCESSIVE METERING DETECTION process has been activated.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

41.2.2 Trunk Option

EMD process is run for all metered lines and trunks. In order to be excluded from this process, specified trunk is assigned with NEMD (No Excessive Metering Detection) option in TRKOPTS table.

Trunks must have ICMOG/OGMOG option in table TRKOPTS in order to assign NEMD option successfully.

Table 4 NEMD Option Datafill Example in Table TRKOPTS

```
TABLE TRKOPTS
lis all
TOP
OPTKEY            OPTINFO
----------------------------------------
ICPRIBA ICMOG   ICMOG MOG_3
ICPRIBA NEMD    NEMD
BOTTOM
```

41.2.3 Activation/Deactivation

Existing EMD process is used with this feature. This process survives forever and sleeps till it is activated. Activation is provided by datafilling ACTIVATION field of existing EMD tuple in MTRSYSPM table as “YES”.

Behavior of EMD process activation/deactivation for metered lines is not changed and it is same for trunks.

In case of activation, the following scenarios and messages are possible:

- System starts to allocate data store for metered lines and trunks and this is informed with a message. Please refer to “Figure 1 Info message for the store allocation” on page 1041. If store allocation fails, the operator is warned with a message and activation is rejected. Please refer to “Figure 2 Message for the store allocation failure” on page 1041. If store allocation is completed successfully then the operator is informed with a message and feature is activated. Please refer to “Figure 3 Info message for the process activation” on page 1041.

Figure 1 Info message for the store allocation

```
Store allocation is running.
Please wait...
```

Figure 2 Message for the store allocation failure

```
There is NOT ENOUGH DSPERM memory available.
Process could not be activated.
```

Figure 3 Info message for the process activation

```
EXCESSIVE METERING DETECTION process has been activated.
```

- If process died a time ago due to traps or some other reasons, in order to activate the feature any kind of a restart is needed and if so the operator is warned with a message and activation is rejected. Please refer to “Figure 4 Warning message if a restart is needed for activation” on page 1042. If

a restart is necessary for the activation, WARM RESTART is recommended.

Figure 4 Warning message if a restart is needed for activation

```
In order to set the ACTIVATION field to YES,
at least a WARM restart should be performed.
```

If the process dies for any reason, while it is already running, the ACTIVATION field is set to "NO" automatically and the data store allocated for storing the previous meter counts is freed.

If the feature is activated successfully, then the initial run time of the EMD process is determined in the following manner:

- If the current time that the feature is activated is less than the start time (HOUR, MINUTE) which is datafilled in table MTRSYSPM via tuple EMD, then the process is invoked at the same day, at the time indicated by HOUR, MINUTE fields. The PERIOD field indicates after how many days the next invocation is. For example, if feature is activated at 14:35 at 1st day of a month and HOUR, MINUTE and PERIOD are datafilled as 18, 15 and 3, then the process is invoked in the following sequence: at 18:15 of 1st, at 18:15 of 4th, at 18:15 of 7th... and etc. days.
- If the current time that the feature is activated is greater than the start time (HOUR, MINUTE), then the process is invoked at the start time of the next day. For example, if the feature is activated at 14:35 at 3rd day of a month and HOUR, MINUTE and PERIOD are datafilled as 14, 25 and 2 days, then process is invoked in the following sequence: 14:25 of 4th, 14:25 of 6th... and etc. days.
- While the process is sleeping, if the system time is changed to an earlier time, the process wake up time is still the same as set before. If the system time is changed to a time later than process wake up time, the process is waked up as soon as "settime" is handled..

Service

The first process waking up after the activation of the feature is always for only copying the meter counts, that is, none of the meter counts of trunk agents are compared since there is no data about previous meter counts.

If the tuple EMD in table MTRSYSPM is being changed, the following controls are applied:

- If the EMD process is running then changing is rejected and the operator is warned with a message as shown in "Figure 5 Reject message for the tuple change while process is running" on page 1042.

Figure 5 Reject message for the tuple change while process is running

```
EXCESSIVE METERING DETECTION process is running.
Please try again later...
```

- If HOUR, MINUTE or PERIOD fields of the tuple is tried to change while the ACTIVATION field is “YES”, then tuple change is rejected and operator is warned with a message as shown in “Figure 6 Reject message for the HOUR, MINUTE or PERIOD change” on page 1043.

Figure 6 Reject message for the HOUR, MINUTE or PERIOD change

```
To change the HOUR, MINUTE or PERIOD fields,
ACTIVATION field must be NO.
```

If the feature is deactivated by setting the ACTIVATION field from “YES” to “NO”, then the operator is informed with a message as shown in “Figure 7 Deactivation message” on page 1043 that EMD process is disabled and the data store allocated for copying the previous meter counts is freed.

Figure 7 Deactivation message

```
Store deallocation is running.
Please wait...
EXCESSIVE METERING DETECTION process has been deactivated.
```

41.2.4 Detection Process

With this activity detection process is just enhanced to include metered trunks too.

When the process wakes up, it detects all trunk agents whose meter counts reach the threshold value within the period time. When the process first wakes up, the current meter counts of all trunk and line agents are stored, and no comparison is made. The following actions are held for each periodic waking up:

- The current meters of line and trunk agents are compared with the previously copied meters and all agents whose meter counts reached the related THRESHOLD values of the tuple EMD in table MTRSYSPM are reported via EMD log. This log is EMD100 for lines and a new EMD 101 log for trunks.
- The current meter counts are copied to be used as previous values at the next invocation.

Periodic EMD process wakes up at the times determined according to the values of HOUR, MINUTE and PERIOD fields of EMD tuple in table MTRSYSPM.

With the waking up of the EMD process two main functionalities are performed:

- Comparison of meters of agents
- Copying of meters of agents

The running and completion of excessive metering detection process are informed with existing MTR107 (process running) and existing MTR109 (process completed) logs respectively.

41.2.4.1 Comparison of S/W meters of trunk agents

When EMD runs, it checks the meters of trunk agents which do not have NEMD option assigned in TRKOPTS table. For this purpose, the process compares the current meter values with the values which had been stored by the previous run of the process.

The delta values of the assigned meters of a trunk agent are calculated and added to the total delta. This calculation is done in the following manner:

For each assigned meter of the trunk agent:

1. If previous meter value is greater than the current meter value and the current wrap bit is set, then previous value minus the current value is subtracted from the meter wrap value (1,000,000,000,000)
2. If previous meter value is greater than the current meter value but the current wrap bit is not set then this meter is ignored since it means a MOG deassignment and reassignment has occurred.
3. If previous meter value is less than or equal to the current meter value and the current meter wrap bit is set and the previous meter wrap bit is not set then current value minus the previous value is added to the meter wrap value (1,000,000,000,000).
4. If previous meter value is less than or equal to the current meter value and the current meter wrap bit is not set and the previous meter wrap bit is set then this meter is ignored since it means a MOG deassignment and reassignment has occurred.
5. If previous meter value is less than or equal to the current meter value and both the previous and the current meter wrap bit is set or not set then previous value is subtracted from the current value.
6. The delta value found for this assigned meter is added to the total delta.

A few examples are given in “Table 5 Meter delta examples” on page 1044 for delta calculation of a meter. Here “Ignore” means “Do not make a delta calculation”.

Table 5 Meter delta examples

E.g. No	Prv. value of the meter	Prv. wrap bit	Cur. value of the meter	Cur. wrap bit	Delta value of the meter
5	000.000.000.100	N	000.000.000.200	N	000.000.000.100

E.g. No	Prv. value of the meter	Prv. wrap bit	Cur. value of the meter	Cur. wrap bit	Delta value of the meter
3	000.000.000.100	N	000.000.000.200	Y	1.000.000.000.100
4	000.000.000.100	Y	000.000.000.200	N	Ignore
5	000.000.000.100	Y	000.000.000.200	Y	000.000.000.100
2	000.000.000.700	N	000.000.000.300	N	Ignore
1	000.000.000.700	N	000.000.000.300	Y	999.999.999.600
2	000.000.000.700	Y	000.000.000.300	N	Ignore
5	000.000.000.700	Y	000.000.000.300	Y	999.999.999.600
3	000.000.000.000	N	999.999.999.999	Y	1.999.999.999.999

After the total meter delta of the trunk agent is calculated, this value is compared with the threshold value of trunk agent and if the total meter delta of the trunk agent reaches this threshold value, it is reported via EMD log with the reason. For trunk agents a new log, EMD 101, is generated.

An example of delta calculation of meters of a trunk agent for different values of previous and current meter count values is given in “Table 6 Delta calculation of meters of a trunk agent” on page 1045.

Table 6 Delta calculation of meters of a trunk agent

Meters	Previous count	Prv. wrap bit	Current count	Cur. wrap bit	Meter delta
TLOCAL	000.000.006.000	N	000.000.006.800	N	000.000.000.800
TTOLL	000.000.000.150	N	000.000.000.050	N	Ignore
			Total delta		000.000.000.800
Threshold	900		Action (800<900)		Nothing to do
Threshold	800		Action (800=800)		Generate EMD 101
Threshold	600		Action (600<800)		Generate EMD 101

41.2.4.2 Copying of current trunk meters

If the data that belongs to the previous meters are not present, then meter blocks are stored (independent of trunk option NEMD) by EMD process to be used at the next run without comparing meters of trunk agents. Otherwise, after all trunk agents except which have NEMD option are compared, current meter

counts of all trunk agents are copied to be used at the next run. For this purpose, same data store size necessary for storing the current meter counts is allocated. If sufficient data store can not be allocated, feature is deactivated automatically which causes all allocated data store to be freed.

When EMD process runs for the first time, it only copies the current meter blocks.

41.2.4.3 Interaction of EMD process with other metering processes

EMD process has interaction with some metering processes as follows:

41.2.4.3.1 Metering Restore Process

When the wake up time of EMD process comes, if the metering restore process is active, EMD waits for the restore process to be completed and upon completion, it compares previous values with newly restored meter counts. At the end of comparison, it copies current meter blocks as previous meter counts.

If restore process begins to run while EMD process is running, EMD is stopped immediately and upon completion of restore process restarts and compares previous meter counts with newly restored meter counts. At the end of comparison, it copies current meter blocks as previous meter counts.

41.2.4.3.2 Billing of Metered Agents

At the end of billing process, if billing is done successfully, wrap bits are reset. But before resetting wrap bit of a meter block, comparison of its meter count with previous meter counts is handled and EMD 101 log is generated with “BILLING” reason indicating that comparison is handled not in periodic time, in billing time.

41.2.4.3.3 Deassignment of ICMOG/OGMOG Option (TOOS)

While ICMOG/OGMOG option is being deassigned from a trunk agent, its meter block is deallocated and sent to TOOS. But before this, comparison of its meter count with previous meter counts is handled and EMD 101 log is generated with “OOS” reason indicating that comparison is handled not in periodic time, in deassignment of ICMOG/OGMOG time.

41.2.5 Robustness

EMD process survives all restarts RELOAD, COLD and WARM.

The store which is created for keeping previous meter counts is resides in DSPERM and affected by only reboot/upgrades. Previous meter counts are saved during all restarts(reload,cold and warm).

41.2.6 ONP

Since existing EMD tuple has been changed, transfer of MTRSYSPM table is enhanced to support transfer of old format of EMD tuple into new format.

41.2.7 Log Format

When a trunk subscriber whose meter counts reach a threshold value is detected, the operator is warned with a new log EMD101 with the reason in case of:

- A time period
- Billing, if billing process resets the wrap bit of a meter
- OOS, if a meter block is sent to the TOOS table due to ICMOG/OGMOG deassignment
- Wrap around more than once

The meters in the log are determined from the ICMOG/OGMOG assigned to the trunk.

This log includes the following fields:

- Current date and time
- CLLI information of the trunk agent
- Reason
  - PERIODIC: if comparison of meter counts is handled at time indicated in EMD tuple in table MTRSYSPM.
  - BILLING: if comparison of meter counts is handled during billing process, before reseting wrap bits.
  - OOS: if comparison of meter counts is handled during deassignment of MOg option, before deallocating meter block.
  - WRAP: if comparison of meter counts is handled during incrementing meter count, before setting wrap bit to “yes”.
- Date information belonging to the previous meters which reflects the time all the meters copied for the next run at the end of the process.
- For each meter, previous wrap bit and meter count (WRAP1, COUNT1), current wrap bit and meter count (WRAP2, COUNT2) and delta value between them. If a meter is not assigned currently or previously then wrap and meter count fields of that meter are filled with ’*’ signs, the delta field which does not have a valid value is also filled with ’*’ signs.
- At the end of the log, threshold and total meter count delta are located.

An example of EMD101 log is shown in “Figure 8 Sample log report for EMD 101” on page 1048

Figure 8 Sample log report for EMD 101

```
EMD101 JUN10 18:10:12 1367 INFO EXCESSIVE TRUNK METERING

CLLI: ICPRIBA

Reason: PERIODIC

Previous date: 2003/08/12  18:05:10

-------------------------------------------------------------------

METER NAME WRP1  COUNT1        WRP2  COUNT2        DELTA

---------- ----  ------------  ----  ------------  -----------

TLOCAL      NO   000000000012  NO    000000000045  00000000000033

TTOLL       NO   999999999999  YES   000000000009  00000000000010

TINTL       NO   ************  ***   ************  **************

-------------------------------------------------------------------

Threshold:0000000000020             Total delta:  00000000000043
```

41.3 Hardware Requirements or Dependencies

N/A.

41.4 Software Requirements or Dependencies

N/A.

41.5 Limitations and restrictions

1. Process runs initially when the day time reaches the datafilled start time whenever the following events occur.
   - Enabling the feature by changing the ACTIVATION field of the tuple EMD in table MTRSYSPM from “NO” to “YES”.
   - Rebooting the system.
   - Meter restore from tape or disk.
   - ONP.

   In the initial run of the process, actual meter counts are copied to the previous meter tables and next process activation time is set according to the PERIOD field
2. Modifying the tuple EMD in table MTRSYSPM is not permitted while excessive metering detection process is running.

3. If HOUR, MINUTE or PERIOD fields of the tuple EMD in table MTRSYSPM are desired to change and ACTIVATION field is "YES" (this means EMD process is active) then tuple change is rejected.
4. First next EMD process skips comparison for a trunk if the following operations are applied to a trunk agent after the current meters are copied.
   - Assigning ICMOG/OGMOG option to a trunk
   - Deassigning ICMOG/OGMOG option from a trunk
5. If any restart occurs while EMD process is running, the process restarts from the beginning after restart is over and previously generated logs are invalid.
6. The concurrent execution of the periodic case and the extreme cases like billing, OOS and wrap around more than once is not handled.
7. If a dump is in progress and more storage is needed for storing any new meters (i.e. via MOG assignment) EMD will not store counts of new meters until the next first run.
8. The process performs the copy, compare and log operations only on the active side.

41.6 Interactions

N/A.

41.7 Applicable customer facing sections

Fault Management	
Logs	__X___
Alarms	_____
Configuration	
Data Schema	__X___
User Interface	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

41.8 Glossary

Term	Description
DSPERM	Permanent data store saved over reloads
DN	Directory Number
EMD	Excessive Metering Detection
NEMD	No Excessive Metering Detection
ONP	One Night Process
OOS	Out of Service

42: Functional Description (FN): A00002884

42.1 Feature name

A00002884 - ETSI BRI Preset Conference Service Interactions.

42.2 Description

42.2.1 Introduction

The activity “ETSI BRI Preset conference service interactions” allows the interworking for preset conference on BRI with the supplementary services indicated in “Preset Conference for BRI Supplementary Services” specification document.

The activity A00002884 is a continuation of activity A00002367 “BRI Preset conference base” which is based on the existing IBN Preset Conference and uses same datafill requirements and restrictions for IBN Preset conference.

The implementation of this activity has no impact with the supplementary services current working behavior.

42.2.2 Provisioning of BRI Preset Conference

BRI Preset Conference allows an ETSI BRI (point-to-multipoint) station or ETSI ISUP V2 trunk to set up a preset conference with up to 35 conferees by dialling a specific directory number. This invokes simultaneous ringing of preselected conference members. To be able to activate this activity, PRECONF, CUSTENG tables should be datafilled.

In table CUSTENG, the customer group of the originator should have ‘CONF6C’ option to let the conference be activable. CUSTENG table datafill example is given in Table 1.

Figure 1 CUSTENG table datafill example

CUSTNAME	ADNUM	NONCOS	NOIBNTMT	CONSOLES	DOMAIN	GROUPID
CUST783A	22	256	63	Y	PRIVATE	105 (CONF6C 12)$

Table PRECONF contains a predefined preset conference DN and the conferees for this DN.

Preset conference DN should be datafilled to be allowed for a customer group, it is possible to datafill up to 64 preset conference DN in this table.

The conferees are specified in advance in this table. 35 conferee numbers can be assigned to each preset conference DN. This includes the originator, all preset conferees and all add on conferees. The preset conference originator is a member of the preset conference's customer group. Conferees does not need to belong to the same customer group. The conferees can have an alternate address. The time outs interval is 15 seconds for both conferees and its alternate address.

PRECONF table datafill example with a predefined preset conference DN, a conferee with alternate address and an other without alternate address is given in Table 2.

Figure 2 PRECONF Datafill example

PCNFKEY CONFADDR PCNFVAR OPTIONS
0 0 1027835599 D IBN CUST783A 0 Y N Y N N N $
0 1 7831016 A 7831003 15 $
0 2 7831002 C 15 $

A served user initiates one preset conference (PRCONF) by dialling a predefined DN, which is associated with conference. The directory number is recognized as a request for a preset conference. A check is made if required number of six-port conference bridges can be seized for the conference and the conference is not already in use. If call is valid and the conference ports are available, the originator will hear audible ringing (ring back tone). The status of conferees is not important at this moment for the originator to be able to hear ring back tone. If call is invalid (Translations checks for the originator's data against the data of preset conference and required number of six-port conference bridges can not be seized for the conference or the conference is already in use), the originator will be routed to treatment. Use of Notification for call valid scenarios is not required. No notification will be sent to served user even if some/all datafilled conferees are busy.

42.2.3 Call Flows

Conference originator initiates one preset conference by dialling a specific DN. Dialing the DN invokes simultaneous ringing of the preselected conference members.The directory number is recognized as a request for a preset conference. A check is made if required number of six-port conference bridges can be seized for the conference and the conference is not already in use. An IMMSTART option can be set in table PRECONF so that the conference starts as soon as the first conferee answers.

The originator of a preset conference can add on conferees as local call, once the preset conference is established. In order to provide this functionality, the field ADDON of the table PRECONF should be set to ‘yes’ and line options AFC and HOLD. Once the maximum number of conferees is reached, no more conferees may be added.To add a new party, the connection to the conference bridge can be either in the (Active Idle) state or in the (Active Held) state and the connection to the party to be added can either be in (Active, Idle) state.

If ORIGCONT field set to “Yes” in table PRECONF, the originator is in control of conference. In this case when he goes on-hook, the conference is taken down, even if there are conferees are still on the bridge.

Basic call flow will be supported by “Preset Conference Base” feature (A00002367). For detailed information please refer to FN document of A00002367.

42.2.3.1 Successful Case

Figure 3 Preset Conference Initialition

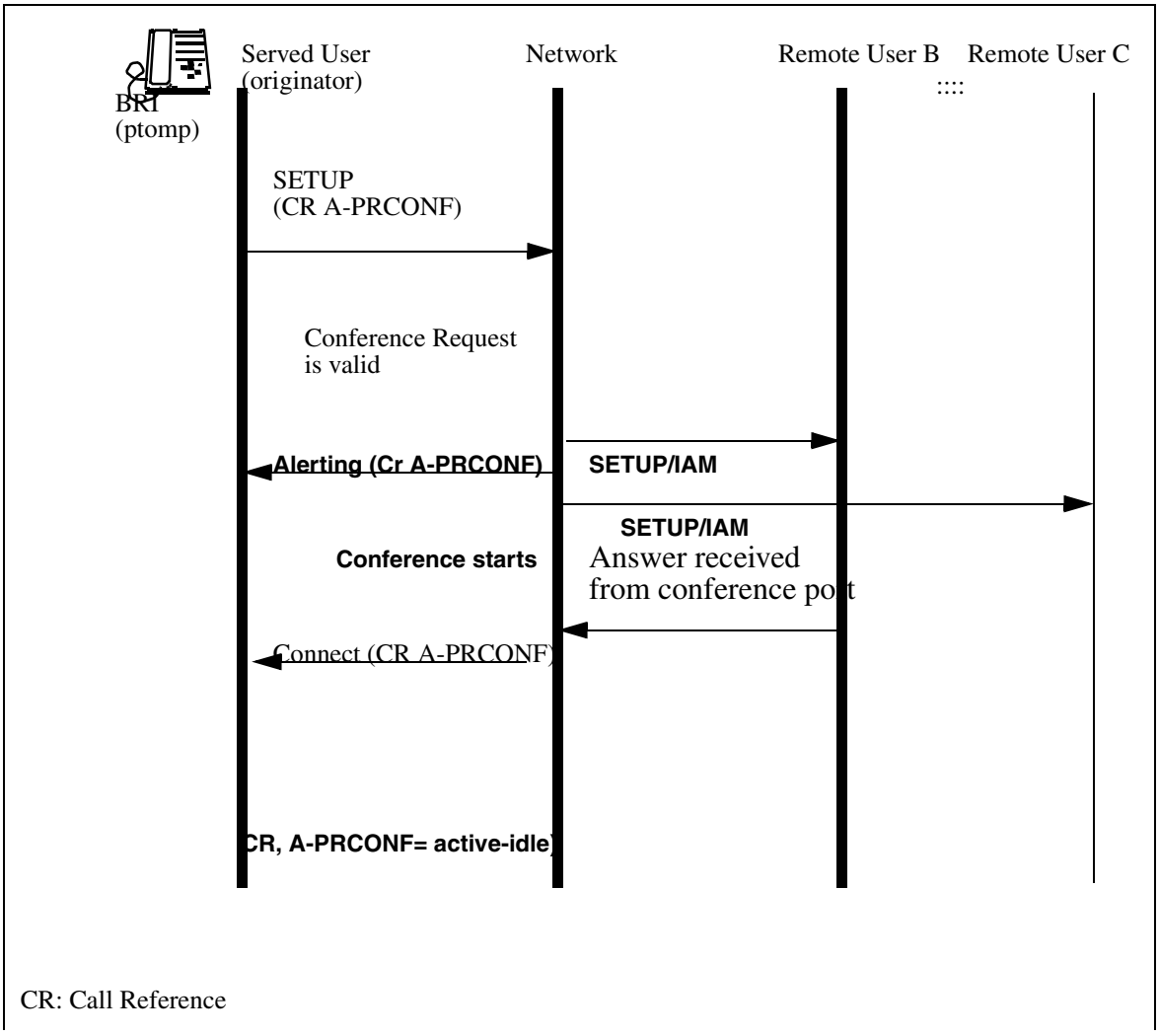


Figure 4 Add-on conferee, when preset conference is in held state

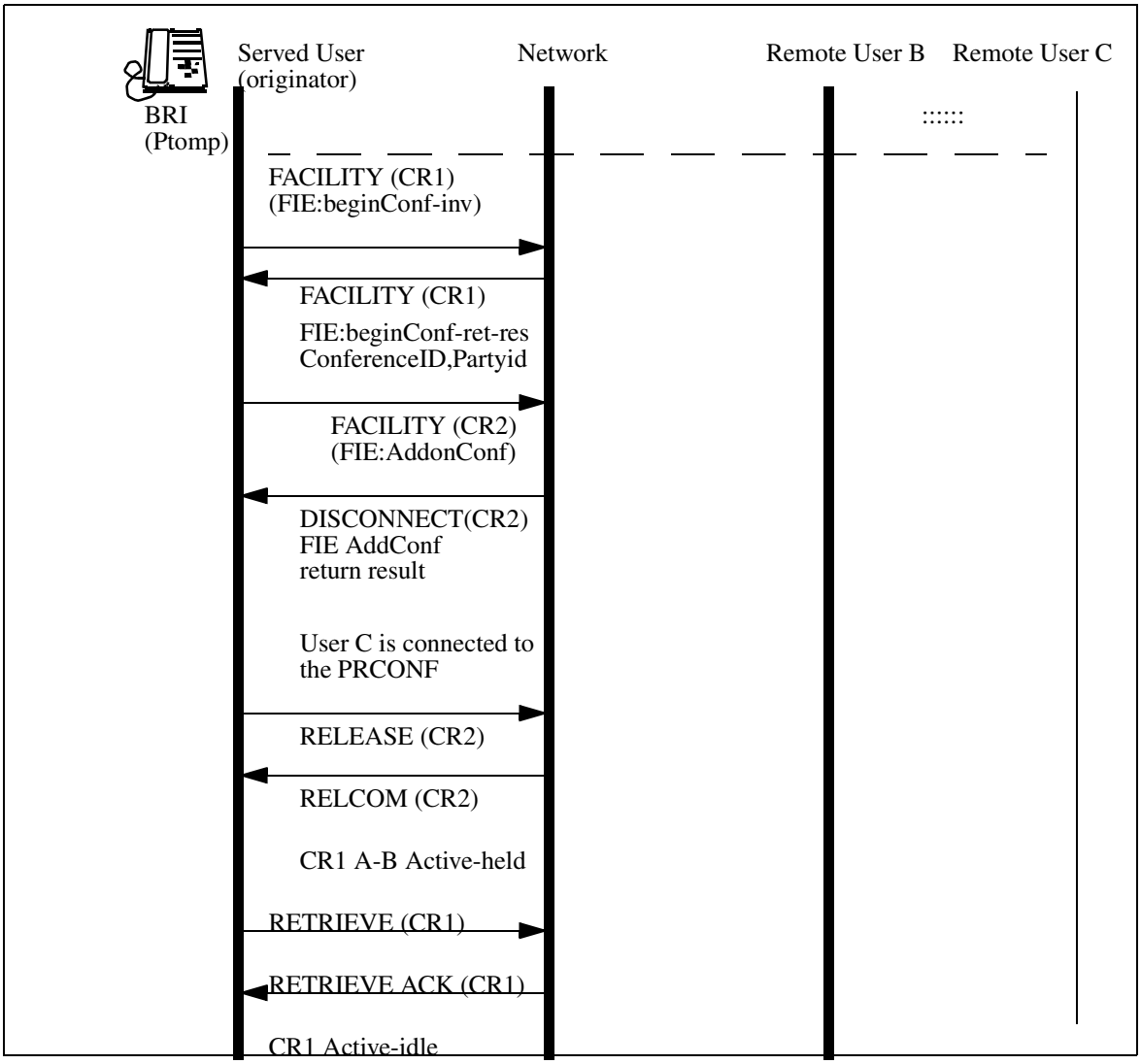
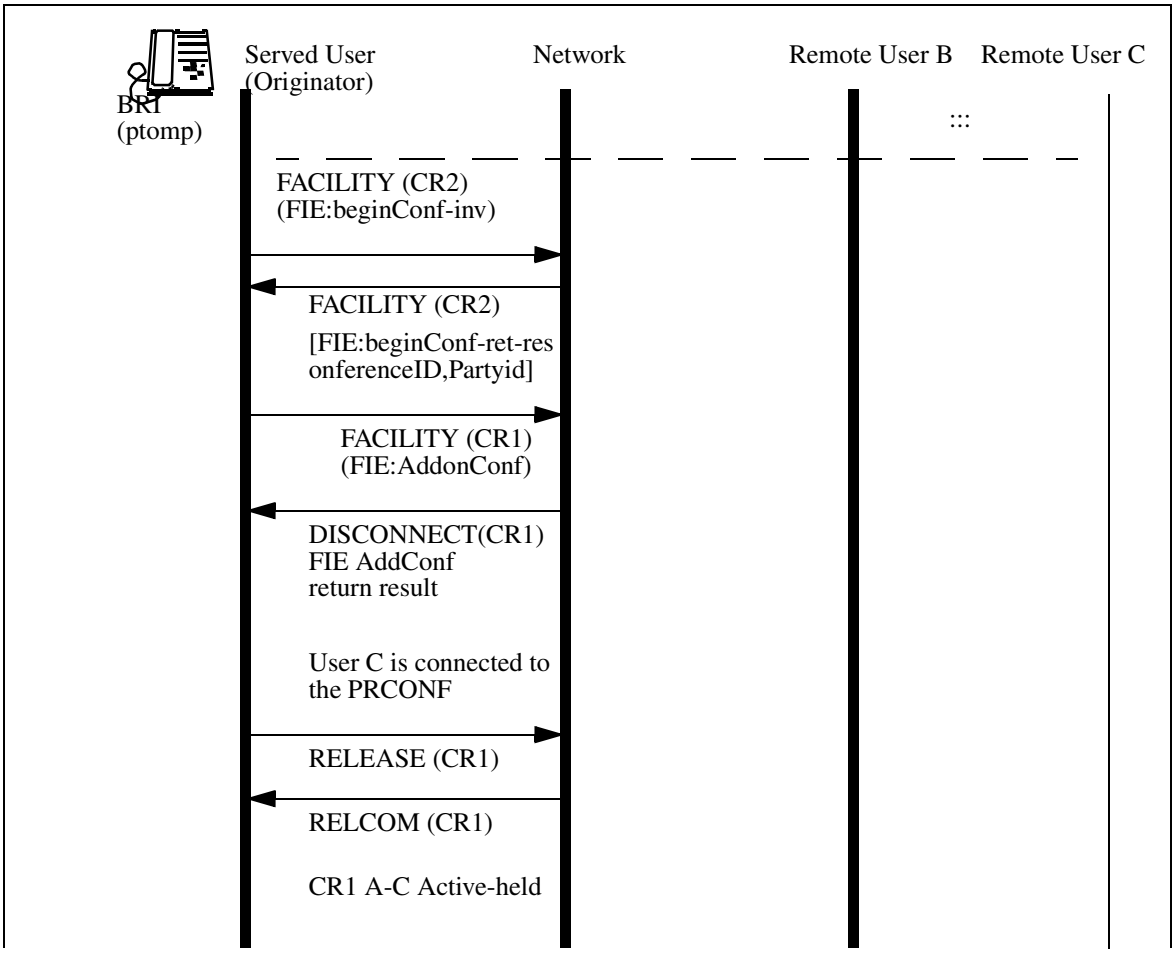


Figure 5 Add-on conferee, when preset conference is active-idle



42.2.3.2 Unsuccessful Case

Figure 6 Network receives a BeginCONF-inv in a state other then Active

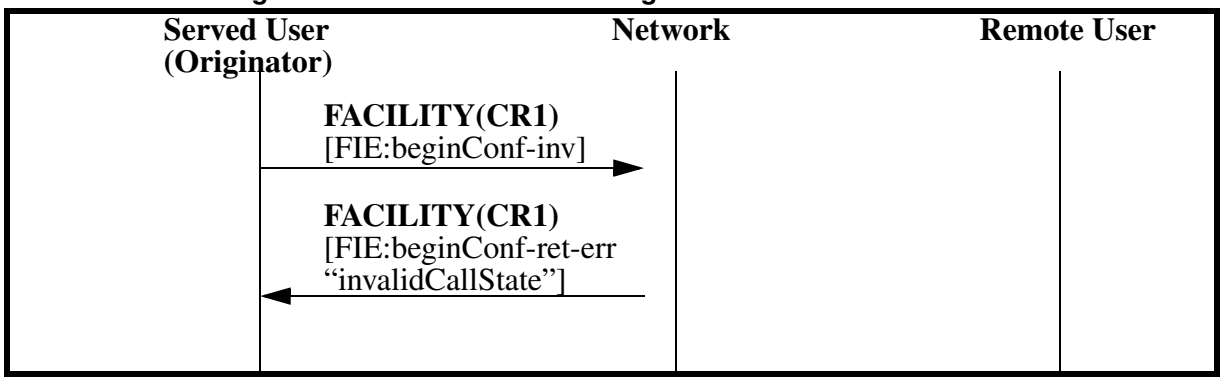


Figure 7 Adding a party which causes interworking restriction violations

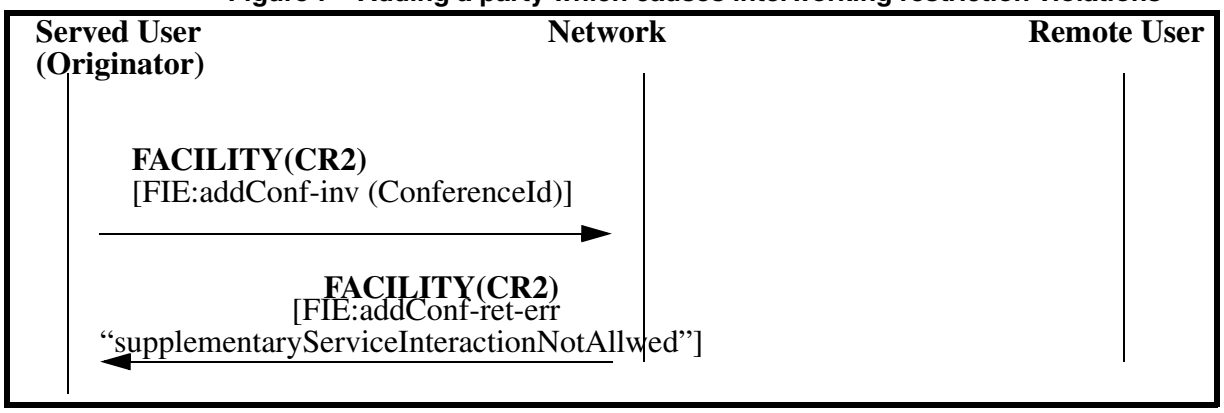


Figure 8 Served user indicates an inappropriate bearer capability.

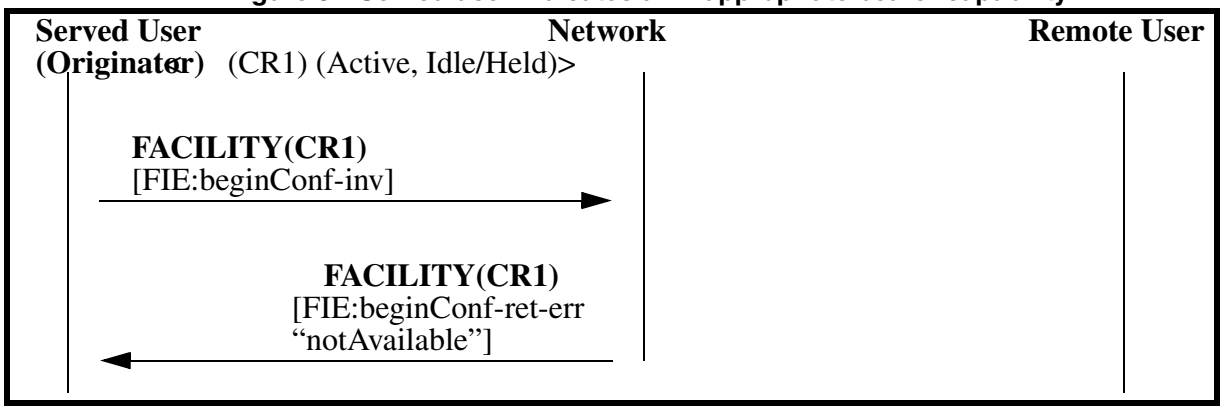
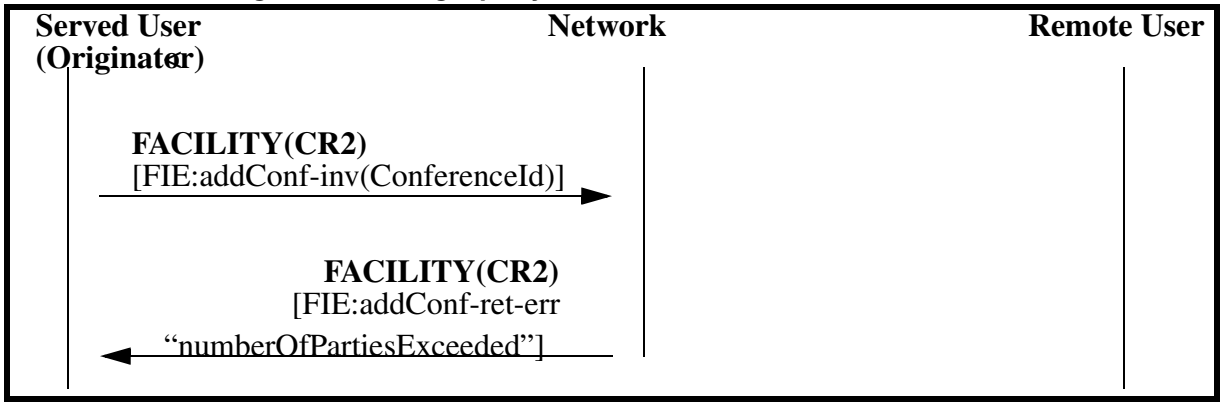


Figure 9 Adding a party when the maximum conference size is reached



Abbreviations used in sections 2.2.3.1 and 2.2.3.2 are described below:

CRx, CRy: Call Reference used-

A-B:call between user A and PRCONF

A-C:call between user A and user C

FIE: Facility information element.

42.2.4 Supplementary Services Interworkings

42.2.4.1 Interaction of Preset Conference with Advice Of Charge

42.2.4.1.1 General Information about AOC

AOC on BRI is a feature which allows ISDN subscribers to get the number of charge units that the calls they originate consumes. AOC can provide the actual charge unit count on a regular basis during a call or only at the end of a call, or both.The AOC functionality can be controlled/provisioned in the following ways:

- BRI loop (customer) basis, through table KSETFEAT via SERVORD. BRI lines provisioned via SERVORD can have a new option called AOC.
- XPM basis, through table LTCINV for PLGCs, in this table option attribute METER has to be present for all the XPMs that need to provide the AOC functionality.
- The zone (MZONE) and logical network (LNET) options are taken from the xxCODE translation table and the MDI index (MDI) is taken from table LINEATTR. With these 3 values, call processing is able to access the tariff database and to determine the tariff to be used for this call.

42.2.4.1.2 Test Considerations

Current behavior.

AOC will be provided for basic call and for add-on phase of preset conference and no AOC information will be generated for the use of PRCONF equipment and for the calls to the remote users with no additional code changes. AOC interaction with ETSI BRI preset conference will be supported for ETSI BRI origination test cases.

42.2.4.2 Interaction of Preset Conference with Call Waiting

42.2.4.2.1 General Information about CWT

CWT is a feature, which gives subscriber X (talking to subscriber Y) attention to a call from subscriber A. Subscriber X gets a special Call Waiting Tone as

sign of the waiting call. Subscriber A gets audible ringing. CWT functionality can be provisioned via Servord.

42.2.4.2.2 Test Considerations

Current behavior.

42.2.4.3 Interaction of Preset Conference with Call Hold/Retrieve

42.2.4.3.1 General Information about HOLD

HOLD is a feature, which enables subscriber A, talking to subscriber B, to hold B and make or receive a new call. HOLD functionality can be provisioned via Servord.

42.2.4.3.2 Test Considerations

Current behavior. Hold Indications including ISUP, hold announcement and silence will be supported.

42.2.4.4 Interaction of Preset Conference with Connected Line Identification Presentation

42.2.4.4.1 General Information about COLP

The COLP supplementary service provides the connected user's ISDN number to the calling user. COLP functionality can be provisioned via Servord.

42.2.4.4.2 Test Considerations

Current behavior.

COLP request is currently restricted in preset conference.

42.2.4.5 Interaction of Preset Conference with Completion of Call to Busy Subscriber

42.2.4.5.1 General Information about CCBS

The CCBS supplementary service enables user A, encountering a busy destination B to have the call completed without having to make a new call attempt when the destination B becomes not busy. When user A accepts the recall, the network will automatically generate a CCBS call to destination B. CCBS functionality can be provisioned via Servord.

42.2.4.5.2 Test Considerations

Current behavior.

CCBS to busy preset conference is currently prevented.

42.2.4.6 Interaction of Preset Conference with Three Party Service

42.2.4.6.1 General Information about 3PTY

The 3PTY supplementary service enables the user to establish, participate in and control, a three-way conversation, i.e. a simultaneous communication involving the served user and two remote parties. This feature requires HOLD functionality, it can be provisioned via Servord and table CONF3PR should be datafilled to activate 3PTY.

42.2.4.6.2 Test Considerations

Current behavior.

3PTY is not currently available for preset conference call.

42.2.4.7 Interaction of Preset Conference with Meet-me Conference

42.2.4.7.1 General Information about MMC

MMC provides a user with the ability to arrange for a call between more than two participants with all participants accessing a conference bridge.It is activated for a specified period booked in advance by the served user. MMC does not use SERVORD. In order for MMC to work properly, tables CUSTENG and MMCONF must be properly datafilled.

42.2.4.7.2 Test Considerations

Current behavior.

A dialing to a local MMC if a local PRCONF is active on the loop, is currently prevented.

42.2.4.8 Interaction of Preset Conference with Conference Call, Add-on

42.2.4.8.1 General Information about ECOF

This feature enables a user A to simultaneously with more than three parties. add any member to a conference, split a conference to have private conversation, isolate a remote user, reattach an isolated user, drop a conferee or disconnect the conference. This service is supported only in point to

multipoint configurations. ETSI HOLD must be present for the conference to function. Table CONF6PR should be datafilled to activate 3PTY.

42.2.4.8.2 Test Considerations

Current behavior.

Preset conference activity is based on ETSI BRI Six party conference.

42.2.4.9 Interaction of Preset Conference with Direct Dialing In

42.2.4.9.1 General Information about DDI

DDI enables a user to directly call another user on ana integrated services private branch exchange or other private system without attendant intervention. The service shall be based on the use of the ISDN number and shall be provided after pre-arrangement with the service provider.

42.2.4.9.2 Test Considerations

Current behavior.

42.2.4.10 Interaction of Preset Conference with Multiple Subscriber Number

42.2.4.10.1 General Information about MSN

MSN provides the possibility for assigning multiple integrated services digital network numbers to a single interface. This enables the selection of one or multiple distinct terminals attached to the same interface.The service provider shall fix the length of the numbers to be transmitted to the user s installation.

42.2.4.10.2 Test Considerations

Current behavior.

42.2.4.11 Interaction of Preset Conference with Diversion Services

42.2.4.11.1 General Information about Diversion Services

CFF, CFFA, CFGD, CFGDA, CFI, CFIND, CFK, CFMDN, CFO, CFRA, CFS, CFTANN, CFTB, CFTD, CFU, CFW, CFWANN,CFX, CFXDNCT, CFXVAL are different kind of diversion services. These functionalities allows the called number to be diverted to an other number under different circumstances.

42.2.4.11.2 Test Considerations

Current behavior.

42.2.4.12 Interaction of Preset Conference with Closed User Group

42.2.4.12.1 General Information about CUG

CUG provides a mechanism for forming groups to and from which access is restricted. A specific user may be member of one or more Closed User Groups. Members of a specific CUG can communicate among each other but not, in general, with users outside of the group. CUG can be provisioned via Servord and table ETSIFEAT should be datafilled to activate this functionality.

42.2.4.12.2 Test Considerations

Current behavior.

It is required that CUG shall be assigned against the PRCONF DN which is in virtual DN type, and handle from the served user to the PRCONF DN according to CUG settings.

42.2.4.13 Interaction of Preset Conference with Malicious Call Identification

42.2.4.13.1 General Information about MCID

Malicious Call Identification is a supplementary service offered to the called party which enables the called party to request that the calling party be identified to the network and be registered in the network. The data to be registered will be the called party number, calling party number, local time and date of the invocation in the network serving the called user; and as a service provider option: calling party sub-address (if provided by the calling user). MCID can be provisioned via Servord.

42.2.4.13.2 Test Considerations

Current behavior.

42.2.4.14 Interaction of Preset Conference with Subaddressing

42.2.4.14.1 General Information about SUB

The sub-addressing supplementary service allows the called (served) user to expand his addressing capacity beyond the one given by the ISDN number. SUB allows one party in a call to provide a network address extension to supplement the party's own network address or that of the other party. SUB can be provisioned via Servord.

42.2.4.14.2 Test Considerations

Current behavior.

SUB information is currently restricted during preset conference.

42.2.4.15 Interaction of Preset Conference with Explicit Call Transfer

42.2.4.15.1 General Information about ECT

Explicit Call Transfer is an ISDN supplementary service which enables a user who has two calls, each of which can be an incoming or an outgoing call, to connect the other parties in the two calls. ECT can be provisioned via Servord.

42.2.4.15.2 Test Considerations

Current behavior.

The served user can not currently transfer the call to the preset conference but remote users can currently use ECT. Use of ECT by the remote user is currently denied, if this would result in chaining of conferences. No addition to the existing code.

42.2.4.16 Interaction of Preset Conference with User to User Signalling

42.2.4.16.1 General Information about UUS

The UUS supplementary service allows the user to send/receive a limited amount of user-generated information to/from another user-network interface. UUS can be provisioned via Servord.

42.2.4.16.2 Test Considerations

If the served user provides UUS information in the SETUP message to the PRCONF DN, the same UUS information shall be included into the call setup to the conferees.This part of feature interaction will be provided by “BRI Preset conference base” feature (A00002367).

If UUS explicit request exist in SETUP message and service request is Required, the call will be released. Any other UUS information shall be discarded.

42.2.4.17 Interaction of Preset Conference with Multi Level Precedence and Preemption

42.2.4.17.1 General Information about MLPP

The Multi-level Precedence and Preemption (MLPP) supplementary service provides prioritized call handling service. This supplementary service has two parts precedence and preemption. Precedence involves assigning a priority level to a call. Preemption involves the seizing of resources, which are in use by a call of a lower precedence, by a higher level precedence call in the absence of idle resources. MLPP can be provisioned via Servord.

42.2.4.17.2 Test Considerations

If the served user provides MLPP information during call setup to the PRCONF DN, the same MLPP information shall be included into the call setup to the conferees. This part of feature interaction will be provided by "BRI Preset conference base" feature (A00002367).

The PRCONF service shall ensure, that the call from the served users is established as MLPP call, if this was requested.

If a PRCONF has been initiated and is still active any other call to this PRCONF DN shall NOT result in the preemption of the existing PRCONF. The second call to the active PRCONF shall result in busy treatment for the caller. Current behavior for this part.

A PRCONF shall not be preempt able by an attempt to initiate the same PRCONF from a served user with higher precedence level, that the served user who initiated the existing PRCONF. The second call to the active PRCONF shall result in busy treatment for the caller.

If a PRCONF, established as MLPP call, has been initiated from subscriber A and if the conferee's channels are occupied with MLPP calls with low precedence, preemption shall be prevented.

If a new MLPP call comes to a subscriber "A" whose both channels are occupied even one of them is involved in preset conference, (it is the case where subscriber "A" is a conferee of the preset conference) if the precedence of the new call is higher than preset conference call precedence, conference call shall be preempted by the new MLPP call. The figure below is a representation of this scenario.

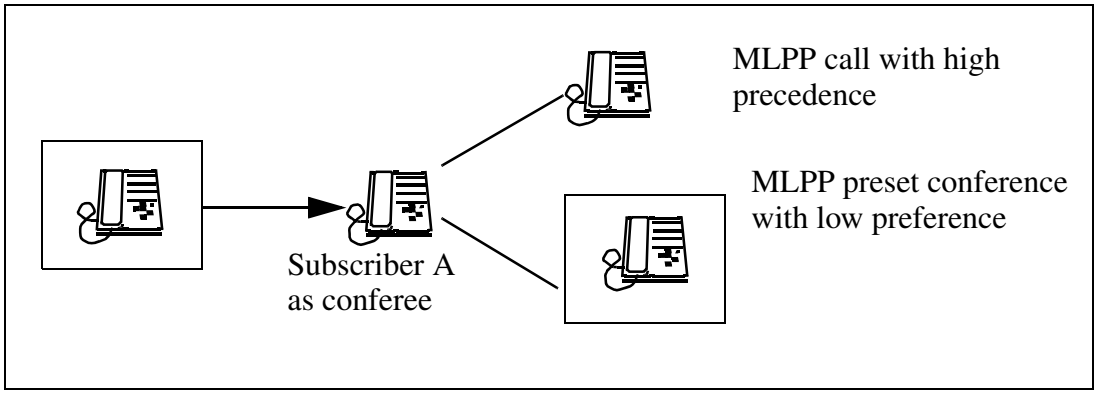


Figure 10 First scenario representation for MLPP - BRI preset conference interaction.

It shall be supported, that a PRCONF DN can be used as a valid Alternate Party for the MLPP service. This requirement will be supported if q955_compliant bool in MLPP_PARMS parameter in table OFCENG is set to “N”. If q955_compliant bool is set to “Y”, connect message will be waiting before routing the call to alternate number, and this timer can erase preset conference route time-out value, to prevent this event, preset conference route timer will be stopped and the call will be route to MLPP alternate number. During an MLPP call if the conferee of preset conference has an alternate number, preset conference tries once to reach the conferee. If the conferee does not answer, the call is routed to MLPP alternate number.

If a new MLPP call comes to served user whose both channels are occupied even one of them is involved in ETSI BRI preset conference, established as MLPP call with low precedence, the new MLPP call shall preempt and drop ETSI BRI preset conference.The figure below is a representation of this scenario

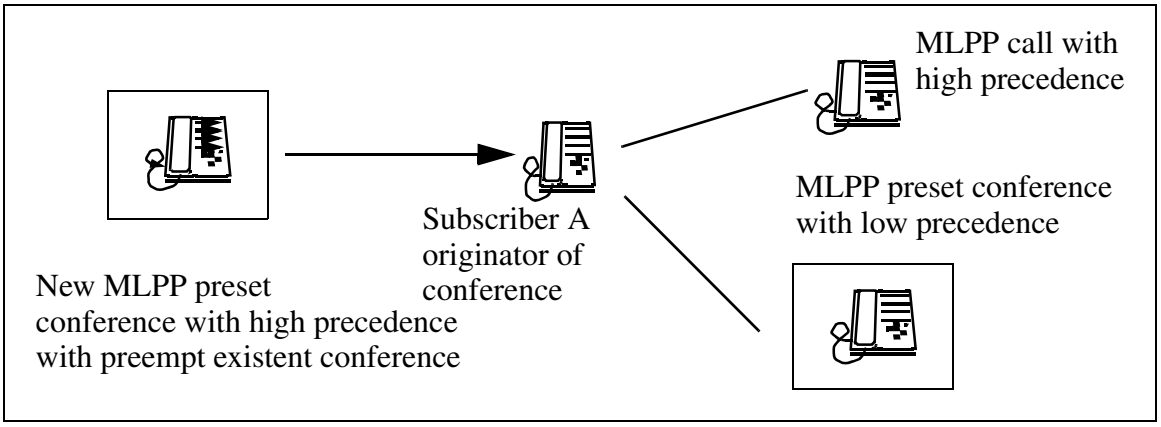


Figure 11 Second scenario representation for MLPP - BRI preset conference interaction.

After preemption, no notification indicator information element will be sent to served user or conferees.

If some of the calls making up the preset conference are non-MLPP (add-on functionality),

- Non-MLPP calls are assigned precedence level given by MLPP_DEFAULT_PRECEDENCE office parameter
- Highest precedence level of the legs is assigned as the precedence level of controller's conference leg. Conferees' legs are preserved their original precedence levels.

If all of the calls making up the conference are non-MLPP,

- Datafilled level on office parameter MLPP_DEFAULT_PRECEDENCE is assigned as the precedence level of both calls.

PRCONF shall ignore all other MLPP related signalling.

42.2.4.18 Interaction of Preset Conference with Calling Line Identification Presentation / Presentation Restriction

42.2.4.18.1 General Information about CLIP/CLIR

Calling Line Identification Presentation is a supplementary service offered to the called party which provides the calling party s ISDN-number, possibly with sub-address information, to the called party. When CLIP is applicable and activated, the network provides the called party with the number of the calling

party at call set-up on all incoming calls. The calling party number may be accompanied by a sub-address.

Calling Line Identification Restriction is a supplementary service offered to the calling party to restrict presentation of the calling party s ISDN-number and sub-address to the called party. When CLIR is applicable and activated, the originating node provides the destination node with a notification that the calling party s ISDN number and any sub-address information are not allowed to be presented to the called party. In this case no calling party number is included in the call offering to the called party's installation.

42.2.4.18.2 Test Considerations

The CLIP/CLIR information sent to the remote users during PRCONF establishing, shall be the same as being provided by the served user to the conference equipment. If the served user provides Generic Address Parameters and additional calling number identifications information in the SETUP message to the PRCONF DN, the same information shall be included into the call setup to the conferees (provided the respective protocol is supporting this).This part of feature interaction will be provided by "BRI Preset conference base" feature (A00002367).

For BRI-BRI, BRI-ISUP and ISUP-BRI interworkings, current working behavior of nosceerning will be kept. For Ex. BRI terminal with special arrangement triggers PRCONF, the unscreened CLI should also be send to the terminators).

42.2.4.19 Interaction of Preset Conference with Conference Chaining

42.2.4.19.1 General Information about Conference Chaining

Conference chaining shall be prohibited, if the conference equipment for both conferences resides on the same local exchange. But it is not possible to prevent conference chaining over remote connections since sent/received notifications are not permitted.

42.2.4.19.2 Test Considerations

No Impact.

42.2.5 OM class for Preset Conference

Since this activity is based on the existing IBN preset conference, the existing OM class PCNF is used.

OM class will be supported by “Preset Conference Base” feature (A00002367). For detailed information please refer to FN document of A00002367.

42.2.6 Billing

No AMA/Billing changes for this activity.

42.3 Hardware Requirements or Dependencies

The NT3X67 six-party conference card provides conference facilities on a single card for use with DMS-100 switches. This activity uses same hardware as IBN Preset Conference.

Since the feature is based on BRI Preset Conference Base, hardware requirements or dependencies of BRI Preset Conference are also valid for this activity.

42.4 Software Requirements or Dependencies

The existing IBN preset Conference is used by this activity.

42.5 Limitations and restrictions

1. Since the feature is based on the existing IBN Preset Conference, and a continuation of BRI Preset Conference Base, the restrictions of IBN preset conference and BRI Preset Conference are also valid for this activity.
2. Since section 4 of Preset Conference for BRI Supplementary Services” specification document which specifies the required interworking for PRCONF on BRI lines, does not contain any information about IBN lines CEPT and CENTREX features interactions, it is assumed in the development of this activity that any changes on the existing interworking which should be supported by the “IBN Preset Conference “feature.
3. If any of the conferees are connected to the DMS switch where the preset conference is being originated and has any of the diversion feature these feature will remain active for incomming preset conference call. If the primary address does not answer call forwarding will be attented if it is activated. On origination to a conference,diversion features will be deactivated. In other words, a direct access user cannot forward incoming calls to a preset conference.

42.6 Interactions

IBN Preset Conference

No Impact

BRI Preset Conference Base

No Impact

10 AFC Keys for BRI Directory Number

“10 AFC Keys for BRI Directory Number” feature (A00002377) allows up to 10 AFC keys on one DN and allows also, 11 call HOLD on one DN and 8 call waiting per loop if the customer is subscribed to these services.To be able to support more than one HELD, it is permitted to make more than two calls on one TEI. That can cause problem if there are two different preset conferences on one TEI and if this TEI tries to send ADDCONF FAC for a new call. Since there is no way to decide to which conference the new call will be added, one of the restrictions below will be followed:

- Two preset Conferences will not be allowed on one TEI.
- Add-on conference will be restricted if there are two preset Conferences on one TEI.
- The new call will be added on a random conference.

According to the information given above, please refer to A00002367 “BRI Preset Conference Base” and A00002377 “10 AFC Keys for BRI Directory Number” features.

42.7 Applicable customer facing sections

Fault Management	
Logs	No
Alarms	No
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A

Performance (includes operational measurements) N/A

42.8 Glossary

Term	Description
ETSI	European Telecommunications Standard Institute
BRI	Basic Rate Interface
DN	Directory Number
IE	Information Element
AOC	Advice Of Charge
CWT	Call Waiting
PRCONF	Preset Conference
COLP	Connected Line Identification Presentation
CCBS	Completion of Call to Busy Subscriber
3PTY	Three Party Service
MMC	Meet-me Conference
DDI	Direct Dialing In
MSN	Multiple Subscriber Number
CUG	Closed User Group
SUB	Subaddressing
ECT	Explicit Call Transfer
MCID	Malicious Call Identification
UUS	User to User Signalling
MLPP	Multi Level Precedence and Preemption

42.9 Appendix A- IBN Preset Conference Interactions Background

“IBN Preset Conference (large)” feature (AF2014) enables the maximum number of conferees for an Meridian Digital Centrex (MDC) preset conference to be increased to 50.
The feature interactions required for this feature are described below:

1) If any of the conferees are connected to the DMS switch where the preset conference is being originated and has any of the following features

- Call forwarding don’t answer
- Call forwarding busy
- Call forwarding intragroup

these features will remain active for the incoming preset conference call (if the primary address does not answer call forwarding will be attempted if it is activated).

2) If the originator is active in any conference, flashes, or depresses a CONF key and dials a preset conference DN busy treatment is given. Two preset conferences can not be in conference together.

3) If the preset conference call has been originated in the switch, SMDR may apply to one or more legs. Each leg will be a separate record with conference identification in the SMDR report.

43: Functional Description (FN): A00002900

43.1 Feature Name

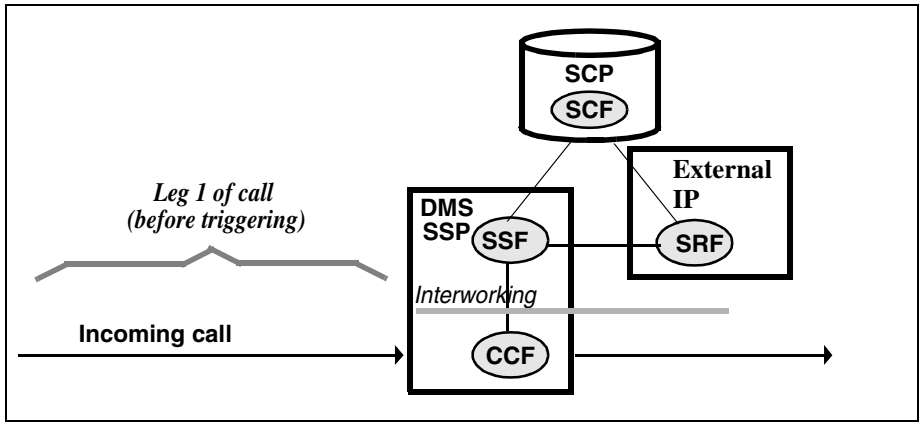
China INAP Compliance Enhancement Part 2

43.2 Description

43.2.1 Functional Overview

This feature will enhance the external IP capabilities and support multiple ApplyChargings on ISN07 TDM and CS2Kc platform for China market. The external IP supported in this feature has direct connection through China ISUP to SCP (as figure 1), SSP would not provide assisting SSP functionality.

Figure 1 Network diagram



This feature is based on feature A89008388: China IN SSP capabilities and feature AG5145: External IP, please see reference 7,10 for more information.

Two main functionalities are implemented in this feature:

- External IP enhancement

  For China INAP, several enhancements are made to fully support external IP:

  - Enhance operation EstablishTemporaryConnection
  - Enhance operation InitialDP

    Parameter iPAvailable and iPSSPCapabilities are required in IDP operation. SSP is able to set these two parameters by datafill.
  - Charging the temporary connection to external IP using ApplyCharging operation

    According to China requirement, charging to the temporary connection to external IP is required. Charging per duration and time are both supported in this feature.
  - Unsuccessful connection to external IP handling enhancement

    Several scenarios of unsuccessful connection to external IP are enhanced to comply with China requirement.
  - CISUP: Map the post answer ANM(CON) to CPG
- Multiple ApplyChargings support
  - Support up to 3 ACs

    Now up to 3 ACs can be accepted and handled simultaneously during an INAP call. For multiple ACs, corresponding ACRs can be sent to SCP if required.

Function ‘CISUP: Map the post answer ANM(CON) to CPG’ is for China ISUP originator only. The other functions are agent independent, i.e. they are supported on the originating agents with the condition: the originating agent <-> INAP interworking is ALREADY supported. For example, China ISUP, IBN lines, SIP-T (no ISUP), China PRI.

These functions are detailed in Section 2.2.2 to 2.2.3.

43.2.1.1 Functional Requirements

The functions to enhance China IN SSP capabilities are based on the following specification:

— China INAP specification (See reference 1)

— China INAP test specification (See reference 2)

— Supplementary Specification of China IN CS-1 INAP (See reference 3)

— Test specification of Supplementary Specification of China IN CS-1 INAP (See reference 4)

43.2.1.2 Data Requirement

The datafill is the same as that for normal IN call.

43.2.2 External IP enhancement

43.2.2.1 EstablishTemporaryConnection enhancement

The ETC is defined as below in China INAP specification:

```
EstablishTemporaryConnection OPERATION
  ARGUMENT
    SEQUENCE {
      assistingSSPIPRoutingaddress [0] IMPLICT OCTET STRING;
      correlationID[1] IMPLICT OCTET STRING OPTIONAL;
      legID [2] CHOICE{
        sendingSideID[0] IMPLICIT OCTET STRING( SIZE(1) )} OP-
        TIONAL;
      scfID [3] IMPLICT OCTET STRING(SIZE (3)OPTIONAL;
      .....}
```

Parameters scfID and legID are supported in this feature. legID indicates which leg of a call is connected to the SRF for user interaction. Currently, external IP can only be connected to calling party. This feature will only support the decode of parameter legID.

Parameter correlationID has fixed length 3 bytes.

Parameter assistingSSPIPRoutingAddress is checked according to China INAP requirement:

— the format is Generic number

— If scfID and correlationID are not contained in assistingSSPIPRoutingaddress, the NOA of assistingSSPIPRoutingaddress should be national number(0000011) or Subscriber number(0000001). For national number, it consists of the prefix 0, Area code and office code, the length of the number is 4~8. For Subscriber number, it consists of office code, the length of the number is 4~5.

For the outgoing IAM to external IP, the format of CDPN within IAM is different considering that the number of CDPN is even or odd. Examples are shown in table 1 and 2:

Table 1 CDPN with 8 digits assistingSSPIPRoutingAddress

	8	7	6	5	4	3	2	1
1	Even	Nature of Address						
2	INN indica-tor	Numbering Plan Indicator			Spare			
3	2nd Assisting Address Signal				1st Assisting Address Signal			
4	4th Assisting Address Signal				3rd Assisting Address Signal			
5	6th Assisting Address Signal				5th Assisting Address Signal			
6	8th Assisting Address Signal				7th Assisting Address Signal			
7	2nd SCF ID				1st SCF ID			
8	4th SCF ID				3rd SCF ID			
9	6th SCF ID				5th SCF ID			
10	2nd Correlation ID				1st Correlation ID			
11	4th Correlation ID				3rd Correlation ID			
12	6th Correlation ID				5th Correlation ID			

Table 2 CDPN with 7 digits assistingSSPIPRoutingAddress

	8	7	6	5	4	3	2	1
1	Odd	Nature of Address						
2	INN indica-tor	Numbering Plan Indicator			Spare			
3	2nd Assisting Address Signal				1st Assisting Address Signal			
4	4th Assisting Address Signal				3rd Assisting Address Signal			
5	6th Assisting Address Signal				5th Assisting Address Signal			
6	1st SCF ID				7th Assisting Address Signal			
7	3rd SCF ID				2st SCF ID			
8	5th SCF ID				4th SCF ID			
9	1st Correlation ID				6th SCF ID			
10	3rd Correlation ID				2nd Correlation ID			
11	5th Correlation ID				4th Correlation ID			

12	Filler (0)	6th Correlation ID

43.2.2.2 InitialDP enhancement

According to China INAP, IPAvailable and IPSSPCapabilities should be supported in IDP operation, SSP should fill these two parameters according to its abilities.

In order to build iPAvailable and iPSSPCapabilities into IDP, option INITDP_PARM of table SERVINFO is extended to add two new fields **IP_AVA** and **IPSSP_CAP** to indicate whether parameters IPAvailable and IPSSPCapabilities will be carried in IDP. These two fields should be datafilled at the same time. These two fields can also be datafilled for those variant other than China.

Meanwhile, option SRF_INFO is extended to add new filed **IP_INFO** to provide detailed information of the IP capability within SSP.

For China market, if IP_AVA and IPSSP_CAP are datafilled and IP_INFO is not datafilled, parameters iPAvailable and iPSSPCapabilities are set to default value according to China INAP, the default value of iPAvailable is ‘01’H (which indicates that the IP is available), the default value of iPSSPCapabilities is ‘#0C00’ (which indicates that DTMF digit collection and tone & announcement is supported). If IP_INFO is datafilled, then iPAvailable and iPSSPCapabilities are set according to this datafill. That means IP_INFO will take effect only if IP_AVA and IPSSP_CAP are datafilled, otherwise, the information of this datafill will not be carried in IDP.

IP_INFO contains two subfields: IP_AVAILABLE and IPSSP_CAPABILITIES, which contains values for parameter IPAvailable and IPSSPCapabilities respectively.

According to China INAP, there are 14 kinds of IP capabilities which are indicated by parameter iPSSPCapabilities. These capabilities can be datafilled in IPSSP_CAPABILITIES as shown in table 3:

Table 3 IP Capabilities defined in China INAP

IPSSPCapabilities parameter	Value	Meaning	IPSSP_CAPABILITIES selections
1st byte, bit 0	0/1	Not support/Support IPRoutingAddress	IPRA
1st byte, bit 1	0/1	Not support/Support VoiceBack	VOICE_BACK
1st byte, bit 2	0/1	Not support/Support VoiceInformation, recognize through voice, speech.	VOICE_INFO_SPEECH
1st byte, bit 3	0/1	Not support/Support VoiceInformation, recognize through voice, voice.	VOICE_INFO_VOICE

1st byte, bit 4	0/1	Not support /SupportText to Voice conversion.	TEXT_TO_VOICE
1st byte, bit 5	0/1	Not support/Support fax.	FAX
1st byte, bit 6	0/1	Not support/Support recorder.	RECORDER
1st byte, bit 7	0/1	Not support/Support script.	SCRIPT
2nd byte, bit 0	0/1	Not support/Support manual operator.	MAN_OPERATOR
2nd byte, bit 1	0/1	Not support/Support conference.	CONFERENCE
2nd byte, bit 2	0/1	Not support/Support tone & announcement.	TONE_ANNC
2nd byte, bit 3	0/1	Not support/Support DTMF digit collection.	DTMF_DIGCOL
2nd byte, bit 4	0/1	Not support/Support sending DTMF signal.	SEND_DTMF_SIG
2nd byte, bit 5	0/1	Not support/Support sending FSK signal.	SEND_FSK_SIG
2nd byte, bit 6,7	To be defined.		
3rd, 4th bytes	To be defined.		

Below is an example of datafill:

Table 4 SERVINFO datafill example

Example of datafill:
TABLE SERVINFO
200 (INITDP_PARMS (SERVKEY) (CDPA) (**IP_AVA**) (**IPSSP_CAP**) $)
(SRF_INFO (EARLY_ANS ANS_ON_ANNS)
(**IP_INFO Y** (**IPRA**) (**VOICE_INFO_SPEECH**)
(**TONE_ANNC**)(**DTMF_DIGCOL**)$)$)$

43.2.2.3 Charging the temporary connection to external IP using ApplyCharging operation

Currently, DMS SSP does not charge the temporary connection to external IP. According to China INAP:

If the charging is based on duration:

— SCP should send AC before ETC, and the startChargePattern is ‘AnswerReceived’

— When SSP receives AC and ETC, SSP begin to prepare for charging. SSP start charging after receiving answer message from external IP.

When originator abandon, SSP releases the connection to external IP or SSP receives release message, the charging is stopped, and ACR is sent to SCP.

— The other requirement of processing AC parameters are not changed.

If the charging is based on time:

— SCP can send AC before ETC or during the speech phase. If AC is sent before ETC, then the startChargePattern can be ‘Immediately’ or ‘AnswerReceived’. Otherwise, if AC is received during the speech phase, the startChargePattern should be ‘Immediately’.

— The fee is carried in surCharge parameter of AC, meanwhile AC does not carry chargeClass parameter.

— SSP can send ACR immediately or after the connection to external IP is released.

43.2.2.4 Unsuccessful connection to external IP handling enhancement

If the ETC is received between PA and SRR, SSP should report unexpected component sequence error.

43.2.2.5 CISUP: Map the post answer ANM(CON) to CPG

There are two conditions under which the mapping will occur:

— Condition 1: SSP has received an answer message from external IP or called party and transmitted it to the originating office, when the SSP connect to the external IP or the called party (if the first connection is to external IP) again, SSP will receive another answer message.

— Condition 2: SSP has received CTR and PCUI, SSP sent ACM and ANM to the originating office, when the called party answer, SSP will receive another answer message.

This functionality will implement that: if the second or later answer message is CISUP ANM containing BCI or CISUP CON, then it will be mapped to CPG and transmitted to the originating office.

43.2.3 Multiple ApplyChargings support

43.2.3.1 Support up to 3 ACs

In this feature, up to 3 ACs can be accepted and handled simultaneously during an INAP call. The number 3 is the maximum number of in-effect ACs, it does not include the number of expired(that is, a final ACR has been sent) ACs.

The chargeRecordIdentifier parameter is used to identify the AC operation, different ACs should have unique chargeRecordIdentifier. If two ACs have an identical chargeRecordIdentifier, then the newly received one will be rejected with ReturnError (UnexpectedDataValue).

If an AC with chargeUserIndicator equaling 1(calling party) or 2(called party) had been received, then any subsequent ACs with the same chargeUserIndicator will be rejected with ReturnError(TaskRefused(generic)). In orther words, on a call at most 1 AC is allowed for the calling/called party. However, this restriction does not apply to the specified charge number(chargeUserIndicator = 127).

If there are already 3 ACs in effect on the call, then all subsequent ACs will be rejected with ReturnError(TaskRefused(generic)).

For multiple ACs, corresponding ACR(s) can be sent respectively for each AC. ACR will be sent to SCP in three conditions:

1. If the calling/called party hangs up, the following actions are taken:
   - The call (or only the called party, depending on the on-hook party and armed EDPs) is taken down
   - ACR for each AC is sent respectively
2. If the cost/time limit for one of the ApplyChargings is reached, the following actions are taken:
   - The call (or only the called party, depending on armed EDPs) is taken down
   - The forceReleaseCause in the ApplyCharging whose charge/time limit is reached is stored in the backward release message
   - ACR for each AC is sent respectively. If the supervisionMethod in the AC for which we are sending ACR is costGranted, the reasonForReport parameter in the ACR is ChargeLimitReached; if the

supervisionMethod is timeGranted, the reasonForReport is TimeLimitReached.

3. If the heartbeat timer for one of the ApplyChargings expires, the following action is taken:
   - An ACR for the AC is sent

Multiple treatments can be played if more than one ACs require warning tone/ announcement to be played at a desired time before the charge/time limit is reached, provided the restrictions below:

— All tones/announcements are only played to the calling party

— If multiple treatments are required to play at almost the same time, DMS SSP will play the 1st started treatment and suppress other treatments which try to start at the time when the 1st treatment is playing.

43.3 Hardware Requirements or Dependencies

N/A.

43.4 Software Requirements or Dependencies

N/A.

43.5 Limitations and restrictions

N/A.

43.6 Interactions

N/A.

43.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	X
User Interface	N/A
Element Management	N/A

Security N/A

Service Order N/A

Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

43.8 Glossary

Term	Description
ACH / AC	Apply Charging
ACR	Apply Charging Report
ACM	Address Complete Message
ANM	Answer Message
CDPN	Called Party Number
CISUP	China ISDN User Part
CODEC	Coder/Decoder
CON	Connect
DMS	Digital Multiplex System
ETC	Establish Temporary Connection
IAM	Initial Address Message
IDP	initial DP
IN	Intelligent Network
INAP	Intelligent Network Application Part
IP	Intelligent Peripheral
ISUP	ISDN User Part
SCP	Service Control Point
SSP	Service Switching Point

43.9 References

1. GF017-1995 China INAP Specification
2. YDN107.2-1999, INAP test spec - SSP part
3. Supplementary Specification of China IN CS-1 INAP (draft)

4. Test specification of Supplementary Specification of China IN CS-1 INAP (draft)

5. Requirement of China Telecom Intelligent Network Intelligent IP Establishment. China Telecom, 2002, January

6. SSP (IP related) INAP Specificationn and Signalling coorperation test specification of China Telecom Intelligent Network. China Telecom, 2001, January

7. AG5145 IN SSP REL 3.0 HLD: External IP

8. AG5089 WT IN SSP REL 3.0

9. A59039729 - CS1R China ISUP Calling Card Service

10. A89008388 - China IN SSP capability

44: Functional Description (FN): A00002904

44.1 Feature name

CTI Toggle.

44.2 Description

The Switch-Computer Applications Interface (SCAI) specifies an architecture and an Open Systems Interconnection (OSI) application layer protocol suite for peer-to-peer data communication between host computer applications and switch applications, thereby enabling the functional integration of computer systems and telephony switching systems.[1]

Remote Operation Service Element (ROSE) is used to support the interactive communication between the switch and host application.

Currently, ICM services exist for the use of four types of customers.

- Automatic Call Distribution (ACD) customers
- Meridian Digital Centrex (MDC) customers
- Residential (RES) customers
- SL-100 Private Branch Exchange (PBX) customers

ICM uses the following Operation Classes.

- Class 1: Synchronous, reporting success or failure
- Class 2: Asynchronous, reporting success or failure
- Class 5: Asynchronous, outcome not reported

This activity adds a Class 2 call control message, DV_TOGGLE_CALL, which is sent from the customer's host computer to the DMS to toggle between an agent's primary call leg and the consult call leg. The existing ICM messages DV_CALL_HELD_U and DV_CALL_UNHELD_U, will be changed to contain a new parameter that would indicate which leg of the call was held/unheld. The DV_CALL_HELD_U and DV_CALL_UNHELD_U messages will be sent out after a successfull completion of the DV_TOGGLE_CALL message. The above two messages will also be sent out when the calls are toggled manually.

[1]Taken from the ANSI SCAI Standard document: ANSI TI.626-1993

44.2.1 Application Logon SCAI Service Version

The dv-Appl-Logon message contains a parameter, Service Version, which uniquely identifies the version of messages which will be sent during the session. A new Service Version value will be created to uniquely identify the stream of messages which are new or changed during this software release. The new Service Version will be SCAI18.

This new Service Version (SCAI18) must be specified in the dv-Appl-Logon message for the host application to send dv_Toggle_Call messages. If a Service Version lower than SCAI18 is specified, dv_Toggle_Call messages will not be availabe to the Host.

The Service Version is upward compatible. This means all of the functionality enabled and provided with any of the previous Service Versions will be provided in SCAI18. Future DMS-100 software releases will provide additional ICM functionality but will continue to allow the specification of the SCAI18 Service Version. Therefore, applications written to use SCAI18 will not require rewriting to continue to work properly.

44.2.2 Subscription to the new call control message and changed call held/ unheld message.

The following changes in the table SCAISSRV are required to provide subscription to send the new ICM call control message DV_TOGGLE_CALL and the changed call event messages DV_CALL_HELD_U and DV_CALL_UNHELD_U.

44.2.2.1 Subscription for ACD

- A new default tuple TPCC16$ under category TPCC will be created with the new function TOGGCALL for the new message DV_TOGGLE_CALL. TPCC16$ will also contain the optional parameter HDUHDLEG of the function CALLHELD and CALLUNHELD set to Y

44.2.2.2 Subscription for Residential and Centrex lines

- A new default tuple SCAI3WC15$ under the category SCAI3WC will be created with the new function TOGGCALL, for the new message DV_TOGGLE_CALL.
- A new default tuple SCAICC10$ under the category SCAICC will be created with the optional parameter HDUHDLEG of the function CALLHELD and CALLUNHELD set to Y.

44.2.3 Toggle Call Message and changed Held/Unheld message Setup and Validation

The following setup and conditions must be met in order for the host application to invoke the dv-Toggle-Call message.

1. The SCAI Service Version is at least SCAI18
2. An ICM switch-host session is established. A successful dv-Appl-Logon request was sent by the host computer.
3. The line which the host application is monitoring must be associated to the session via dv-DN-Associate.
4. For Centrex/Res lines the line option ECM with suboption CONF_XFER set to 'Y' needs to be assigned to send DV_TOGGLE_CALL.
5. For Centrex/Res lines the line option ECM with suboption SCAICC set to 'Y' needs to be assigned to receive the changed DV_CALL_HELD_U and DV_CALL_UNHELD_U messages.
6. The switch-host session is subscribed to the new call control message, DV_TOGGLE_CALL and the changed messages DV_CALL_HELD_U and DV_CALL_UNHELD_U (SEE SECTION 2.2.2).

44.2.4 Message Protocol

The ASN.1 notations for the new call control message provided by this activity, DV_TOGGLE_CALL is shown in this section. A sample X.209 hex encoding has been provided here. The length fields are variable because the length depends on the variable content. The tag values are taken from the ROSE protocols.

44.2.4.1 Toggle Call ASN.1 Encoding

```
dv-Toggle-Call          OPERATION
                        ARGUMENT        ToggleCallArgument
                        RESULT          ToggleCallResult
                        ERRORS          { invalid-Call-State, missing-Parameter,
                                          invalid-Parameter, not-Allowed,
                                          agent not Logged In}
::= 51
ToggleCallArgument          ::=     SEQUENCE
    { origAddress           [2] AddressType                     OPTIONAL}

    AddressType             ::=     CHOICE
        { positionID        [0] IMPLICIT INTEGER,
          dialedDigits      [1] IMPLICIT IA5String,
          stationNumber     [2] IMPLICIT OCTET STRING,
          q.931Address      [3] Q.931AddressType }

    ToggleCallResult        ::=     SEQUENCE
        { networkCallID     [0] IMPLICIT SEQUENCE
```

```
        { networkNodeID      [0] IMPLICIT INTEGER          OPTIONAL,
          localCallID        [1] IMPLICIT INTEGER          OPTIONAL }
                                                           OPTIONAL }

invalid-Call-State      ERROR           ::= 0

missing-Parameter       ERROR           ::= 1
                        PARAMETER       MissingParameter

MissingParameter            ::=     SEQUENCE
 { missingParameterType     [0]     IMPLICIT ENUMERATED
   { missingOrigAddress             (1) }                 OPTIONAL }

invalid-Parameter       ERROR           ::= 2
                        PARAMETER       InvalidParameter

InvalidParameter            ::=     SEQUENCE
 { invalidParameterType     [0]     IMPLICIT ENUMERATED
   { invalidOrigAddress             (2) }                 OPTIONAL }

not-Allowed             ERROR           ::= 3
agent-Not-Logged-In     ERROR           ::= 5
```

44.2.4.2 Toggle Call Coded Example

As shown in "Toggle call between Customer and Advisor2," a host has requested the switch to toggle the call from Customer - Adviosor1 call to Customer-Advisor2 call. The following encoding has to be sent from the host to the DMS to cause the Customer-Advisor1 call to be put on hold and the Customer-Advisor2 call to become active. It is assumed that before the message is sent, the Customer-Advisor1 call was active and Customer-Advisor2 call was on hold.

INVOKE **HOST ===> DMS**

Table 4: dv-Toggle-Call Coded Example

Hex Dump			Information Element	Comments
Tag	Len	Content		
A1	10		INVOKE	the message length is 16 bytes decimal
02	01	1F	. .InvokeID	its Invoke ID is decimal 31
02	01	33	. .Operation	its operation value is dv-Toggle-Call [51] decimal
Hex dump = A1 10 02 01 1F 02 01 33 30 08 A2 0C 82 04 01 05 0A 04				

Table 4: dv-Toggle-Call Coded Example

Hex Dump			Information Element	Comments
Tag	**Len**	**Content**		
30	08		. .Argument	Toggle Call Arg is of type Sequence and is 8 bytes long decimal
A2	0C		. . . . origAddress	the origination address is of type constructor and is 12 bytes long
82	04	01 05 0A 04	. . . . . . posid	the posid is 5540
Hex dump = A1 10 02 01 1F 02 01 33 30 08 A2 0C 82 04 01 05 0A 04				

RETURN-RESULT HOST <=== DMS

Table 5: dv-Toggle-Call Return Result Coded Example

Hex Dump			Information Element	Comments
Tag	**Len**	**Content**		
A2	13		RETURN RESULT	the message length is 19 bytes decimal
02	01	1F	. .InvokeID	its Invoke ID is decimal 31
30	0E		. .Return Result Sequence	this sequence is 14 bytes long decimal
02	01	33	. . . . Operation	its operation is dv-Toggle-Call [51]
30	09		. . . . Toggle Call Result	the Toggle CallResult is of type Sequence and is 9 bytes long
A0	07		. . . . . . Network Call ID	NetworkCallId is of type Sequence and is 7 bytes long
80	01	01	. . . . NetworkNodeID	Network Node ID is 1
81	02	05 55	. . . . Local Call ID	Local Call ID is 1365.
Hex dump = A2 13 02 01 1F 30 0E 02 01 33 30 09 A0 07 80 01 01 81 02 05 55				

The following return error would be sent if a toggle call was requested on a set that did not have a consult leg call or if the set has conferenced the primary call and the consult leg call.

RETURN-ERROR HOST <=== DMS

Table 6: dv-Toggle-Call Return Error Coded Example

Hex Dump			Information Element	Comments
Tag	Len	Content		
A3	06		RETURN Error	the message length is 6 bytes decimal
02	01	1F	. .InvokeID	its Invoke ID is decimal 31
02	01	00	. . . . Error Value	Error Value is 0 representing Invalid Call State.
Hex dump =A3 06 02 01 1F 02 01 00				

44.2.5 Message Protocol

The ASN.1 notations for the changed call event message provided by this activity, DV_CALL_HELD_U is shown in this section. A sample X.209 hex encoding has been provided here. The length fields are variable because the length depends on the variable content. The tag values are taken from the ROSE protocols.

44.2.5.0.1 Call Held ASN.1 Definition

```
dv-CALL-HELD-U          OPERATION
                        ARGUMENT        CallHeldArgument

::= 50

CallHeldArgument::=             SEQUENCE
    {networkCallID      [0]     IMPLICIT SEQUENCE
        {networkNodeID          [0] IMPLICIT INTEGER        OPTIONAL,
         localCallID            [1]     IMPLICIT INTEGER OPTIONAL}
                                                            OPTIONAL,
         heldParty      [1]     Address Type                OPTIONAL,

        heldLeg         [2]     IMPLICIT ENUMERATED

            {heldPrimaryLeg             [0] OPTIONAL,

             heldConsultLeg             [1] OPTIONAL}

                                                    OPTIONAL}

AddressType:=                   CHOICE
 {positionID            [0]     IMPLICIT        INTEGER, (ONLY CHOICE)
```

```
dialedDigits              [1]    IMPLICIT      IA5STRING,
stationNumber             [2]    IMPLICIT      OCTET STRING,
q.931Address              [3]    Q.931AddressType}

Q.931AddressType:=                SEQUENCE
 {numberTypeNumberPlan [0]IMPLICIT                OCTET STRING OPTIONAL,
presentationScreeningIndicator[1]IMPLICIT          OCTET STRING OPTIONAL,
digits                    [2]    IMPLICIT      IA5STRING OPTIONAL}
```

44.2.5.0.2 Call Held Coded Example

This example illustrates when the user has put the call on hold either using DV-HOLD-CALL or manually. The scenario is, B(DN 919-2463001) calls A(DN 919-4814210) and both of them are in talking state. The host application of A sends the call control message DV_HOLD_CALL to the switch. The call event message DV_CALL_HELD_U, is sent back to the host application, indicating that the primary call on A has been put on hold.

DMS ====>HOST

Table 1 Call Held

Hex Dump			Information Element	Comments
Tag	**Len**	**Content**		
A1	1E		INVOKE	Message length is 30 bytes.
02	01	0F	. . InvokeID	Invoke ID is 15.
02	01	32	. . Operation	Operation value for dv_call_held_U is decimal 50.
30	16		. . CallHeldArgument	Type SEQUENCE and 22 bytes long.
A0	06		. . . . Network Call ID	NetworkCallId is of type Constructor and is 6 bytes long
80	01	02	. . . . . .NetworkNodeID	Network Node ID is 2
81	01	02	. . . . . .Local Call ID	Local Call ID is 2.
A1	0C		. . . . heldParty	HeldParty is a 12 byte constructor.
82	0A	39 31 39 34 38 31 34 32 31 30	. . . . . .stationNumber	The DN of the phone is 919-481-4210
82	01	00	.....heldLeg	HeldLeg is a primary leg

```
Hex Dump = A1 1E 02 01 0F 02 01 32 30 16 A0 06 80 01 02 81 01 02 A1 0C 82 0A 39 31 39 34
38 31 34 32 31 30 82 01 00
```

44.2.6 Message Protocol

The ASN.1 notations for the changed call event message provided by this activity, DV_CALL_UNHELD_U is shown in this section. A sample X.209 hex encoding has been provided here. The length fields are variable because the length depends on the variable content. The tag values are taken from the ROSE protocols.

44.2.6.1 Call Unheld ASN.1 Definition

```
dv-CALL-UNHELD-U    OPERATION
                    ARGUMENT    CallUnheldArgument

::= 30

CallUnheldArgument::=       SEQUENCE
    {networkCallID          [0]  IMPLICIT SEQUENCE
            {networkNodeID      [0]  IMPLICIT INTEGER       OPTIONAL,
             localCallID        [1]  IMPLICIT INTEGER       OPTIONAL}
                                                            OPTIONAL,
    unheldParty             [1] Address Type                OPTIONAL,

    unheldLeg               [2] IMPLICIT ENUMERATED

            {unheldPrimaryLeg       [0] OPTIONAL,

             unheldConsultLeg       [1] OPTIONAL}

                                        OPTIONAL}


AddressType::=              CHOICE
{positionID                 [0]  IMPLICIT       INTEGER, (ONLY CHOICE)
 dialedDigits               [1]  IMPLICIT       IA5STRING,
 stationNumber              [2]  IMPLICIT       OCTET STRING,
 q.931Address               [3]  Q.931AddressType}

Q.931AddressType::=         SEQUENCE
{numberTypeNumberPlan       [0]  IMPLICIT       OCTET STRING OPTIONAL,
 presentationScreeningIndicator [1] IMPLICIT    OCTET STRING OPTIONAL,
 digits                     [2]  IMPLICIT       IA5STRING OPTIONAL}
```

44.2.6.2 Call Unheld Coded Example

This example illustrates when the user unholds either using DV-UNHOLD-CALL or manually. The scenario is,A(DN 919-7823640) consults B(DN 919-2463001)and both of them are in talking state. The host application of A sends the call control message DV_HOLD_CALL to the switch. Then the agent manually unholds the held call. The call event message DV_CALL_UNHELD_U, is sent back to the host application, indicating that the held consult leg on A has been unheld.

DMS ===> HOST

Table 7 Call Unheld

Hex Dump			Information Element	Comments
Tag	**Len**	**Content**		
A1	1E		INVOKE	Message length is 30 bytes.
02	01	0F	. . InvokeID	Invoke ID is 15.
02	01	1E	. . Operation	Operation value for dv-Call-Unheld-U is decimal 30.
30	16		. . CallUnheldArgument	Type SEQUENCE and 22 bytes long.
A0	06		. . . . Network Call ID	NetworkCallId is of type Constructor and is 6 bytes long
80	01	01	. . . . . .NetworkNodeID	Network Node ID is 1
81	01	02	. . . . . .Local Call ID	Local Call ID is 2.
A1	0C		. . . . unheldParty	unheldParty is a 12 byte constructor.
82	0A	39 31 39 37 38 32 33 36 34 30	. . . . . .stationNumber	The DN of the phone is 919-782-3640
82	01	01	.....unheldleg	unheld leg is a consult leg.
Hex Dump = A1 1E 02 01 0F 02 01 1E 30 16 A0 06 80 01 01 81 01 02 A1 0C 82 0A 39 31 39 37 38 32 33 36 34 30 82 01 01				

44.2.7 Operational Measurements (OM)

44.2.7.1 New/Modified OM groups

When a new ICM message is created it is necessary to create new registers in the associated OM group to peg any application specific outgoing SCAI messages. Two new registers are being added to the SCAISRV4 OM group. These registers are pegged on a SCAIGRP basis.

The following new registers are created by this feature:

- TOGCLLRR - pegged when the switch sends out a RR in response to a valid DV_TOGGLE_CALL message request being received and processed.
- TOGCLLRE - pegged when the switch sends out a RE in response to an invalid DV_TOGGLE_CALL message request being received.

44.2.8 Toggle Call invoke message flow examples

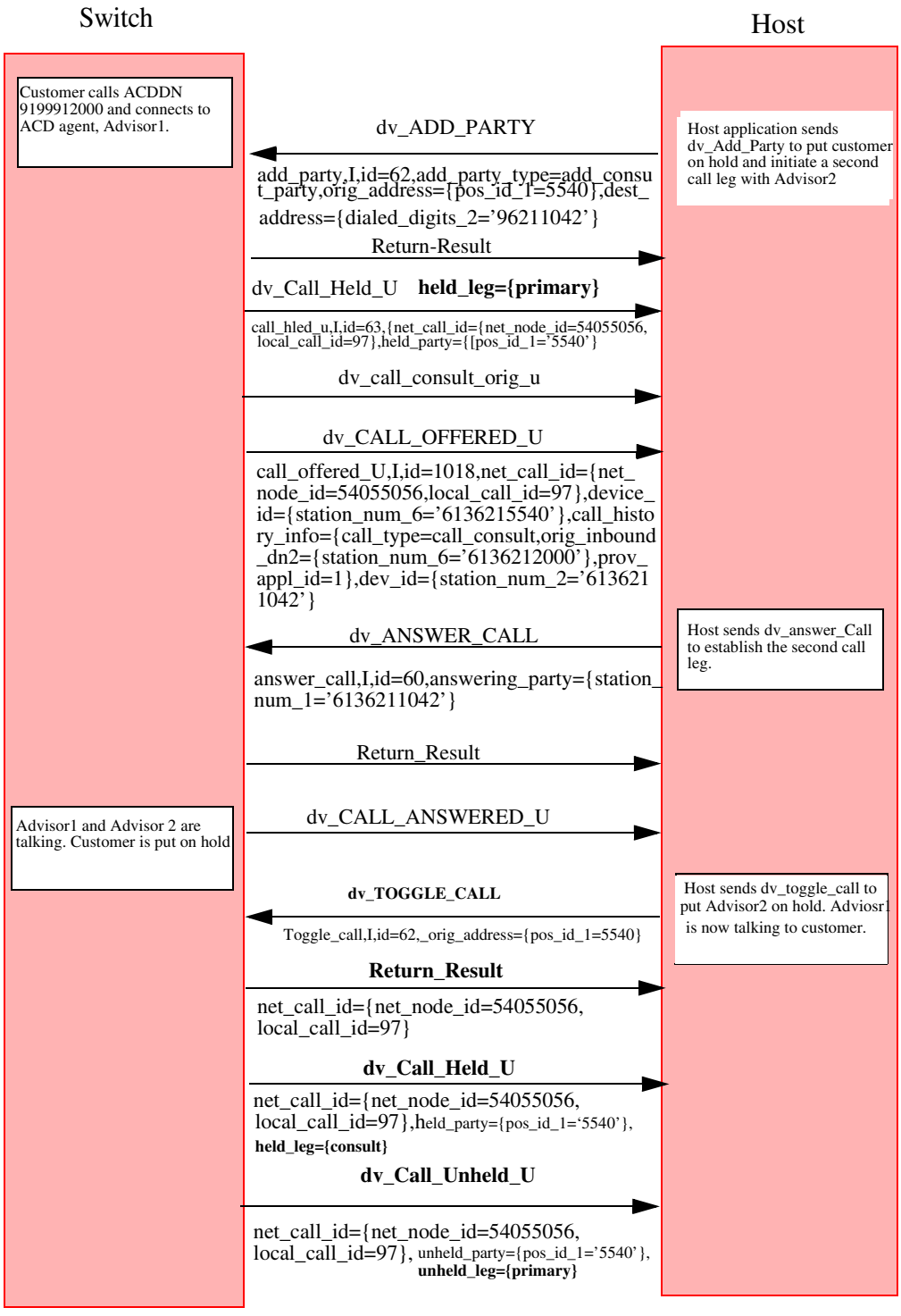
This message is used when an agent has two calls with one being active and the other on hold, and wants to go back and forth between the two calls. When an agent is active on call one and call two is on hold, the host sends the DV_TOGGLE_CALL message, now call one will be put on hold and call two will become active.

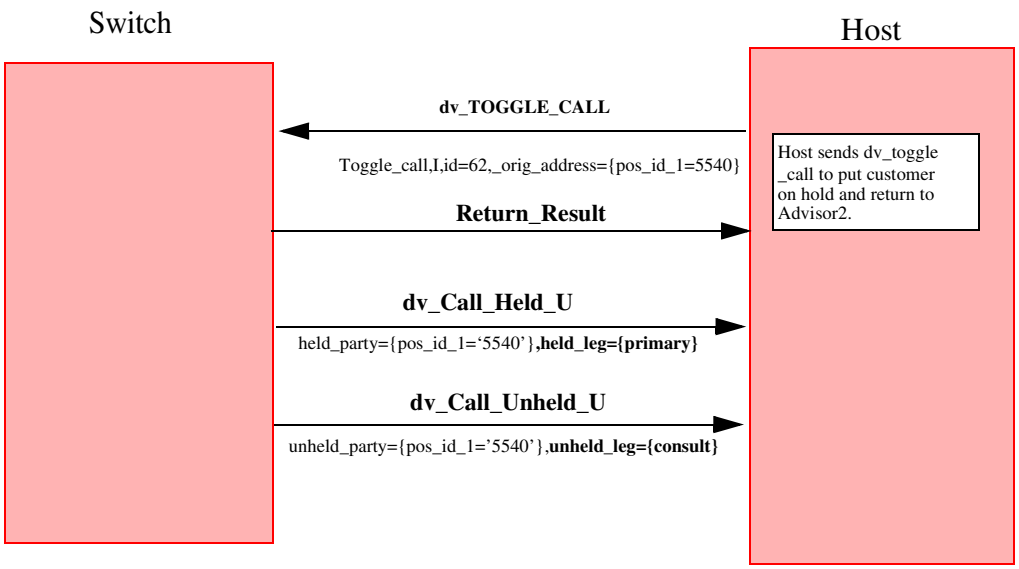
SCAI 3WC/call transfer toggle and set based 3WC/call transfer toggle are not interchangeable on a per call basis. When a call is extended by dv_add_party message, it cannot be controlled by the 3WC/call transfer set feature. Similarly if a call is extended via the 3WC/call transfer set feature, it cannot be controlled by the SCAI 3WC/call transfer.

Some message flow scenarios are considered in this section to get a better understanding of the feature functionality.

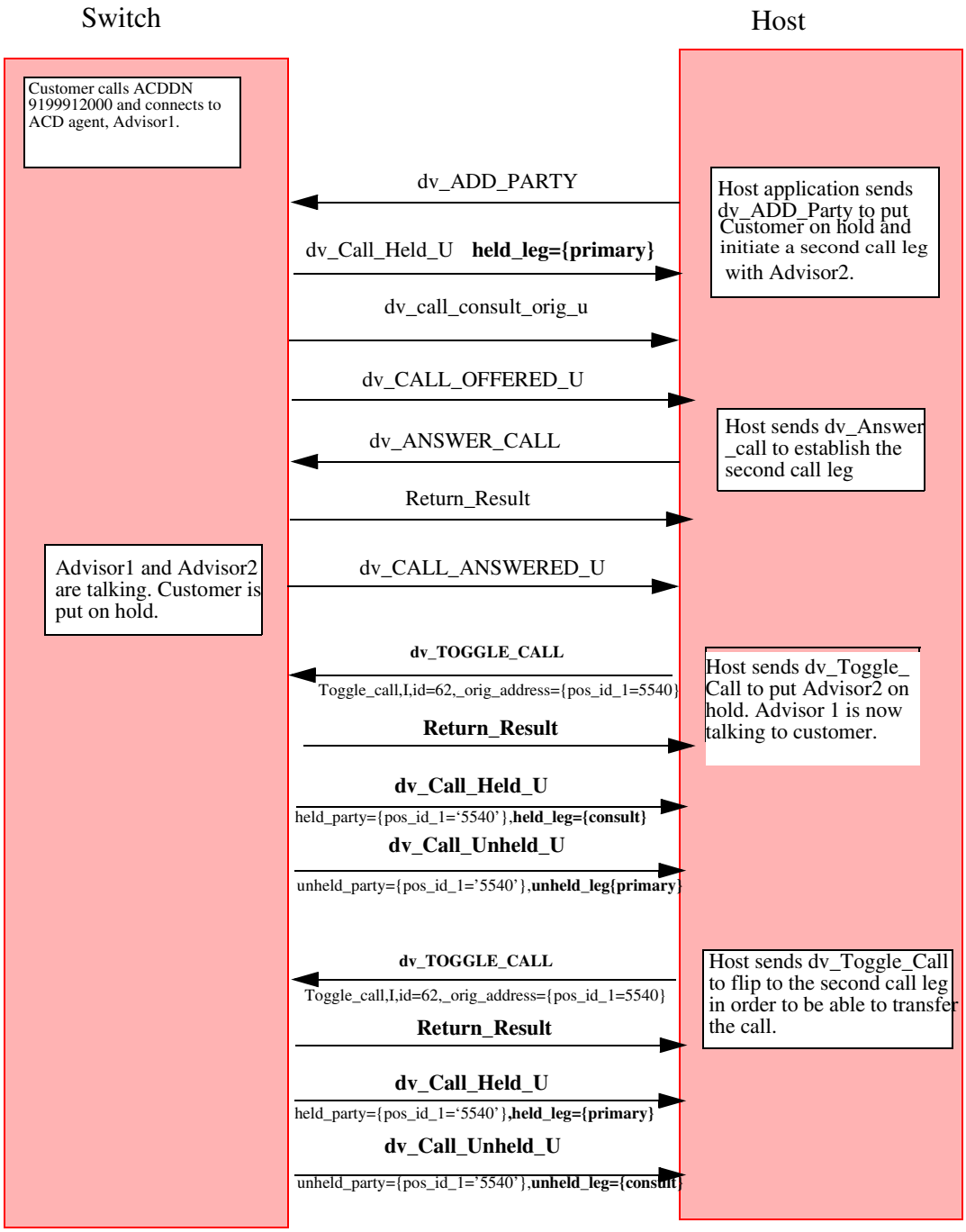
The proposed call control message and the additional dv_call_held_u and dv_call_unheld_u messages are highlighted in the figures.

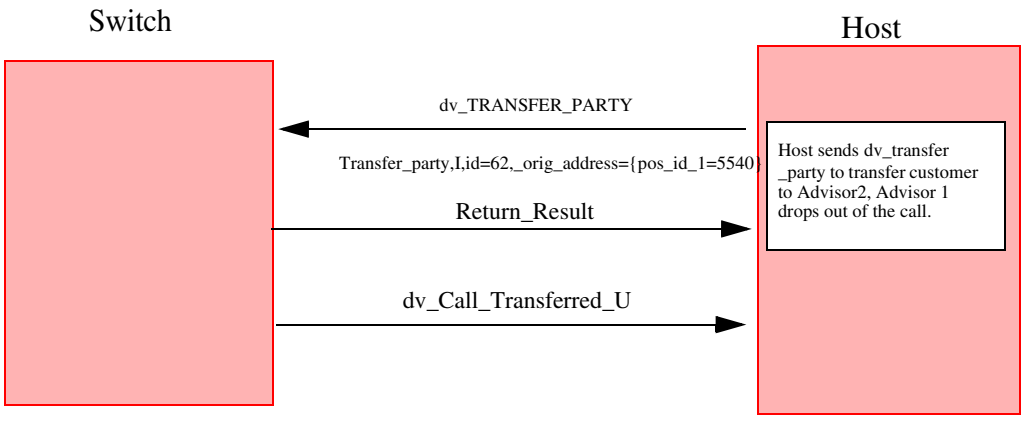
44.2.8.1 Toggle call between Customer and Advisor2



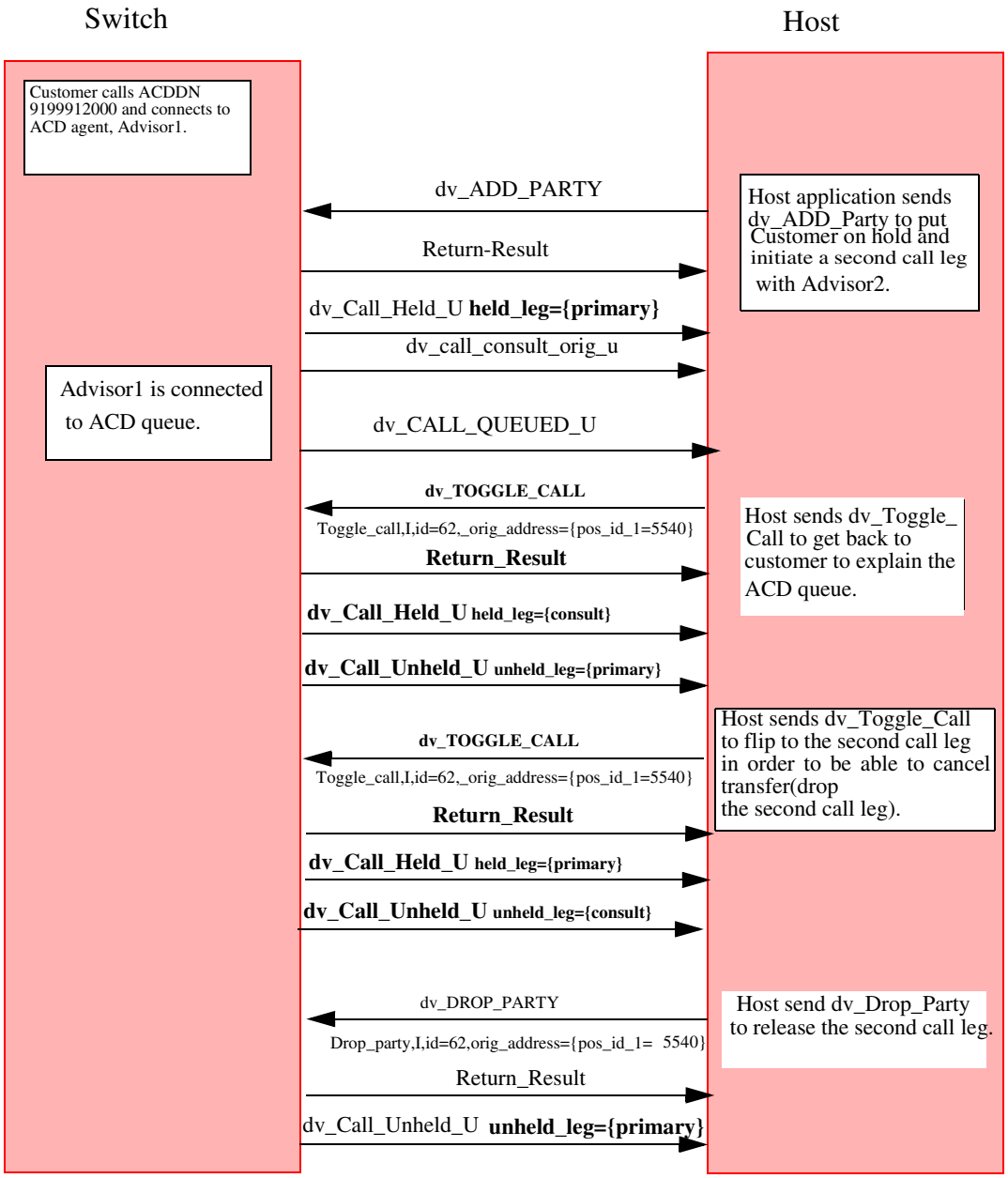

Switch
Host
dv_TOGGLE_CALL
Toggle_call,I,id=62,_orig_address={pos_id_1=5540}
Host sends dv_toggle _call to put customer on hold and return to Advisor2.
Return_Result
dv_Call_Held_U
held_party={pos_id_1='5540'},held_leg={primary}
dv_Call_Unheld_U
unheld_party={pos_id_1='5540'},unheld_leg={consult}

44.2.8.2 Toggle with Transfer




Switch
Host
dv_TRANSFER_PARTY
Transfer_party,I,id=62,_orig_address={pos_id_1=5540}
Host sends dv_transfer _party to transfer customer to Advisor2, Advisor 1 drops out of the call.
Return_Result
dv_Call_Transferred_U

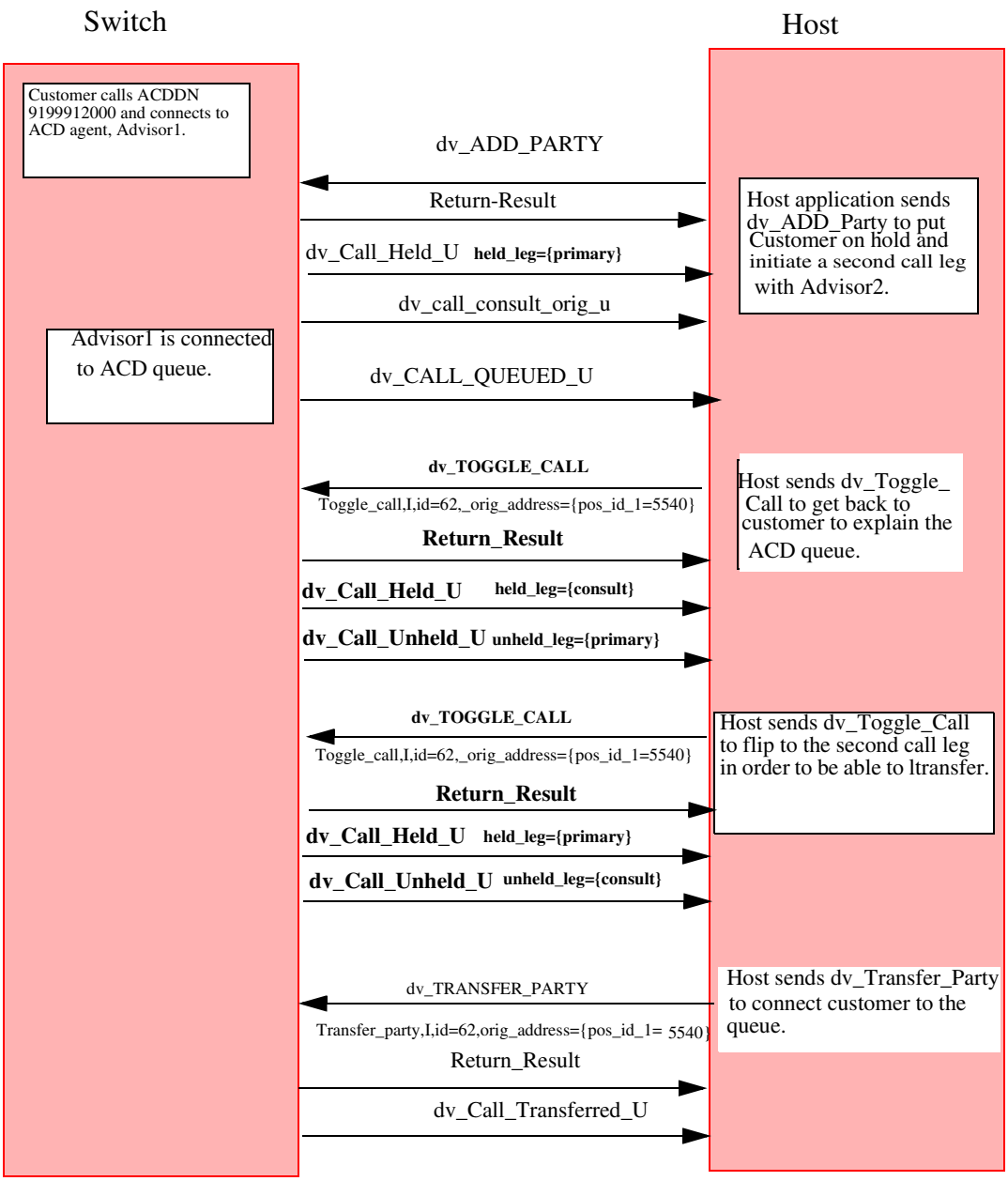
44.2.8.3 Toggle call with cancel transfer



Note:

- Manual toggle cannot be done when a call is in an ACD queue.
- When an ACD queue is reached over a trunk, Toggling is allowed using ICM only when the Audio option is datafilled for that ACD group.

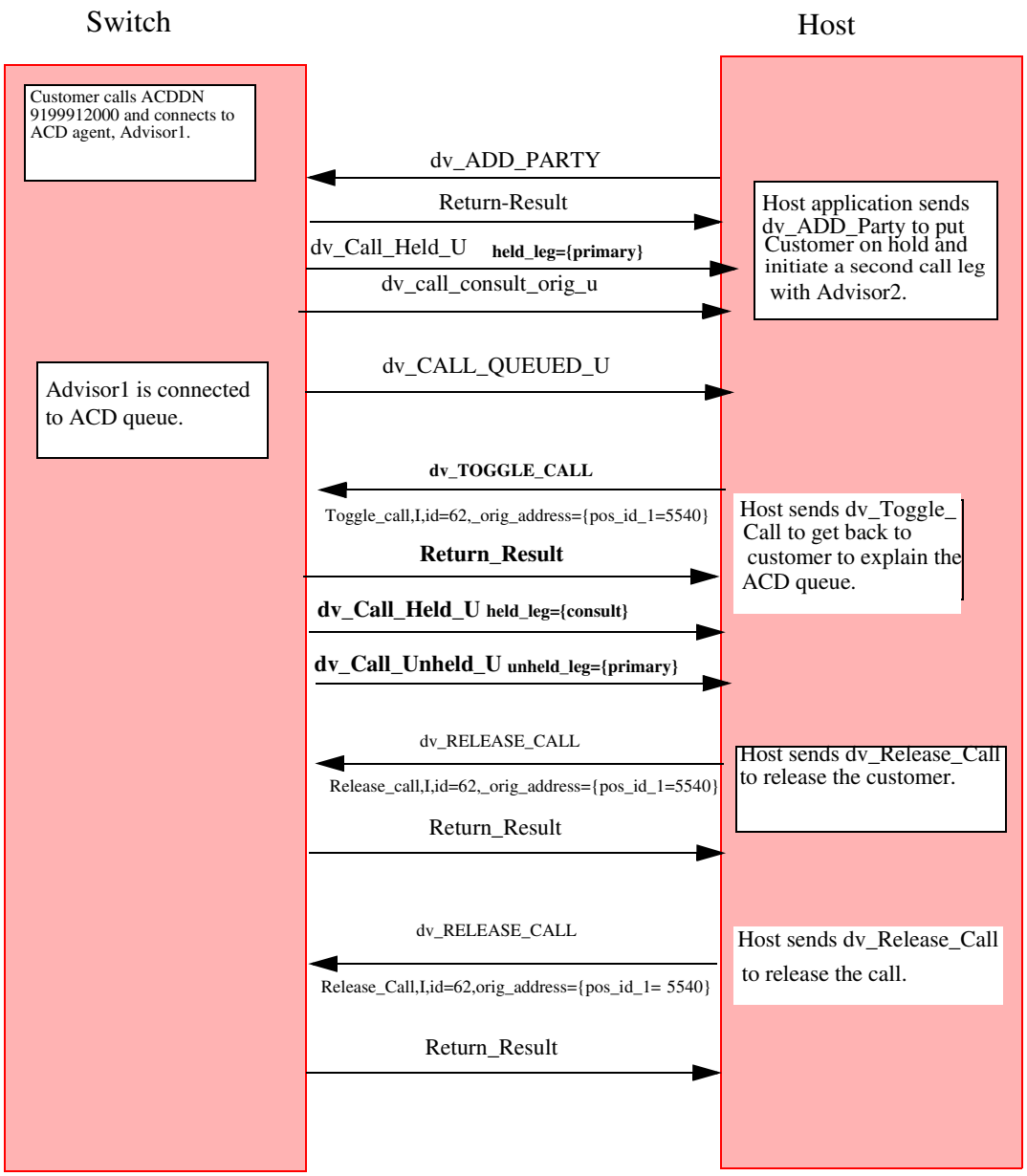
44.2.8.4 Toggle and connect call to queue



Note:

- Manual toggle cannot be done when a call is in an ACD queue.
- When an ACD queue is reached over a trunk, Toggling is allowed using ICM only when the Audio option is datafilled for that ACD group.

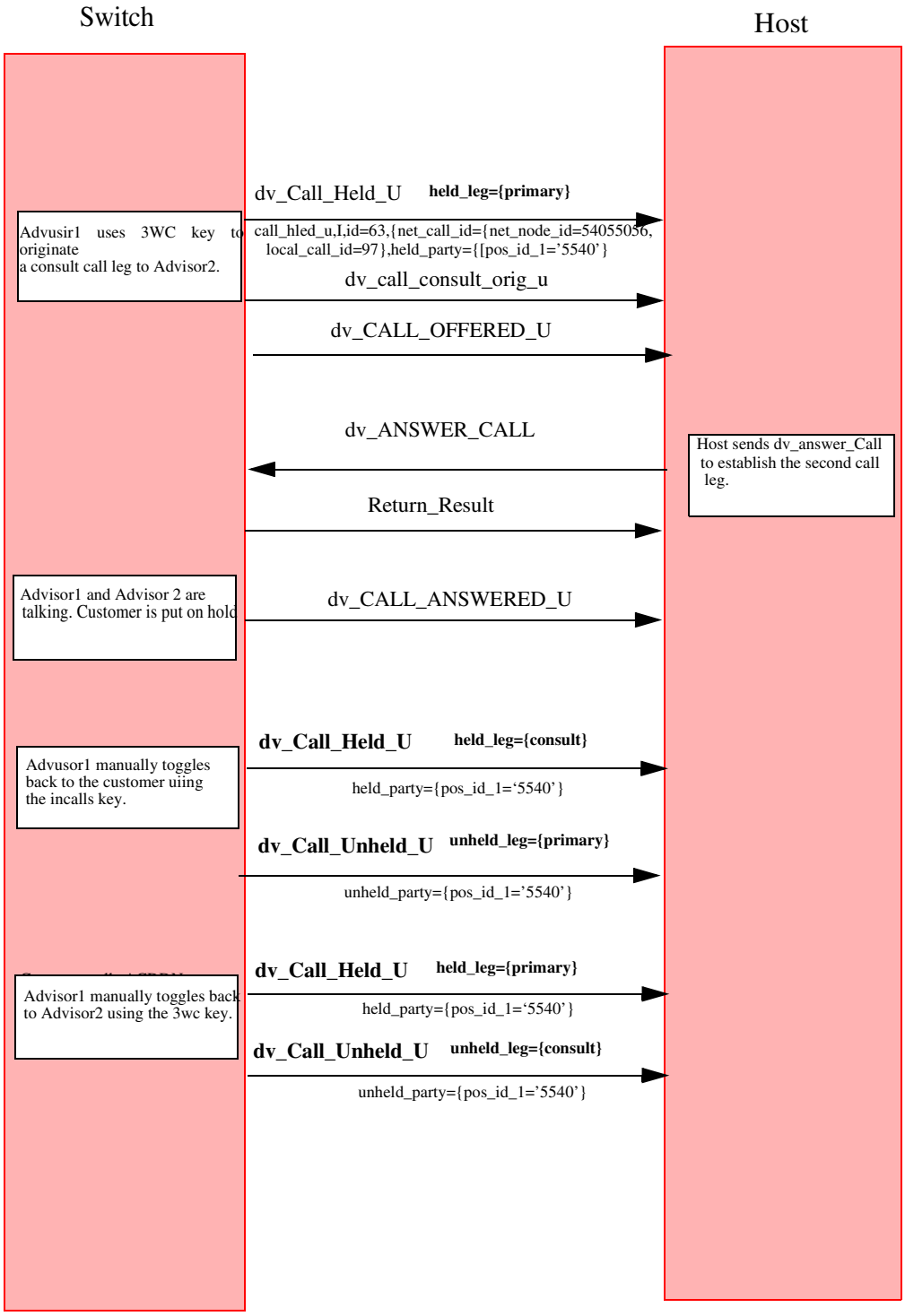
44.2.8.5 Toggle and release call



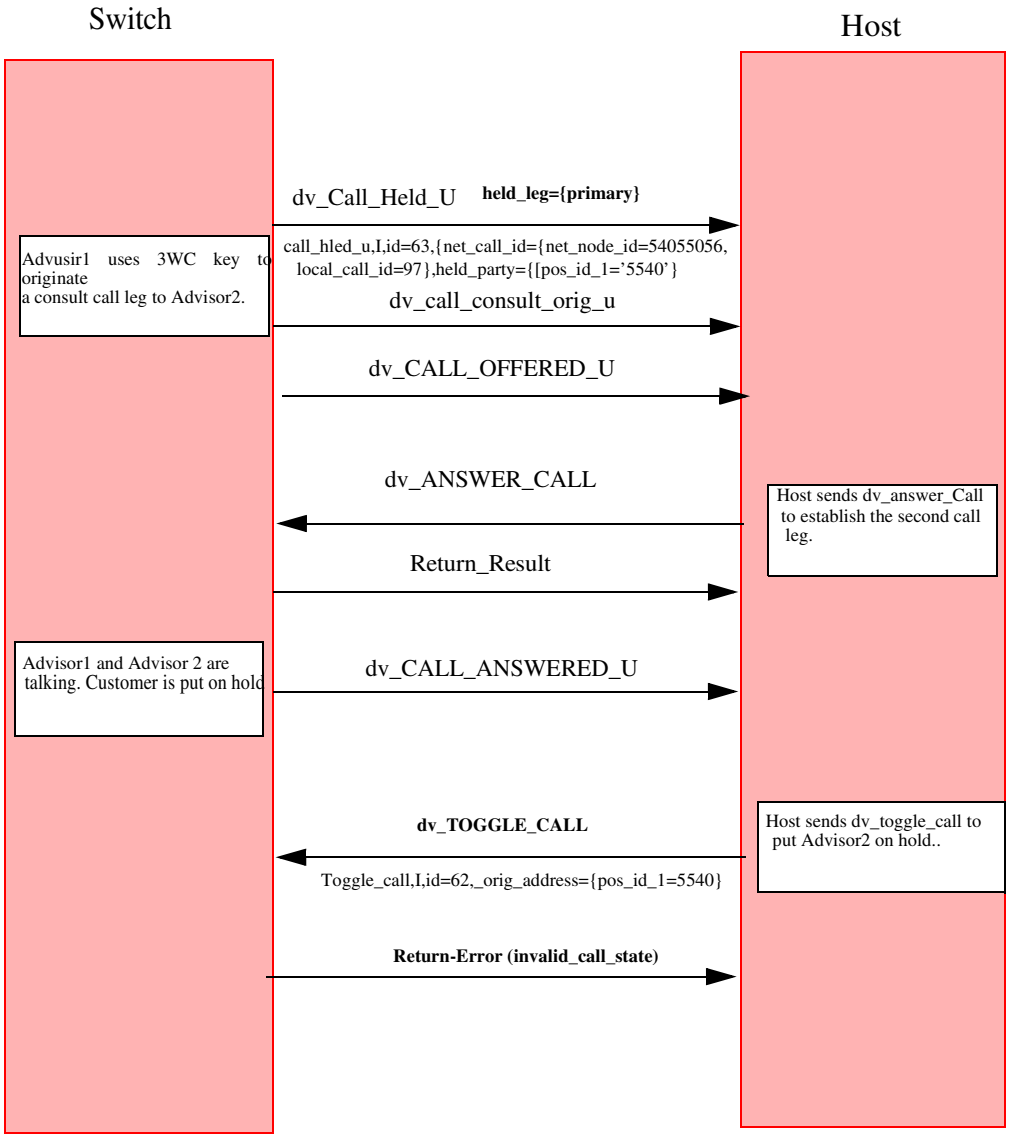
Note:

- Manual toggle cannot be done when a call is in an ACD queue.
- When an ACD queue is reached over a trunk, Toggling is allowed using ICM only when the Audio option is datafilled for that ACD group.

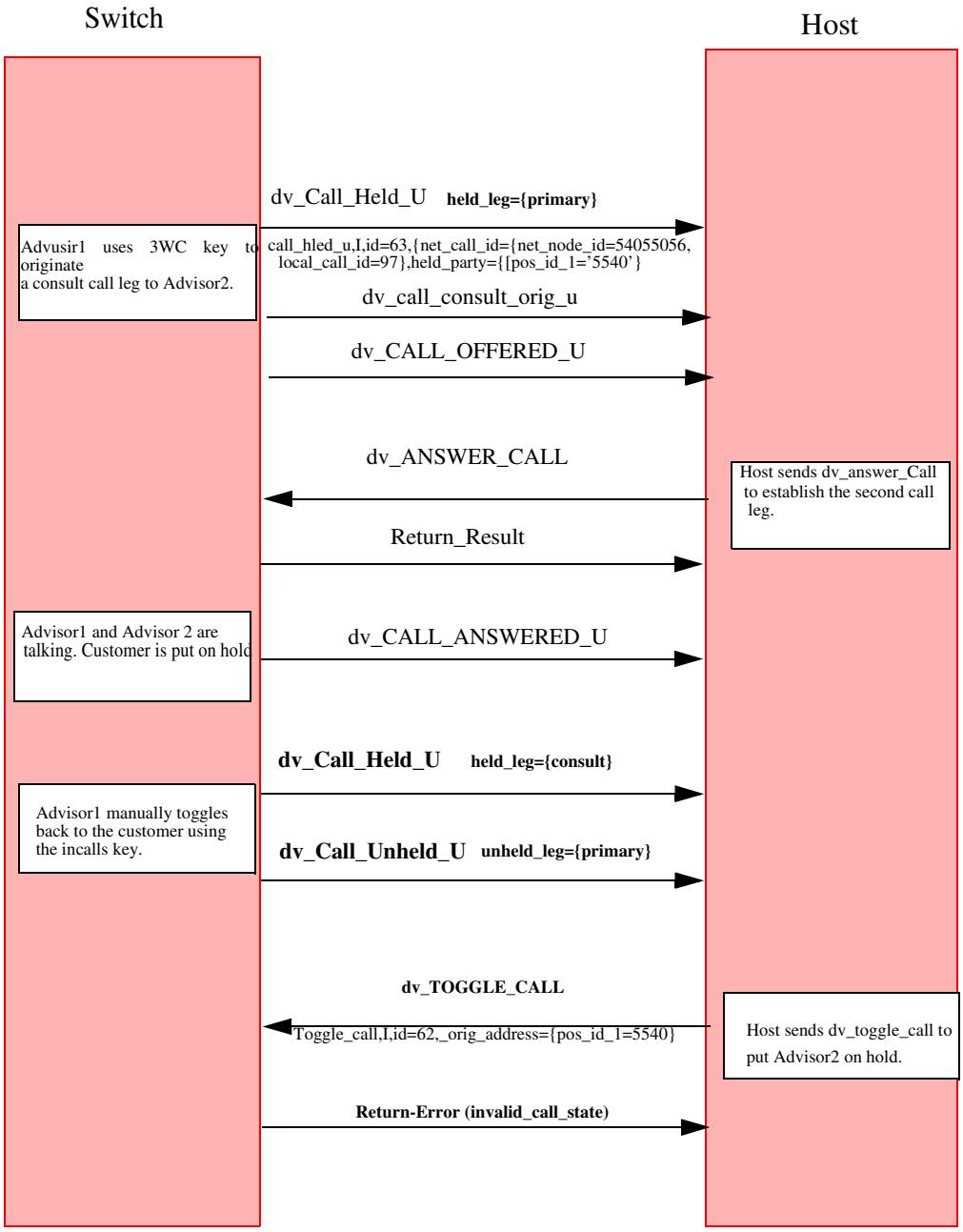
44.2.8.6 Manual toggle call between Customer and Advisor2



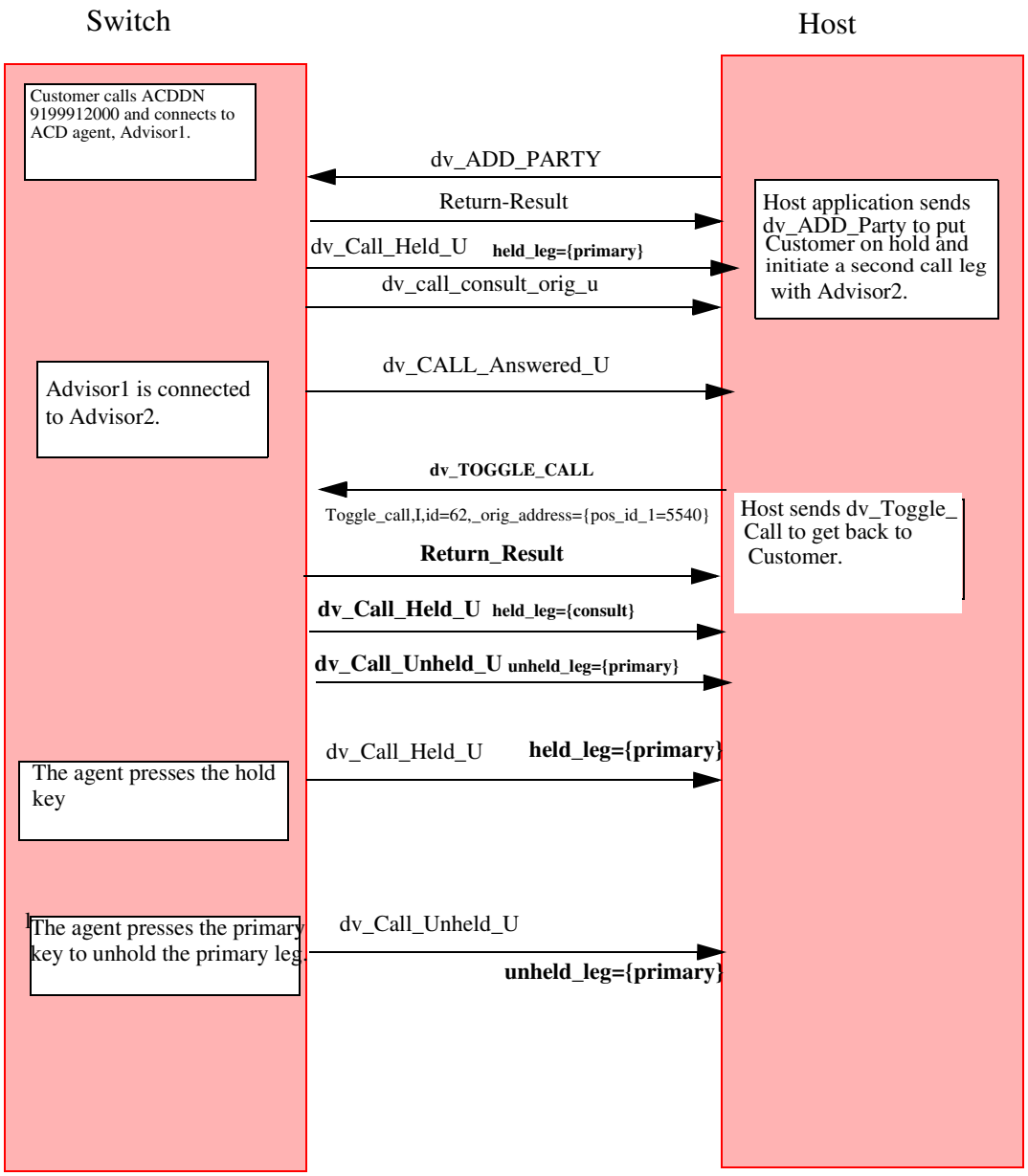
44.2.8.7 Manual consult party with CTI toggle



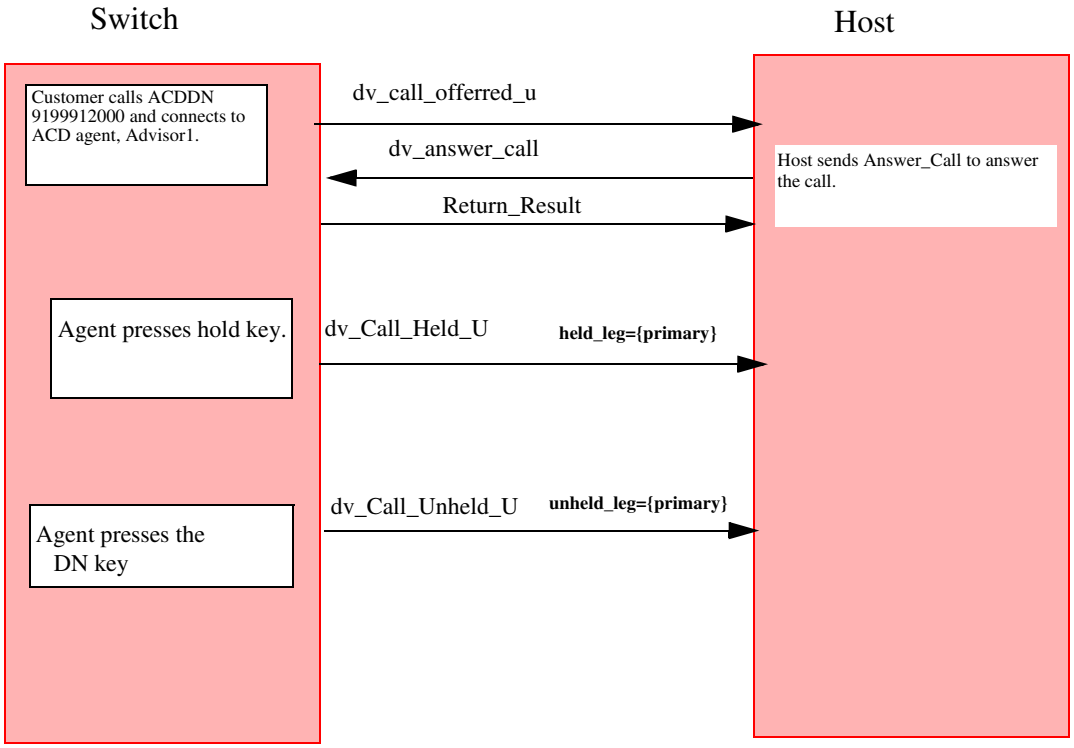
44.2.8.8 Manual toggle with CTI toggle



44.2.8.9 CTI toggle with manual hold



44.2.8.10 Two Party call with Hold



44.2.8.11 Consult and release Advisor2

The following scenario does not require the new message.

1. Customer calls ACD group and is connected to Advisor1.
2. Advisor1 puts customer on hold and connects to Advisor2, using the dv_Add_Party message.
3. Advisor1 ends call with Advisor2 by using the dv_Drop_Party message.
4. Advisor1 is now connected to customer.

44.3 Hardware Requirements or Dependencies

Not Applicable.

44.4 Software Requirements or Dependencies

Not Applicable

44.5 Limitations and restrictions

- The limitations and restrictions that apply to the functionalities of the 3WC flip flop apply to this feature as well. An exception is made by this feature when a call is queued in an ACD queue. Before this feature with 3WC, one could not toggle when the second leg is connected to an ACD queue. With this feature, this restriction has been removed only for ICM initiated toggle. Manual toggle will not be changed or affected.
- When the second call leg is connected to an ACD queue, toggling is ONLY allowed using ICM. Manual toggle is not allowed. The exception to this is when the queued ACD call is over a trunk and when that ACD group has the Audio option datafilled on it.
- Toggling is also not allowed when the call gets presented to an ACD agent..(i.e Call is ringing on the agent) The exception to this is when the ACD agent is reached over a trunk after being given queued audio.
- When the second call leg is connected to an ACD queue which is located in a different switch than the originator of the second call leg, (i.e termination to ACD queue is using a trunk) toggling is not possible unless the Audio option is datafilled in that ACD group.
- When the second call leg is a trunk ACDcall and it gets requeued due to the ACD agent not answering the call, the requeued call cannot be toggled either using ICM or by manual toggle.
- This feature is not supported on IBN (2500) sets.
- The existing restriction for Add_Party, Transfer_Party, Conference_Party and Drop_Party applies to this feature as well. When a consult leg is originated using dv_Add_Party, toggling must also be originated using ICM. When a consult leg is originated manually, toggling must also be done manually.

44.6 Interactions

None of the existing interactions will be affected or changed by this activity. No new interactions will be introduced by this activity.

44.7 Applicable customer facing sections

FaultManagement

- Logs __N/A__
- Alarms __N/A__

Configuration

- Data Schema __X__
- User Interface __N/A_
- Element Management __N/A_
- Security __N/A_
- Service Order __N/A__
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __X__

44.8 Glossary

Term	Description
ACD	Automatic Call Distribution
ASN	Abstract Syntax Notation
CTI	Computer Telephone Integration
DN	Directory Number
ICM	Intelligent Call Management
IBN	Integrated Business Network
MDC	Meridian Digital Centrex
RES	Residential Enhanced Services
SCAICC	Switch Computer Application Interface Call Control
SCAISSRV	Switch Computer Application Interface SCAI Service
TPCC	Third party Call Control

45: Functional Description (FN): A00002916

45.1 Feature name

CS2K connectivity to XPM remote

45.2 Description

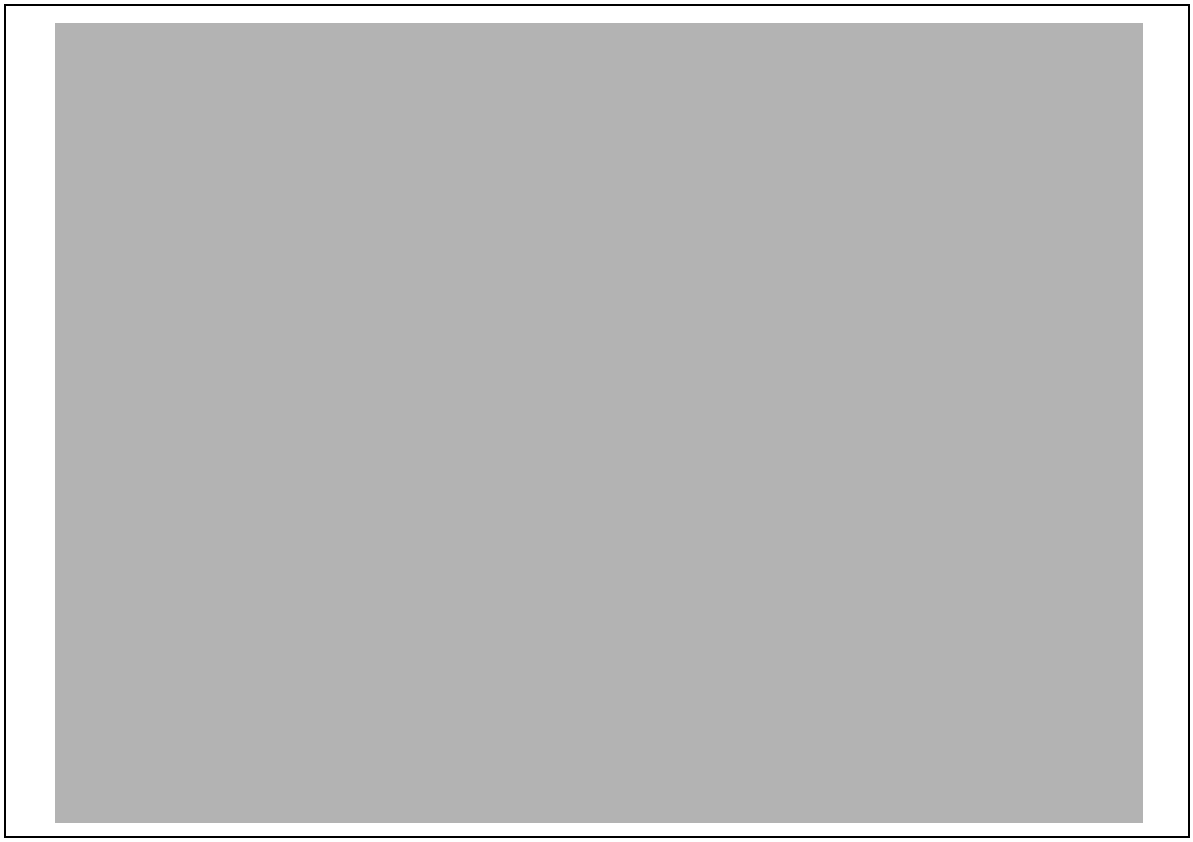
This activity provides a cost effective Succession POTS upgrade, with low POTS port cost. MBS, ETSI BRI and CAS mux lines are also supported by this activity.

This is achieved by directly connecting an RCO2 node to a PVG Gateway via PRI carriers controlled by a GWC, and by removing the dependancy on PLGC and ENET hardware.

The activity is targetted at multiple International customers.

The following Figure shows the network configuration, with the RCO2 connected to a PVG Gateway via PRI carriers controlled by a CS2K Gateway Controller. Standard PRI mapping between trunks, TIDs and PVG endpoints is used. RCO2 virtual c-side messaging links are associated with a real PRI D-channel, and RCO2 virtual c-side speech links are associated with real PRI B-channels. Standard IUAP backhaul is used to transfer PRI messages between the PVG Gateway and the CS2K Gateway Controller. Existing media control protocol is used between the PVG Gateway and the CS2K Gateway Controller.

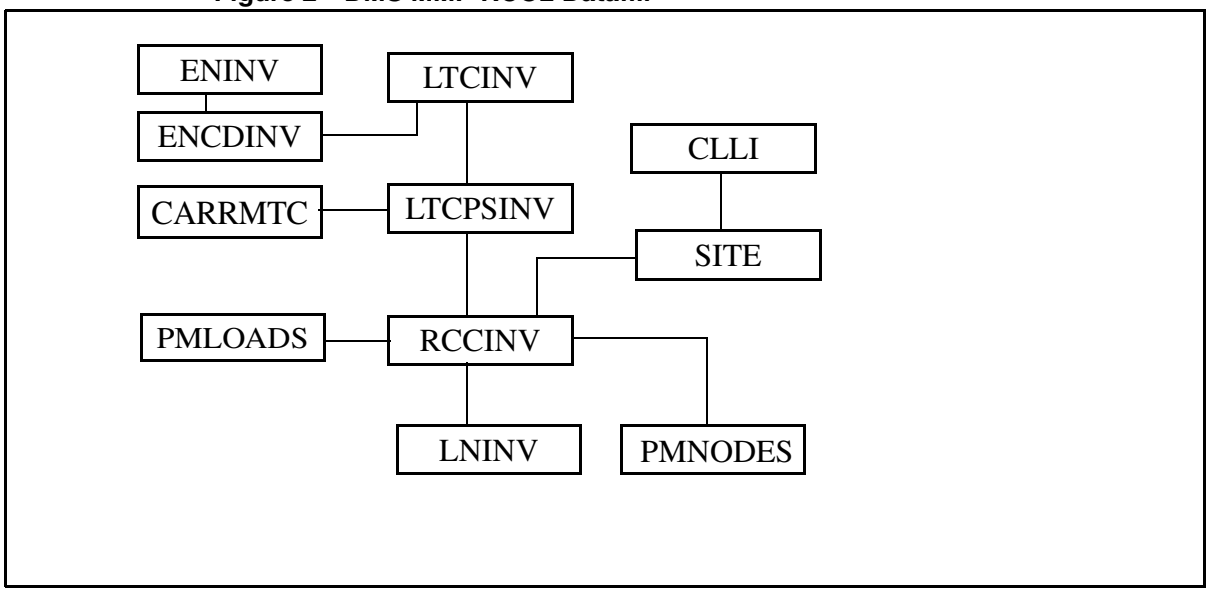
Figure 1 Network configuration diagram



45.2.1 Datafill

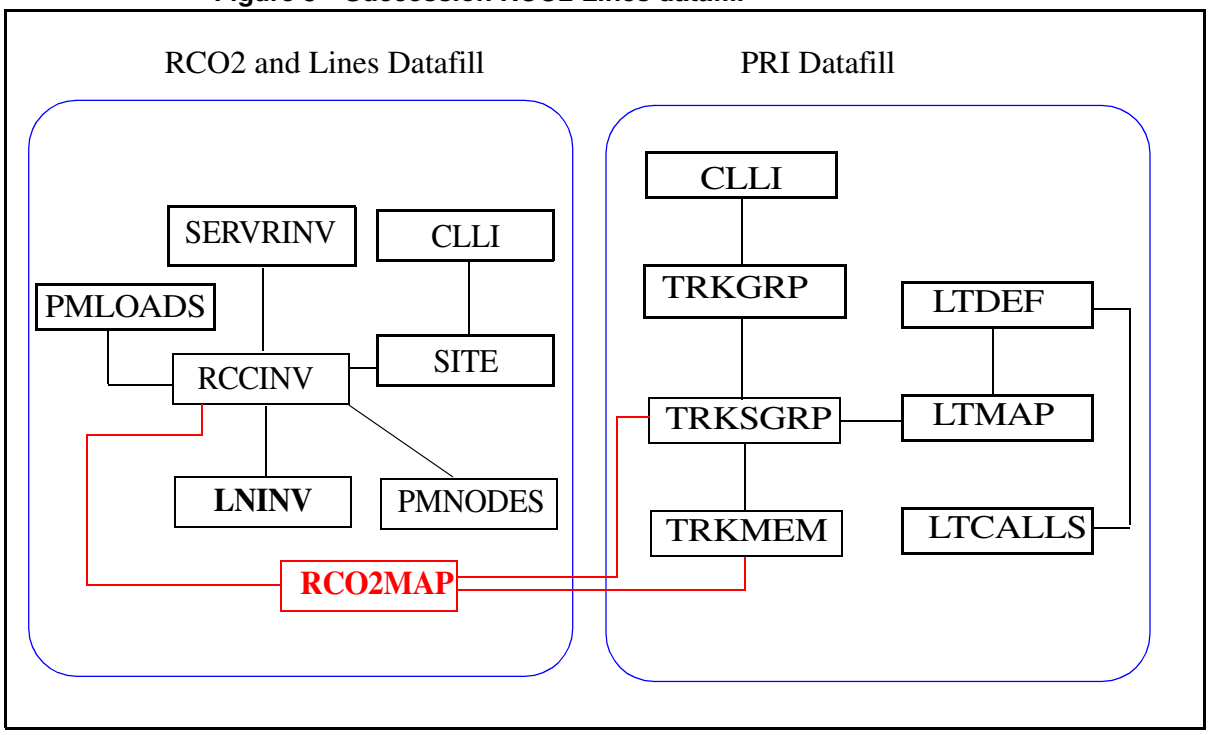
Provisioning of RCO2 lines on a DMS MMP involves datafilling tables in the CM at the mapci level. These tables are shown in the following figure. On the DMS MMP the RCO2 is connected to the PLGC's by PCM30 links. These carriers are datafilled in table CARRMTC.

Figure 2 DMS MMP RCO2 Datafill



In the Succession network the RCO2's are connected to the PVG via PRI trunks. The RCO2's c-side messaging and speech links are associated with PRI D- and B-channels respectively. This association is achieved by the introduction of new table RCO2MAP. The tables that need to be datafilled are shown in the following figure.

Figure 3 Succession RCO2 Lines datafill



The RCO2 subtending off the GWC is datafilled in table RCCINV. Sample datafill is as per the following figure. The CSPM field contains the c-side PM for the RCO2 and consists of two sub-fields - XPMTYPE and XPMNO. The CSLNKTAB field is datafilled with the RCO2's c-side links. The number of entries in the CSLNKTAB field corresponds to the number of RCO2 c-side links. For a RCO2 a minimum of three c-side links must be datafilled. A maximum of 16 c-side links can be provisioned.

Figure 4 Table RCCINV- Sample Datafill

```
RCCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD
 EXECTAB CSPM CSLNKTAB ESA INTRASW ADDLMSGL OPTCARD TONESET
 PROCPEC E2LOAD EXTINFO OPTATTR
-------------------------------------------------------------------------
RM02 RCO2 0 1 CRSC 0 6 1 C 4 MX85AA WRI17AY
(RMM_TERM RSMEX) (ESALINES ESAEX) $
GWC 205 (1) (2) (3) $Y Y N (UTR6 )(RAM6X69 ) (ISP 16) $ UK100
AX74AA AX74AA UPFWNU01 Y CEXT 1 6 1 C 5 MX86AA L$
```

Datafilling table RCCINV results in table PMNODES being autodatafilled with host GWC and subtending RCO2 node information. Sample datafill in table PMNODES is as per the following figure.

Figure 5 Sample tuple in Table PMNODES :

```
TABKEY EXTNDNUM NODETYPE PMTYPE LEVEL MSGHOST PHYSHOST PORTS STPORT TERMS
STTERM PROTOCOL MS IPML MODE SLLCON NT6X28 LCMLGMEM RSVPORTS RSVTERMS
MATENODE PACKED SUPPCDM CMINCTRL
-------------------------------------------------------------------------
113 1 113 GWC_NODE GWC  0 113 113 16 0 4095 1 MDS30 S N P N N N Y Y N Y YY Y
113 2 114 RCC_NODE RCO2 1 113 113 16 641 4096 MDMSX M N P N N N Y Y N Y YY Y
```

On DMS MMP, the RCO2 tuple in table PMNODES is datafilled with PM_LEVEL of 1.

On DMS MMP, where RCO2's are datafilled off CSPM (C-Side PM) type PLGC's, the datafill in field CSLNKTAB contains the PLGC link (0 to 15) on which the RCO2 is assigned. The PLGC link correspond to the RCO2 c-side links 0 to 15.

In the Succession network, the RCO2's c-side is connected to the PVG by a special PRI agent. This PRI substitutes the messaging and speech links between the RCO2 and PLGC in DMS MMP architecture.

From the CM perspective, the RCO2 is provisioned as a subtending node of the GWC node. Table RCCINV is modified to provision an RCO2 subtending node off a GWC. The following figure shows the existing fields in table RCCINV. The fields for which functionality is modified by this feature are highlighted.

Figure 6 Fields in Table RCCINV

```
>ran
 1 RCCNAME          RCC_KEY_TYPE
 2 ADNUM            ADMIN_NUMBER
 3 FRTYPE           FRAME_NAME
 4 FRNO             FRAME_NO
 5 SHPOS            SHELF_POS
 6 FLOOR            FLOOR_POS
 7 ROW              ROW_POS
 8 FRPOS            FRAME_POS
 9 EQPEC            PEC
10 LOAD             NPMLOAD_INFO
11 EXECTAB          TERM_EXEC_TC_TAB
12 CSPM             XPM_INX
13 CSLNKTAB         RCC_CSLINK_TC_TAB
14 ESA              BOOL
15 INTRASW          BOOL
16 ADDLMSGL         BOOL
17 OPTCARD          EXT_OPT_CARD_TC_TAB
18 TONESET          TONE_SET_TYPE
19 PROCPEC          XPM_PEC_AREA_TAB
20 E2LOAD           NPMLOAD_INFO
21 EXTINFO          EXTENSION_INFO
22 OPTATTR          RCCINV_OPT_ATTR_VECTOR
LOGICAL TUPLE TYPE: RCC_LOGTUPLE
```

For Succession-based RCO2's, the c-side messaging and speech links are no longer datafilled in the CSLNKTAB field of table RCCINV. They are now associated with PRI B-channels and PRI D-channels via new table RCO2MAP.

Table RCO2MAP consists of three fields :

- RCCNAME - this is the key to the tuple. This field is the same as the key to table RCCINV
- CSPM - host c-side PM type and PM number
- GWCPRITAB - PRI trunk CLLI datafill

Datafilling an RCO2 hosted off a GWC in table RCCINV results in table RCO2MAP being datafilled with a nil tuple as follows :

Figure 7 Table RCO2MAP- sample tuple auto-datafilled

```
TABLE RCO2MAP

RCCNAME CSPM GWCPRITAB
-------------------------------------------------------------------------
RM02 RCO2 0 GWC 205 NIL 0
```

This tuple may then be modified by the craftsperson by datafilling the PRI[1] trunk. The PRI CLLI datafilled in RCO2MAP will be a PRI variant that supports NFAS (Non-Facility Associated Signalling) functionality, on which one D-channel supports B-channels from a number of PRI trunks. A sample tuple in table RCO2MAP is as per Figure 8 .

Figure 8 Table RCO2MAP- PRI NFAS Variant

```
TABLE RCO2MAP
RCCNAME CSPM GWCPRITAB
-------------------------------------------------------------------------
RM02 RCO2 0 GWC 205 (PRICLLITST1 1) (PRICLLITST2 1) (PRICLLITST1 31)
```

The first and second PRI starting terminal number will correspond to the D-channel for RCO2 unit 0 and unit 1 respectively. Hence, the first and second starting CLLI must be unique. Also, for these CLLI's Table TRKSGRP must be datafilled with the D-channel information. The subsequent PRI starting terminal numbers correspond to the messaging links. For each of these messaging links table TRKMEM must have the next consecutive 31 time slots datafilled.

The above sample tuple has three PRI trunk starting CLLI's - (PRICLLITST1 1) (PRICLLITST2 1) and (PRICLLITST1 31). Each PRI trunk starting terminal number corresponds to an E1 on the RCO2's c-side. Hence, it is imperative that the number of PRI trunk starting terminal numbers keyed in by the user in table RCO2MAP, must be equal to the number of RCO2 c-side links provisioned in the CSLNKTAB field in table RCCINV.

[1]This is a PRI NFAS variant

The following rules apply to tuples in table RCO2MAP :

- Datafilling a tuple in table RCCINV that has an RCO2 with a c-side PM type of GWC will result in a tuple being autodatafilled in table RCO2MAP.
- Deleting a tuple in table RCCINV that has an RCO2 hosted off a GWC will result in the corresponding tuple being deleted from table RCO2MAP.
- Deletion of tuples in table RCO2MAP is not permitted.
- Changes are permitted only to the GWCPRITAB field. Changing the GWCPRITAB field results in Static Data being downloaded to the GWC with the updated RCO2's c-side link information.
- Changes are not permitted to the CSPM field as it is the RCO2's host PM as datafilled in table RCCINV.
- PRI B-channels must be datafilled in table TRKMEM.
- PRI D-channels must be datafilled in table TRKSGRP.

Impact on other tables :

- SERVRINV - GWC's tuples datafilled in table SERVRINV cannot be deleted if they are referenced by tuples in table RCO2MAP that have RCO2's hosted off that GWC.
- TRKMEM - Tuples that have their trunk TIDs datafilled in table RCO2MAP cannot be deleted.
- TRKSGRP - Tuples that have their trunk TID's datafilled in table RCO2MAP cannot be deleted.

45.2.2 MAPCI

Succession-based RCO2's can be posted at the mapci;mtc;pm level. The following subcommands are supported :

- Post
- Listset
- Trnsl
- Tst
- Bsy
- Rts
- Offl
- LoadPM
- Disp
- Next
- Swact

- QueryPM
- DCH
- IRLINK
- Perform
- ISG

Maintenance of the RCO2's c-side links is disabled at the mapci;mtc;pm level. In addition, the RCO2's c-side carrier information is not displayed at the mapci;mtc;pm level and its sublevel.

45.2.3 Message flow charts

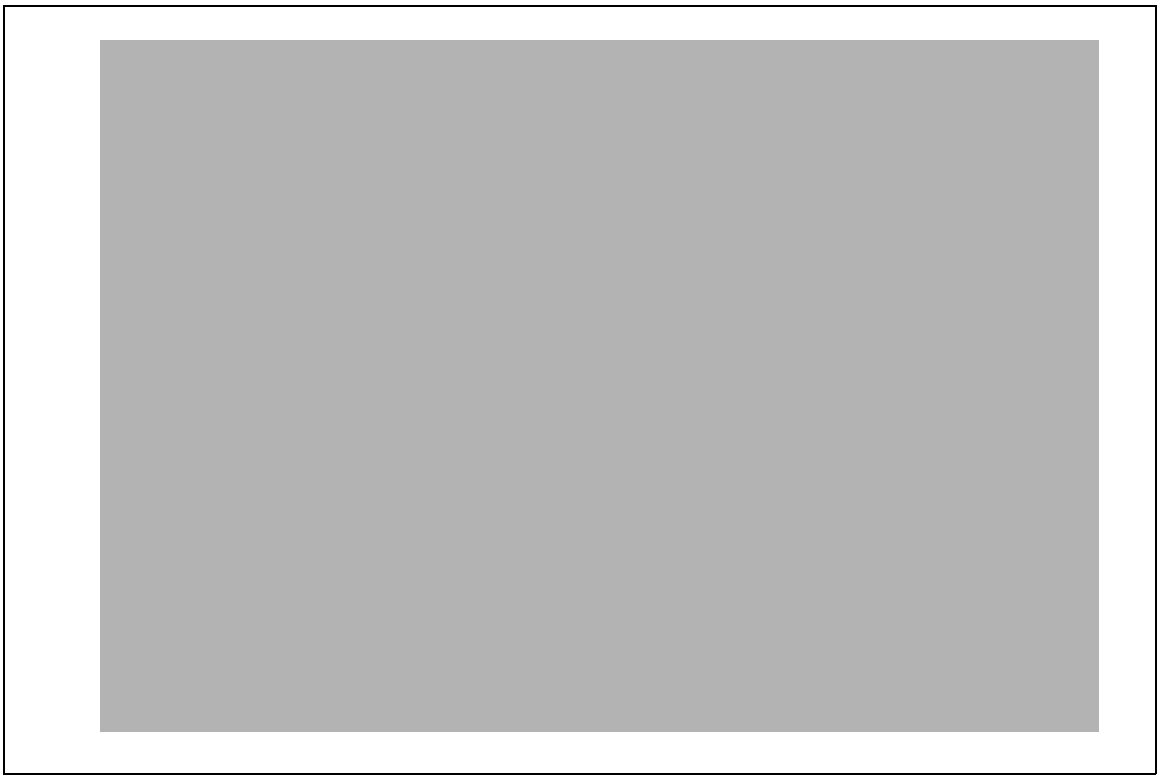
The following message flow charts show messaging between the CS2K and the RCO2. PVG is included in the charts for information purposes only i.e. All messages shown will pass transparently through the PVG. Messages are shown in their basic unwrapped form for clarity i.e. PRI/IUAP headers are not shown.

Messages between PVG and RCO2 will be transported via PRI protocol, using Facility messages. Messages between CS2K and PVG will be transported via IUAP protocol.

45.2.3.1 RCO2 load sequence

Figure 9 RCO2 power on

Figure 10 RCO2 loading



45.3 Hardware Requirements or Dependencies

Both the RSC-M (4xRCO2) and RSC-S (1xRCO2) cabinets will be supported. No new RCO2 hardware is required as part of this activity (e.g. MX76 card).

45.4 Software Requirements or Dependencies

None.

45.5 Firmware Requirements or Dependencies

Upgraded firmware is required for the MX76 combined messaging and CSM card within the RCO2. This allows line signalling to be mapped to Q.931 protocol. The MX76 firmware is part of the UP firmware load e.g. UPFWQM01.

45.6 Limitations and restrictions

- Supported interworking of ETSI BRI supplementary services with POTS and MBS line services are described in A59021068. Unsupported services interworking will require ETSI ISUP V2 loop-arounds.

- Interworking between PVG/RCO2 ETSI BRI lines and TDM lines/trunks must be done via an ETSI ISUP loop-around.
- The ETSI BRI portions of this activity are PV only. Although it is not expected that any ETSI BRI issues will be found specific to this solution, any that are found will be documented in this section at the completion of the activity.
- PCM30 remotes off the RSC-S (e.g. PRLCM) are not supported by this activity.
- GPP and V5.2 lines are not supported by this activity.
- Attendant Console is not supported by this activity.
- DMS MMP does not currently support trunks on an International RCO2. This will also be true for Succession-based International RCO2.
- The 6X69 messaging card for the RCO2 is not supported by this activity.
- The connection of an RCO2 to a PVG Gateway is not supported in the CS2K Hybrid environment.

45.7 Interactions

The following basic call types will be supported :

- PVG/RCO2 POTS-PVG/RCO2 POTS
- PVG/RCO2 MBS-PVG/RCO2 MBS
- PVG/RCO2 ETSI BRI -PVG/RCO2 ETSI BRI
- PVG/RCO2 POTS-PVG/RCO2 MBS
- PVG/RCO2 POTS-PVG/RCO2 ETSI BRI
- PVG/RCO2 MBS-PVG/RCO2 ETSI BRI
- PVG/RCO2 POTS-GWC line[1]
- PVG/RCO2 MBS-GWC line
- PVG/RCO2 ETSI BRI-GWC line

The following trunk interworkings will be supported :

- PVG/RCO2 POTS line to IBN7/ETSI ISUP V1/ETSI ISUPV2/PRI
- PVG/RCO2 ETSI BRI line to IBN7/ETSI ISUP V1/ETSI ISUPV2/PRI

The following CEPT services will be supported : ICWT, I3WC, CFD, ILR and Wake up.

[1]GWC line refers to a Succession line terminated on a small lines Gateway i.e. Mediatrix Analogue Line Gateway (1124).

The following regulatory services will be supported : Lawful Intercept, Number Portability, Carrier Pre-Selection, CLIP, CLIR, Malicious Call Trace.

The following POTS line services will be supported : CLASS[1] on POTS (Calling Name Delivery, Anonymous Call Rejection), Call Forwarding Busy, Call Forwarding No Reply, Call Completion Busy Subscriber, Selective Call Editing, Outgoing Call Barring, 3WC.

The following MBS line services will be supported : CLASS on MBS, same as POTS.

ETSI BRI basic call is supported, including point-to-point (1 terminal) and point-to-multipoint (1-8 terminals).

The following ETSI BRI supplementary services will be supported : 3PTY, AOC-D, AOC-E, CCBS, CD, CFB, CFNR, CFU, CLIP, CLIR, COLP, COLR, CONF, CUG, CW, DDI, ECT, HOLD, MCID, MSN, OCB, SUB, TP, UUS-1, MWI, CCNR, HUNT.

Reference is made to the following two documents for detailed limitations and restrictions for ETSI BRI, as well as ETSI BRI supplemental services and interworkings :

- DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the S/T Reference Point NIS S223-1 01.02
- DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the T Reference Point NIS S223-2 01.02

Note that these two documents describe the full TDM ETSI BRI support. The ETSI BRI support provided by activity A00002916 is a subset. Only ETSI BRI services and interworkings listed in this FN are supported.

There are no new market specific interactions supported by this activity, however, re-use of existing line templates is supported i.e. tones, cadences, Worldline card templates and ringing frequencies.

45.8 Applicable customer facing sections

Fault Management

Logs	_N/A_
Alarms	_N/A_

Configuration

Data Schema	__X__

[1]Both V.23 and Bell303 CMR cards.

User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_
Accounting (includes AMA billing)	_N/A_
Performance (includes operational measurements)	_N/A_

45.9 References

i. **A59021068** E.164 ETSI BRI-IBN service interworking

ii. **NIS S223-1 01.02** DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the S/T Reference Point

iii. **NIS S223-2 01.02** DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the T Reference Point

45.10 Glossary

Term	Description
BRI	Basic Rate Interface
CAS	Channel Associated Signalling
EDC	Extended Distance Capabilities
GPP	Global Peripheral Platform
IUAP	ISDN User Adaptation Protocol
MBS	Meridian Business Set
NFAS	Non-Facility Associated Signalling
PCM30	2 Mb/s interface providing 64 Kb/s channels for digital trunks
PLGC	PCM30 Line Group Controller
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PVG	Packet Voice Gateway

Term	Description
RCO2	Remote Controller Overseas
SCTP	Stream Control Transmission Protocol
TID	Terminal IDentifier
UP	Unified Processor
WAI	Who Am I

46: Functional Description (FN): A00003147

46.1 Feature name

A00003147 DP Digit Reception Control

46.2 Description

46.2.1 Purpose

The goal of the work covered by this activity is to provide a mechanism that eliminates the problem about generation of fake emergency service calls and unwanted billing records by line faults, which is a serious nuisance.

46.2.2 Background information

Insulation breakdown due to moisture or chafing of the cable pair due to wind causes the line to appear to be outpulsing digits.With the dial plan for the DMS switches, a pulse of 1 represents digit 1. Since digit "1" is only one pulse, for example, if there are three of these occurring within the interdigit pause, then the DMS routes the call as "111" which is an emergency service number in some countries.

46.2.3 Functional description

By disabling DP digit collection on lines assigned DGT option, the impacts of these fake calls can be eliminated.

The functionality thus provided eliminates the possible generation of these phantom calls by completely disabling DP digit collection with the use of an office parameter; scanning for only offhook, flashes and DTMF tones are permitted.

The change has the following operational impacts/effects:

- Prevents the generation of phantom calls on lines assigned DGT option.
- Dial pulse equipment is not supported on lines assigned DGT option.

46.2.4 Feature Operation

This activity provides control of DP Digit Collection on lines assigned DGT option by introducing a new office parameter DISABLE_DP_RECEPTION_ON_DGT in table OFCENG.

When office parameter DISABLE_DP_RECEPTION_ON_DGT in table OFCENG is assigned to Y, DP digit collection is disabled on lines assigned DGT option, only offhook, flashes and DTMF tones are permitted.

When office parameter DISABLE_DP_RECEPTION_ON_DGT in table OFCENG is set to N, DP digit collection functionality remains unchanged.

The diagram below shows the desired behaviour.

Table 1 Functional Behavior Diagram

'Disable DP Reception on DGT' office parameter	DIGITONE PHONE ON DGT LINE	DIAL PULSE PHONE ON DGT LINE	DIAL PULSE PHONE ON DP LINE
office parameter set to N (dp digit collection allowed)	possible generation of fake calls, DP digit reception allowed.	possible generation of fake calls, DP digit reception allowed.	possible generation of fake calls
office parameter set to Y (dp digit collection disabled)	possible generation of offhook, flashes and DTMF tones only, not fake calls, DP digit reception not allowed.	not supported, DP digit reception not allowed.	possible generation of fake calls.

The new office parameter DISABLE_DP_RECEPTION_ON_DGT is not directly related to the OFCVAR parameter DEFAULT_SIGNALLING_TYPE. DEFAULT_SIGNALLING_TYPE parameter decides which option to be assigned to the line by default when no option is added to the line.If the DEFAULT_SIGNALLING_TYPE=DP and no option is assigned to the line, DP option is assigned automatically and the line is not affected by the new parameter DISABLE_DP_RECEPTION_ON_DGT. If the DEFAULT_SIGNALLING_TYPE=DT and no option is assigned to the line, DGT option is assigned automatically and the line is affected from the new parameter according to Table 1. If the DEFAULT_SIGNALLING_TYPE=DT and DP option is assigned to a line, the line is not affected from the new parameter, DP digit collection is allowed.

The new office parameter is downloaded to the targetted XPMs under following conditions:

- Static data download after XPM loading.
- Static data download during RTS of XPM.
- Change in the value of DISABLE_DP_RECEPTION_ON_DGT in table OFCENG.

One of the available locations of protected global data area in the XPM is reserved to store the new office parameter value.

Whenever a change occurs in the office parameter value, a msg is sent to all the targetted peripherals immediately, with the updated value.

Also, the XPMs are updated with the existing office parameter value whenever a loading or RTS of supported peripherals occur.

This does not cause any outage or static data mismatch in the peripherals.

There is no need for a reload, swact, etc on the peripherals for the parameter value update.

46.2.5 Supported Peripherals

The definitive line/XPM types that need to be covered under this activity are:

- GPP V5.2 IBN Lines.
- GPP MelCAS IBN Lines.
- IBN Lines on PLGC.
- IBN Lines in RCO2.

All DMS-100 customers that deploy line services are able to use this functionality.

46.2.6 Error Detection

A PM181 informational log is generated whenever a failure in updating the pre-defined global data location in the XPM is detected.

Refer to the Fault Management section for more details.

46.2.7 Activation

Feature activation is done by setting the office parameter DISABLE_DP_RECEPTION_ON_DGT to Y.

Changes to DISABLE_DP_RECEPTION_ON_DGT are immediately effective.

The targetted PM's are immediately updated with the new value, without causing any outage in the XPM, no action is needed in the peripherals for the parameter value update.

By default, the office parameter value is set to N.

46.3 Hardware Requirements or Dependencies

No changes due to this feature.

46.4 Software Requirements or Dependencies

The new functionality provided by this activity is being implemented using the existing interfaces. As such, no new software dependencies are being introduced.

This functionality requires release SN07 or higher loads.

46.5 Limitations and restrictions

The functionality that is provided by this feature restricts the use of Dial Pulse phones on lines assigned DGT option.

When the office parameter DISABLE_DP_RECEPTION_ON_DGT is set to Y, Dial Pulse phones on lines assigned DGT option are not supported.

46.6 Patch Availability

The activity is implemented in SN07 and patched back to SN04.

46.7 Interactions

There are no interactions with other features.

This feature has no effect on flash functionality and on features using flash functionality.

46.8 Applicable customer facing sections

Fault Management	
Logs	____X____
Alarms	___N/A___
Configuration	
Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___

Office Parameters	____X____
Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

46.9 Glossary

Term	Explanation
DGT	Digitone
DMS	Digital Multiplex System
DP	Dial Pulse
DT	Digitone
GPP	Global Peripheral Platform
PLGC	Peripheral Line Group Controller
RCO2	Remote switching Center Offshore #2
XPM	Extended Peripheral Module
DTMF	Digitone Multifrequency

47: Functional Description (FN): A00003051

47.1 Feature name

CFGD (Call Forward Group Don't Answer) for BRI Hunt Groups.

47.2 Description

This activity A00003051 in MMP20, enhances the CFGD option (AD1164) for BRI Hunt Groups (AR2189) for Turk Telecom.

The CFGD option allows the user to assign call forwarding do not answer to separate hunt groups. The hunt groups are directory number hunt (DNH), distributed line hunt (DLH), and multiline hunt (MLH). With CFGD, calls to idle hunt group stations ring for a set amount of time before the system forwards the calls. The system can forward the calls to the next station in the hunt sequence and to an external directory number (DN).

Currently, the CFGD option is restricted if the hunt group contains a BRI agent (pilot or member). This activity removes this restriction.

47.3 Hardware Requirements or Dependencies

No new hardware requirements have been identified.

This will be supported on resident and remote BRI access including BRI access on V5.2.

47.4 Software Requirements or Dependencies

None.

47.5 Limitations and restrictions

- CFGD option can only be assigned to pilot.
- CFGD option will be ignored if the call has been terminated on a p-p BRI.
- Backward notification to the calling user is not applicable.
- Notification to Served user that a call has been forwarded is not applicable.

47.6 Interactions

Interactions introduced by this activity are considered.

47.6.1 CLIP

No impact

47.6.2 CLIR

No impact

47.6.3 CCBS / CCNR (on hunting DN/ member)

No impact

47.6.4 CCBS / CCNR (on calling subscriber which is not a member of huntgroup)

Not applicable

47.6.5 Emergency

No impact

47.6.6 PCOS

No impact

47.6.7 AOC

No impact

47.6.8 MLPP

Not applicable

47.6.9 PROVCDS & PROVCGS (Sub=Addressing, (SUB))

No impact

47.6.10 CUG

No impact

47.6.11 MCID

No impact

47.6.12 CH

No impact

47.6.13 TP

No impact

47.6.14 COLP / COLR

No impact

47.6.15 UUS

No impact to be tested

47.6.16 ECT

ECT can be activated on the ringback from a hunt group agent with CFGD. If this event occurs the system forwards the call when the forwarding timer expires.

47.6.17 REV-C

No impact

47.6.18 CONF / 3PTY

No impact

47.6.19 CD

No impact

47.6.20 Hot Line / Warm Line

No impact

47.6.21 OCB-F

No impact

47.6.22 OCB-UC

No impact

47.6.23 WUC

Not applicable

47.6.24 MSN

Not applicable

47.6.25 CFB / CFNR

Not applicable

47.6.26 CFU

Precedence to Line Hunting

47.6.27 CFD

CFD can be assigned to an individual member of a DNH group.

- For calls to pilot DN, CFGD takes priority over CFD.
- For calls terminated on a DNH group member because of a direct call to that DN, CFD takes priority over CFGD.
- For calls terminated on a DNH group member because of hunting, CFGD takes priority over CFD.

47.6.28 CW

Not applicable

47.6.29 LOR / LOD

Overflowing occurs when all members are busy or not answered.

47.6.30 RMB

As with normal hunt, the system does not forward a call to a hunt group member that activates RMB. If these conditions occur the hunt group member that rings continues to ring.

47.6.31 SHU

As with normal hunt, the system does not forward a to a hunt group member that activates SHU. If these conditions occur the hunt group member that rings continues to ring.

47.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

47.8 Glossary

Term	Description
3PTY	3 ParTY Conference
AOC	Advice of Charge
BRI	Basic Rate Interface
CCBS	Completion of Calls to Busy Subscribers

Term	Description
CCNR	Call Completion No Reply
CD	Call Deflection
CFB	Call Forwarding Busy
CFD	Call Forwarding Don't answer
CFGD	Call Forward Group Don't answer
CFNR	Call Forwarding No Reply
CFU	Call Forwarding Unconditional
CH	Call Hold
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restriction
CONF	CONFerence
CUG	Closed User Group
CW	Call Waiting
DDI	Direct Dialling In
DLH	Distributed Line Hunt
DN	Directory Number
DNH	Directory Number Hunt
ECT	Explicit Call Transfer
LCC	Line Class Code
LOD	Line Overflow Route
LOR	Line Overflow DN
MCID	Malicious Call IDentification
MLH	MultiLine Hunt
MLPP	Multi Level Precedence and Preemption
MSN	Multiple Subscriber Number
OCB	Outgoing Call Barring
OCB-F	Outgoing Call Barring-Fixed

Term	Description
OCB-UC	Outgoing Call Barring User Controlled
PCOS	Priority Class of Service
PROVCDS	Called party subaddress
PROVCGS	Calling party subaddress
p-p	point-to-point
REV-C	Reverse Charging
RMB	Random Make Busy
SHU	Stop HUnt
SUB	SUB addressing
TP	Terminal Portability
UUS	User to User Signalling
WUC	Wake-Up Call

48: Functional Description (FN): A00003227

48.1 Feature name

ISN07, IN support for User to User Service (UUS)

48.2 Description

48.2.1 Overview

This activity performs the followings for MMP:

- Introduction of the User-to-User information (UUI) parameter to the INAP InitDP operation as a Nortel defined InitDP parameter. This parameter is controlled via table SERVINFO datafill.
- Integration of the Continue opr XLA REENTRY function and the IN Auto-Continue functionality, i.e. the Auto-Continue functionality supports the XLA REENTRY option.
- Enhancement of the EINTRACE CI tool to display the UUI extension if it is sent within an InitDP operation.

48.2.2 UUI Parameter

The description in this section assumes the following:

- An incoming call triggers as an IN call (TDP2 or TDP3), i.e. an InitDP is sent to the SCP.

The UUI data, i.e. the real user information without the parameter header octets (i.e. without UUI element identifier, length and protocol discriminator octets), of an incoming BASE and GERMAN ETSI ISUP V2 IAM is read out and transferred within the InitDP operation to the SCP. UUI is only supported towards SCP. It can not be sent back.

If there is no UUI data contained in an incoming ETSI ISUP V2 IAM no UUI related data is sent within the InitDP operation to the SCP.

UUI functionality is only supported for ETSI ISUP V2 signalling.

When auto-continue is invoked, the UUI information is not removed and is passed on to the terminating agents which are ETSI BRI, ETSI PRI and ETSI ISUP.

The ASN.1 format of the UUI extension field of the InitDP looks as follows:

-- Definition of the Nortel UUI Extension

```
NortelUUIExtension EXTENSION
    EXTENSION-SYNTAX ExtUUIType
    CRITICALITY ignore

-- Assignment of value (integer identifier)
nortelUUIExtension NortelUUIExtension ::= 20

-- Type definition (format / possible values)
ExtUUIType ::= INExtUUI
INExtUUI ::= OCTET STRING (SIZE(1..128))
```

An SSP example datafill for UUI functionality is shown below ;

```
>TABLE SERVINFO

SERVIDX                                                    OPTION

-------------------------------------------------------------------------

   99    (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (EVENT_TYPE)
(UUI) $)

         (RESPONSE_INFO (CONTINUE_OPT (XLA_REENTRY (
UNIV_XLA PX NETXLA) $)$)$)

(TCAP_INFO ( INAP_OPT (AUTO_CONTINUE) $)$)$
```

48.2.3 Auto-Continue with translation reentry functionality

The requirement is to be able to re-translate a TDP-3 triggered failing SCP query using a pre-defined translator. This functionality is supported in by ‘merging’ the existing Auto-Continue operation and the existing REENTRY XLA option. For that, both options have to be provisioned within table SERVINFO for a service index.

Please note that the documented existing SSP functionality is as follows:

- Continue operation with REENTRY:
  In this call scenario the call is either translated using the REENTRY translator (if triggered at TDP-2), or re-translated using the REENTRY translator (if triggered at TDP-3). Armed and encountered EDPs are properly handled.
- Auto-Continue operation (alone):
  In this call scenarios the call is resumed either at TDP-2 (for TDP-2 triggered calls) or TDP-3 (for TDP-3 triggered calls) and behaves the same as a regular Continue operation. Any armed EDP is not handled as the IN feature is cleared as soon as the Auto-Continue opr finishes.

The merger of both above functionalities, i.e. Auto-Continue opr with REENTRY option, does properly work with TDP-2 and TDP-3 triggering but without consideration of EDP handling.

When Auto-continue is invoked , existing EIN301 log is generated.

An SSP example datafill for Auto-Continue with REENTRY functionality is shown below;

```
>TABLE SERVINFO
SERVIDX                                                    OPTION
-------------------------------------------------------------------------------1
(RESPONSE_INFO (CONTINUE_OPT (XLA_REENTRY (UNIV_XLA
PX NETXLA ) $)$)$)

    (TCAP_INFO (INAP_OPT (AUTO_CONTINUE) $)$)$

BOTTOM
```

48.2.4 UUI extension display by EINTRACE CI tool

The EINTRACE CI tool supports the UUI extension within an InitDP operation. If an InitDP operation contains an UUI extension field, then the EINTRACE CI tool decodes and displays the UUI data within the InitDP operation trace.

48.3 Hardware Requirements or Dependencies

None

48.4 Software Requirements or Dependencies

None

48.5 Limitations and restrictions

- The Auto-Continue with XLA reentry utilization is only supported on TDP-3 triggered IN calls without utilization of EDPs or IPs. The Auto-Continue with XLA reentry utilization on TDP-2 triggered IN call is not considered in this activity.
- This activity only supports Base and German ETSI ISUP V2.

48.6 Interactions

None

48.7 Applicable customer facing sections

Fault Management

- Logs N/A
- Alarms N/A

Configuration

- Data Schema X
- User Interface N/A
- Element Management N/A
- Security N/A
- Service Order N/A
- Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

48.8 Glossary

Term	Description
EDP	Event Detection Point
IP	Intelligent Peripheral
SCP	Service Control Point
SSP	Service Switching Point
UUI	User-User information
IN	Intelligence Network
TDP	Trigger Detection Point
INAP	IN Application Part

48.9 References

A59033629 INAP Auto-Continue

A59022169 ISDN PRI UUS

A59023626 BRI Explicit Call Transfer

49: Functional Description (FN): A00003405

49.1 Feature name

ECAN Support for International Trunks

49.2 Description

Currently, the SPMECMON tool allows a craftsperson to query a resource module to obtain echo canceller performance data such as Echo Return Loss (ERL) and Echo Return Loss Enhancement (ERLE). This capability is available and limited to 24 channels per carrier on NA trunks off of SPMs. However, there are 32 channels per carrier on the international SPM (iSPM) and the capability of monitoring all channels is needed on the iSPM. Therefore, this feature enhances SPMECMON's functionality by increasing its capability to monitor all 32 channels on international trunks.

49.3 Software Requirements or Dependencies

This feature does not affect any hardware configurations or settings. The SPMECMON command is only valid when used for trunks that are set up for internal echo cancellation and assigned to an echo canceller equipped SPM.

49.4 Limitations and restrictions

No restrictions or limitations have been added to this tool.

49.5 Interactions

None.

49.6 Applicable customer facing sections

N/A

49.7 Glossary

iSPM International Spectrum Peripheral Module

50: Functional Description (FN): A00003410

50.1 Feature name

Honduras ETSI ISUP variant

50.2 Description

The purpose of this feature is to introduce a new ETSI ISUP variant for Honduras market in MMP20. This variant should be defined under ETSI ISUP Version 2 (White Book).

The reason to use the new variant is that Honduras market requirements may not be provided neither by the BASE ETSI ISUP nor by one of existing variants. The detailed description of Honduras market requirements may be found in the Product Spec “ETSI ISUP for Honduras (HONDUTEL)” , module **P008287PS.AA05** in FMDOC library.

The brief description of Honduras market requirements:

- Honduras ISUP variant should be supported in QDT and QCI loads.
- Prohibit specific ISUP messages and parameters.
- Support of INR/INF ISUP messages.
- Support of national Calling Party Categories (CPC) in interworking between Honduras ETSI ISUP and FDCP protocols.
- Support of TrunK Offering (TKO) feature.
- Support of Malicious Call Trace feature.

The detailed description of Honduras market requirements is below.

50.2.1 New Honduras variant

The type CCITT_ISUP_VARIANT_TYPE should be extended with HONDURAS variant (new decimal value 43 will be used), see figure 1 below. Trunk definition in the TRKSGRP table is shown on the figure 2.

Figure 1 Extention of CCITT_ISUP_VARIANT_TYPE

```
type CCITT_ISUP_VARIANT_TYPE
{BASE,GERMANY,FRANCE,SPAIN,BELGIUM,ITALY,ISRAEL,PNG,SPARE,UK,
CHILE,COSTA_RICA,NORWAY,NEW_ZEALAND,ETHIOPIA,GEORGIA,MYANAMAR,
VIETNAM,ISDEFO,SAUDI,ACIF_AUSTRALIA,BRAZIL,MEXICO,TURKEY,PORTUG
AL,DENMARK,SPIROU,SWEDEN,AUSTRIA,EGYPT,JPN_INTERCONN,PERU,
ARGENTINA,POLAND,CZECH,HUNGARY,CA30_AUSTRALIA,HONGKONG,TAIWAN,
SINGAPORE,CHINA,BANGLADESH,RUSSIA, HONDURAS}
```

Figure 2 HONDURAS variant in TRKSGRP

```
TABLE TRKSGRP
pos orisup2 0

>orisup2 0 ORISUP2 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0
TMX100 N N HONDURAS 100_WHITE (ALL_NOA ) $ NIL CIC
```

The Honduras ETSI ISUP variant should be supported in the following crosses.

Table 1 Supported crosses

port2 / port1	ISUP	FDCP	IBN
ISUP	Y	Y	Y
FDCP	Y		
IBN	Y		

50.2.2 Alowed ISUP Messages and Optional Parameters

Messages that should be **supported** in Honduras market are shown in the Table 2 below. If any other message will be received in the trunk it should be responsed with ISUP_CNF (confusion).

Table 2 Supported messages

Message	Code
Address complete	0 0 0 0 0 1 1 0
Answer	0 0 0 0 1 0 0 1
Blocking	0 0 0 1 0 0 1 1

Table 2 Supported messages

Message	Code
Blocking acknowledgement	0 0 0 1 0 1 0 1
Call progress	0 0 1 0 1 1 0 0
Circuit group blocking	0 0 0 1 1 0 0 0
Circuit group blocking acknowledgement	0 0 0 1 1 0 1 0
Circuit group reset	0 0 0 1 0 1 1 1
Circuit group reset acknowledgement	0 0 1 0 1 0 0 1
Circuit group unblocking	0 0 0 1 1 0 0 1
Circuit group unblocking acknowledgement	0 0 0 1 1 0 1 1
Confusion	0 0 1 0 1 1 1 1
Connect	0 0 0 0 0 1 1 1
Continuity	0 0 0 0 0 1 0 1
Continuity check request	0 0 0 1 0 0 0 1
Information (national use)	0 0 0 0 0 1 0 0
Information request (national use)	0 0 0 0 0 0 1 1
Initial address	0 0 0 0 0 0 0 1
Operator (for TKO)	1 1 1 1 1 0 0 1
Release	0 0 0 0 1 1 0 0
Release complete	0 0 0 1 0 0 0 0
Reset circuit	0 0 0 1 0 0 1 0
Resume	0 0 0 0 1 1 1 0
Subsequent address	0 0 0 0 0 0 1 0
Suspend	0 0 0 0 1 1 0 1
Unblocking	0 0 0 1 0 1 0 0
Unblocking acknowledgement	0 0 0 1 0 1 1 0

Parameters that should be **supported** for Honduras variant are shown in the “Table 3 Supported parameters”. Parameters that are not suported should

not be included in the ISUP messages taht are built in the switch, and being received from another switch should be discarded.

Table 3 Supported parameters

Parameter	Code
Access transport	0 0 0 0 0 0 1 1
Automatic congestion level	0 0 1 0 0 1 1 1
Backward call indicators	0 0 0 1 0 0 0 1
Called party number	0 0 0 0 0 1 0 0
Calling party number	0 0 0 0 1 0 1 0
Calling party's category	0 0 0 0 1 0 0 1
Cause indicators	0 0 0 1 0 0 1 0
Circuit group supervision message type	0 0 0 1 0 1 0 1
Closed user group interlock code	0 0 0 1 1 0 1 0
Connected number	0 0 1 0 0 0 0 1
Continuity indicators	0 0 0 1 0 0 0 0
End of optional parameters	0 0 0 0 0 0 0 0
Event information	0 0 1 0 0 1 0 0
Forward call indicators	0 0 0 0 0 1 1 1
Information indicators	0 0 0 0 1 1 1 1
Information request indicators	0 0 0 0 1 1 1 0
Nature of connection indicators	0 0 0 0 0 1 1 0
Optional backward call indicators	0 0 1 0 1 0 0 1
Optional forward call indicators	0 0 0 0 1 0 0 0
Range and status	0 0 0 1 0 1 1 0
Subsequent number	0 0 0 0 0 1 0 1
Suspend/Resume indicators	0 0 1 0 0 0 1 0
Transmission medium requirement	0 0 0 0 0 0 1 0
User service information	0 0 0 1 1 1 0 1
User-to-user indicators	0 0 1 0 1 0 1 0
User-to-user information	0 0 1 0 0 0 0 0

Note: parameteres and indicators supported in INR/INF messages are described below in the section “50.2.3 Support of INR/INF”.

50.2.3 Support of INR/INF

Information request indicators under the INformation Request (INR) message and Information indicators under the INFormation (INF) message should support only calling party address.

Supported information indicators are shown in the “Table 4 INR / INF - Indicators support”.

Table 4 INR / INF - Indicators support

Message	Indicators	Bits	Value
INR	**calling party address request**	**A**	**Y**
	holding indicator	B	N
	calling party category request	D	N
	charge information request	E	N
	malicious call identification	H	N
INF	**calling party address response**	**BA**	**Y**
	hold provided	C	N
	calling party category response	F	N
	charge information response	G	N
	solicited information	H	N

Table 5 INR/INF Indicators supported

Message	Indicator supported	Not supported
INR	calling party address (bit A)	Bits B - P should be 0
INF	calling party address response (bits A - B)	Bits C - P should be 0

Optional parameters supported in INR/INF are shown in the “Table 6 INR / INF - Optional Parameters support”, see below.

Table 6 INR / INF - Optional Parameters support

Message	Indicators	Supported
INR	call reference	N
	network specific facility	N
	parameter compatibility information	N

Table 6 INR / INF - Optional Parameters support

Message	Indicators	Supported
INF	calling party category	N
	calling party number	**Y**
	call reference	N
	connection request	N
	parameter compatibility information	N
	network specific facility	N

Table 7 Message Type : INR and INF messages.

Message	Parameter	Type	Length
INR	Message Type	F	1
	Information request indicators	F	2
	End of optional parameters	O	1
INF	Message Type	F	1
	Information indicators	F	2
	calling party number	O	5-12
	End of optional parameters	O	1

50.2.3.1 INR / INF in Tandem switch.

Figure 3 INR / INF for regular CPC

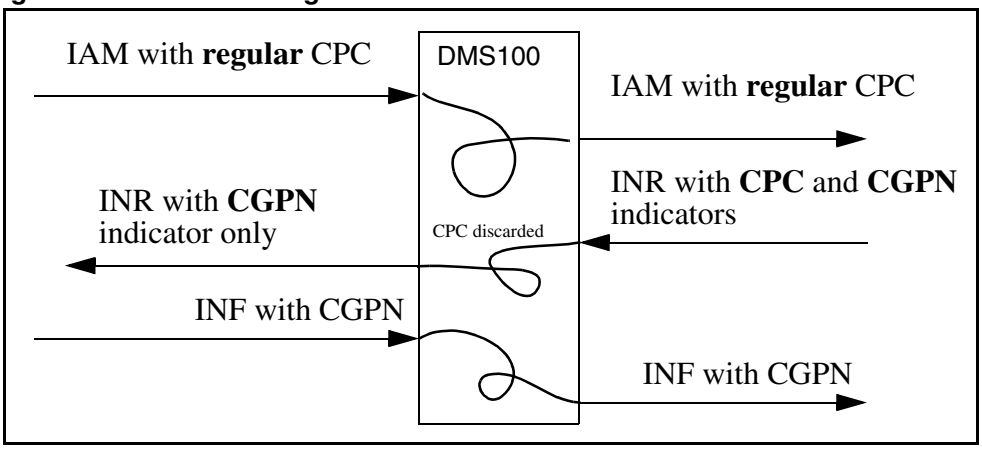
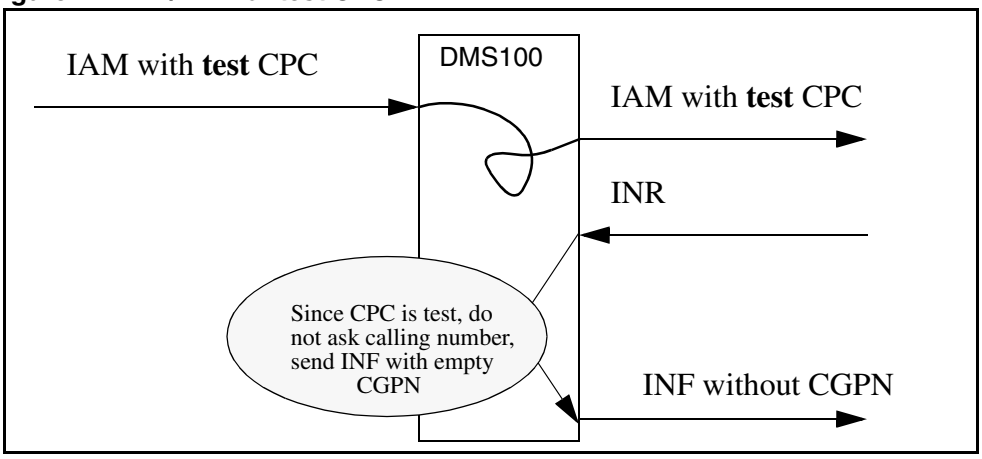


Figure 4 INR / INF for test CPC



50.2.3.2 INR / INF in Originating switch.

Figure 5 INR / INF for regular CPC

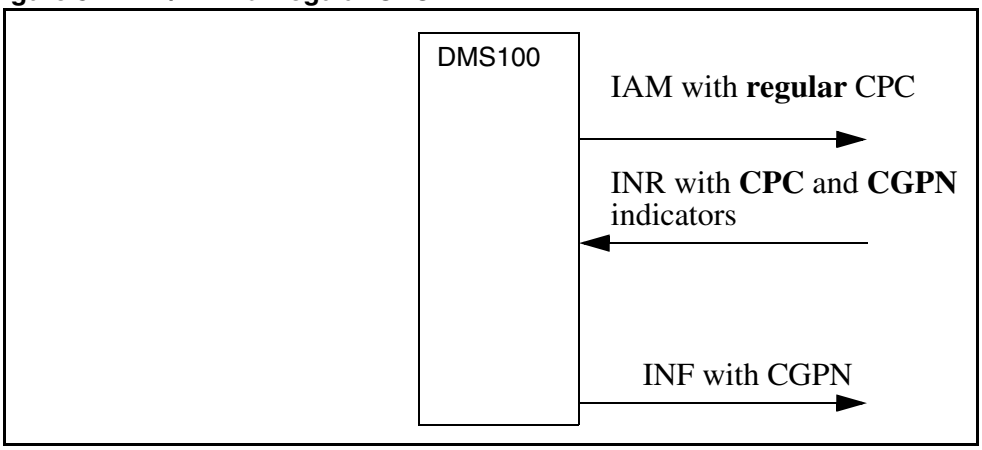
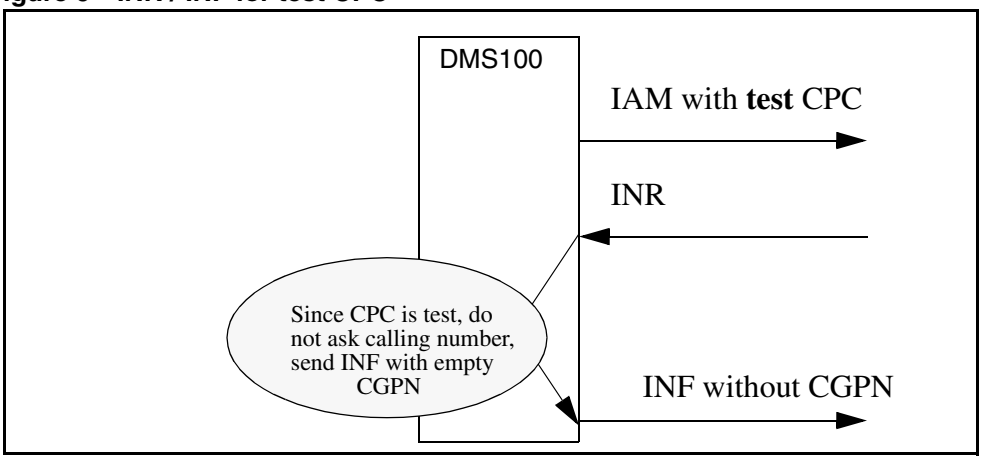
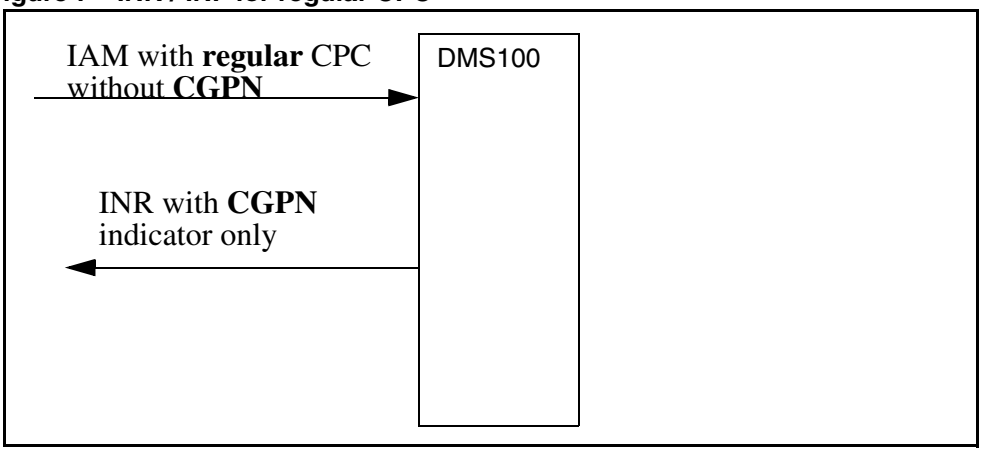


Figure 6 INR / INF for test CPC



50.2.3.3 INR / INF in Terminating switch.

Figure 7 INR / INF for regular CPC



50.2.4 Calling Patry Categories: Values and Mapping.

The following calling party categories should be supported for Honduras variant (see table below).

Table 8 Calling Patry Categories

CPC	Value
Regular	#0A
Priority	#0B

Table 8 Calling Patry Categories

CPC	Value
Public phone	#0F
National Operator	#E1
Test	#0D

In the ISUP - FDCP and FDCP - ISUP crosses that should be supported by Honduras ETSI ISUP variant the mapping between ISUP CPC categories and MFC activities is following:

Table 9 CPC Mapping

ISUP CPC	Value	MFC Activity	Signal
ISUP_CPC_SUBSCRIBER_1	#0A	REG_SUB	1
ISUP_CPC_TOF_OPER	#E1	OPER	5
ISUP_CPC_PRIORITY	#0B	PR_SUB	2
ISUP_CPC_PAYPHONE	#0F	LOCAL_COIN	4
ISUP_CPC_TEST_CALL	#0D	MTC_EQ	3

In the mapping for ISUP to FDCP - Convert all ISUP_CPC categories except the above mentioned to REG_SUB MFC Activity.

In the mapping for FDCP to ISUP - Convert all MFC Activities categories except the above mentioned to ISUP_CPC_Subscriber_1.

50.2.5 Trunk Offering

The Honduras requirements for trunk offering are the same that for Costa-Rica market, detailed information on it may be found in the feature **A00002291.AA15** “Trunk Offering Expansion”, FMDOC library.

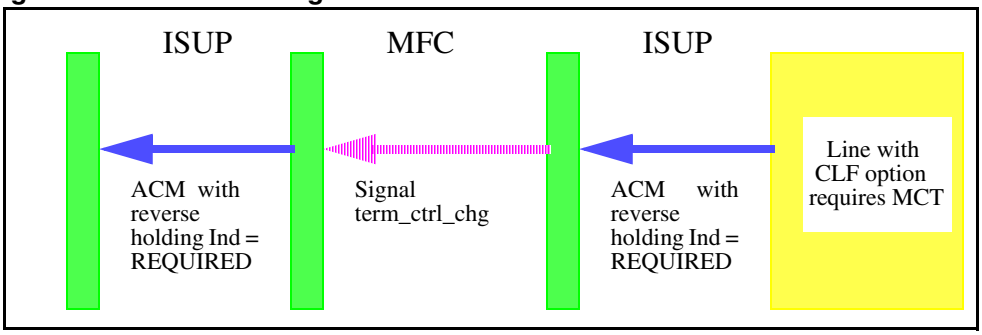
- The ISUP Operator signal should be #F9.
- The operator calling party category should be #E1 (see Table 8 above).

50.2.6 Malicious Call Trace

MCT support means that the field **Reverse_Holding_Ind** in the ACM message (that is set acording to the will of MCT terminator) should be transferred via net.

In the FDCP to ISUP tandem ACM with Reverse_Holding_Ind = REQUIRED should be transferred into activity TERM_CTRL_CHG, and into activity CONNECT_CALL_CHG otherwise.

Figure 8 Reverse holding indicator transfer



50.3 Hardware Requirements or Dependencies

N/A

50.4 Software Requirements or Dependencies

N/A

50.5 Limitations and restrictions

A. Messages that should be **supported** in Honduras market are shown in Table 2. If any other message will be received in the trunk, it should be responsed with ISUP_CNF (confusion) message.

B. Parameters that should be **supported** for Honduras variant are shown in Table 3. Parameters that are not suported should not be included in the ISUP messages taht are built in the switch, and being received from another switch should be discarded.

C. The definition of Honduras variant will be only for SX05 release.

50.6 Interactions

N/A

50.7 Glossary

Term	Description
CPC	Calling Party Category
INF	Information

Term	Description
INR	Information Request
MCT	Malicious Call Trace
TKO	Trunk Offering

50.8 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	**X**
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

50.9 References

ETSI ISUP for Honduras (HONDUTEL) - Product Spec, module **P008287PS.AA05** in FMDOC library.

“Protocols for Telrad markets”, module **AF7822.AA06** in DOC library.

“Manual Trunk Offering for Egypt ISUP”, module **A59017279.AA10** in FMDOC library.

“Trunk Offering Expansion”, module **A00002291.AA15** in FMDOC library.

51: Functional Description (FN): A00003411

51.1 Feature name

New TONESET for Honduras.

51.2 Description

This feature provides new loadable tones for the Honduras market on the base of existing NTMX76AB and NTMX76CA tone cards for the GPP and DTCO2 peripherals in the MMP20 stream.

The tone set includes:

- DTMF (Dual-Tone Multi-Frequency) tones
  - — The DTMF tones are added to support EBS (Electronic Business Set) and signalling to PABXs (Private Automatic Branch Exchanges). The following is the list the DTMF tones that should be defined for Honduras market: dtmf digit 1, dtmf digit 2, dtmf digit 3, dtmf digit 4, dtmf digit 5, dtmf digit 6, dtmf digit 7, dtmf digit 8, dtmf digit 9, dtmf digit 0, dtmf tone *, dtmf tone #, dtmf tone A, dtmf tone B, dtmf tone C, dtmf tone D.
- MFC (Forward Multi-Frequency Compelled) tones
  - — The MFC tones are added to support R2 protocol signalling. The following is the list the MFC tones that should be defined for Honduras market: MFC 1, MFC 2, MFC 3, MFC 4, MFC 5, MFC 6, MFC 7, MFC 8, MFC 9, MFC 10, MFC 11, MFC 12, MFC 13, MFC 14, MFC 15.
- B MFC (Backward Multi-Frequency Compelled) tones
  - — The following is the list the B MFC tones that should be defined for Honduras market: MFC B1, MFC B2, MFC B3, MFC B4, MFC B5, MFC B6, MFC B7, MFC B8, MFC B9, MFC B10, MFC B11, MFC B12, MFC B13, MFC B14, MFC B15.
- Supervisory Tones
  - — The supervisory tones consist of standard voice band supervisory tones generated by equipment connected to public exchanges. The following is the list the supervisory tones that should be defined for Honduras market: Dial Tone, Silent Tone, Milliwat Tone, Low Tone, High Tone, SF Loud tone, Audible Ringing Tone, Busy Tone, Congestion (Reorder), ROH (Howler), Call Waiting Tone, Confirmation Tone (PIT), Special Dial Tone, Vacant.

By specifying the appropriate TONESET field in table LTCINV, the tone-making process generates the tone samples required by Honduras market. The

TONESET field should be set to 'HONTONES'. These tone samples are sent to the tone memory (RAM).

51.2.1 Continuous tones

51.2.1.1 Continuous Tones definition

Table 1

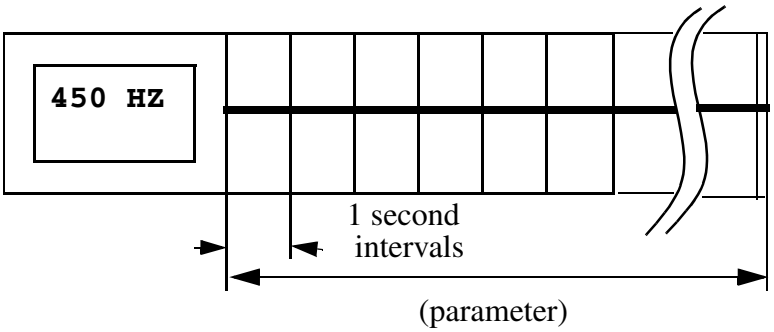
Tone	Description
DIAL TONE	Is sent to the call originator after off-hook until the first digit is received by the exchange.
SILENT TONE	Is sent as a quiet termination for the tone-off periods to prevent noise.
MILLIWAT TONE	Is sent through an O/G or an I/C trunk at 0 dBm level (1 mW) so that the far end can measure losses of the trunk. The tone is used for trunk tests T902 and T904.
LOW TONE	The LOW Tone is for future use.
HIGH TONE	The HIGH Tone is for future use.
SF LOUD TONE	The SF LOUD tone is used for XPM tests.

51.2.1.2 Continuous Tones description

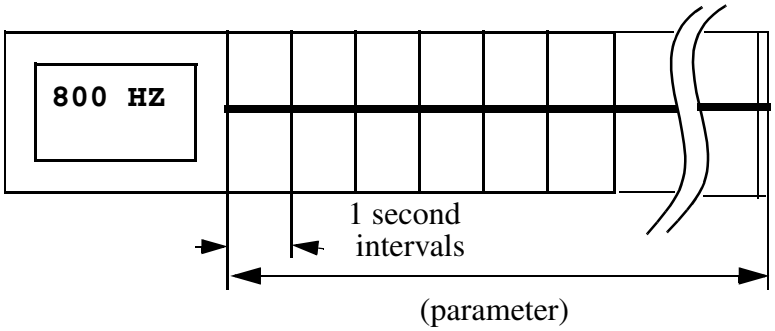
SILENT TONE

Is sent as a quiet termination for the tone-off periods to prevent noise.

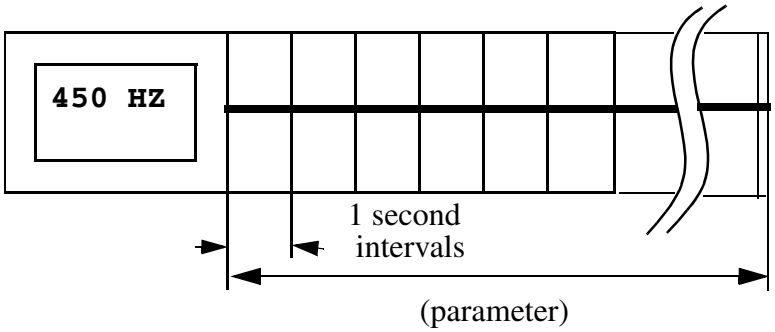
DIAL TONE



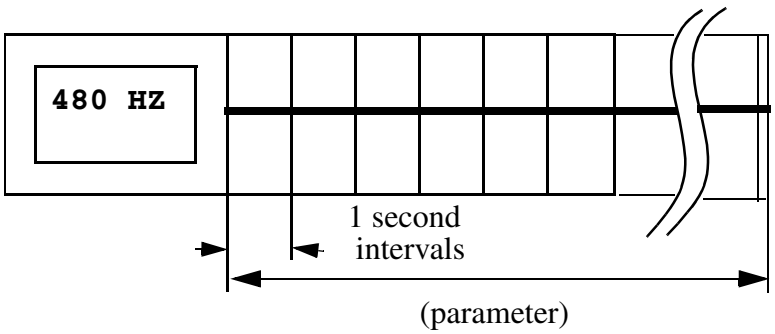
MILLIWAT TONE



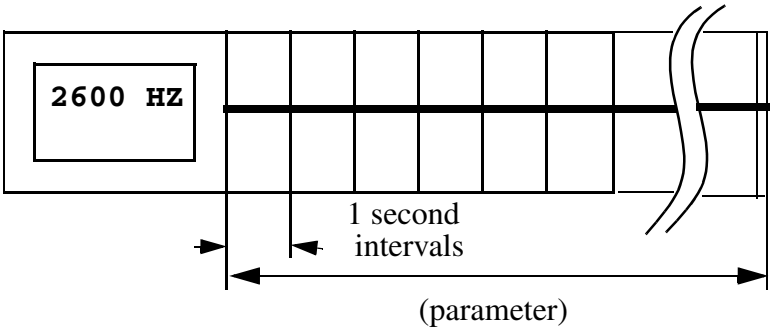
LOW TONE



HIGH TONE



SF LOUD TONE



51.2.1.3 Simple Tones allocation

The list of the simple Honduras tones is shown below in Figure 2, "Honduras, Simple Tones."

Table 2 Honduras, Simple Tones.

Index	Tone description	in use
01		
02		
03	ROH (Howler)	+
04	AUDIBLE RINGING	-
05	LOW TONE	+
06	DIAL TONE	+
07		
08		
09	HIGH TONE	+
0A		
0B	SF LOUD TONE	+
0C		
0D	B MFC2	+
0E	B MFC3	+
0F		

Table 2 Honduras, Simple Tones.

Index	Tone description	in use
10	SILENT TONE	+
11	MFC I1	+
12	MFC I2	+
13	MFC I3	+
14	MFC I4	+
15	MFC I5	+
16	MFC I6	+
17	MFC I7	+
18	MFC I8	+
19	MFC I9	+
1A	MFC I10	+
1B	MFC I11	+
1C	MFC I12	+
1D	MFC I13	+
1E	MFC I14	+
1F	MFC I15	+
20	DTMF D	+
21	DTMF 1	+
22	DTMF 2	+
23	DTMF 3	+
24	DTMF 4	+
25	DTMF 5	+
26	DTMF 6	+
27	DTMF 7	+
28	DTMF 8	+
29	DTMF 9	+
2A	DTMF 0	+
2B	DTMF *	+

Table 2 Honduras, Simple Tones.

Index	Tone description	in use
2C	DTMF #	+
2D	DTMF A	+
2E	DTMF B	+
2F	DTMF C	+
30	MW TONE	+
31	BMFC1	+
32	COT1	-
33	COT2	-
34	B MFC4	+
35	B MFC5	+
36	B MFC6	+
37	B MFC7	+
38	B MFC8	+
39	B MFC9	+
3A	B MFC10	+
3B	B MFC11	+
3C	B MFC12	+
3D	B MFC13	+
3E	B MFC14	+
3F	B MFC15	+

51.2.2 Periodic Tones

51.2.2.1 Tones definition

Table 3

Tone	Description
CONGESTION TONE	Is sent in the backward direction to indicate to the calling party congestion on the O/G trunk, or blocking condition in the NET module
BUSY TONE	Is sent to the subscriber to indicate unavailable destination.

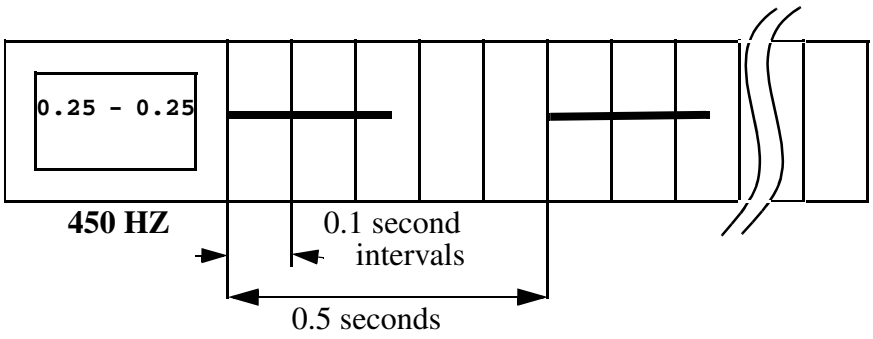
Table 3

Tone	Description
RING BACK TONE	Is sent to the originator during wait for answer state.
VACANT TONE	Is sent due to one of the following treatment conditions: FNAL - Feature Not Allowed. HNPI - Home NPA Intercept. VACT - Vacant Code.
ROH (HOWLER)	The Receiver Off Hook tone (ROH) is sent to the subscriber as a loud tone after it was left off-hook for more than a predefined time and no digits dialed. It is also sent when the terminator remains off-hook for more than a predefined time after originator disconnect. The ROH tone consists of 4 frequencies, 470Hz, 940Hz, 1410Hz and 1880Hz mixed together. Each frequency has a -2dBm level so that the total bursts ROH level is 4dBm.
SPECIAL DIAL TONE (SPDT)	Is given to a subscriber in various features to allow him continue with the dialling.
CALL WAITING TONE	Is given to a terminator (who subscribed to the CWT feature) as a warning signal that another call has entered and is waiting for an answer.
CONFIRMATION TONE	Is given to a subscriber that has activated a feature as a positive acknowledge that the feature has been received by the switch.
INTRUSION TONE	This Tone is used to provide the warning for a subscriber that is occupied in a call that an operator has just established a TPS/ ENQ as part of the Trunk Offering feature. We shall probably provide the intrusion tone for the operator trunk offering feature, directly from the CTM card. In which case the pattern will remain as it is provided in the CTM and will not be changed.

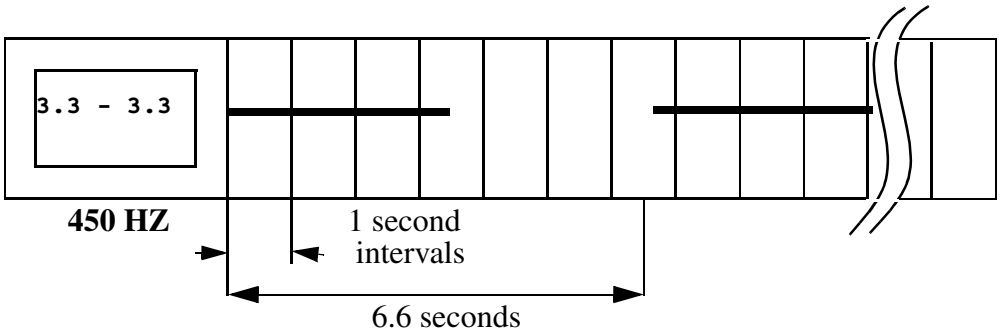
Note: The meaning of (+) is that it is in use, the meaning of (-) is that it is not currently in use.

51.2.2.2 Periodic Tones cadences

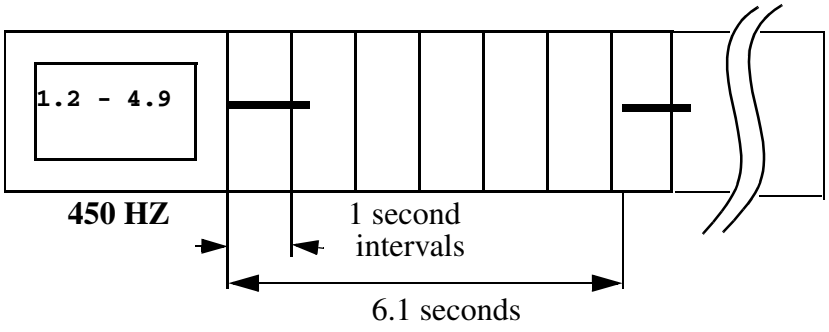
CONGESTION TONE



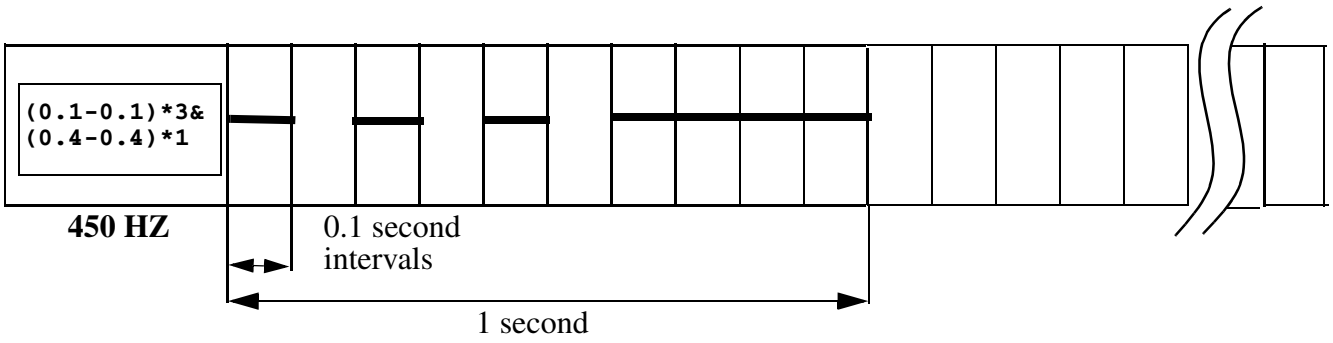
BUSY TONE



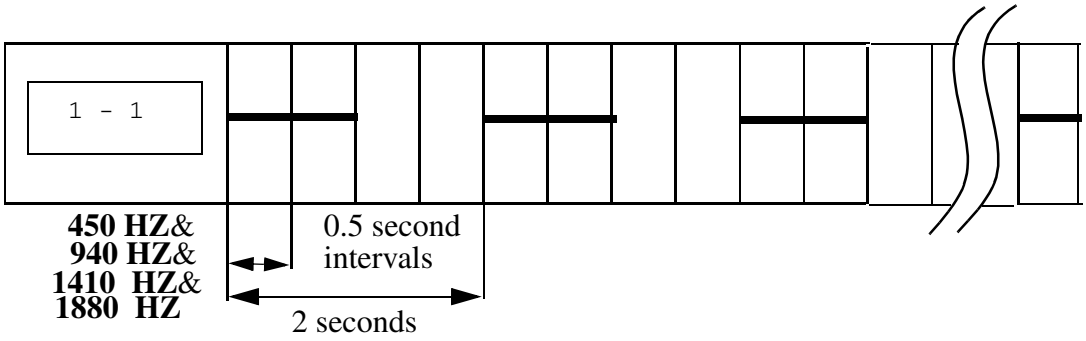
RING BACK TONE



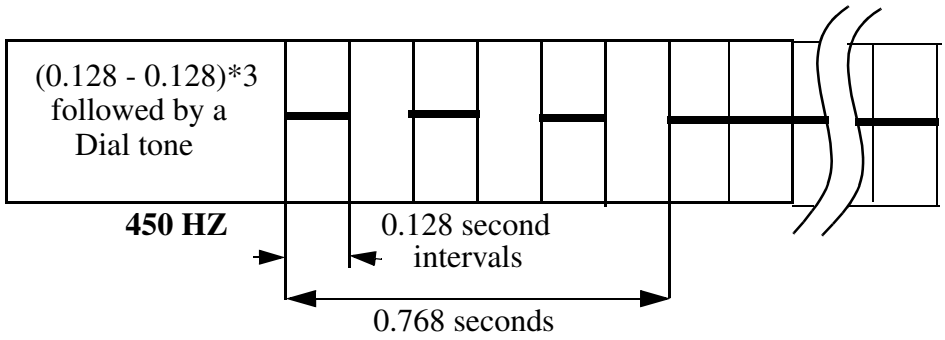
VACANT TONE



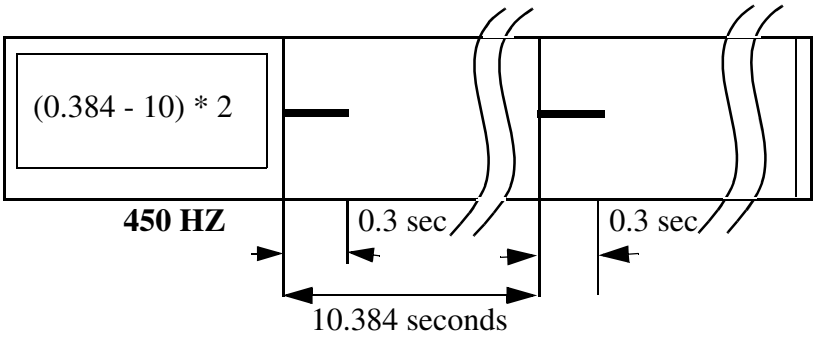
ROH (HOWLER)



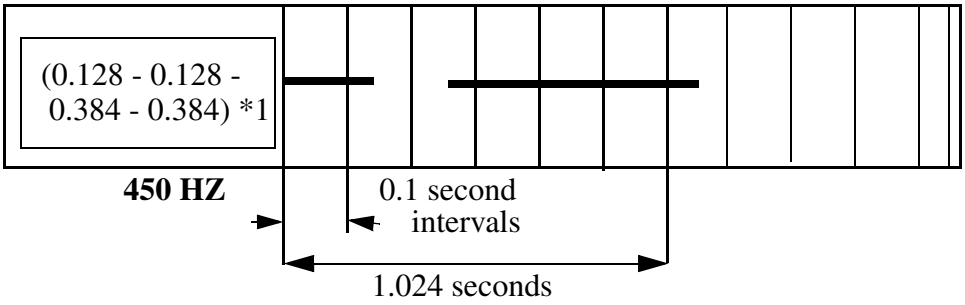
SPECIAL DIAL TONE (SPDT)



CALL WAITING TONE



CONFIRMATION TONE



51.2.2.3 Periodic Tones allocation

The list of the periodic Honduras tones is shown below in Figure 4, "Honduras, Periodic Tones.".

Table 4 Honduras, Periodic Tones.

Tone-Id	Tone	in use
80	Audible Ringing Tone	+
81	Busy Tone	(treatment)
82	Congestion (Reorder) Tone	(treatment)
83	ROH (Howler)	+
84	Busy Verification Tone	-
85	Call Waiting Tone	+

Table 4 Honduras, Periodic Tones.

Tone-Id	Tone	in use
86	PABX confirmation	-
87	Confirmation Tone (PIT)	(treatment)
88	PABX confirmation	-
89	Special Dial Tone (SPDT)	+
8A	PABX Audible Ringing	-
8B	Special Audible Ringing	-
8C	Intercept Tone	-
8D	Warble Tone	-
8E	Toll Break-in	-
8F	Vacant Tone	(treatment)
90		
91		
92	Holding Tone	Silent Tone
93		
94	Special Information Tone	-
95	Switching Indication Tone	-
96		
97	Line Lockout	Silent Tone
98		
99	Stuttered Dial tone	-
9A		
9B	Caller Waiting Tone	Audible Ringing Tone
9C	Negative Indication Tone (NIT)	-
9D	Warning Tone	-
9E	Intrusion Tone	-
9F		

51.2.2.4 Transmission Requirements

Characteristics of simple and periodic tones in Honduras market are shown below.

Table 5 Honduras. Transmission Requirements.

Tone Name	Frequency (Hz)	Frequency Tolerance	Level (dbm0)	Cadence rate Tolerance	Tone Id. in hex
Dial Tone	450	0.5%	-8	--	06
Silent Tone	0	--	-100	--	10
MFC 1	1380/1500	+/-4hz	-11.5/-11.5	--	11
MFC 2	1380/1600	+/-4hz	-11.5/-11.5	--	12
MFC 3	1500/1620	+/-4hz	-11.5/-11.5	--	13
MFC 4	1380/1740	+/-4hz	-11.5/-11.5	--	14
MFC 5	1500/1740	+/-4hz	-11.5/-11.5	--	15
MFC 6	1620/1740	+/-4hz	-11.5/-11.5	--	16
MFC 7	1380/1860	+/-4hz	-11.5/-11.5	--	17
MFC 8	1500/1860	+/-4hz	-11.5/-11.5	--	18
MFC 9	1620/1860	+/-4hz	-11.5/-11.5	--	19
MFC 10	1740/1860	+/-4hz	-11.5/-11.5	--	1A
MFC 11	1380/1980	+/-4hz	-11.5/-11.5	--	1B
MFC 12	1500/1980	+/-4hz	-11.5/-11.5	--	1C
MFC 13	1620/1980	+/-4hz	-11.5/-11.5	--	1D
MFC 14	1740/1980	+/-4hz	-11.5/-11.5	--	1E
MFC 15	1860/1980	+/-4hz	-11.5/-11.5	--	1F
DTMF 1	697/1209	1.5%	-5 / -5	--	21
DTMF 2	697/1336	1.5%	-5 / -5	--	22
DTMF 3	697/1477	1.5%	-5 / -5	--	23
DTMF 4	770/1209	1.5%	-5 / -5	--	24
DTMF 5	770/1336	1.5%	-5 / -5	--	25
DTMF 6	770/1477	1.5%	-5 / -5	--	26
DTMF 7	852/1209	1.5%	-5 / -5	--	27
DTMF 8	852/1336	1.5%	-5 / -5	--	28

Table 5 Honduras. Transmission Requirements.

Tone Name	Frequency (Hz)	Frequency Tolerance	Level (dbm0)	Cadence rate Tolerance	Tone Id. in hex
DTMF 9	852/1477	1.5%	-5 / -5	--	29
DTMF 0	941/1336	1.5%	-5 / -5	--	2A
DTMF *	941/1209	1.5%	-5 / -5	--	2B
DTMF #	941/1477	1.5%	-5 / -5	--	2C
DTMF A	697/1633	1.5%	-5 / -5	--	2D
DTMF B	770/1633	1.5%	-5 / -5	--	2E
DTMF C	852/1633	1.5%	-5 / -5	--	2F
DTMF D	941/1633	1.5%	-5 / -5	--	20
MFC B1	1020/1140	+/-4hz	-11.5/-11.5	--	31
MFC B2	900/1140	+/-4hz	-11.5/-11.5	--	0D
MFC B3	900/1020	+/-4hz	-11.5/-11.5	--	0E
MFC B4	780/1140	+/-4hz	-11.5/-11.5	--	34
MFC B5	780/1020	+/-4hz	-11.5/-11.5	--	35
MFC B6	780/900	+/-4hz	-11.5/-11.5	--	36
MFC B7	660/1140	+/-4hz	-11.5/-11.5	--	37
MFC B8	660/1020	+/-4hz	-11.5/-11.5	--	38
MFC B9	660/900	+/-4hz	-11.5/-11.5	--	39
MFC B10	660/780	+/-4hz	-11.5/-11.5	--	3A
MFC B11	540/1140	+/-4hz	-11.5/-11.5	--	3B
MFC B12	540/1020	+/-4hz	-11.5/-11.5	--	3C
MFC B13	540/900	+/-4hz	-11.5/-11.5	--	3D
MFC B14	540/780	+/-4hz	-11.5/-11.5	--	3E
MFC B15	540/660	+/-4hz	-11.5/-11.5	--	3F
Milliwat Tone	800	1.5%	0	--	30
Low Tone	450	0.5%	-8	--	05
High Tone	480	0.5%	-8	--	09
SF Loud tone	2600	2.5%	-8	--	0B
Audible Ringing Tone	450	0.5%	-8	± 10%	80

Table 5 Honduras. Transmission Requirements.

Tone Name	Frequency (Hz)	Frequency Tolerance	Level (dbm0)	Cadence rate Tolerance	Tone Id. in hex
Busy Tone	450	0.5%	-8	± 10%	81
Congestion (Reorder)	450	0.5%	-8	± 10%	82
ROH (Howler)	470/940	2.5%	-2/-2	± 10%	83
	1410/1880	2.5%	-2/-2	± 10%	
Call Waiting Tone	450	0.5%	-10	± 10%	85
Confirmation Tone (PIT)	450	0.5%	-8	± 10%	87
Special Dial Tone	450	0.5%	-8	± 10%	89
Vacant	450	0.5%	-8	± 10%	8F

51.3 Hardware Requirements or Dependencies

The NTMX76AB card must be equipped on GPP line peripherals with SX05 processor.
The NTMX76CA card must be equipped on DTCO2 trunk peripherals SX05 processor.

51.4 Software Requirements or Dependencies

The QPO20xx or QCI20xx load files should be supported for SX05 processor.

51.5 Limitations and restrictions

This feature can only be used with peripherals equipped with the NTMX76AB, NTMX76CA tone cards.

51.6 Interactions

N/A

51.7 Applicable customer facing sections

Fault Management

Logs N/A

Alarms N/A

Configuration

Data Schema X

User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

51.8 Glossary

Term	Description
New term	Definition
DTCO2	Digital Trunk Controller Overseas
GPP	Global Peripheral Platform
Hz	Hertz
MFC	Multi-Frequency Compelled
PIT	Positive Indication Tone
RAM	Random Access Memory
DTMF	Dual-Tone Multi-Frequency

52: Functional Description (FN): A00003465

52.1 Feature name

ETSI BRI Channel reservation override

52.2 Description

This feature provides the user to override the channel reservations for the calls on a loop. This enables the user to steal channel reserved for any other non-CW incoming alerting call for another call. Incoming alerting call is a call which ALERT is sent by the set to the switch.

Channel steal request is sent by SETUP, CONNECT or RETRIEVE messages with a proprietary facility information element.

This feature is required to enable subscribers to be able to freely answer incoming calls.

For DBArt, Stationary Train dispatchers use specially developed terminals for telecommunication purposes, called GeFo. The telecommunication I/F to the fixed network is based on ETSI BRI point to multipoint connections. When a call is presented to the user, the network always reserves a free B-channel. The user is not allowed to answer a waiting call, if both B-channels are reserved. To overcome this operational restriction, the terminal will be allowed to request allocation override on a reserved B-channel.

52.2.1 Requesting channel steal

To override the B-channel allocation for incoming alerting non-CW calls in case of incoming CW calls and outgoing calls, the mechanism for a user control of network-side channel reservation provided in ETS 300196-1 "Generic functional protocol for the support of supplementary services" in chapter 10.1.2 is used.

In order to minimize potential future implementations, the optional argument controlOption is extended by the proprietary value "reservationRequiredOverrideAllocations" with the value 128 (#80).The extended ASN.1 definition from table D.7 is outlined below.

```
ExplicitReservationCreationControl ::= OPERATION
   ARGUMENT controlOption ENUMERATED {
            noReservationRequired (0),
            reservationRequiredWithReservationIndicator (1),
            reservationRequiredWithoutReservationIndicator (2),
            reservationRequiredOverrideAllocations (128)} -- optional
   RESULT ReservationIndicator -- optional
   ERRORS { maximumNumberOfReservationsReached,
            notAvailable,
```

```
notSubscribed,
unwantedReservationCreated}
```

The reservation FAC IE can be sent in outgoing SETUP messages (to free up an allocated B-channel for an outgoing call) and in outgoing CONNECT or RETRIEVE messages (to free up an allocated B-channel for an incoming CW call).

Figure 1 Channel stealing with CONN message

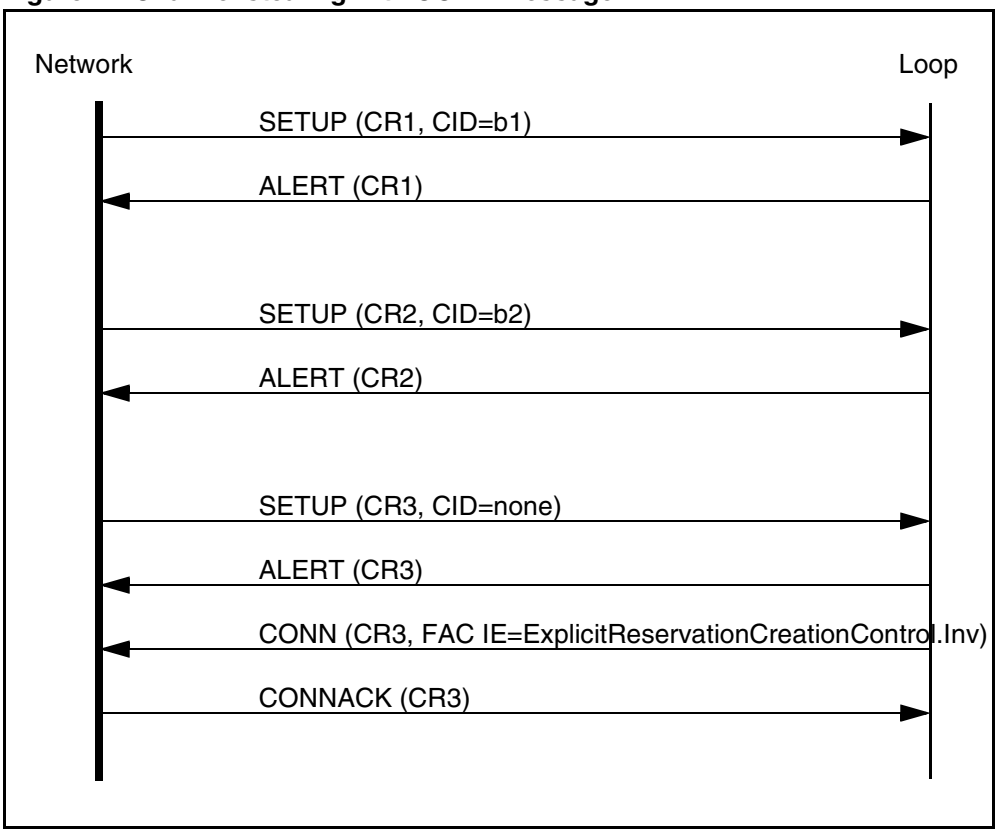


Figure 2 Channel stealing with SETUP message

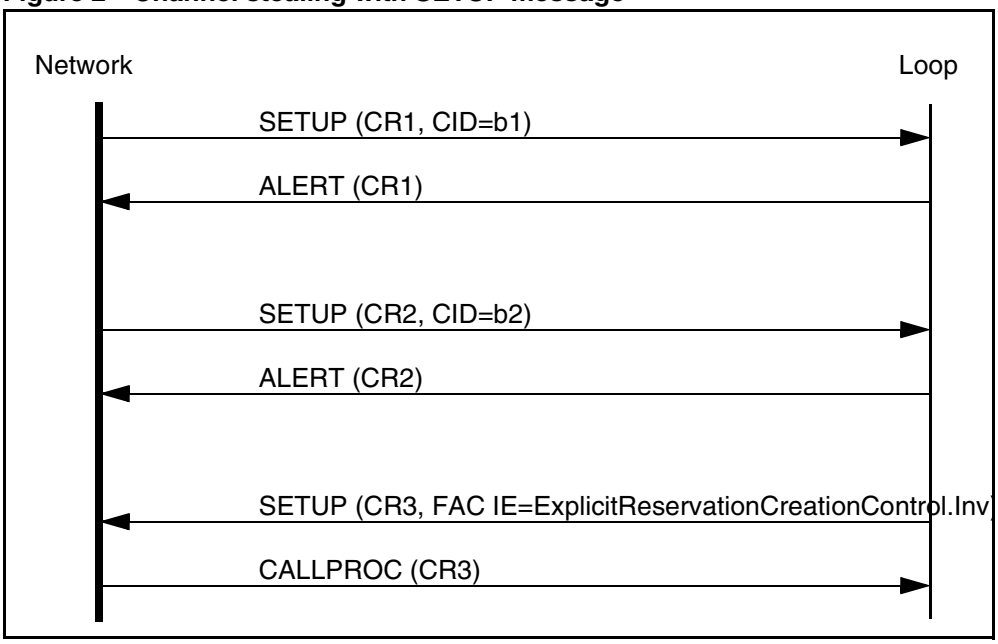
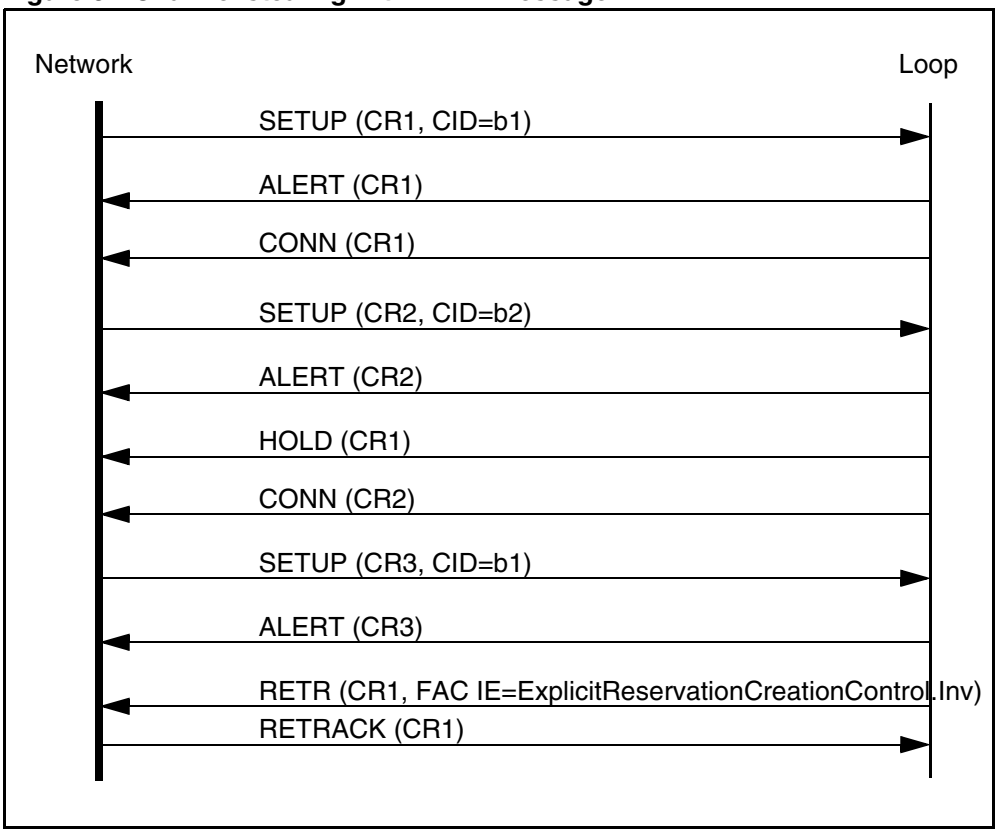


Figure 3 Channel stealing with RETR message



The terminal can pass the channel ID (CID) which it wants to reserve, but in case this preferred CID cannot be reserved (e.g. already stolen) the other b-channel will be returned in the next call control message.

During an attempt to setup an outgoing call while both B-channels are busy, the terminal is responsible to automatically hold or release one of its calls to free up a B-channel.

Table 1 ExplicitReservationCreationControl.Invoke

Hex Value	Description
1C	Facility
0C	Facility Length
91	Supplementary Service Spare
A1	Invoke Operation
09	Invoke Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
A unique invoke Iidentifier	Invoke Identifier
02 - Universal Integer	Operation Tag
01	Operation Length
14 - ExplicitReservationCreationControl	Operation Identifier
02 - Universal Integer	controlOption Tag
01	controlOption Length
80 - reservationRequiredOverrideAllocations	controlOption

If an allocated B-channel will be provided (an allocated B-channel from another incoming alerting non-CW call) or if a B-channel is available the response from the XPM in the next call control message is a FAC Return Result.

Table 2 ExplicitReservationCreationControl.ReturnResult

Hex Value	Description
1C	Facility
06	Facility Length
91	Supplementary Service Spare
A2	ReturnResult Operation

03	ReturnResult Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
InvokeID of the Invoke component, set sent	Invoke Identifier

In case the request can not be fulfilled (e.g. both B-channels are busy), the response from the XPM is a FAC return error component with the error "maximumNumberOfReservationsReached".

If the optional parameter in Invoke component is different than #80, the request can not be fulfilled. If no parameter is included, or the parameter has the value 0, 1 or 2 the request is valid and a FAC RE component with error code "notAvailable" will be sent (valid request, not supported).

If the value is between 2 and #80 or greater than #80 the request is invalid (coding error) and a FAC reject with the problem code "mistyped-argument" will be sent.

Table 3 ExplicitReservationCreationControl.ReturnError

Hex Value	Description
1C	Facility
09	Facility Length
91	Supplementary Service Spare
A3	ReturnError Operation
06	ReturnError Length
02 - Universal Integer	Invoke ID Tag
01	Invoke ID Length
InvokeID of the Invoke component, set sent	Invoke Identifier
02 - Universal Integer	Error Tag
01	Error Length
00 - maximumNumberOfReservationsReached	Error Code

52.2.2 Software optionality control (SOC) option

The soc option SULN0028 “SULN BRI Call Queuing” which is created by the activity A00002377 “10 AFC Keys for BRI Directory Number” is also used for this activity. The functionality of this activity is depend on the SOC option SULN0028. When the SOC option is changed, static data of PLGCs and GPPs should be updated. A warning is printed when SOC is changed in CI level;

"*Static data update is required for related PLGCs and GPPs. Please BSY/RTS the inactive unit and perform swact*" .

52.3 Hardware Requirements or Dependencies

N/A

52.4 Software Requirements or Dependencies

N/A

52.5 Limitations and restrictions

1. Preemption services (MLPP): If a call selected to be pre-empted has had its b-channel stolen, the preemption does not successfully free up a b-channel and the pre-empting call will not complete. Therefore, the operator must disable MLPP network preemption in datafill by setting NONPREEMPT=YES, if B-channel stealing is to be used. Please note that, precedence calls are still allowed.
2. Busy determination services (CW, CF, CCBS, MLPP): A channel that has been made available after b-channel stealing is not available to CW, CF and CCBS. Specifically, if there is an alerting call that has had its b-channel stolen and there is also a free b-channel, CW, CF and CCBS consider that free channel as reserved against the call that had its b-channel stolen. A basic scenario could be as follows:
   - Consider, b1 and b2 are reserved for two different alerting calls and there is an additional waiting call on loop.
   - Assume b1 is stolen for the waiting call.
   - Let call holding b2 to terminate.
   - We have a free b-channel available on XPM and the set can originate a new call. However CM thinks that both channels are in use and no normal calls are terminated to the loop. Therefore CW, CF, CCBS, MLPP preemption or MLPP alternate party diversion may be tried.
3. Terminal Impact (1): A call that has had its b-channel stolen cannot be answered unless there is another channel available for stealing or one has been freed by the terminal. Therefore, the terminals used must be specially designed to first verify that a call can be answered under this new algorithm if b-channel stealing is to be used. A terminal can always send the stealing request, even there is no need for stealing since there are available b-channels.

4. Terminal Impact (2): Since the terminals used must have complete knowledge of all calls on the loop to make the determination of which calls can be answered (see previous point), the operator must ensure only one terminal may be active on the loop if b-channel stealing is used.
5. Terminal Impact (3): Since b-channel stealing may cause the b-channel specificied in the next call control message (RETR ACK, CONN ACK, CALL PROC) to the channel stealing request to be different that previous messages, the terminals must always use the b-channel specified in the CONNECT ACK and ignore b-channels specified in earlier messages.

52.6 Interactions

52.6.1 Pre-emption services (MLPP):

Preemption services (MLPP): If a call selected to be pre-empted has had its b-channel stolen, the preemption does not successfully free up a b-channel and the pre-empting call will not complete. Therefore, the operator must disable MLPP network preemption in datafill by setting NONPREEMPT=YES, if B-channel stealing is to be used. Please note that, precedence calls are still allowed.

52.6.2 Busy determination services (CW, CF, CCBS):

Busy determination services (CW, CF, CCBS, MLPP): A channel that has been made available after b-channel stealing is not available to CW, CF and CCBS. Specifically, if there is an alerting call that has had its b-channel stolen and there is also a free b-channel, CW, CF and CCBS consider that free channel as reserved against the call that had its b-channel stolen. A basic scenario could be as follows:

- — Consider, b1 and b2 are reserved for two different alerting calls and there is an additional waiting call on loop.
- — Assume b1 is stolen for the waiting call.
- — Let call holding b2 to terminate.
- — We have a free b-channel available on XPM and the set can originate a new call. However CM thinks that both channels are in use and no normal calls are terminated to the loop. Therefore CW, CF, CCBS, MLPP preemption or MLPP alternate party diversion may be tried.

52.7 Applicable customer facing sections

Fault Management

Logs	__N/A_
Alarms	__N/A_

Configuration

Data Schema	__N/A_
User Interface	__N/A_
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	__N/A_
Accounting (includes AMA billing)	__N/A_
Performance (includes operational measurements)	__N/A_

52.8 References

A00000154 - ETSI BRI MLPP Service

A00002377-10 AFC Keys for BRI Directory Number

AR2179 - MULTI PARTY SERVICES

53: Functional Description (FN): A00003466

53.1 Feature name

MLPP Default Precedence Level on Terminations

53.2 Description

This feature A00003466 MLPP Default Precedence Level on Terminations is an extension of the feature A00000154 Multi-Level Precedence and Preemption supplementary service that is implemented in MMP19/ISN06, for point-to-multipoint ETSI BRI.

In feature A00000154 Multi-Level Precedence and Preemption, calls from non-MLPP sources do not have a precedence when terminating to an MLPP BRI loop. They are not marked as MLPP call and treated as ordinary calls.

This feature is specified to meet Railway Dispatcher System requirements which are not compliant with specification Q955. The implementation for this activity will be done using Q955_COMPLIANT office parameter.

This feature provide assigning precedence level ROUTINE to calls originated from non-MLPP sources when terminating to an MLPP BRI loop if Q955_COMPLIANT is set to N. MLPP information (notifications, FAC data, causes) is not sent in the backwards direction to the non-MLPP originator.

Any MLPP related information is not included in IAM in the case of call forwarding or alternate party diversion over ISUP in which call is originated from non-MLPP resource.

53.3 Hardware Requirements or Dependencies

N/A

53.4 Software Requirements or Dependencies

N/A

53.5 Limitations and restrictions

1. This feature is in effect only if Q955_COMPLIANT office parameter is set to N.
2. Non_MLPP sources mentioned in function description are ETSI BRI, PRI, ETSI ISUP V2
3. Calls from non_MLPP sources cannot be preempted by network preemption.

53.6 Interactions

If an MLPP call originated from non-MLPP resource is taken into conference -3pty, addon, preset-it can be preempted by any other higher precedence MLPP call.

53.7 Applicable customer facing sections

Fault Management

- Logs __N/A_
- Alarms __N/A_

Configuration

- Data Schema __N/A_
- User Interface __N/A_
- Element Management __N/A_
- Security __N/A_
- Service Order __N/A_
- Office Parameters __N/A_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

53.8 Glossary

Term	Description
BRI	Basic Rate Interface
ETSI	European Telecommunications Standard Institute
ISUP	ISDN User Part
MLPP	Multi Level Precedence and Preemption
IAM	Initial Address Message

54: Functional Description (FN): A00003467

54.1 Feature name

REVERSE TRANSLATIONS ENHANCEMENTS VIA CUSTMOD OPTION

54.2 Description

54.2.1 Background Information

The purpose of this feature is to enhance Reverse Translations to co-exist with CS1R.

The current DMS100 MMP product has requirements to alter the default dialling on a per CLI basis, which is originally determined by the incoming trunk group (Customer Group and NCOS). This is done by assignment of the CUSTMOD option against the given CLI(s) (Calling Line Identity) and assigning a new customer group. In order to make use of the new customer group, in the routing phase (IBNRTxx), the routing option invoked is IBNRX. This allows a form of re-translations to occur, which is not exactly re-entering Universal Translations at the top of the digit analysis phase. The digits then are re-examined using the new Customer Group info and when entering Universal Translations, the call will then re-route according to this data.

The limitation is that CS1R and IBNRX are not integrated to be supported in the same call. This is due to the fact that the CS1R functions are ONLY designed to work within the digit translations phase of the call and IBNRX is invoked in the routing phase. Thus, the call will fail.

The primary enhancement is to allow Reverse Translations to be invoked within the digit analysis phase of the call. The preferred place to provide the enhancement is within the "Featinfo Validate".

54.2.2 Introduction

The functional diagram of this feature is shown in figure 2.

CUSTMOD, which is an option in refinement VALDATOP for XLASEL FEATINFO in universal translation tables, is enhanced by this feature; and the new field REV_XLA (Reverse_Translations_Trigger) and its refinement DELDIGS (Delete Prefix Digits) are added to the CUSTMOD option.

The entry in new field REV_XLA can be either Y or N.

When the CUSTMOD option is encountered in one of the translation tables (for ex in table PXCODE), and when these conditions are satisfied

i. The entry in field REV_XLA is “Y”

ii. The customer group or NCOS is changed in table DNSCRNx

the Reverse Translation starts within the "Featinfo Validate" option in Universal Translation tables, i.e. within the digit analysis phase of the call, and digit analysis stops and re-enters at the standard IBN translations block with the new Customer Group and NCOS.

So, based on the Access Code used to invoke CLI Screening, the customer can decide on a per CLI basis if they want to change the default Customer Group/ NCOS from the Trunk Group assigned or override the default with the one defined against the CLI. The new Customer Group/NCOS is used immediately during digit analysis without having to wait for the routing phase of call as per current implementation of IBNRX (an example for previous implementation of reverse translation is shown in Figure 3 on page 1178 and in Figure 4 on page 1179).

The new refinement DELDIGS allows the removal of prefix digits before retranslation (re-enter of IBNXLA) begins. DELDIGS is a mandatory field only if the entry in field REV_XLA is “Y”. The entry in new refinement DELDIGS can be an integer from 0 to 18, inclusive.

Sample datafill is shown in figure 1.

Figure 1 Sample Datafill

```
TABLE PXCODE

PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y Y 6) $ 0 0 24 PX VALIDATE

PTTXLA 890 890 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y N) $ 0 0 24 PX VALIDATE
```

REV_XLA option starts the reverse translation once per call.

Activation of the functionality is controlled by the SOC option XLAS0054 “XLAS Rev Trans Custmod”. If the SOC is turned OFF or ON, it is possible to datafill the new field REV_XLA but this option is ignored when the SOC is turned OFF.

Also,

- No changes are done in Table DNSCRN and the other DNSCRNx tables. This is to ensure integrity of the provisioning systems.

- If the entry in new field REV_XLA is Y or N, then if IBNRX is encountered in the routing phase, then IBNRX still functions as it always did. So, there is full transparency to this feature with existing capabilities.
- If the entry in 'new' field REV_XLA is Y, and the CLI does not have defined any Customer Group info, then any options in Featinfo selector will be completed and translation continues on universal translations.

If the call hits an AMAGRPID option in lineattr tables after the reverse translation starts, then this second AMAGRPID over-writes the previous one. And, the last AMAXLAID option (which can be datafilled in universal translation tables) over-writes the previous AMAXLAID option, too. An example for these options is shown in figure 5 and figure 6.

The translations verification (traver) tool is enhanced by this feature. It is now possible to trace the reverse translation via traver; after REV_XLA is hit, the traver shows the translation tables, the CS1R trigger points, the terminator, the outpulsed digits, and so on. Please refer to Figure 5, "New traver output - Part 1 / 2" on page 1180 and Figure 6, "New traver output - Part 2 / 2" on page 1181.

Figure 2 Functional Behavior Diagram

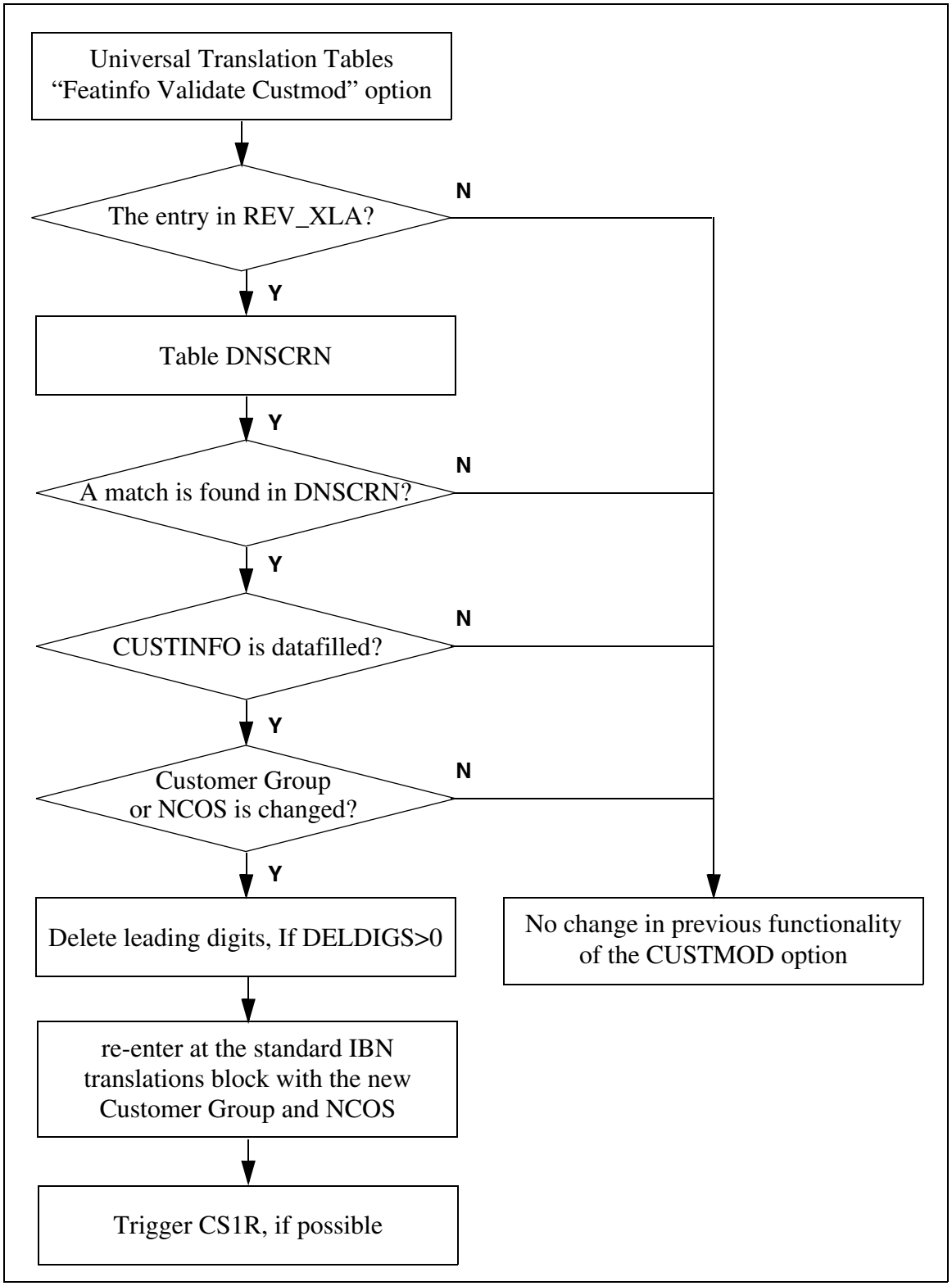


Figure 3 Traver output of the previous implementation - Part 1 / 2

```
CI:
>traver tr 2wisupba 8887835470 b
TABLE TRKGRP
2WISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675451 ANSDISC
0 Y N N N N N Y 0
    0 N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
PTTXLA 88 NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1
NLCA_NILLA_1)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:    8887835470
TABLE PXCODE
PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
```

Figure 4 Traver output of the previous implementation - Part 2 / 2

```
PLEASE ENTER CLI DIGITS:
>7835476
TABLE DNSCRN
 . 7835476 (CUSTINFO VALID 0) $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:    8887835470
TABLE PXCODE
VALIDATE 888 888 RTE ( DEST 888)$
TABLE: PXRTE
KEY: VALIDATE  888
 . T IBNRTE 888
 .  . TABLE IBNRTE
 .  .  888 IBNRX
 .  . EXIT TABLE IBNRTE
EXIT TABLE PXRTE
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP1AB              8887835470                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 5 New traver output - Part 1 / 2

```
CI:
>traver tr 2wisupba 8887835470 b
TABLE TRKGRP
2WISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675451 ANSDISC
0 Y N N N N N Y 0
    0 N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
PTTXLA 88 NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1
NLCA_NILLA_1)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 (AMAGRPID DSDSG) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:    8887835470
TABLE PXCODE
PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y Y 0) $ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>7835476
TABLE DNSCRN
 . 7835476 (CUSTINFO VALID 0) $
```

Figure 6 New traver output - Part 2 / 2

```
 . 7835476 (CUSTINFO VALID 0) $
REV_XLA set to Y - Now translating using new assigned CUSTGRP
and NCOS
TABLE NCOS
VALID 0 0 0 $ ( XLAS NETXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL
VALID NXLA VALIDXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP: no subscribed trigger.
TABLE IBNXLA: XLANAME NETXLA
NETXLA 88 NET N Y 0 N NDGT N Y GEN (LATTR 1 102_NPRT_1
NLCA_NILLA_1)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 (AMAGRPID NEW) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:     8887835470
TABLE PXCODE
NETXLA 888 888 RTE ( DEST 888) (AMAXLAID TEST) $
TABLE: PXRTE
KEY:   NETXLA  888
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
NEW DFLT (FLEXOCI 6)$
TABLE AMAXLAID
TEST DFLT (FLEXCTYP GENERIC 804 OVRDALL )$
TABLE FLEXAMA
NEW TEST GRPDATA (FLEXOCI 12)$
Originator is not an EIN agent, therefore EIN info is not
processed.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES
1 OGISP1AB              8887835470                    ST
```

54.2.3 IN Interaction

The new functionality enables to support CS1R and the CUSTMOD option to be supported in the same call, as explained in the following paragraph.

The new functionality is to be able to trigger IN system after execution of the CUSTMOD option when the reverse translation is triggered; functional Behavior Diagram is shown in figure 2; and an example is shown in figure 9 and figure 10.

Also, the traver output shows the outpulsed digit result and the route choice(s) for both standard and CS1R triggered calls. Traver outputs of the previous implementation of CUSTMOD option is shown in figure 7 and figure 8; the new outputs are shown in figure 9 and figure 10.

Both TDP2 and TDP3 are supported by this feature. TDP2 occurs at the Info Collected point in the call (This can be seen in the traver - INAP Info Collected TDP). The reverse XLA occurs after this so we will do a TDP2 check, then reverse XLA.When this happens, the call will go back through the INFOCOL point in call. (Normally this occurs between DGCOL and IBNXLA. Reverse XLA does go back through these table so we will go back through another TDP2 trigger point. As shown in figure 9 and figure 10.

An another traver example is shown in figures 11, 12 and 13.

The working principle of CS1R is not effected.

AIN (Advanced Intelligent Networks; the North American standard of IN) and GIN (GSP IN) are not supported. Only EIN (ETSI INAP V8) is supported.

After the CONNECT message is received by the SSP, the original customer group and ncos of the originator trunk is used by the IN translation system. For ex: When the call triggers at TDP-3 on the SSP to provide an IN number translation service, after the IBNRX option, the translation system uses the customer group of the originating trunk, not the customer group and the ncos values defined in DNSCRN table.

Figure 7 Traver output of the previous implementation - Part 1 / 2

```
CI:
>traver tr ISUPBA 888998 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0
Y N N N N N Y 0 0
    N 0 0 0 0 Y N N N N N N N N NATL $
 .  . TABLE TRKAIN
 .  . ISUPBA MDCGRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
MDCGRP INFOCOL
 . GENTRIG ( SPC KCDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to individual trunk.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME PTTXLA
PTTXLA 888 NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1
NLCA_NILLA_1)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:         888998
TABLE PXCODE
PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y)$ 0 0 24 PX VALIDATE
```

Figure 8 Traver output of the previous implementation - Part 2 / 2

```
PLEASE ENTER CLI DIGITS:
>1027835402
TABLE DNSCRN
 . 1027835402 (CUSTINFO VALID 0) $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:         888998
TABLE PXCODE
VALIDATE 888 888 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:            998
TABLE PXCODE
LINCUXL 998 998 RTE ( DEST 998)$
TABLE: PXRTE
KEY:  LINCUXL  998
 . T IBNRTE 888
 .  . TABLE IBNRTE
 .  .  888 IBNRX
 .  . EXIT TABLE IBNRTE
EXIT TABLE PXRTE
TABLE TRIGGRP
MDCGRP INFOANAL
 . GENTRIG ( CDPN KCDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to individual trunk.
 .  . TABLE TRIGDIG
 .  . KCDIG GENTRIG 998 GENTRIG EVENT TCAP INAPV8 TCPIP 0
(SERVKEY 111)
 .  .     (SERVINFO_INDEX 99) $
 .  .  . TABLE SERVINFO
 .  .  . 99
 .  .  .    (INITDP_PARMS (SERVKEY)(CDPA)(CLI)(EVENT_TYPE) $)$
INAP Info Analyzed TDP:  trigger criteria met, querying the
database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


INAP Info Analyzed TDP:  trigger criteria met, querying the
database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 9 New traver output - Part 1 / 2

```
CI:
>traver tr ISUPBA 888998 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0
Y N N N N N Y 0 0
    N 0 0 0 0 Y N N N N N N N N NATL $
 .  . TABLE TRKAIN
 .  . ISUPBA MDCGRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
MDCGRP INFOCOL
 . GENTRIG ( SPC KCDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to individual trunk.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME PTTXLA
PTTXLA 888 NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1
NLCA_NILLA_1)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:         888998
TABLE PXCODE
PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y
Y)$) ( CUSTMOD Y Y 3)$ 0 0 24 PX VALIDATE
```

Figure 10 New traver output - Part 2 / 2

```
PLEASE ENTER CLI DIGITS:
>1027835402
TABLE DNSCRN
 . 1027835402 (CUSTINFO VALID 0) $
REV_XLA set to Y - Now translating using new assigned CUSTGRP
and NCOS
TABLE NCOS
VALID 0 0 0 $ ( XLAS NETXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL
VALID NXLA VALIDXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
MDCGRP INFOCOL
 . GENTRIG ( SPC KCDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to individual trunk.
 .  . TABLE TRIGDIG
 .  . KCDIG GENTRIG 998 GENTRIG EVENT TCAP INAPV8 TCPIP 0
(SERVKEY 111)
 .  .    (SERVINFO_INDEX 99) $
 .  .  . TABLE SERVINFO
 .  .  . 99
 .  .  .   (INITDP_PARMS (SERVKEY)(CDPA)(CLI)(EVENT_TYPE) $)$
INAP Info Collected TDP:  trigger criteria met, querying the
database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


INAP Info Collected TDP:  trigger criteria met, querying the
database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 11 Traver example - Part 1 / 3

```
CI:
>>traver tr 2wbtupba 9870555 ainres icsx connect 1587835407 b
TABLE TRKGRP
2WBTUPBA IBNT2 0 NPDGP NCRT PTTPUB 0 LIDL 0 N ANSDISC 0 Y N N
N N N N 0 0 N 0 1
    0 1 N N N N N N N Y VPN NATL $
TABLE NSCDEFS
VPN 1 (STDACC 162) (RETMET CHG) $
 .  . TABLE TRKAIN
 .  . 2WBTUPBA AIN AIN SMGRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
PTTPUB 0 0 0 PTTCOS ( XLAS PTTXLA PTTFEAT NDGT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
PTTPUB NXLA PTTXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT N Y DOD N 100 102_NPRT_1 NLCA_NILLA_1
NONE $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1
NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT CONT ( AMAXLAID STNPAID) ( XLT NSC GNP)$ NODFOP
NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:       9870555
TABLE PXCODE
PTTXLA 987 987 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y N N
N)$) ( CUSTMOD Y Y 3) ( CLISERV DENEME)$ 0 3 19 PX TEST
```

Figure 12 Traver Example - Part 2/ 3

```
PLEASE ENTER CLI DIGITS:
>1027835407
TABLE CLISERV
 . DENEME 1 ( PARTIAL )$
TABLE DNSCRN
 . 102 (CUSTINFO CUST783 0) $
REV_XLA SET TO Y - NOW TRANSLATING USING NEW ASSIGNED CUSTGRP
AND NCOS
TABLE NCOS
CUST783 0 0 0 $ ( XLAS NETXLA STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE  CUSTHEAD:  CUSTGRP,  PRELIMXLA,  CUSTXLA,  FEATXLA,
VACTRMT, AND DIGCOL
CUST783 NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME NETXLA
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA
    (NET N Y 0 N NDGT N Y GEN (LATTR 1 102_NPRT_1 NLCA_NILLA_1)
$ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1  IBN  NONE  NT  0  0  NILSFC  4  PX  NETXLA  NIL  00  102_NPRT_1
NLCA_NILLA_1
    (AMAGRPID NEW) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA DFLT CONT ( CONSUME 0) ( XLT CT CUST783A)$ NODFOP CON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:          0555
TABLE PXCODE
NETXLA 05 05 RTE ( PF 0) ( MM 4 15) ( DEST 555) ( CLASS NATL)
( AMAXLAID TEST)$
TABLE: PXRTE
KEY:   NETXLA  555
. S 2WISUPAB
EXIT TABLE PXRTE
TABLE AMAGRPID
NEW DFLT (FLEXOCI 6)$
TABLE AMAXLAID
TEST DFLT (FLEXCTYP GENERIC 804 OVRDALL )$
```

Figure 13 Traver Example - Part 3/ 3

```
TABLE FLEXAMA
NEW TEST GRPDATA (FLEXOCI 12)$
TABLE TRIGGRP
SMGRP INFOANAL
. GENTRIG ( CDPN SMDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to individual trunk.
Trigger INAPV8 GENTRIG is applicable to individual trunk.
.. TABLE TRIGDIG
.. SMDIG GENTRIG 0555 GENTRIG EVENT TCAP INAPV8 TCPIP 0
(SERVKEY 99)
..   (SERVINFO_INDEX 99) $
...TABLE SERVINFO
...99
... (INITDP_PARMS (SERVKEY)(CDPA)(CLI)(CPC)(EVENT_TYPE)$)
... (BILL_INFO (AMA_OPT (DIALED_DIGITS_INFO MODULE_40)
... (AMA_XLA_OPT (MAINTN_CALLCODE)$) (CORRELATION_ID$) $)$)
... (DIGIT_COLLECTION_INFO ( FULL_CDPA) $)
... (RESPONSE_INFO (CONNECT_OPT (XLA_REENTRY (UNIV_XLA PX
INCPXLA)$)$)$)
... (EDPS_INFO (EXPLICIT) $) (CS1R (CONTINUE) (CWA) $)$
INAP Info Analyzed TDP:  trigger criteria met, querying the
database.
INAP Info Analyzed TDP:  AINRES CONNECT option specified
TABLE PXHEAD
INCPXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
1587835407
TABLE PXCODE
INCPXLA 158 158 RTE ( PF 3) ( MM 10 10) ( DEST 158) ( AMAXLAID
TEST)$
TABLE: PXRTE
KEY:  INCPXLA  158
 . S OGISP2BC
EXIT TABLE PXRTE
TABLE AMAXLAID
TEST DFLT (FLEXCTYP GENERIC 804 OVRDALL )$
EXIT TABLE PXRTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 OGISP2BC              7835407                         ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL
+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

54.3 Hardware Requirements or Dependencies

N/A

54.4 Software Requirements or Dependencies

Activation of the functionality is controlled by the SOC option XLAS0054 “XLAS Rev Trans Custmod”.

This feature is patched backed to SW000004. The patch ID is NAP43. NAP43 is a password activateble patch. For an ONP from (ISN04 - ISN06) to (ISN07 and beyond), the state of the SOC option XLAS0054 will automatically be set to ‘ON’, if NAP43 was activated before the ONP, and also all of the functionalities of this feature will be ON after the ONP, too. But for this ONP, a password for SOC option is still required to change the RTU field of the SOC option XLAS0054 in loads SW000007 and beyond. “SOC states and RTU values of the SOC optionXLAS0054 after ONPs” is described in table 3.

Table 1 SOC states and RTU values of the SOC option XLAS0054 after ONPs

ONP	State of SOC option after ONP		RTU of SOC option after ONP	
	IF State of SOC option in ISN07 (nodatafill load) before ONP is IDLE	IF State of SOC option in ISN07 (nodatafill load) before ONP is ON	IF RTU of SOC option in ISN07 (nodatafill load) before ONP is N	IF RTU of SOC option in ISN07 (nodatafill load) before ONP is Y
ISN04 (ISN04 or ISN06) to ISN07 (ISN07 or beyond) NAP43 is active on ISN04 (or ISN06)	ON	ON	N	Y
ISN04 (ISN04 or ISN06) to ISN07 (ISN07 or beyond) NAP43 is not active on ISN04 (or ISN06)	IDLE	ON	N	Y

54.5 Limitations and restrictions

REV_XLA option starts the reverse translation once per call.

AIN (Advanced Intelligent Networks; the North American standard of IN) and GIN (GSP IN) are not supported. Only EIN (ETSI INAP V8) is supported.

Only TDM trunks are supported by the REV_XLA option.

REV_XLA is functional for only the trunk originated calls. Supported Trunk types are:

- ETSI ISUP V1, V2, V3
- All National variants of ETSI ISUP (can be V1 or V2 based)
- BTUP V2, V2+
- SSUTR2
- SPIROU
- National variants of ETSI PRI
- QSIG
- Numeris VN4 PRI
- Numeris VN6 PRI
- DPNSS

54.6 Interactions

When a call is initiated by a feature, REV_XLA does not start the reverse translation after the featinfo selector; i.e. feature initiated calls are not supported by this activity. Some examples for the unsupported features are:

- Call diversion favors
- CFRA
- Attendant Console’s night service
- CCBS
- MONA
- IBN Auth code and Acct code features
- RSA
- DISA

Supported feature interworkings are:

- Calling Party Category Screening and Routing

- CDN
- BC, as exists plus Universal MMP15 feature.
- PN screen
- IN CS-1, CS-2, CS-3, CS-4
- All existing AMA functionality
- Forced overlap outgoing - Eire
- NETINFO
- All existing Validate CLI functionality
- IN Billing - all current IN billing to be supported (including FCI)
- French NAOC (AU3283) base feature support required along with the new NAOC features in ISN07

REV_XLA is supported only in the translation phase of the call. Therefore REV_XLA option is not supported after the other re-translation options in routing tables. But those other re-translation options in routing tables are supported by the REV_XLA option when the call hits the REV_XLA option before these options. For ex: REV_XLA option is not supported after

- RT, GBL options in universal routing tables
- RT, RX, GBL options in OVRx and OFRx tables
- RX, IBNRX, GBL options in IBNRTx tables
- VFGs

54.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A

Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

Activation of the functionality is controlled by the SOC option XLAS0054 “XLAS Rev Trans Custmod”.

54.8 Glossary

Term	Description
REV_XLA	Reverse_Translations_Trigger
XLA	Translation
CS1R	Capability Set 1 (Refined)
CLI	Calling Line Identity
TDP	Trigger Detection Point
TDP2	Information Collected
TDP3	Analyze Info
AIN	Advanced Intelligent Networks
GIN	GSP IN
EIN	ETSI INAP V8

54.9 Traver Examples

54.9.1 Traver Example #1

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “N”

CLISERV option exists in Universal Code table

The customer group or ncos is changed in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y N
) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 (CUSTINFO VALID 0) $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
VALIDATE 889 889 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
```

```
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          7835475
TABLE PXCODE
LINCUXL 783 783 RTE ( MM 7 10) ( DEST 783) ( CLASS NATL)$
TABLE: PXRTE
KEY:  LINCUXL  783
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP1AB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.2 Traver Example #2

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “N”

CLISERV option exists in Universal Code table

No CUSTINFO option in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
```

```
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y N
) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
```

```
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.3 Traver Example #3

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “N”

CLISERV option does not exist in Universal Code table

No CUSTINFO option in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
```

```
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y N
)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE DNSCRN
 . 1027835479 $
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
TABLE TMTCNTL
TITRKGRP ( 0)
 . SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 64)
 . SUBTABLE TREAT
KEY NOT FOUND
TRMT NOT FOUND - USE RODR

+++ TRAVER: CALL TRACE TERMINATED DUE TO DATA TROUBLE +++

TABLE TMTCNTL SUB OFFTREAT NOT DATAFILLED


TREATMENT ROUTES.  TREATMENT IS: CNAD
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.4 Traver Example #4

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

The customer group or ncos is changed in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
```

```
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 (CUSTINFO VALID 0) $
REV_XLA SET TO Y - NOW TRANSLATING USING NEW ASSIGNED CUSTGRP AND NCOS
TABLE NCOS
VALID 0 0 0 $ ( XLAS VALIDXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
VALID NXLA VALIDXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME VALIDXLA
TUPLE NOT FOUND
Default from table XLANAME:
VALIDXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 11 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
11 IBN NONE NT 0 0 NILSFC 0 PX VALIDXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID NEW) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
VALIDXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                      7835475
TABLE PXCODE
VALIDXLA 783 783 RTE ( DEST 889) ( CLASS NATL) ( AMAXLAID TEST) ( LNET LOC) (
MZONE 2)$
TABLE: PXRTE
KEY: VALIDXLA  889
 . S OGISP2AB
EXIT TABLE PXRTE
TABLE AMAGRPID
NEW DFLT (FLEXOCI 6)$
TABLE AMAXLAID
TEST DFLT (FLEXCTYP GENERIC 804 OVRDALL )$
TABLE FLEXAMA
NEW TEST GRPDATA (FLEXOCI 12)$
INAP Info Analyzed TDP:  no subscribed trigger.
```

```
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP2AB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.5 Traver Example #5

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

CUSTINFO option exists in table DNSCRN

The customer group or ncos is not changed in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
```

```
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 (CUSTINFO CUST783A 2) $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
VALIDATE 889 889 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                       7835475
TABLE PXCODE
LINCUXL 783 783 RTE ( MM 7 10) ( DEST 783) ( CLASS NATL)$
TABLE: PXRTE
KEY:  LINCUXL  783
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES
```

```
1 OGISP1AB              7835475                     ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.6 Traver Example #6

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “N”

The value of REV_XLA refinement is “Y”

No CLISERV option in Universal Code table

No CUSTINFO option in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
```

```
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD N Y
3)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
VALIDATE 889 889 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                       7835475
TABLE PXCODE
LINCUXL 783 783 RTE ( MM 7 10) ( DEST 783) ( CLASS NATL)$
TABLE: PXRTE
KEY:  LINCUXL  783
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP1AB              7835475                     ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.7 Traver Example #7

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

No CLISERV option in Universal Code table

No CUSTINFO option in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
```

```
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y Y
3)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE DNSCRN
 . 1027835479 $
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
TABLE TMTCNTL
TITRKGRP ( 0)
 . SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 64)
 . SUBTABLE TREAT
KEY NOT FOUND
TRMT NOT FOUND - USE RODR

+++ TRAVER: CALL TRACE TERMINATED DUE TO DATA TROUBLE +++

TABLE TMTCNTL SUB OFFTREAT NOT DATAFILLED


TREATMENT ROUTES.  TREATMENT IS: CNAD
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.8 Traver Example #8

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No CUSTINFO option in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
```

```
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
```

```
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.9 Traver Example #9

The value of WHITLIST in Universal Code table is “Y”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No entry matched in table DNSCRN

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
```

```
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . No match found
 . Screening failed
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST
```

```
TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.10 Traver Example #10

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

The customer group or ncos is changed in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
```

```
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 (CUSTINFO VALID 0) $
REV_XLA SET TO Y - NOW TRANSLATING USING NEW ASSIGNED CUSTGRP AND NCOS
TABLE NCOS
VALID 0 0 0 $ ( XLAS VALIDXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
VALID NXLA VALIDXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME VALIDXLA
TUPLE NOT FOUND
Default from table XLANAME:
VALIDXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 11 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
11 IBN NONE NT 0 0 NILSFC 0 PX VALIDXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID NEW) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
VALIDXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          7835475
TABLE PXCODE
VALIDXLA 783 783 RTE ( DEST 889) ( CLASS NATL) ( AMAXLAID TEST) ( LNET LOC) (
MZONE 2)$
TABLE: PXRTE
KEY: VALIDXLA  889
 . S OGISP2AB
EXIT TABLE PXRTE
TABLE AMAGRPID
NEW DFLT (FLEXOCI 6)$
```

```
TABLE AMAXLAID
TEST DFLT (FLEXCTYP GENERIC 804 OVRDALL )$
TABLE FLEXAMA
NEW TEST GRPDATA (FLEXOCI 12)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP2AB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.11 Traver Example #11

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No entry found in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
```

```
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . No match found
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST
```

```
TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.12 Traver Example #12

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “N”

The value of REV_XLA refinement is “Y”

No CLISERV option in Universal Code table

No CUSTINFO option in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
```

```
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD N Y
3)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8897835475
TABLE PXCODE
VALIDATE 889 889 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                           7835475
TABLE PXCODE
LINCUXL 783 783 RTE ( MM 7 10) ( DEST 783) ( CLASS NATL)$
TABLE: PXRTE
KEY:  LINCUXL  783
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGISP1AB              7835475                     ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.13 Traver Example #13

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

No CLISERV option in Universal Code table

No CUSTINFO option in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8897835475
```

```
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD Y Y
3)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE DNSCRN
 . 1027835479 $
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
TABLE TMTCNTL
TITRKGRP ( 0)
 . SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 64)
 . SUBTABLE TREAT
KEY NOT FOUND
TRMT NOT FOUND - USE RODR

+++ TRAVER: CALL TRACE TERMINATED DUE TO DATA TROUBLE +++

TABLE TMTCNTL SUB OFFTREAT NOT DATAFILLED


TREATMENT ROUTES.  TREATMENT IS: CNAD
1 UKREORDER

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.14 Traver Example #14

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No CUSTINFO option in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
```

```
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
```

```
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.15 Traver Example #15

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “N”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No CUSTINFO option in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
```

```
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                      8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD N Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . 1027835479 $
TABLE PXHEAD
VALIDATE DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                      8897835475
TABLE PXCODE
VALIDATE 889 889 DMOD ( DEL 3) ( XLT PX LINCUXL)$
TABLE PXHEAD
LINCUXL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        7835475
TABLE PXCODE
LINCUXL 783 783 RTE ( MM 7 10) ( DEST 783) ( CLASS NATL)$
TABLE: PXRTE
KEY:  LINCUXL  783
 . S OGISP1AB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

```
DIGIT TRANSLATION ROUTES

1 OGISP1AB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

54.9.16 Traver Example #16

The value of WHITLIST in Universal Code table is “N”

CUSTMOD option exists in Universal Code table

The value of CUSTSCRN refinement if “Y”

The value of REV_XLA refinement is “Y”

CLISERV option exists in Universal Code table

No entry found in table dnscrn

```
>traver tr isupba 8897835475 b
TABLE TRKGRP
ISUPBA IBNT2 0 NPDGP NCRT CUST783A 0 MIDL 2 7675499 ANSDISC 0 Y N N N N N Y 0
0
    N 0 0 0 0 Y N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 2 0 0 $ ( XLAS PTTXLA NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PTTXLA
TUPLE NOT FOUND
Default from table XLANAME:
PTTXLA
    (NET N Y 0 N NDGT Y Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $)$ 9
TABLE DIGCOL
```

```
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 4 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1
    (AMAGRPID OLD) $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
PTTXLA 889 889 FEATINFO VALIDATE ( SUBSCRN ( GENERAL N Y Y Y)$) ( CUSTMOD Y Y
3) ( CLISERV SERVNAME)$ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>1027835479
TABLE CLISERV
 . SERVNAME 0 ( PARTIAL ) ( FAILRTE PX SERVFAIL)$
TABLE DNSCRN
 . No match found
TABLE PXHEAD
SERVFAIL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    8897835475
TABLE PXCODE
SERVFAIL 889 889 RTE ( PF 3) ( MM 10 10) ( DEST 889) ( CLASS NATL)$
TABLE: PXRTE
KEY: SERVFAIL  889
 . S 2WISUPAB
EXIT TABLE PXRTE
TABLE AMAGRPID
OLD DFLT (FLEXOCI 1)$
INAP Info Analyzed TDP:  no subscribed trigger.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WISUPAB              7835475                      ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

55: Functional Description (FN): A00003624

55.1 Feature name

H.323 Out Of Band Interworking with APG

55.2 Description

This SN07 activity builds on the work done by activity A00001895 by enabling support for H.323 out-of-band DTMF signalling from and to a connection that has an Anchor Packet Gateway (APG) inserted. This activity covers out-of-band DTMF signalling between

- H.323 GW and **any** other Gateway when an APG has already been inserted by another service

55.2.1 Background

There are three different ways for an H.323 gateway to carry DTMF(Dual-Tone Multifrequency) digits:

- DTMF digits are carried as inband DTMF tones. But low bit-rate voice codecs such as G.729 cannot be guaranteed to reproduce these tone signals accurately enough for automatic recognition
- Out of band DTMF digits carried in an H.245 message
- Using RTP Payload to carry DTMF digits, Telephony Tones and Telephony Signals as specified in RFC2833.

As stated above, inband DTMF is not sufficient for certain codecs such as G.729. RFC 2833 solves the problem by carrying DTMF digits in the RTP Payload, but not all H.323 gateways support RFC 2833. SN06.1 activity A00001895 provided support of out of band DTMF signalling between:

- H.323 Gateway and H.323 Gateway
- PVG and H.323 Gateway

55.2.2 Out of Band DTMF Interworking with Anchor Packet Gateway (APG)

The APG may have been inserted at the terminating call server or at the originating call server.

The APG only supports G.711. This means that an H.323 GW in a call with an APG inserted will also have to use G.711. However the H.323 GW may still

send DTMF digits out of band using H.245 and this is the case covered by this activity.

If an APG has been inserted at the terminating Call Server and a terminating H.323 gateway sends a DTMF digit using H.245 User Input Indication, the APG applies the DTMF tone towards the originating GW, as shown in Figure 1.

If an APG has been inserted at the terminating Call Server and an originating H.323 gateway wishes to send digits to the terminating gateway, then SIP INFO is used to send the digits. At the terminating Call Server the DTMF tone is applied by the APG towards the terminating gateway, as shown in Figure 2.

Similar signalling occurs if the APG was inserted at the originating Call Server.

Figure 1 APG inserted at terminating Call Server.

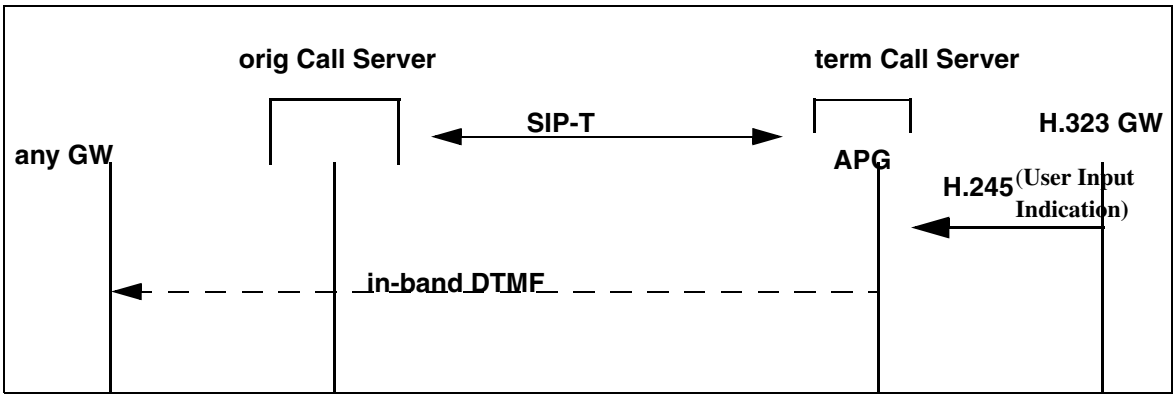
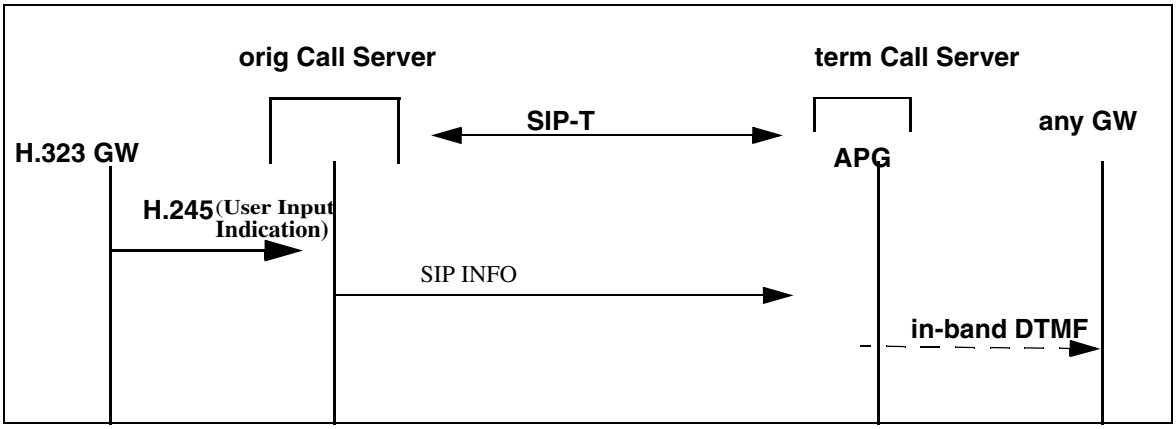


Figure 2 APG inserted at terminating Call Server.



55.3 Hardware Requirements or Dependencies

None

55.4 Software Requirements or Dependencies

None

55.5 Limitations and restrictions

None

55.6 Interactions

None

55.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

55.8 Glossary

Term	Description
New term	Definition

56: Functional Description (FN): A00003495

56.1 Feature name

APG integration with MP for NAT traversal.

56.2 Description

This feature is an enhancement of the CS 2000 Media Proxy NAT (Network Address Translator) traversal solution. It adds support for the APG (Anchor Packet Gateway) to this solution.

The MP (Media Proxy) NAT traversal solution was developed in SN06 under activity 89007980. It involves proxying a media path through an MP if the calling agents are in different IP (Internet Protocol) address domains, in order to ensure that media can flow between both parties.

The APG is a network device needed to support certain SIP-T (Session Initiation Protocol for Telephony) features on the CS 2000, mainly those that require the SIP-T leg to collect digits or play tones. The APG is inserted into the media path whenever SIP-T control logic determines that it is needed. The APG was developed in SN04 under activity 59031163.

Previous to this feature, calls requiring both an MP and an APG were not supported.

56.3 Hardware Requirements or Dependencies

None, apart from the hardware requirements and dependencies inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

56.4 Software Requirements or Dependencies

None, apart from the software requirements and dependencies inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

56.5 Limitations and restrictions

None, apart from the limitations and restrictions inherited from the APG and NAT traversal features, on which this feature is based. Please refer to the functional descriptions of these features for more details.

56.6 Interactions

None.

56.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

56.8 Glossary

Term	Description
APG	Anchor Packet Gateway
CS 2000	Communications Server 2000
IP	Internet Protocol
MP	Media Proxy
NAT	Network Address Translator
SIP-T	Session Initiation Protocol for Telephony

56.9 References

a. FN section of ACT.89007980 (NAT Traversal feature)

b. FN section of ACT.59031163 (APG feature)

57: Functional Description (FN): A00003624

57.1 Feature name

H.323 Out Of Band Interworking with APG

57.2 Description

This SN07 activity builds on the work done by activity A00001895 by enabling support for H.323 out-of-band DTMF signalling from and to a connection that has an Anchor Packet Gateway (APG) inserted. This activity covers out-of-band DTMF signalling between

- H.323 GW and **any** other Gateway when an APG has already been inserted by another service

57.2.1 Background

There are three different ways for an H.323 gateway to carry DTMF(Dual-Tone Multifrequency) digits:

- DTMF digits are carried as inband DTMF tones. But low bit-rate voice codecs such as G.729 cannot be guaranteed to reproduce these tone signals accurately enough for automatic recognition
- Out of band DTMF digits carried in an H.245 message
- Using RTP Payload to carry DTMF digits, Telephony Tones and Telephony Signals as specified in RFC2833.

As stated above, inband DTMF is not sufficient for certain codecs such as G.729. RFC 2833 solves the problem by carrying DTMF digits in the RTP Payload, but not all H.323 gateways support RFC 2833. SN06.1 activity A00001895 provided support of out of band DTMF signalling between:

- H.323 Gateway and H.323 Gateway
- PVG and H.323 Gateway

57.2.2 Out of Band DTMF Interworking with Anchor Packet Gateway (APG)

The APG may have been inserted at the terminating call server or at the originating call server.

The APG only supports G.711. This means that an H.323 GW in a call with an APG inserted will also have to use G.711. However the H.323 GW may still

send DTMF digits out of band using H.245 and this is the case covered by this activity.

If an APG has been inserted at the terminating Call Server and a terminating H.323 gateway sends a DTMF digit using H.245 User Input Indication, the APG applies the DTMF tone towards the originating GW, as shown in Figure 1.

If an APG has been inserted at the terminating Call Server and an originating H.323 gateway wishes to send digits to the terminating gateway, then SIP INFO is used to send the digits. At the terminating Call Server the DTMF tone is applied by the APG towards the terminating gateway, as shown in Figure 2.

Similar signalling occurs if the APG was inserted at the originating Call Server.

Figure 1 APG inserted at terminating Call Server.

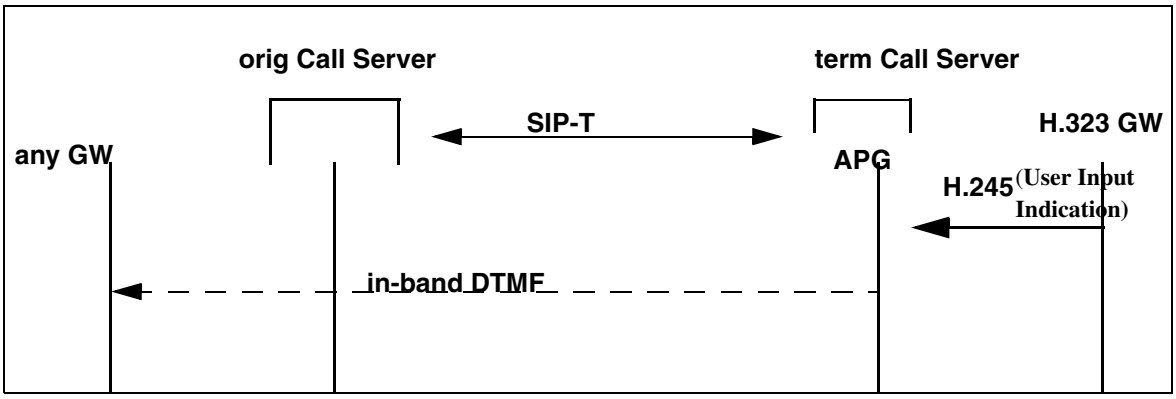
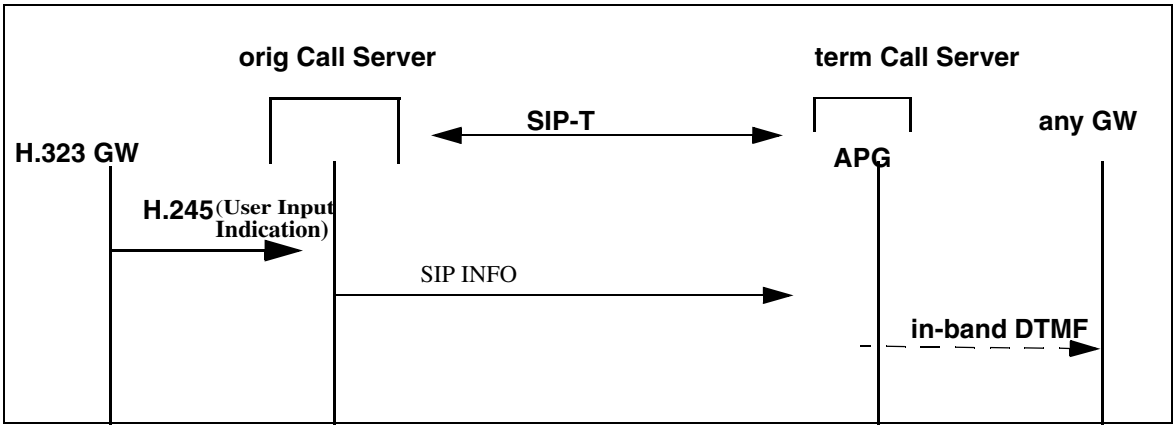


Figure 2 APG inserted at terminating Call Server.



57.3 Hardware Requirements or Dependencies

None

57.4 Software Requirements or Dependencies

None

57.5 Limitations and restrictions

None

57.6 Interactions

None

57.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

57.8 Glossary

Term	Description
New term	Definition

58: Functional Description (FN): A00003627

58.1 Feature name

T.38 FAX Support for International H.323 (Actid A00003627, ISN07 Release)

58.2 Description

58.2.1 Overview

This activity provides “Call Server controlled switchover to T.38 (or G.711)” for Call Server routed H.323 calls. Fax interworking is supported on calls between H.323 GWs (e.g. Meridian, Cisco, BCM) and H.248 GWs (e.g. PVG) or MGCP GWs (e.g. Mediatrix). At least one involved agent must be H.323.

Fax interworking is provided over Session Initiation Protocol (SIP-T). All involved Call Servers must support the prerequisites given in chapter 58.2.8.

This feature provides “Call Server controlled switchover to T.38 (or G.711)” depending on T.38 network option:

- If **Netopt is set to “T.38”** and both GW support T.38, then upon fax detection, switchover is done from G.729 (or G.711) to T.38 codec.
- If **Netopt is not set to “T.38”**, or a GW does not support T.38, then switchover to T.38 does not apply. If the call was set up with G.729 codec, switching is done from G.729 to G.711 codec. If the call was set up with G.711, no switchover occurs.

This activity builds on top of the SN06.1 activity A00001895 “H.323 Base Application” that included development to support basic call capabilities for H.323 GWs connected to the CS2K.

This feature does not impact the capability of a GW to do autonomous switchover to T.38 in a call that does not involve an H.323 GW (e.g. PVG to PVG call).

Digital call control signaling (ISUP, ISDN, H.323) may request a Group 3 fax call within the first setup message (IAM, SETUP) by BC IE = “3.1 kHz audio” and HLC IE = “Facsimile Group 3”. Checking this teleservice “Fax Group 3” and opening a T.38 channel from beginning is not considered by this feature.

Testing is done on the international CS2K load only. Testing for NA load is captured by feature .... tbd. Testing T.38 fax interworking to MCS 5200 is not part of this feature, is captured by feature ... tbd.

58.2.2 ISN06 restrictions

The ISN06 CS2K solution does not provide interworking to Group 3 facsimile equipment (G3FE) connected to H.323 GW.

There are three different methods to do Group 3 fax over IP signalling:

1. Autonomous GW switching to fax transport mode via inband indication.
2. Call Server control of GW switching to fax transport mode.
3. GW switching to fax transport mode - peer-to-peer out of band indication.

The ISN06 CS2K solution provides autonomous switching to fax transport mode (G.711 codec or T.38 mode) if a fax tone (e.g. CNG, V.21 header) was received. The H.248 GW does not notify the H.248 GWC or far end GWC/GW about fax tone event or about autonomous switchover to T.38 mode.

H.323 generally supports method #2 for gatekeeper (GK) routed calls and method #3 for peer-to-peer calls. SIP GWs tend to support method #2 and #3.

To support fax interworking to H.323 GW, method #2 “Call Server controlled switchover to T.38 mode” is implemented on CS2K.

> ***Note:*** The peer-to-peer approach (#3) does not work for GK controlled calls and is therefore out of scope for this CS2K implementation.

58.2.3 VoIP Network Model

Figure 1 shows an example for T.38 fax data transmission over IP networks.

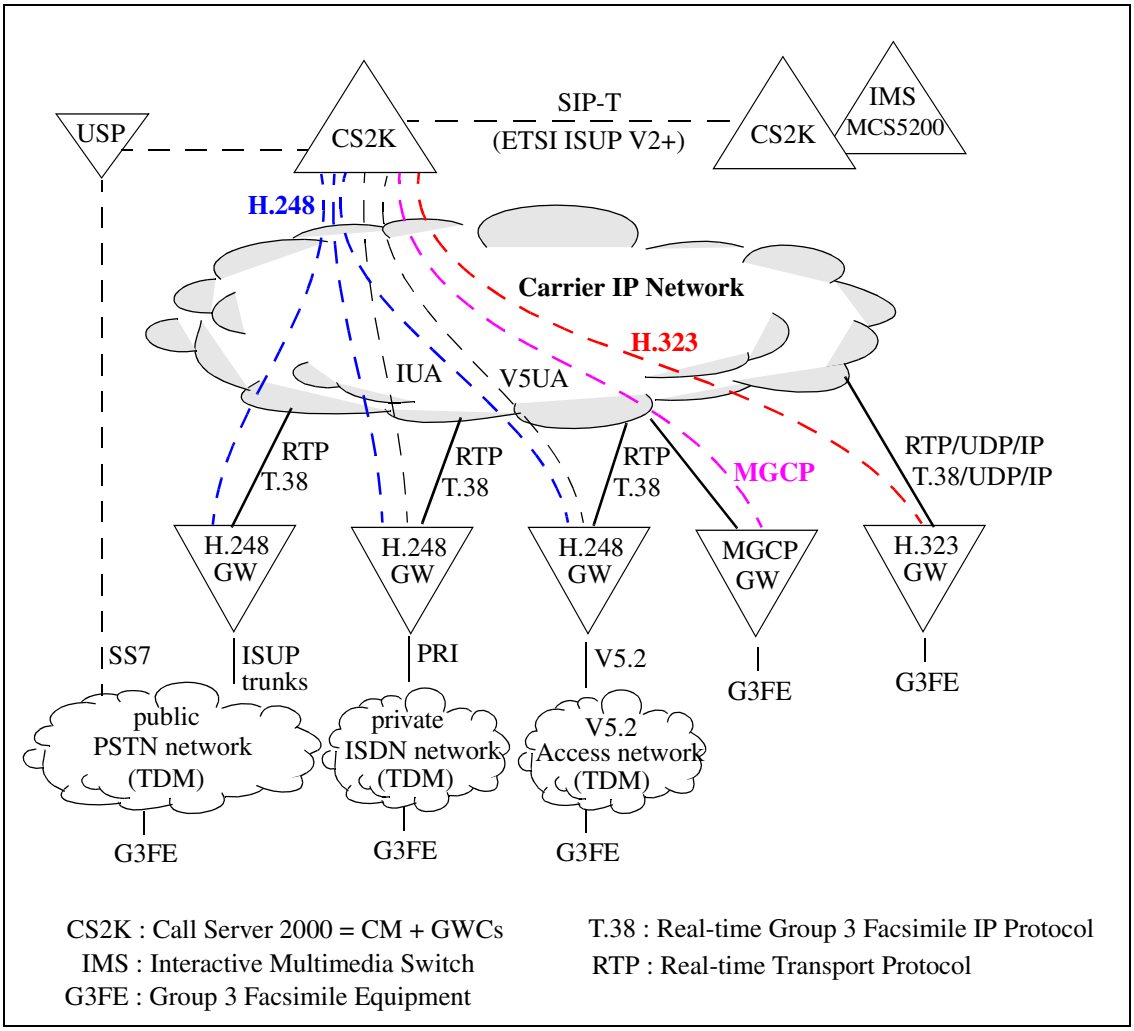
The H.323 GW is connected via H.323 protocol to the CS2K, which consist of H.225 protocol (Call control signaling) and H.245 protocol (Multimedia communication control). The G3FE devices are connected directly to the GW.

The H.248 GW supports voice trunking for public PSTN and private ISDN network. The GW is controlled via Media gateway control protocol H.248 from Call Server 2000 (CS2K). Call control signaling is relayed via IUA for ETSI PRI and via V5UA for V5.2 access between GW and CS2K.

The MGCP GW supports analog lines and is controlled by MGCP protocol only.

Media stream is transported via Real Time Protocol (RTP/UDP/IP) for voice calls and via Internet Facsimile Protocol (T.38/UDP/IP) for Group 3 fax calls.

Figure 1 Configuration example for facsimile transmission over IP networks



58.2.4 Applicable Standards

The ITU-T recommendations T.30 [1], T.38 [2] + [3], H.323 [4], T.225.0 [5], T.245 [6], H.248.1 [7], H.248.2 [8] applies for this feature They are listed in chapter 2.9 of this document with title and issue date.

58.2.5 H.323 Support for T.38 fax

Implementation of “Call Server controlled switchover to T.38 mode” is based on T.38 [2] Annex B, D and E, Draft Amendment to T.38 [3] Annex E and H.323 [4] Annex D.

The H.323 GWC requests the remote H.248 or MGCP side to detect fax tone and to notify the H.323 GWC about a fax event.

Upon receipt of fax event notification from remote H.248 or MGCP side, the H.323 GWC controls switching to T.38 mode. The logical voice channel is cleared and a T.38 fax channel is opened. The SDP(T.38) data is sent to the remote side, which is invited to switch over to T.38.

A remote H.248 or MGCP GW may send a SDP indicating simultaneous support of voice media stream via “m=audio ..” and T.38 media stream via “m=image ...” line. The “m=image 1 udptl t38” line in SDP means that T.38 codec is supported and “autonomous switchover to T.38” might be used lateron - see [3] Annex E.2.2.

> ***Note:*** A SDP coding sample for simultaneous voice and T.38 support is given in Figure 10, on page 1240 .

A H.323 GW which does not support voice media stream and T.38 media stream at the same time, removes/rejects the “m=image 1 udptl t38” line. This means that “autonomous switchover to T.38” is not used for this call.

> ***Note:*** To switch successfully to T.38, each side should know the T.38 capability of the other side. A GW indicates T.38 capability, by including a “a=cdsc: 1 image udptl t38” line in SDP. This means that “Call Server controlled switchover to T.38” is supported and might be used lateron.

58.2.6 H.248 Support for T.38 fax

Implementation of “Call Server controlled switchover to T.38 mode”, makes use of “Call Type Discriminator package” (ctyp) with event “Discriminating Tone detected” (dtone). See H.248.2 [8], chapter 7.

The GWC checks the GW capability to support T.38 via H.248 AuditValue command. If the H.248 GW replies with H.248 package “ctyp-1”, then “Call Server controlled switchover to T.38 mode” is supported - see Figure 2, on page 1236 .

> ***Note:*** If Netopt = “T.38”, the H.248 GWC add the ephemeral termination with voice and T.38 codec - see Figure 5, on page 1236 .

The H.248 GW does not switch over to T.38, before the remote SDP is received.

- If the remote SDP contains T.38 codec (m=image 1 udptl t38), then “autonomaous switchover to T.38” applies.
- If the remote SDP indicates T.38 capability (a=cdsc: 1 image udptl t38), then “Call Server controlled switchover to T.38 mode” applies.

The H.248 coding examples below display H.248 message as used in the call flow examples in chapter 58.2.10.

Figure 2 Coding example: Check supported H.248 packages

Transaction (GWC -> MG)	Reply (GWC <- MG)

MEGACO/1 [47.174.66.80]:2944
Transaction=62 {
Context=-{
AuditValue=Root{
Audit {Packages}
}}}
	MEGACO/1 [47.166.34.20]:2944
	Reply=62 {
	Context=-{
	AuditValue=Root{
	Audit {Packages {.., ctyp-1, ..}}
	}}}

Figure 3 Coding example: Request fax event detection

Transaction (GWC -> MG)	Reply (GWC <- MG)

MEGACO/1 [47.174.66.80]:2944
Transaction=63 {
Context=$ {
Add=e1/03/05/1 {
M{O{MO=RC, tdmc/ec=ON }},
Events = 234 {ctyp/dtone}
}}}
	MEGACO/1 [47.166.34.20]:2944
	Reply=63 {
	Context= 1234{
	Add=e1/03/05/1
	}}

Figure 4 Coding example: Notify fax event V.21 flag

Transaction (GWC <-MG)	Reply (GWC -> MG)

MEGACO/1 [47.166.34.20]:2944
Transaction=64 {
Context=1234 {
Notify=e1/03/05/1 {
ObservedEvents=234 {
20030924T14001201:ctyp/dtone{dtt=V21flag}
}}}}
	MEGACO/1 [47.174.66.80]:2944
	Reply=64{
	Context= 1234{
	Notify=e1/03/05/1
	}}

Figure 5 Coding example: Add ephemeral with G.729 and T.38 codec”

Transaction (GWC ->MG)	Reply (GWC <- MG)

MEGACO/1 [47.166.34.20]:2944
Transaction=64 {
Context=1234 {
Add = $ {
Media {LocalControl {
v=0
c=IN IP4 $
m=audio$ RTP/AVP 18
a=ptime:20
m=image $ udptl t38
...
}}}}}
	MEGACO/1 [47.174.66.80]:2944
	Reply=64{
	Context= 1234{
	Add = rtp/34 {
	Media {Local {
	v=0
	c=IN IP4 47.174.66.14
	m=audio 1111 RTP/AVP 18 13 19
	a=ptime:20
	m=image 2222 udptl t38
	a=T38Fax ...
	a=T38Fax...
	...
	}}}}}

Note 1: The ephemeral termination is added with T.38 codec, to support “autonomous switchover to T.38” for e.g. PVG to PVG calls. At this point the remote GW type is unknown. If the remote side is H.323, then the T.38 codec is removed by the H.323 GW (codec negotiation). Note 2: This example shows 2 media lines in one session descriptor, as implemented in ISN06.2. This example will be updated at end of this feature to display real used SDP syntax.	

58.2.7 MGCP Support for T.38 fax

Implementation of “Call Server controlled switchover to T.38 mode”, makes use of Fax tone (ft) defined in the Generic Media Package (G). See Basic MGCP Packages [9], chapter 2.1.

The MGCP GW does not switch over to T.38, before the remote SDP is received.

- If the remote SDP contains T.38 codec (m=image 1 udptl t38), then “autonomaous switchover to T.38” applies.
- If the remote SDP indicates T.38 capability (a=cdsc: 1 image udptl t38), then “Call Server controlled switchover to T.38 mode” applies.

  Note: According [9], the MGCP GW detect a fax call by detecting the V.21 fax preamble. The fax tone event SHOULD also be generated when the T.30 CNG tone is detected

58.2.8 SIP-T Support for T.38 fax

SIP-T/SDP support for T.38 fax call is implemented according ITU T.38 [2] Annex D, Draft Amendment to T.38 [3] Annex E and IETF SIP Support for Real-time Fax[13].

T.38 fax interworking is supported over SIP-T. Support via native SIP is not covered by this activity.

58.2.8.1 Fax call CS2K to CS2K

This feature provides and verifies T.38 fax calls for H.323 GW interworking to H.323 GWs, H.248 GWs and MGCP GWs over SIP-T (ETSI ISUP V2+).

The SIP messages SUBSCRIBE and NOTIFY are used, which are defined in IETF RFC 3265 [11].

- With SUBSCRIBE(reqFaxDet), the H.323 GWC requests the remote side to detect fax event and to notify the H.323 side about a fax event.
- With NOTIFY(FaxDet), the H.248 or MGCP GWC notifies the event “fax call detected” to the remote H.323 side.

The content of both messages is proprietary and is needed on interworking between H.323 GWs with H.248 or MGCP GWs. The coding is specified in chapter 58.2.8.3.

58.2.8.2 Fax call CS2K to other Call Server

Prerequisite: The other Call Server with connected GW must support the functionality chapter 58.2.8.4. Additionally option 1 or option 2 below must be supported:

Option 1: The SIP SUBSCRIBE(reqFaxDet) and SIP NOTIFY(FaxDet) message are supported and processed as defined in chapter 58.2.8.1.

Option 2: The SIP SUBSCRIBE(reqFaxDet) and SIP NOTIFY(FaxDet) message are not supported. In this case the other Call Server must support:

- Autonomous fax event detection.
- Upon detection of fax, a Re-INVITE (T.38) message is sent to the far end.
- Receipt of SUBSCRIBE(reqFaxDet) message is ignored or rejected.

Feature ... tbd ... verifies Fax interworking between H.323 GWs connected to CS2K and a SIP-GW connected to MCS 5200 over SIP-T. No design work is planned to support T.38 interworking with other Call Servers.

58.2.8.3 Coding of SIP-T messages SUBSCRIBE and NOTIFY

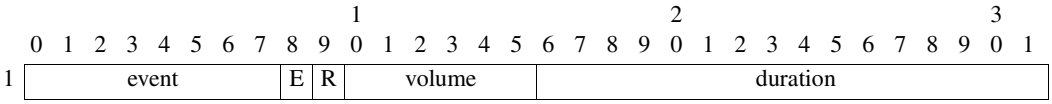
Figure 6 Sample message SUBSCRIBE

```
SUBSCRIBE sip:bob@biloxi.com SIP/2.0
Call-ID: 1234567
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=88sja8x
CSeq: 4 SUBSCRIBE
Event: telephone-event; events=32-60
Expires: 360
Content-Length: 0
```

Figure 7 Sample message NOTIFY

```
NOTIFY sip:alice@atlanta.com SIP/2.0
Call-ID: 1234567
To: Alice <sip:alice@atlanta.com>
From: Bob <sip:bob@biloxi.com>; tag=55afp93
CSeq: 7 NOTIFY
Event: telephone-event
Subscription-State: active
Content-Type: audio/telephone-event
Content-Length: 4
< four octets in network order, as coded in Figure 8 >
```

Figure 8 Coding of RFC 2833 Payload Format



With event = 32, E = 0, R = 0, volume = 0, duration = 0

58.2.8.4 Coding of Session Description Protocol (SDP)

To switch successfully from G.729/G.711 codec to T.38 codec (or from G.729 to G.711) the codec capability of the remote GW side must be well-known. To indicate T.38 or G.711 capability to the remote GW, the capability declaration mechanism of RFC 3047 [12] is used.

T.38 capability is indicated to the remote GW with “a=cdsc: 1 image udptl t38“ line in SDP data as shown in Figure 9.

With “a=cpar: a=T38 ..” additional T.38 parameters are defined, which applies in ISN07 release.

G.729 and G.711 capability is indicated to the remote GW with “a=cdsc: 2 audio RTP/AVP 18 8“ line in SDP data.

Figure 9 T.38 parameter in capability description

v=0
c=IN IP4 128.96.41.1
a=sqn: 0
a=cdsc: 1 image udptl t38 - indicates T.38 capability
a=cpar: a=T38FaxVersion: 1
a=cpar: a=T38FaxMaxBuffer:3341
a=cpar: a=T38FaxMaxDatagram:333
a=cpar: a=T38FaxMaxBitRate: 10000
m=audio 1111 RTP/AVP 18
a=ptime:20
a=cdsc: 2 audio RTP/AVP 18 8 - indicates G.729 and G.711 capability
a=cpar: a=ptime:20

Note: For clarity, T.38 parameters are omitted in the subsequent figures.

Figure 10 to Figure 14 show SDP coding examples for interworking H.248 to H.323.

Note: SDP coding for H.248 side applies also for non-H.323 e.g. MGCP.

Figure 10 and Figure 11 show SDP coding examples for interworking H.248 GW supporting “autonomous switching to T.38” and H.323 GW supporting “Call Server controlled T.38 switching”. Fast start (FS) applies on H.323 side.

Figure 10 SDP sample for H.248 -> H.323 (FS) interworking over SIP-T

H.248 -> H.323: INVITE (SDP)	**H.248 <- H.323: 200 OK (SDP)**
v=0 c=IN IP4 128.96.41.1 m=audio 1111 RTP/AVP 18 (Note 1) a=ptime:20 m=image 1112 udptl t38 (Note 2)	v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 3) m=audio 2222 RTP/AVP 18 (Note 1) a=ptime:20 ~~m=image 0 udptl t38~~ (Note 4)

Note 1: Both sides supports G.729 codec. The voice call is set up with G.729 codec. Note 2: Originating H.248 side commits simultaneous support for T.38 and indicates usage of “autonomous T.38 switching”. Note 3: Terminating H.323 side indicates T.38 capability (not simultaneous to G.729). Note 4: Terminating H.323 does not support “autonomous T.38 switching”. Current ISN07 implementation does not sent “m=image 0 udptl t38” back. Omitting “m=image ...” indicates, that “autonomous T.38 switching” is not supported by terminating side. Note 5: Upon detection of fax call, “Call Server controlled T.38 switching” takes place.

Figure 11 SDP sample for H.323 (FS) -> H.248 interworking over SIP-T

H.323 -> H.248: INVITE (SDP)	**H.323 <- H.248: 200 OK (SDP)**
v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 1) m=audio 1111 RTP/AVP 18 (Note 2) a=ptime:20	v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 1) m=audio 2222 RTP/AVP 18 (Note 2) a=ptime:20
Note 1: Both sides indicates T.38 capability. Note 2: Both sides supports G.729 codec. The voice call is set up with G.729 codec. Note 3: Upon detection of fax call, “Call Server controlled T.38 switching” takes place.	

Figure 12 and Figure 13 show SDP coding example for interworking H.248 GW supporting “autonomous switching to T.38” and H.323 GW supporting “Call Server controlled T.38 switching”. Slow start (SS) applies on H.323 side.

Figure 12 SDP sample for H.248 -> H.323 (SS) interworking over SIP-T

H.248 -> H.323: INVITE (SDP)	**H.248 <- H.323: Ringing (SDP)**
v=0 c=IN IP4 128.96.41.1 m=audio 1111 RTP/AVP 18 (Note 1) a=ptime:20 m=image 1112 udptl t38 (Note 2)	v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 3) m=audio 2222 RTP/AVP 18 (Note 1) a=ptime:20 ~~m=image 0 udptl t38~~ (Note 4)
H.248 -> H.323: ACK - 200 OK (SDP)	
v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 5) m=audio 1111 RTP/AVP 18 (Note 1) a=ptime:20	

Note 1: Both sides supports G.729 codec. The voice call is set up with G.729 codec. Note 2: Originating H.248 side commits simultaneous support for T.38 and indicates usage of “autonomous T.38 switching”. Note 3: Terminating H.323 side indicates T.38 capability. Note 4: Terminating H.323 does not support “autonomous T.38 switching”. Current ISN07 implementation does not sent “m=image 0 udptl t38” back. Omitting “m=image ...” indicates, that “autonomous T.38 switching” is not supported by terminating side. Note 5: Originating H.248 side indicates T.38 capability. Note 5: Upon detection of fax call, “Call Server controlled T.38 switching” takes place.

Figure 13 SDP sample for H.323 (SS) -> H.248 interworking over SIP-T

H.323 -> H.248: INVITE (SDP = empty)	**H.323 <- H.248: RINGING (SDP)**
H.323 -> H.248: ACK (SDP)	v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 1) m=audio 2222 RTP/AVP 18 (Note 2) a=ptime:20
v=0 c=IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 1) m=audio 1111 RTP/AVP 18 (Note 2) a=ptime:20	
Note 1: Both sides indicates T.38 capability. Note 2: Both sides supports G.729 codec. The voice call is set up with G.729 codec. Note 3: Upon detection of fax call, “Call Server controlled T.38 switching” takes place.	

Figure 14 show SDP coding example for interworking H.248 GW supporting G.729 and G.711 codec with H.323 GW supporting G.729, G.711 and T.38 codec. Fast start (FS) applies on H.323 side.

Figure 14 SDP sample for H.248 -> H.323 (FS) interworking over SIP-T

H.248 -> H.323: INVITE (SDP)	**H.248 <- H.323: 200 OK (SDP)**
v=0 c=IN IP4 128.96.41.1 m=audio 1111 RTP/AVP 18 8 (Note 1, 2) a=ptime:20	v=0 c= IN IP4 ... a=sqn: 0 a=cdsc: 1 image udptl t38 (Note 3) m=audio 2222 RTP/AVP 18 (Note 1) a=ptime:20 a=cdsc: 2 audio RTP/AVP 18 8 (Note 4) a=cpar: a=ptime:20
Note 1: Both sides supports G.729 codec. The voice call is set up with G.729 codec. Note 2: Originating H.248 side supports additionally codec G.711 a-law. Note 3: Terminating H.323 side indicates T.38 capability.	

Note 4: Terminating H.248 side indicates additionally G.729, G.711 a-law capability
Note 5: Upon detection of fax call, “Call Server controlled G.729 -> G.711 switching” takes place, because originating side does not indicate/support T.38 capability.

58.2.9 Interworking

This feature supports “Call Server controlled switchover to T.38 (or to G.711)” for **nodal calls** and for **inter-Call Server calls** over SIP-T (ETSI ISUP V2+) when the originating or terminating agent is H.323.

This feature provides Call Server controlled switchover to T.38 (or G.711) codec depending on T.38 network option:

- If **Netopt is set to “T.38”** and both GW support T.38, then upon fax detection, switchover is done from G.729 (or G.711) to T.38 codec.
- If **Netopt is not set to “T.38”**, or a GW does not support T.38, then switchover to T.38 does not apply. If the call was set up with G.729 codec, switching is done from G.729 to G.711 codec. If the call was set up with G.711, no switchover occurs.

Table 1 Supported fax interworkings for nodal calls and for inter-Call Server calls via SIP-T

<table>
<tr><th>Terminating side:

Originating side:</th><th>H.323</th><th>H.248</th><th>MGCP</th><th>SIP-T</th></tr>
<tr><td>H.323</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>H.248</td><td>✓</td><td colspan="2" rowspan="2">Out of scope
for this activity
Note 3</td><td rowspan="2">✓
Note 2</td></tr>
<tr><td>MGCP</td><td>✓</td></tr>
<tr><td>SIP-T</td><td>✓</td><td colspan="2">✓
Note 1</td><td>Out of scope
for this activity</td></tr>
</table>

Note 1: Provided, if the originating side sends SUBSCRIBE(reqFaxDet) and processes NOTIFY(FaxDet) as defined in chapter 58.2.8.

Note 2: Provided, if the terminating side sends SUBSCRIBE(reqFaxDet) and processes NOTIFY(FaxDet) as defined in chapter 58.2.8.

Note 3: Calls where only H.248 GWs or MGCP GWs are involved, are out of scope for this feature. “Autonomous switching to T.38 (or to G.711)” may apply for these calls.

T.38 fax interworking to H.323 is provided for currently available protocol agents on H.248 GW: ETSI ISUP, ETSI PRI and ETSI V5.2.

In case of CS2K Hybrid, the interworking between TDM platform and IP platform is provided via ISUP-looparound.

58.2.10 Call Flows

Description of T.38 functionality is provided via annotated call flows. The description of the first call flow is given in detail and may be applied to other subsequent call flows.

> ***Note:*** Focus of the call flows is to show "Call Server controlled switchover to T.38 mode". Call control messages (e.g. H.225, IUA, SIP) and Media control messages (e.g. H.245, H.248, MGCP) are not complete. Furtheron TCS-Ack messages have been omitted for clarity.

Mapping between H.248 or H.323 messages and SIP-T messages can be obtained from the call flows. Coding of SIP-T messages SUBSCRIBE and NOTIFY is specified in chapter 58.2.8.3. Coding of SDP content is specified in chapter 58.2.8.4.

In the case that the originating and terminating GW are located on the same Call Server, the SIP-T part is not applicable and shall be neglected.

T.38 fax call flows are presented for:

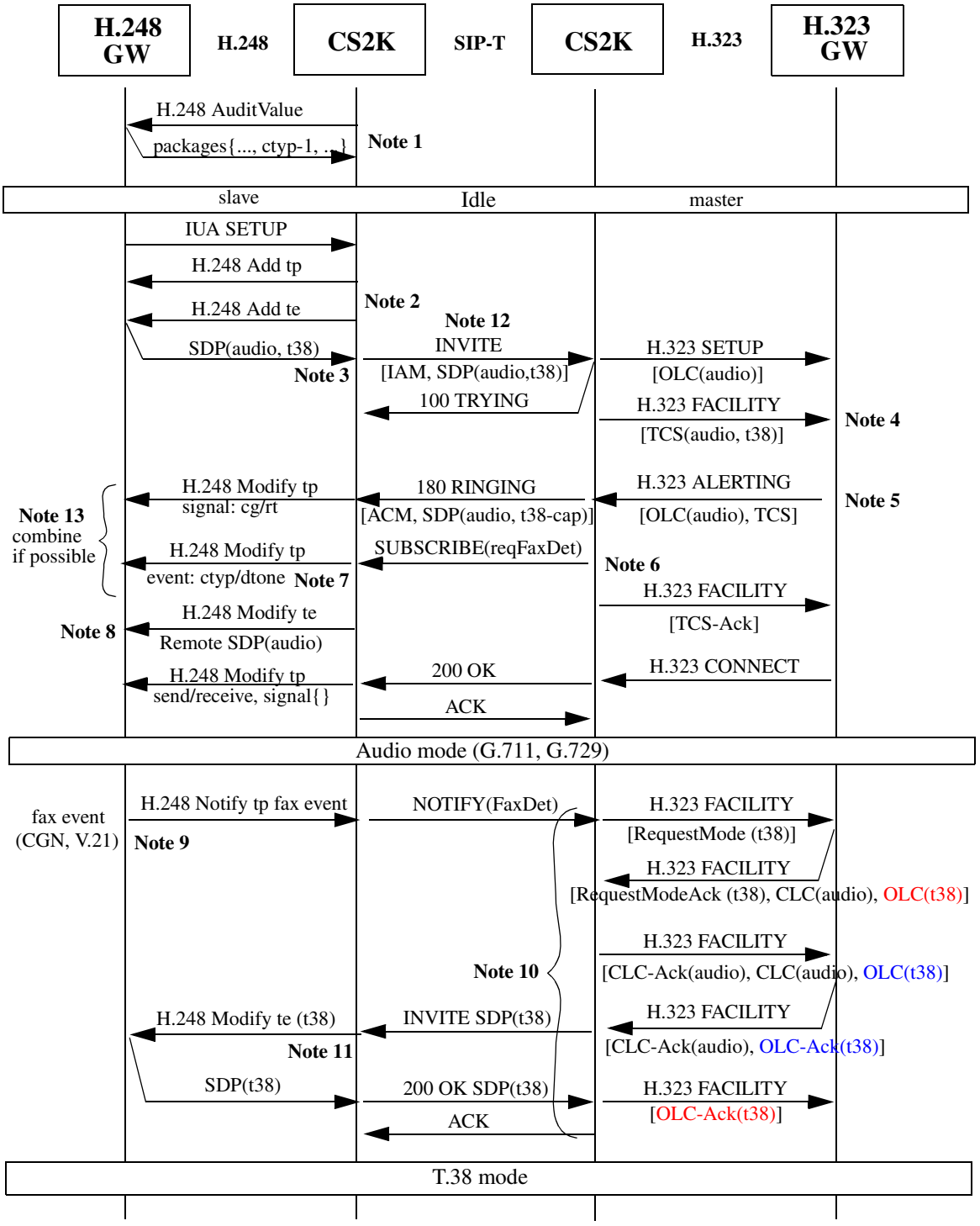
- fast start: H.248(FS) -> H.323(FS) - see chapter 58.2.10.1
- fast start: H.323(FS) -> H.248 (FS) - see chapter 58.2.10.2
- fast start: H.323(FS) -> H.323(FS) - see chapter 58.2.10.3
- slow start: H.248(FS) -> H.323(SS) - see chapter 58.2.10.4
- slow start: H.323(SS) -> H.248(FS) - see chapter 58.2.10.5

58.2.10.1 Call flow for H.248 to H.323 interworking (fast start)

Figure 15 displays a sample messaging of a successful fax call between PRI (H.248 controlled) and H.323. First a voice call is established. After a fax call was detected, "Call Server controlled switchover to T.38" occurs.

Selection: Fast start applies - the H.248 side is "slave", the H.323 side is "master". Both sides support "Call Server controlled switchover to T.38" and Netopt is set to "T.38"

Figure 15 Sample flow for H.248 to H.323 interworking



Note 1: The H.248 GWC checks GW T.38 capability via H.248 AuditValue command at GW registration. If GW replies to the AuditValue request with H.248.2 fax package “ctyp-1”, then “Call Server controlled switchover to T.38 mode” is supported by the H.248 GW.

Coding sample of H.248 AuditValue is shown in Figure 2, on page 1236

Note 2: After adding the physical TDM termination (Add tp), the ephemeral termination (te) is added for a voice call (e.g. G.711 or G.729 codec). If the Network Option is set to “T.38”, the GWC request “T.38 mode”, by including T.38 codec in Add te request command.

Note 3: The H.248 GW replies with local Session Description Protocol (SDP) containing the preferred voice codec and optional with T.38 codec.

Coding sample of H.248 Add te is shown in Figure 5, on page 1236

Note 4: The H.323 GWC sends a Terminal Capability Set (TCS) message to the H.323 GW, to indicate that “CS controlled switchover to T.38” is supported by the remote side.

Note 5: The H.323 GW supporting “CS controlled switchover to T.38” responds with the preferred audio codec and indicates T.38 capability.

SDP coding samples are available in section “58.2.8.4 Coding of Session Description Protocol (SDP)” on page 1239

Note 6: The H.323 GWC checks “CS controlled switchover to T.38” capability via H.323 GW profile. If supported, the remote H.248 side is requested to detect fax call.

Note 7: If H.248 GW supports “CS controlled switchover to T.38” i.e. AuditValue Reply included “ctyp-1” package, fax event detection (CNG tone, V.21 Preamble) is requested on the physical termination.

Coding sample of H.248 Modify tp event=ctyp/dtone is shown in Figure 3, on page 1236

Note 8: The ephemeral termination is modified with the remote SDP. If the remote SDP indicates T.38 capability via “a=cdsc: 1 image udptl t38”, then “CS controlled switchover to T.38” applies for this call. The H.248 GW does not switch over autonomously to T.38 or G.711.

Note 9: Upon detection of “fax call”, the H.248 GW notifies the H.248 GWC. The Notification is transferred to the remote H.323 GWC/GW side.

Coding sample of H.248 Notify tp fax call is shown in Figure 4, on page 1236

Note 10: Upon receipt of Notify fax detection, the H.323 GWC sends RequestMode (T.38) to the H.323 GW. The H.323 GWC handles the H.323 CLC and OLC messaging locally. Switchover to T.38 mode is always invoked by the H.323 GWC. The remote side is requested to switch over to T.38 by exchanging SDP(T.38) data.

Note 11: Upon receipt of SDP(T.38) data, a H.248 Modify command is sent, which request the ephemeral termination to switch over to T.38.

Note 12: The content of SDP uses following abbreviation:

— SDP(audio) for processing of audio media stream.

— SDP(t38) for processing of t38 media stream.

— SDP(audio, t38) for simultaneous processing of audio and t38 media streams.

— SDP(audio, t38-cap) for processing of audio media stream and for t38 capability indication.

Note 13: To reduce H.248 messaging, the “H.248 request detect fax tone” shall be sent within other available H.248 messages, if possible:

— combination of “Modify event = ctyp/dtone” and “Modify signal cg/rt” is possible, if ALERTING and SUBSCRIBE messages are sent coincidently.

— combination of “Add tp” and “Modify event = ctyp/dtone” is possible, if the H.248 GW is the terminator and runs in “master mode”.

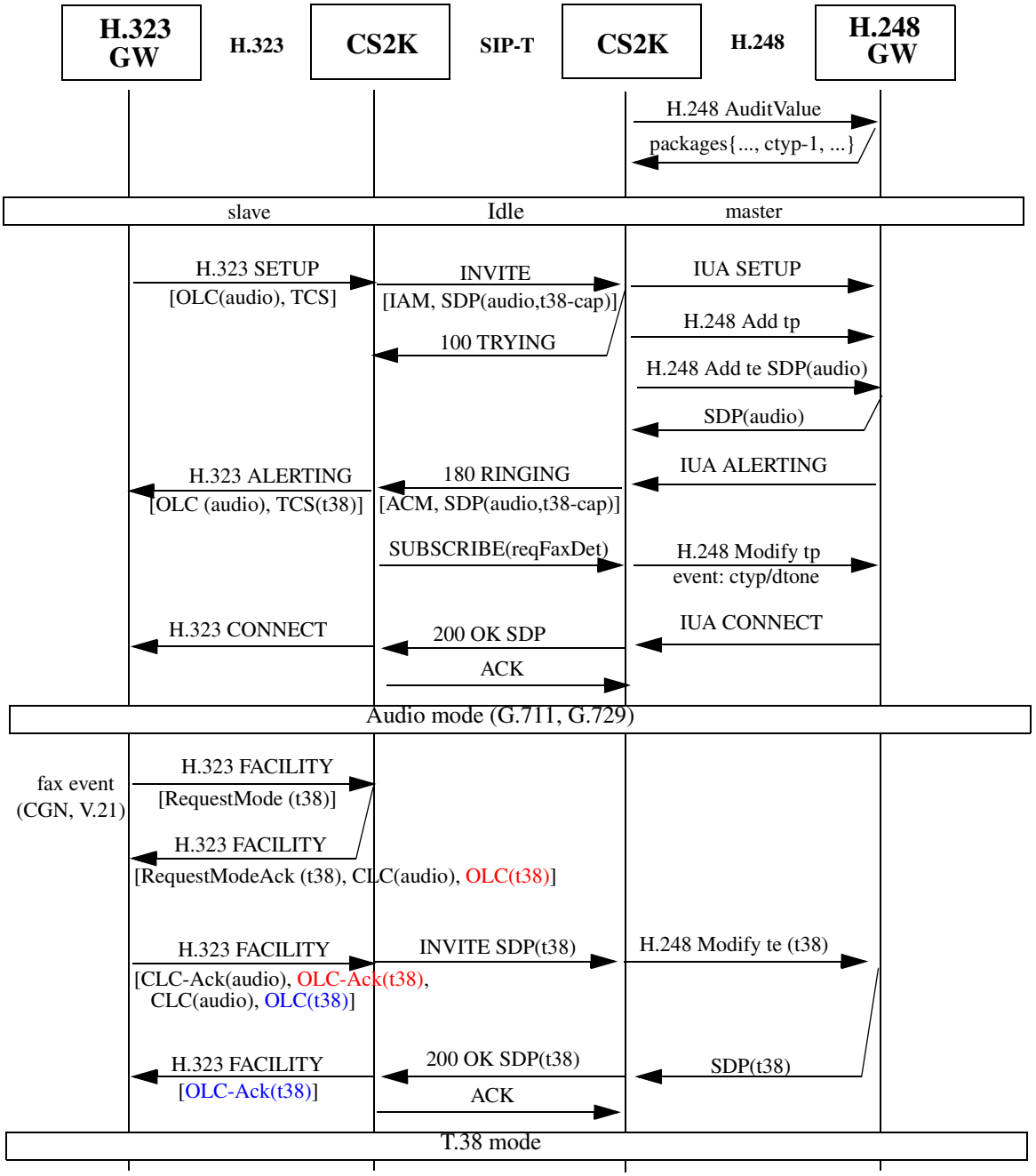
The “event = ctyp/dtone” is only requested, if the remote side is H.323, which request fax detection. On H.248 to H.248 interworking or H.248 to MGCP interworking, fax detection event is not requested.

58.2.10.2 Call flow for H.323 to H.248 interworking (fast start)

Figure 16 displays a sample messaging of a successful fax call between H.323 and PRI (H.248 controlled). First a voice call is established. Upon detection of fax call by originating H.323 side, “Call Server controlled switchover to T.38” applies.

Selection: Fast start applies - the H.323 side is “slave”, the H.248 side is “master”. Both sides supports “Call Server controlled switchover to T.38” and Netopt is set to “T.38”

Figure 16 Sample flow for H.323 to H.248 interworking

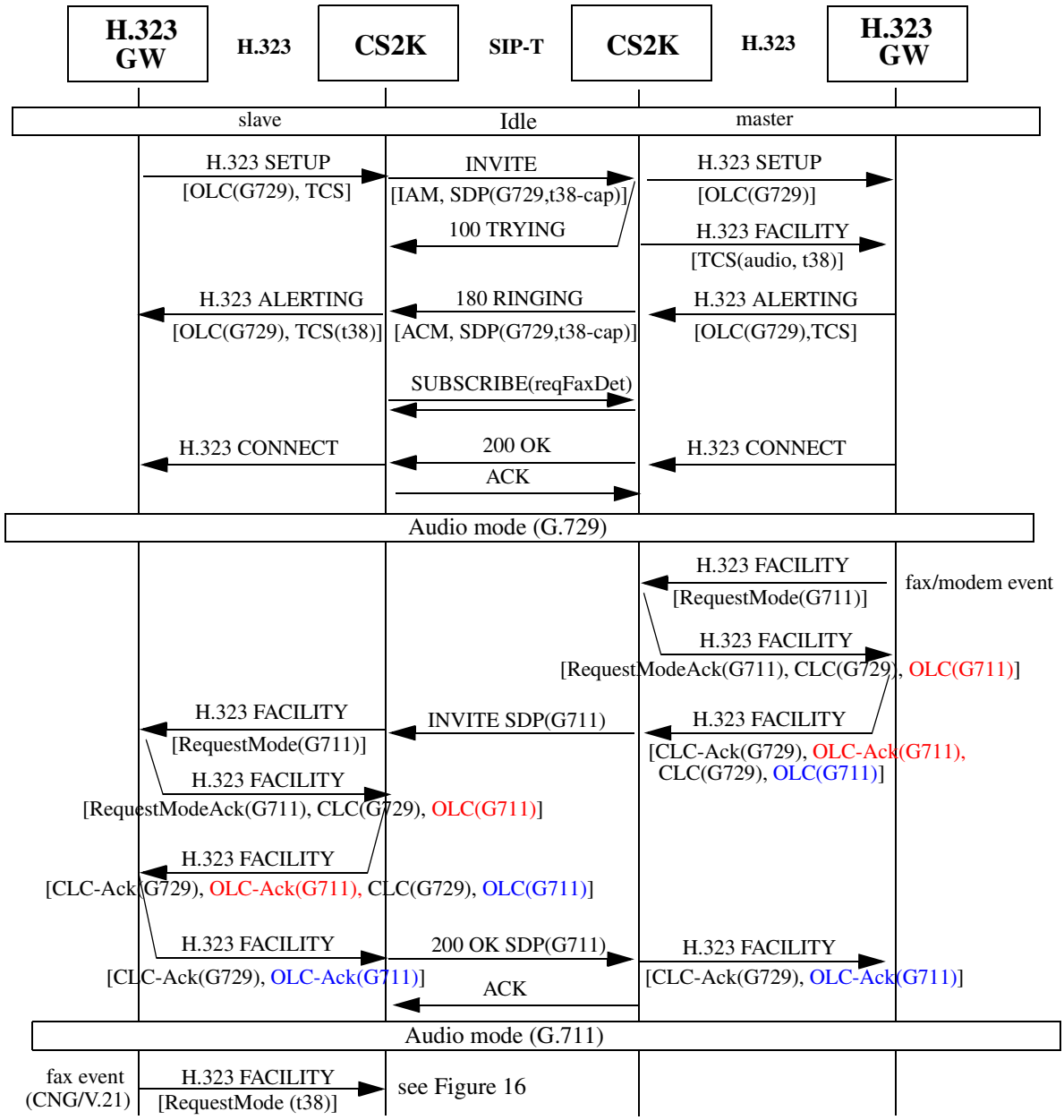


58.2.10.3 Call flow for H.323 to H.323 interworking (fast start)

Figure 17 displays a sample messaging for “Call Server controlled switchover to G.711” between two H.323 GWs, First a voice call with G.729 codec is established. Upon detection of CED tone, switching to G.711 codec is

requested by the terminating side in this example. Upon detection of CNG or V.21 preamble a further switching to T.38 codec may take place as displayed in previous Figure 16.

Figure 17 Sample flow for H.323 to H.323 interworking

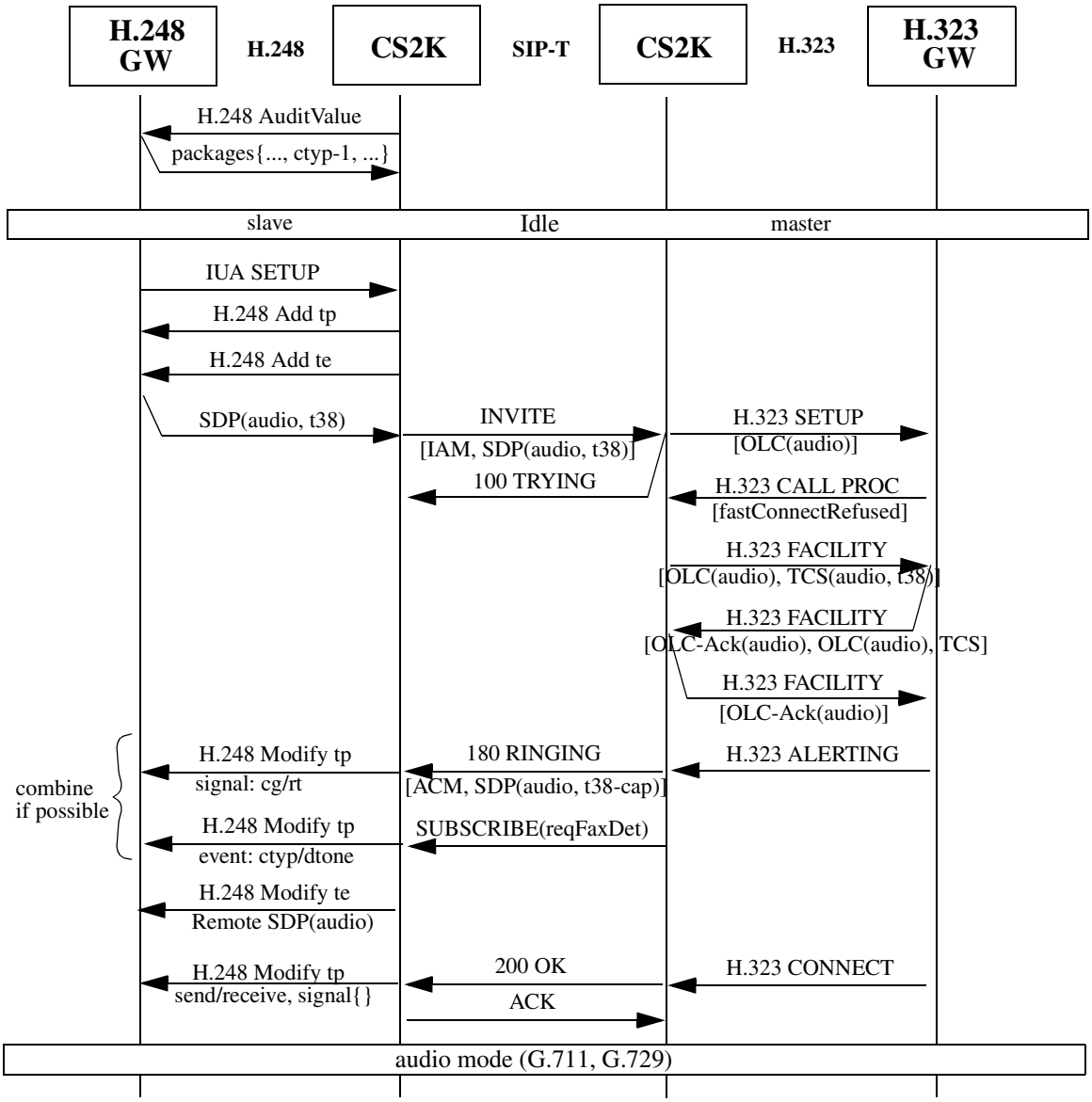


58.2.10.4 Call flow for H.248 to H.323 interworking (slow start)

Figure 18 displays a sample messaging of a voice call establishment between PRI (H.248 controlled) and H.323. In case of a fax event, the same sequence applies as displayed in Figure 15 or Figure 16.

Selection: Originating side (H.248) starts with fast connect, the terminating side (H.323) rejects fast connect. The H.323 side is “master”, the H.248 side is “slave”. Netopt is set to “T.38”

Figure 18 Sample flow for H.248 (FS) to H.323 (SS) interworking

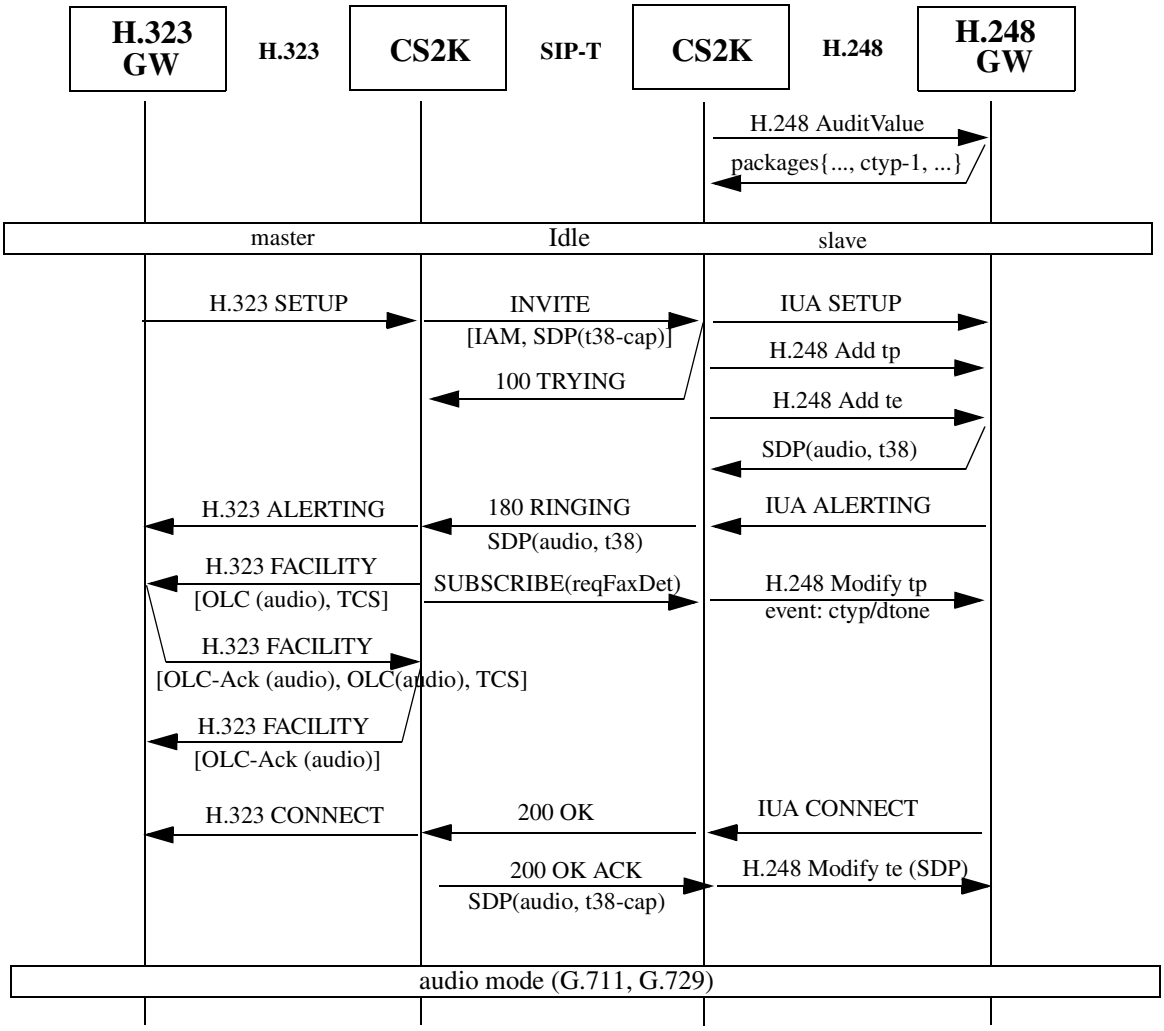


58.2.10.5 Call flow for H.323 to H.248 interworking (slow start)

Figure 18 displays a sample messaging of a voice call establishment between H.323 and PRI (H.248 controlled). Provisions are made to detect a fax call. In case of a fax event, the same sequence applies as displayed in Figure 15 or Figure 16.

Selection: Originating side (H.323) uses slow start. The H.323 side is “master”, the H.248 side is “slave”. Netopt is set to “T.38”

Figure 19 Sample flow for H.323 (SS) to H.248 interworking



58.2.11 G3FE operation modes

This feature supports fax operation modes specified in ITU-T T.30 [1]. The originating side can invoke a fax call manually or automatically. Same happens on terminating side, call acceptance can be manually or automatically.

Detection of a fax call and subsequent “Call Server controlled switchover to T.38 mode” is complicated by the following facts:

- Sending Calling tone (CNG tone) is mandatory for calling fax devices. However manual calling terminals conforming to 1993 or previous T.30 versions may not transmit this signal.
- Called terminal identification answer tone (CED tone) is mandatory for called fax devices using automatic mode. For manual operation mode the sending of CED is optional.
- Upon receipt of CED tone, it is not clear whether a fax call or a modem call will be established. Because of the time-critical nature of a modem call, it is recommended to switch from G.729 codec to G.711 codec. If a fax call is determined by detection of CGN tone or V.21 preamble, an additional switch to T.38 may occur.
- V.21 Preamble is sent by all G3FE devices except fax devices which use V.8 or V.34 operation mode. These devices may send CNG tone.
- Upon receipt of V.21 Preamble flag, the switchover to T.38 must occur quickly (within ca. 2 sec), otherwise the fax call will fail.

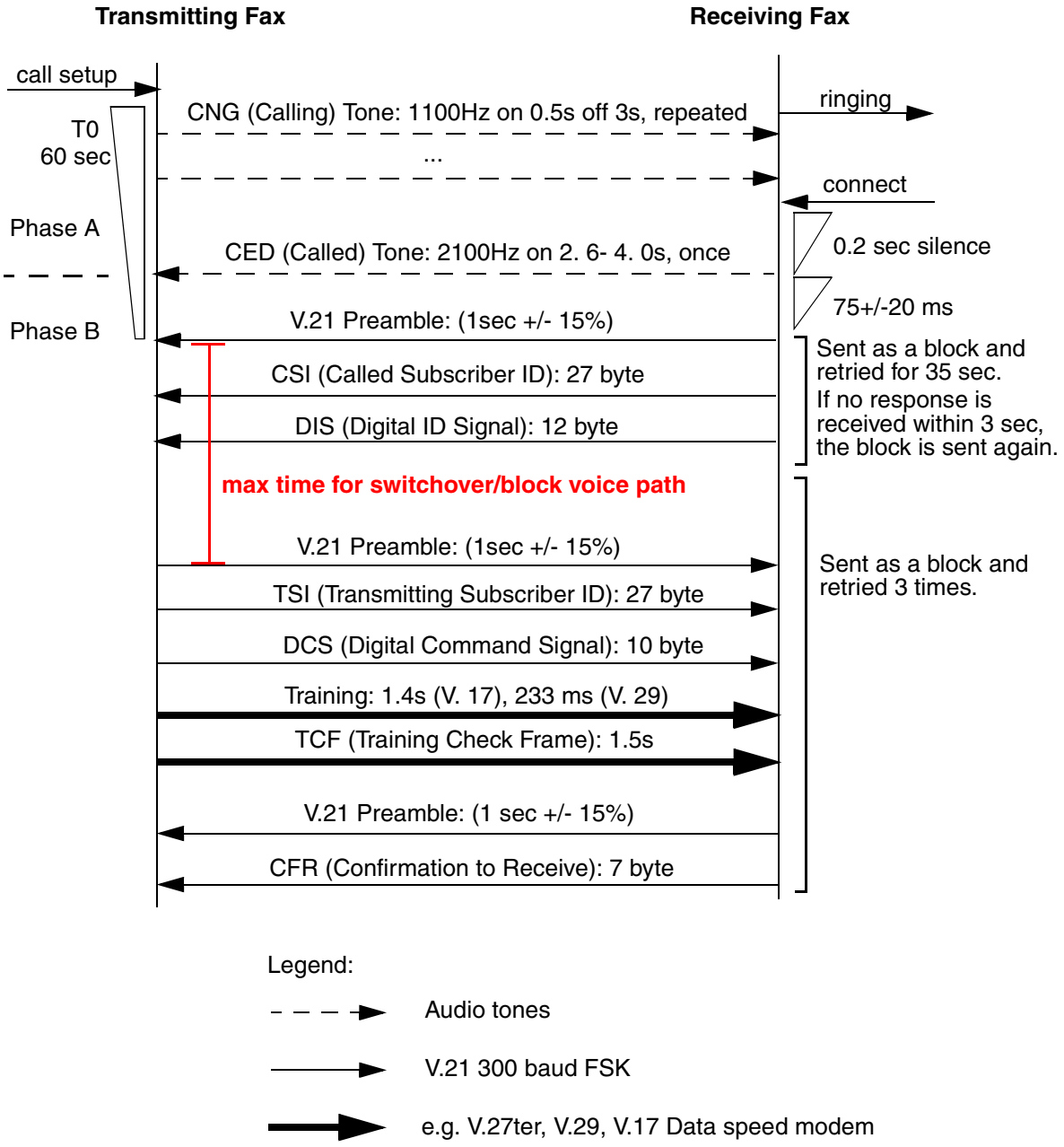
Note 1: A GW may identify a fax call by monitoring the physical termination (TDM bearer channel) for CNG tone and V.21 Preamble flags.

Note 2: Fax calls, without CNG tone and V.21 Preamble, will not be recognized by the GW.

Note 3: H.323 GWs seem to detect a fax call with CED and V.21 Preamble.

Figure 20 display an example of a T.30 fax call establishment. If switchover to T.38 mode is triggered by V.21 Preamble, the switchover must occur before Digital Command Signal (DCS) is transmitted. To prevent the exchange of DIS/DCS during switchover phase, the voice path should be blocked. If no DCS is received on terminating side, V.21/CSI/DIS is sent again after 3 sec.

Figure 20 Establishment of T.30 Fax call (automatic operation example)



58.3 Hardware Requirements or Dependencies

New hardware is not required.

58.4 Software Requirements or Dependencies

- CM/GWC: ISN07 load
- H.248 GW - supporting H.248.1, H.248.2 ctyp package, T.38 mode.
- H.323 GW - supporting H.323, H.225, H.245 protocol, T.38 mode
- MGCP GW - supporting Generic media package/fax tone (G/ft), T.38 mode

58.5 Limitations and restrictions

- T.38 fax interworking to non-Nortel Call Servers are out of scope for this feature and will not be tested. **(Note 1)**

  Note 1: Interworking to non-Nortel Call Servers may work, if the non-Nortel Call Server supports the prerequisites as defined in chapter 58.2.8.2.
- T.38 fax interworking is supported over SIP-T (ETSI ISUP V2+). Native SIP support for T.38 fax interworking is not covered by this feature.
- T.38 fax interworking with MCS 5200 (IMS) is not tested by this feature. It is tested by feature ... tbd.
- This feature verifies T.38 fax interworking for H.323 GW on one call leg and H.323 GW or H.248 GW or MGCP GW on the other call leg. Feature verification is done for:
  - H.323 GW: Succession1000M
  - H.323 GW: BCM
  - H.323 GW: Cisco IOS gateway 2600 **(Note 2)**
  - H.248 GW: PVG Passport 15k with VSP3 cards
  - MGCP GW: Mediatrix

  Note 2: This should also cover support for Cisco IOS gateway 36xx, although it isn't explicitly tested by this feature.

  T.38 interworking with other GWs are out of scope and will not be tested within this feature.
  - Testing Westell and SBC interoperability is tested by feature ... tbd.
- Interworking to Group 4 fax, Modem and Data Transmissions are out of scope for this feature.
- "Facsimile-only over IP environment" (T.38 Annex D.2.2.3) is out of scope for this feature. This feature addresses "Facsimile and voice over IP environment" (T.38 Annex D.2.2.4) in which first a voice call is established and then switchover to T.38 mode occurs.

- This feature does not support switching back to voice codec, when a fax call has ended.
- This feature uses the transport layer UDP/IP for T.38 packets (T.38 Annex D.2.3.2). Transport of T.38 packets via TCP/IP is not used by this feature.
- The optional transport of T.38 packets via one bidirectional reliable channel is not used. Instead two logical channels are used. (T.38 Annex B.3.3, D.2.3.2)
- Testing is done on the international CS2K load only. Testing for NA load is captured by feature .... tbd.
- Testing T.38 fax interworking to MCS 5200 is not part of this feature, is captured by feature ... tbd.
- T.38 fax interworking to Cable MTAs is out of scope for this feature.
- *Due to the DSP implementation on the BCM, currently BCM calls are not supported over a Media Portal (MP). BCM calls are only supported in the same network segment. A solution is currently estimated for the BCM 3.7 load which is post SN07 content which involves changes to the BCM software implementation.*
  The deployment of the T.38 functionality is currently only possible with the S1KM/S1K, if used behind a NAT / Firewall.
- *BCM and S1KM will not request G.711, if the codec is G.729 and a fax is detected, but T.38 is unavailable. Therefore no support for G.729 to G.711 switchover is possible between two H.323 GWs. Solution planned for post SN07 GW loads.*
- *Currently the only supported H.323 GWs are BCM and S1KM. Westell, Cisco and Mediatrix are not included in the IT content and will be tested in the ICAF A00005122 which is currently post SN07 content.*
- *The FN will be updated upon completion of A00005122 including the final restrictions for SN07.*

58.6 Interactions

Not identified.

58.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	N/A

User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

58.8 Glossary

Term	Description
BCM	Business Communication Server (H.323 Gateway)
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec) see T.30 chapter 4.1
CLC	Close Logical Channel (H.245 message)
CM	Call Manager, Computing Modules
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec on, 3.0 sec off, duration 60-120 sec) see T.30 chapter 4.2.
CS	Call Server
CS2K	Call Server 2000
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.
GW	Gateway (Signalling Gateway and Media Gateway)
GWC	Gateway Controller
IAF	Internet Aware Fax device
IMS	Interactive Multimedia Server New name is Multimedia Communication Server 5200
ISDN	Integrated Services Digital Network
ISN07	International Succession Product Release

Term	Description
ISUP	ISDN User Part
IUA	ISDN Q.921-User Adaptation Layer Protocol (IETF)
MCS 5200	Multimedia Communication Server 5200
MG	Media Gateway
MGC	Media Gateway Controller MGC as seen by IETF consists of Gateway Controller and Call Manager and is therefore equivalent to DMS Communication Server 2000.
MP	Media Portal, Media Proxy, RTP Portal
OLC	Open Logical Channel (H.245 message)
PSTN	Public Switched Telephone Network.
PVG	Passport Packet Voice Gateway (Passport15000)
RFC	Request For Comments (IETF)
RTP	Real-time Transport Protocol (IETF 1889, 3550)
S1K	Meridian Succession 1000 (H.323 GW)
S1KM	Meridian Succession 1000M (H.323 GW)
SBC	Session Border Controller other names are: ACME box, H.323 Proxy
SDP	Session Description Protocol (IETF RFC 3266)
SIP	Session Initiation Protocol (IETF RFC 3261)
SIP-T	Session Initiation Protocol - Telephony ITU-T based standard, that encapsulates ISUP messaging as payload within SIP messages.
TCS	Terminal Capability Set message (see H.245 B.2.2)
te	Ephemeral (RTP/UDP/IP) termination for voice calls Ephemeral (T.38/UDP/IP) termination for fax calls
tp	Physical (TDM) termination
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

58.9 References

[1] ITU-T Recommendation T.30
Procedures for document facsimile transmission in the general switched telephone network, 04/1999

[2] ITU-T Recommendation T.38
Procedures for real-time Group 3 facsimile communications over IP networks, 03/2002

[3] Draft Amendment 1 to Recommendation T.38 (2002) (for Consent)

[4] ITU-T Recommendation H.323
Packet-based multimedia communications systems, 11/2000

[5] ITU-T Recommendation H.225.0
Call signalling protocols and media stream packetization for packet-based multimedia communication systems, 11/2000

[6] ITU-T Recommendation H.245
Control protocol for multimedia communication, 07/2001

[7] ITU-T Recommendation H.248.1
Gateway Control Protocol, 03/2002

[8] ITU-T Recommendation H.248.2
Gateway control protocol: Facsimile, text conversation and call discrimination packages, 11/2000

[9] Basic MGCP Packages
draft-foster-mgcp-basic-packages-10.txt, February 2003

[10] Session Initiation Protocol (SIP)
IETF RFC 3261, June 2002

[11] Session Initiation Protocol (SIP) - Specific Event Notification
IETF RFC 3265, June 2002

[12] Session Initiation Protocol (SIP) - Simple Capability Declaration
IETF RFC 3407, October 2002

[13] SIP Support for Real-time Fax: Call Flow Examples and Best Current Practices, draft-ietf-sipping-realtimefax-01.txt, August 2003

[14] RTP Payload for DTMF Digits, Telephony Tones and Signals
IETF RFC 2833, May 2000

[15] Feature A00001895 ‘H.323 Base Support’
PLS library FMDOC

[16] CS2000 Product Specification for ISN06, 19/08/2003
http://product-planning.europe.nortel.com/product-description

59: Functional Description (FN): A00003686

59.1 Feature name

Re-Routing Based on Release Cause Value.

59.2 Description

This feature provides re-routing of a call, when the release message (before ACM message) with ISUP cause value is received for terminating ETSI ISUP V1 and V2 agent (Base ETSI ISUP V1 and V2) and Belgian ISUP agent on a trunk route.

The activity provides re-routing on ETSI ISUP trunks for pre-datafilled release causes.

In current system ISUP Re-Routing on Congestion Cause value (No Circuit Available(34) or Switching Equipment Congestion(42)) is provided by Feature A59013395 called ISUP Re-routing on Congestion MMP13. It supports re-routing when congestion takes place for calls terminating to ETSI ISUP.

In current system, re-routing criteria depends on:

- CND NRR selector in the routing tuple
- Rel message received with congestion cause value

For this activity, Re-routing criteria will depend on:

- presence of CND NRR selector in routing tuple
- Rel message (before ACM message) received with ISUP cause value for which RTEADV field in table FLXCMAP was provisioned.
- optionality of feature

This feature has no affect on feature A59013395.

The activity is optional with a SOC option. When state of SOC is ON, feature becomes active, otherwise system behaves as it was before this functionality.

Through the fndocs of this activity, ‘ISUP cause value’ is used to address ISUP cause value except following cause values:

Normal Call Clearing (CI=16),

Normal Unspecified (CI=30),

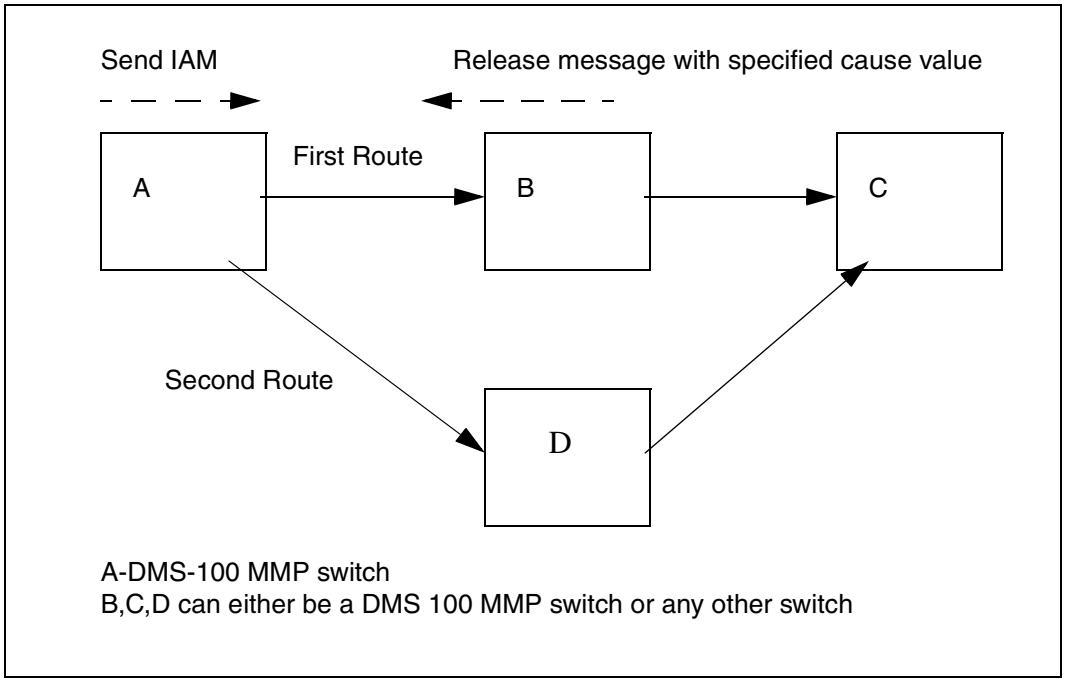
Interworking Unspecified (CI=127).

The feature is implemented in ISN07.

59.2.1 Functional Description

Figure 1 describes functional behavior of the feature.In this case, ISUP IAM is sent out on first route. When REL message with ISUP cause value is returned in response along the first route, second route is determined in route list in office A. If second route is present and required conditions are provided, IAM is sent on second route.

Figure 1 Functional Behavior of the Feature



The conditions mentioned above are shown in Figure 2 and can be listed as follows.

a. If ISUP cause value in REL message is congestion (No Circuit Available(34) or Switching Equipment Congestion(42)):

- It is directly checked CND NRR datafill as alternate route. If CND NRR selector is present in route list for terminating side (A office), call is routed to another trunk (second route). Otherwise, call goes to treatment.

b. If ISUP cause value in REL message is not congestion, following conditions are determined respectively:

- Checking whether REL message is received before ACM message. Re-routing is provided for REL message before ACM message.
- Checking of SOC option. It must be ON state for re-route.
- Determining of RTEADV field in FLXCMAP table. It must be Y for re-route
- Checking of CND NRR datafill as alternate route. CND NRR selector must be present in the route list for re-route.

  If these three conditions are provided, call is routed to another trunk (second route). Otherwise, call is terminated to treatment

59.2.2 Activation of Feature

Activation of feature is controlled by SOC XLAS0053.

XLAS Reroute Rel Cause is a state SOC and it has two states, ON and IDLE.Default state of XLAS Reroute Rel Cause is IDLE. When its state is ON, this feature becomes functional.

59.2.3 Provisioning Table FLXCMAP

Normally, there is a map in FLXCMAP table for ISUP cause value in release message. It should be mapped ISUP cause value to Network Re-Routing Capability for each ISUP cause value in REL message. For providing this, RTEADV field of table FLXCMAP is used. RTEADV field for ISUP cause value in FLXCMAP table must be provisioned to Yes so as to perform re-routing

SOC option ISP70008 must be ON state so as to be provisioned RTEADV field in FLXCMAP table. So this feature is dependent on activation of SOC option ISP70008.

Figure 3 shows an example for datafill of table FLXCMAP.

Figure 2 Design Flow of The Feature

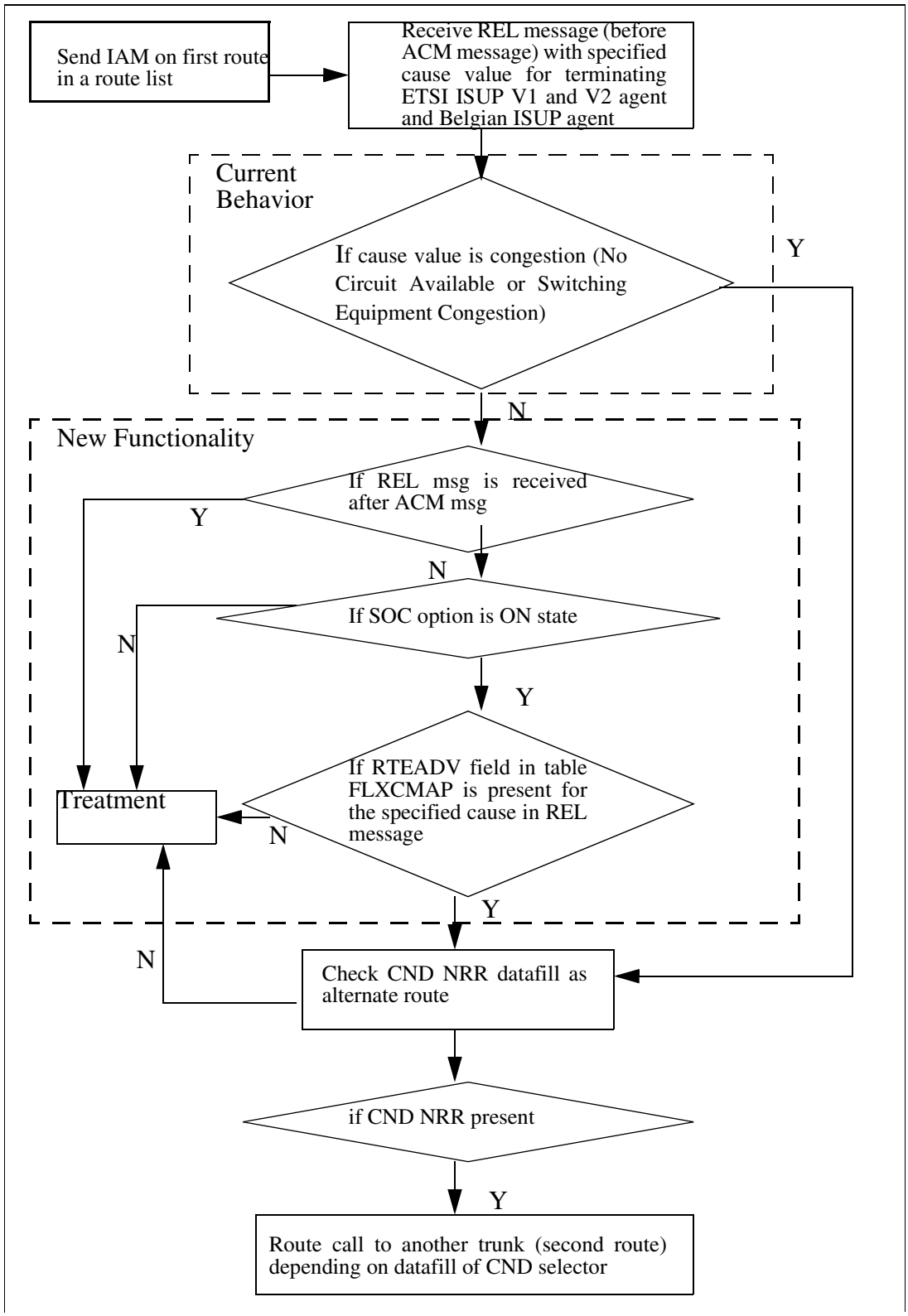


Figure 3 Example for FLXCMAP Table Datafill

```
CSEMPKEY                        TREAT          RTEADV
- - - - - - - - -              - - - - - -    - - - - - - -
USERBUSY   CCITT_STANDARD      BUSY           Y
NOCIRCAV   CCITT_STANDARD      NCRT           Y
```

59.2.4 Provisioning CND NRR selector

CND NRR selector must be provisioned in the route list at the terminating side for re-route. In figure 4, it is given an example for datafill of route table.

Figure 4 Example for Route Table Datafill

```
XLANAME        RTEREF      RTELIST
- - - - - - - - -  - - - - - - -  - - - - - - -
TEXTXLA        10          S TRUNK1
                           S TRUNK2

TEXTXLA1       12          S TRUNK3
                           S TRUNK4
                           CND NRR SK 0
                           S TRUNK5
```

Note: The routing tables that support the CND NRR selector include: XXRTE, OFRX, IBNRTX tables.

59.3 Hardware Requirements or Dependencies

None

59.4 Software Requirements or Dependencies

- Feature C59015296 must be active for re-route since SOC option ISP70008 is implemented by C59015296 feature.
- SOC option XLAS0053 must be on for activation of this feature
- This feature is patched backed to ISN04. The patch ID is NAP45. NAP45 is an password activateble patch. When NAP45 is active, for an ONP from ISN04 to ISN07 and beyond, the state of the SOC option XLAS0053 will automatically be set to 'ON'. And all of the functionalities of this feature will be ON. But after the ONP, a password for SOC option is still required to change the RTU field of the SOC option XLAS0053 in loads ISN07 and beyond.

59.5 Limitations and restrictions

Since this is enhancement in feature A59013395, it's limitations and restrictions are valid for this feature too. These are two items as follows:

- Rerouting will not be supported when REL message with ISUP cause value is received after an ACM (PostACM).
- It should be noted that re-routing will be limited to a specific number of route attempts(8 re-routing attempts). It is possible that the datafill may cause an infinite re-routing to occur, if the datafill is such that we are trying to select the already congested trunk.

Furthermore, following limitation and restriction will be valid for this feature.

- Whilst this functionality should work for terminating agents ETSI ISUP V1, ETSI ISUP V2 and all national ISUP variants based on ETSI V1 / V2, it is only being validated for use with terminating agents ETSI ISUP V1, ETSI ISUP V2 and Belgian ISUP.

59.6 Interactions

59.6.1 IN Functionality

In a call where IN is involved, current behavior is such that, if the received ISUP Release Cause Value is mapped in Table CSEDPMAP to an EDP for which IN has requested reporting, this ISUP Release Cause is passed to IN via the EDP value depending on this CSEDPMAP table. The EDP values involved for our purposes may be as follows:

- EDP-4 (Route _Select_Failure) RSF can be aimed to detect a failure to route a call to a final destination. In the current functionality, Congestion Cause Value is mapped to RSF.
- EDP-5 (o_Called_Party_Busy) For Called Party being Busy
- EDP-9(o-Disconnect) For Called Party Disconnecting

Currently, the IN behavior for Congestion Cause Value (No_Circuit_ Available_ or Switching Equipment Congestion) does not check CSEDPMAP table and reattempts translation with CND NRR selector. In other words, IN involvement is skipped. This behavior for Congestion Cause Value is kept as it is.

With this feature, the interaction of the IN functionality with the CND NRR selector for other ISUP Release Causes will be as follows:

1. If the related ISUP Release Cause has a mapping to an EDP in Table CSEDPMAP:
   - I*f the SCP has requested reporting of this EDP*: The handling will be left to IN, and the EDP will be reported to the SCP.
   - I*f IN has not requested the reporting of this EDP*: CND NRR selector will be functional.
2. If the related ISUP Release Cause does not have a mapping to an EDP in Table CSEDPMAP: CND NRR will be functional.

59.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

59.8 Glossary

Term	Description
IAM	Initial Address Message
ISUP	ISDN User Part
ETSI	European Telecommunications Standards Institute
SOC	Software Optionality Control
EDP	Event Detection Point
CND NRR	Network Re-Routing Conditional Selector

60: Functional Description (FN): A00003695

60.1 Feature name

AT.A00003695 - ANSI ISUP FGD on CS2K

60.2 Description

This activity provides ANSI ISUP FGD functionality on CS2K international load. This is done by porting the functionality of existing TDM MMP 17 feature with actid AT.59036475 into the ISN load.

The purpose is to enable CS2K with ISN load to directly interconnect to Inter Exchange Carriers (IEC) in North America.

This activity verifies the following agents interworkings only:

- ANSI ISUP FGD to/from ANSI ISUP FGD
- ANSI ISUP FGD to/from ETSI ISUP V1

60.3 Hardware Requirements or Dependencies

None

60.4 Software Requirements or Dependencies

None

60.5 Limitations and restrictions

Following interworkings are not verified with this activity:

ISUP V2 - ANSI ISUP FGD

ANSI ISUP FGD - ISUP V2

ANSI ISUP+ - ANSI ISUP FGD

ANSI ISUP FGD - ANSI ISUP+

ANSI ISUP FGD - ITU-R2

ITU-R2 - ANSI ISUP FGD

60.6 Interactions

Following interactions will be verified with this activity:

- ANSI ISUP FGD - ANSI ISUP FGD
- ANSI ISUP FGD - ETSI ISUP V1
- ETSI ISUP V1 - ANSI ISUP FGD

60.7 Applicable customer facing sections

The reader is referred to the FN of the original MMP feature (Ref a).

60.8 Glossary

ETSI	European Telecommunications Standards Institute
FGD	Feature Group D
ISUP	ISDN User Part
ITU	International Telecommunication Union
IXC	Inter Exchange Carrier

60.9 References

a. FN document of the activity A59036475.AA18 (in pls fmdoc)

61: Functional Description (FN): A00003696

61.1 Feature name

G-ISUP ROUTING ENHANCEMENTS

61.2 Description

This feature focuses on the routing enhancement for Deutsche Telecom G-ISUP, using the new national parameter UKK (#F5).

Additionally it also covers the

- Identification procedures for T-ISUP.
- Capturing of Originating ISC point Code.
- Blocking of Connected Number and Calling Party Number based on presentation indicator

These are described in the subsection below

61.2.1 Routing Enhancement for DTAG GISUP

DTAG Specifications introduces a new field Kundenkennung (KK) i.e Customer ID for the special routing.

KK is field in the national Parameter UKK, received in the IAM, from DTAG network.

The special routing is based on the following Criteria.

- Customer ID
- Destination
- IPI
- TMR

61.2.1.1 Routing based on Kundenkennung

To provide the ability to allow a different routing depending on the special routing criteria, the call control and universal screen framework is used (A59028780, A59033687). This frame work already provides the ability to route depending on BC and IPI.

Since TMR and BC are correlated, we use the BC screening, in place of the TMR screening,

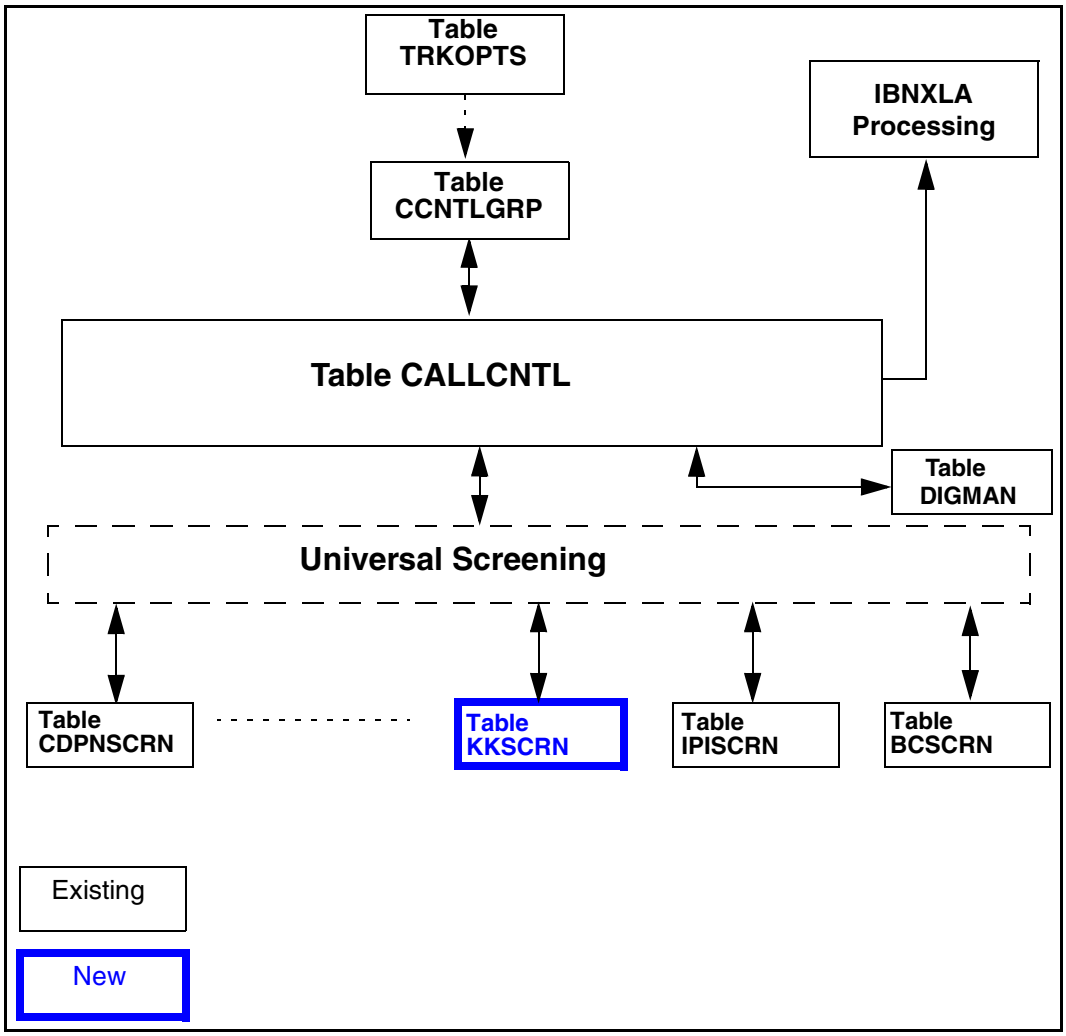
Table 1 TMR - BC correlation

TMR	BC
TMR_SPEECH	BC_SPEECH
TMR_64KB_UNRES	BC_64K_DATA
	BC_7_KHZ: ITC -GEN_ITC_DIG_TONES_ANNOUNC or GEN_ITC_7_KHZ_AUDIO
TMR_3_1KHZ_AUDIO	BC_3_1_KHZ
TMR_ALT_SPEECH_64KB_UNRES	BC_64K_DATA
TMR_ALT_64KB_UNRES_SPEECH	BC_64K_DATA
TMR_64KB_PREFERRED	BC_64K_RES

Table 1, “TMR - BC correlation,” on page 1271 captures the correlation of TMR and BC. The value TMR_64KB_UNRES, has different BC values based on ITC, hence TELCO will have to provision both these BC values for handling TMR_64KB_UNRES.

A new Table KKSCRN is created to store the KK values and the framework is extended to also allow routing dependent on KK. Please refer to “Figure 1 Call control and Universal screening Tables” on page 1272.

Figure 1 Call control and Universal screening Tables



The screening framework provides a flexible structure for modifying translations. For the purpose of DTAG, the recommended usage is as follows:

An entry screen index is datafilled against the trunk group and the table to screen against first (KKSCRN). The format of the table is as shown “Table 2 Format of Table KKSCRN” on page 1272

Table 2 Format of Table KKSCRN

Field	Range of Values	Description
SCRN_KEY	Any valid index from table CALLCTNL	Key Field: Index from table CALLCNTL
KK	KK value {0-16383}	Key Field: Kundenkennung.

Table 2 Format of Table KKSCRN

Field	Range of Values	Description
NEWSCRN_KEY	Any valid index in table CALLCNTL	Updated CALLCNTL Index
CALLCNTL_OPTIONS	Call Control Options: CUSTGRP, TREAT, POECNAME, DIGEDIT, CLICNTL.	Allows setting of call processing variables or treatment as performed in table CALLCNTL

1. The KK for the call is used along with this screen index to look up the entry in table KKSCRN. This entry can specify a customer group to use for translations (if no other BC or IPI specific routing is required), or a new screen index and the next screening table (IPISCRN).
2. The IPI for the call is used along with the current screen index to look up the entry in table IPISCRN. This entry can specify a customer group to use for translations (if no other IPI specific routing is required), or a new screen index and the next screening table (BCSCRN).
3. The BC for the call is used along with the current screen index to look up the entry in BCSCRN. This entry specifies the customer group to use for translations.

The datafill is as shown in Figure 2, "Sample datafill for KK/IPI/BC routing"

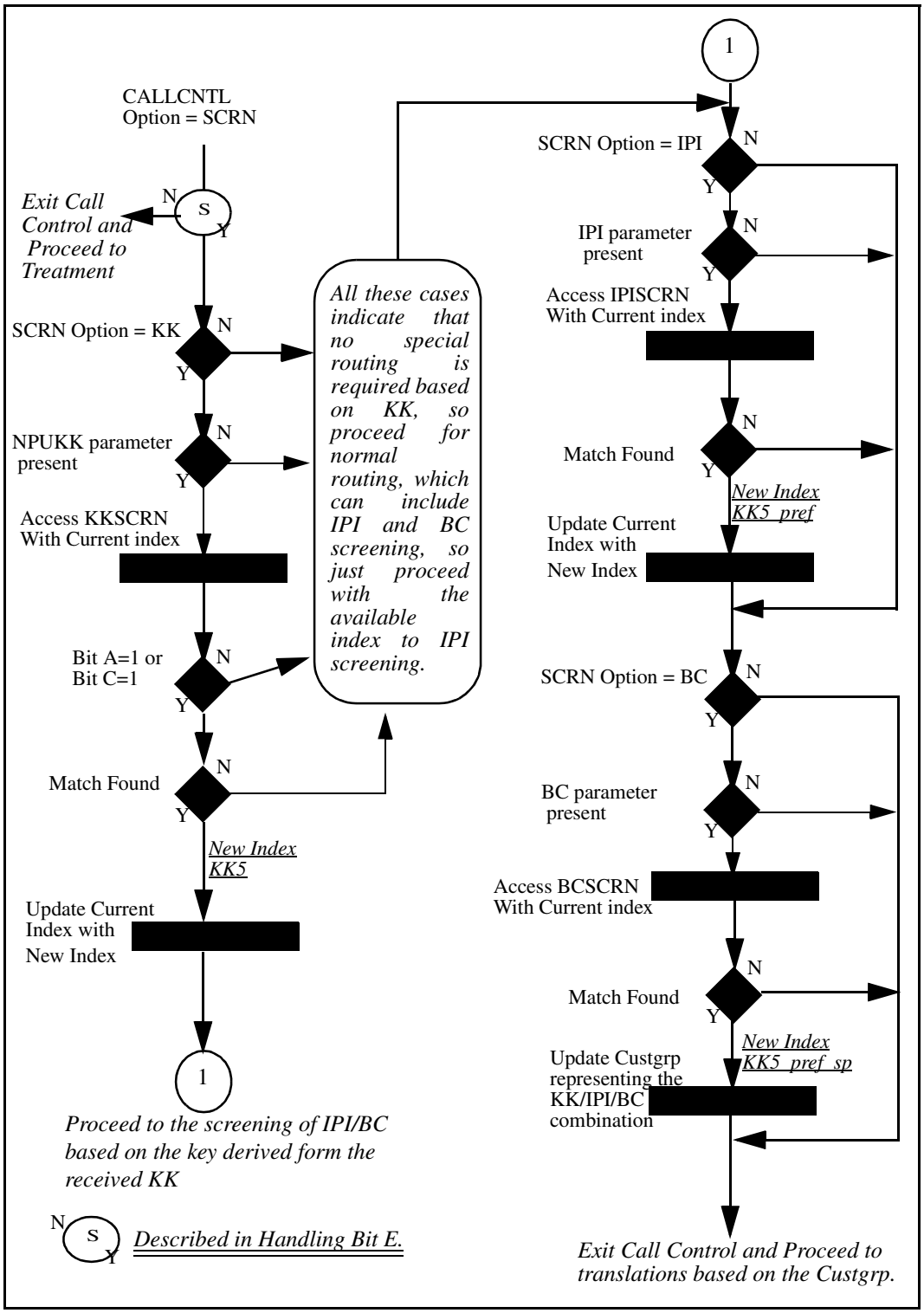
Figure 2 Sample datafill for KK/IPI/BC routing

```
TABLE TRKOPTS
STEP27ISUPV2 CCNTLIDX CCNTLIDX INDEX

TABLE CALLCNTL
INDEX (SCRN (KK) (IPI) (BC) $)$

TABLE KKSCRN
INDEX 5 KK5 $

TABLE IPISCRN
KK5 PREFERRED KK5_PREF $

TABLE BCSCRN
KK5_PREF SPEECH KK5_PREF_SP (CUSTGRP
KK5_PREFERRED_SPEECH_CUSTGRP1) $
```

The end result is that the customer group for the call can be specified uniquely for each KK/IPI/BC combination. These customer groups can each have their own translations defined.

The special routing will be invoked based if either Bit A = 1 or Bit C = 1 is set in the message, else it proceeds for Normal routing.

Figure 3 Flow Diagram for KK screening.



The flow diagram as shown in Figure 3, "Flow Diagram for KK screening." captures the screening (routing) done based on the sample datafill for KK/IPI/BC combination.

The flow captures only a part of the screening framework, concentrating on the KK screening.

In cases where special routing is not required, the flow would proceed to normal routing. If the normal routing requires the IPI and BC to be screened, then IPISCRN tables and BCSCRN table should have provisioning to handle the index provisioned in Call Control table.

The translation for updated custgrp are set to route the call based on the called party number to a restricted routelist, as needed by the special routing KK/IPI/BC combination.

Interworking of Customer Id screening with other possible screening options may lead to incorrect result, if the index are not handled properly. This may even lead to have no KK screening done in spite of the UKK parameter available in the IAM.

61.2.1.2 Handling of failures for special routing

The routelist obtained after screening of KK/IPI/BC, restricts the available routes as compared to the default routes.

In cases where this special routing fails, the decision to fall back to the default routing is based on capabilities provided.

This is handled by adding all the default routes to routelist for the customer groups where the customer ID demands to fall back to the default Routing.

The example below details the handling.

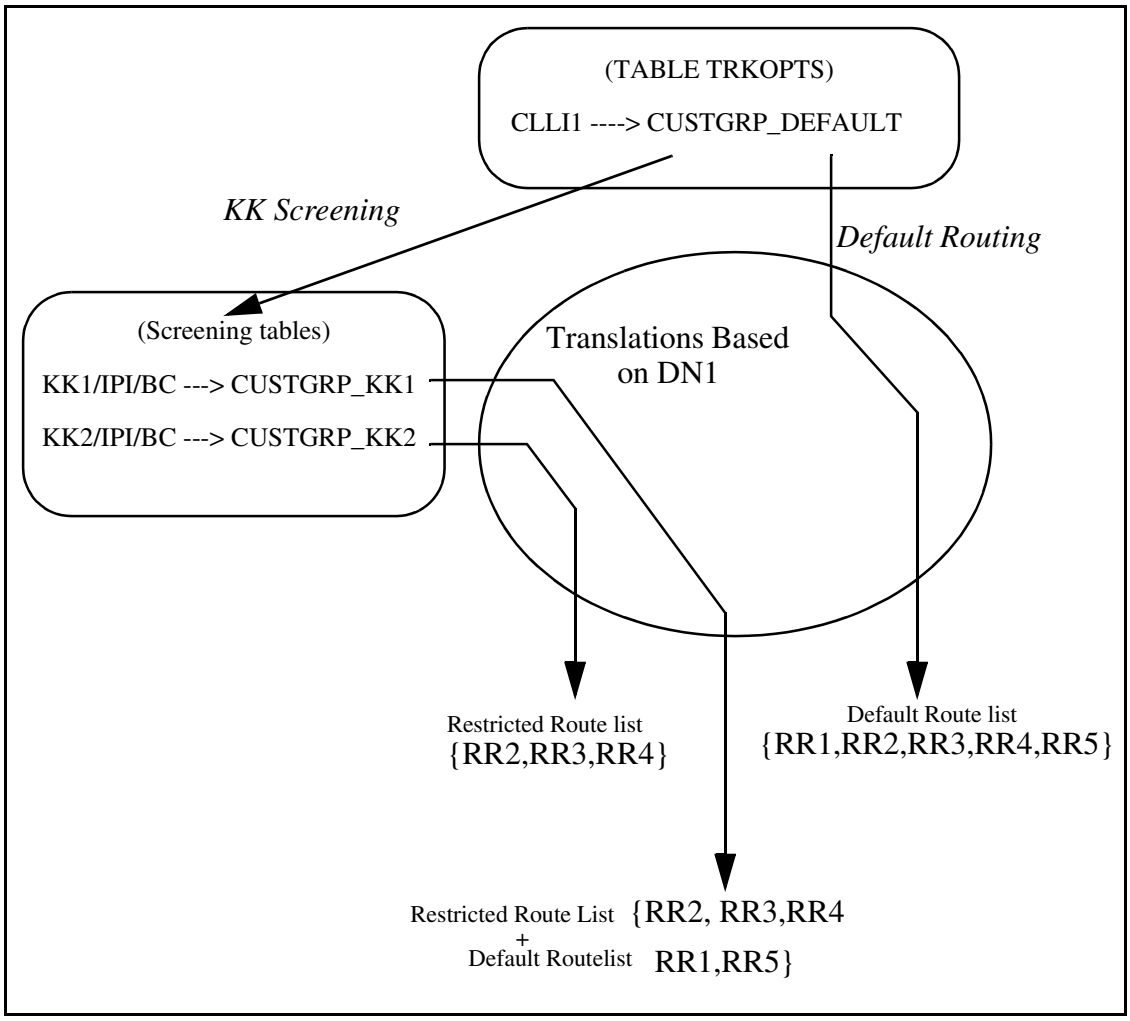
Scenario

- The default routelist for all customers with calls coming on Trunk CLLI1 for Called party number DN1 is {RR1, RR2, RR3, RR4, RR5}
- For the customers with Kundenkennung KK1 and KK2 the routes are restricted to {RR2,RR3,RR4}.
- But customer with KK1 have the facility to fallback back to the default routing when special routing to the restricted routelist fails.

Provisioning

The provisioning for the above scenario is as explained in the Figure 4 on page 1277.

Figure 4 Provisioning for special routing.



61.2.1.3 Capacity for provisioning of Kundenkennung

The Feature approach suggested derives the Customer group, based on the KK/ IPI/BC combinations. The Translations system completes the further routing based on the called number using Customer Group as index.

With the current provisioning capacity, total number of customer groups allowed is 4094.

In a completely unoptimized system, the resulting combinations can lead to 64000 KKs x 3 IPIs x 11 BCs = 2,112,000 different routing systems. This far exceeds the abilities of the CS2K XLA system.

But the realistic requirement specifics the International Gateway should support an average of 1000 Customer ID (KK), 80 destinations per customer group and an average of 2 IPI/BC combinations per destination. Since the screening of destination is done in translations, we do the IPI/BC screening before the destination. Thus the system will provide support for all 9 combinations of IPI/TMR. This results to 9000 customer group, which is beyond the current capacity of 4086.

But it is expected that there will be a significant number of combinations of KK/IPI/BC that result in the same routing. For example, two KK may share the same routing or one KK may have one routing for all IPI/BC combinations. Refer to the Appendix section “61.9.1 Example Datafill Setup” on page 1295 for examples of how this can be done.

61.2.1.4 Handling of the Bit E

In addition to special routing, the UKK parameter also provides information regarding bypassing the Black List numbers using Bit E (Blocking Indicator). If bit E = 1, then the black list will be ignored.

Screening for Bit E is handled by providing an additional screen option UKKCDPN in the table CALLCNTL. This option will use the existing CDPNSCRN table in conjunction with bit i.e it will not perform CDPN screening if the bit E is set to 1.

Figure 5 Table CALLCNTL(UKKCDPN option)

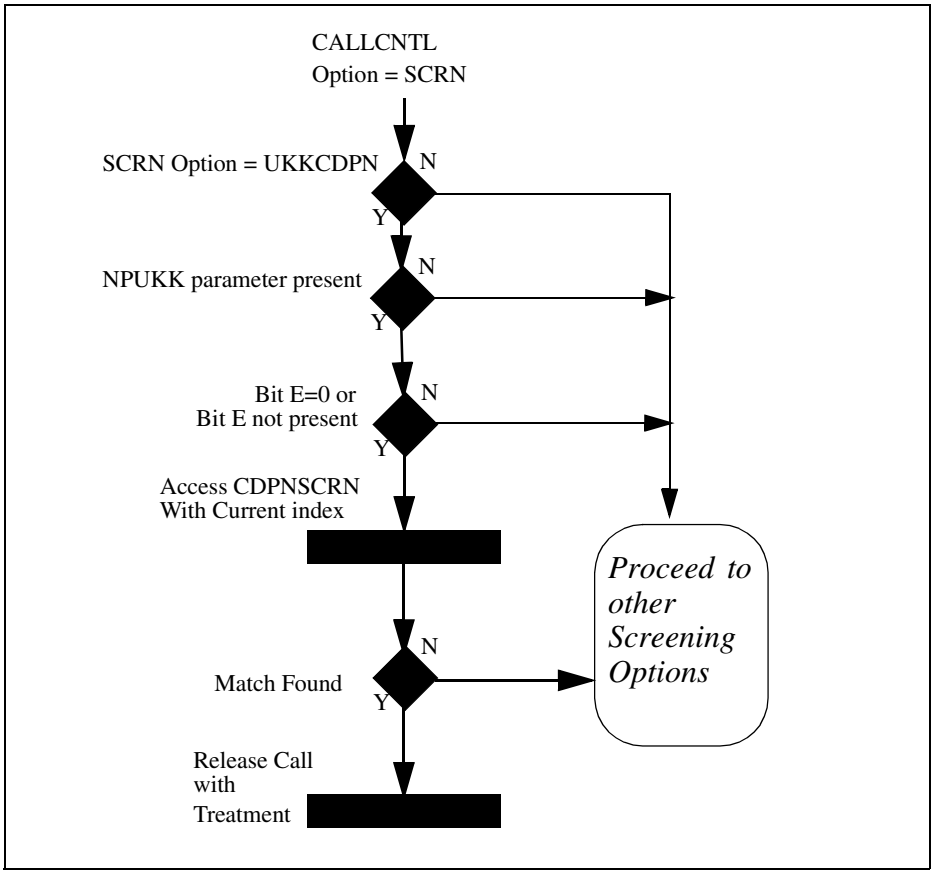
```
TABLE: CALLCNTL
CALCTL_KEY CALCTL_OPTIONS
-------------------------
ENTRY (SCRN (UKKCDPN ) (KK ) (IPI ) (BC ) $)$
```

Figure 6 Sample datafill for table CDPNSCRN

```
TABLE TRKOPTS
STEP27ISUPV2 CCNTLIDX CCNTLIDX INDEX

TABLE: CALLCNTL
ENTRY (SCRN (UKKCDPN ) (KK ) (IPI ) (BC ) $)$

TABLE: CDPNSCRN
ENTRY (1)
.................SUBTABLE CDPNDATA
003336 003336 NO_KEY (TREAT PDIL) $ $

TABLE KKSCRN
INDEX 5 KK5 $

Proceed as described in sample datafill for KKSCRN
```

The flowchart for the above datafill is as shown in Figure 7 on page 1279

Figure 7 Handling of Bit E



61.2.1.5 Setup of UKK

The UKK parameter needs to be setup trunk based, for incoming International calls coming on GISUP/V1 trunks.

This capability is provided by providing a new option in table TRKOPTS.

The Option will allow the complete parameter to be provisioned, as per it's specification. Please refer to "Figure 8 NP.UKK parameter layout" on page 1280.

Figure 8 NP.UKK parameter layout

8	7	6	5	4	3	2	1	
Ext.i	G	F	E	D	C	B	A	
Ext.i	Kundenkennung (customer ID)							Kundenindikator (customer indicator)
Ext. i	Dienst-Typenkennung (type of service ID)							Registrierungsindicator (registration indicator)

The OPTINFO will contain, fields, representing from A to G, the Customer ID (Kundenkennung) and the Service ID.

Please refer to section 3.118 of TISUP Q.763 for :-

- **parameter NP.UKK and its fields.**
- **coding of Kundenkennung (customer ID)**

Figure 9 Table TRKOPTS (UKK option)

```
TABLE: TRKOPTS
OPTKEY                              OPTINFO
-----------------------------------------------
STEP27ISUPV2 UKK     UKK 1 0 0 0 0 0 0 100 0
```

The provisioned parameter will only be used to transit it in outgoing IAM on TISUP (National trunks) or GISUP (sipt) and not for routing.

The provisioning of the NPUKK on the trkopts is allowed on all ISUP trunk AGent. But interworking are currently supported only for GISUP,TISUP, ETSI V2 and ETSI V1 trunks.

Note: Bit A to E can take values '0' or '1' . Bit F and Bit G are spare bits and hence accept value '0' ONLY

The format of trunk option NPUKK is given below:

Table 3 Format of trunk option NPUKK

Field	Range of Values	Description
UKK_SPECIAL_ROUT_IND	{ 0 to 1}	Bit A of octate 1 (NP.UKK)
UKK_SPECIAL_ZONE_IND	{ 0 to 1}	Bit B of octate 1 (NP.UKK)
UKK_SPECIAL_INTL_CAR_IND	{ 0 to 1}	Bit C of octate 1 (NP.UKK)
UKK_SPECIAL_NTL_CAR_IND	{ 0 to 1}	Bit D of octate 1 (NP.UKK)
UKK_SPECIAL_BLOCK_IND	{ 0 to 1}	Bit E of octate 1 (NP.UKK)
BIT_F_SPARE	{ 0 to 1}	Bit F of octate 1 (NP.UKK)
BIT_G_SPARE	{ 0 to 1}	Bit F of octate 1 (NP.UKK)
KUNDENKENNUNG	{0 to 16383}	Octate 2 & 2a (NP.UKK)
REGISTRIERUNGS_INDICATOR	{0 to 127}	Octate 3 (NP.UKK)

61.2.1.6 Interworking for NP.UKK

The table below captures the Interworking for the NPUKK parameter.

Since the NPUKK parameter is only built for TISUP and GISUP-T. The interworking having these trunks as outgoing are considered.

Table 4 Interworking For NPUKK

Interworking	NPUKK on the outgoing end.
GISUP->TISUP	Built if provisioned on the GISUP
ETSI V1->TISUP	Built if provisioned on the ETSI V1
ETSI V2->TISUP	Built if provisioned on the ETSI V2
GISUP(sipt)->TISUP	If NPUKK is received in IAM, then it is transited, otherwise built if provisioned on GISUP(sipt)
TISUP -> TISUP	If NPUKK is received in IAM, then it is transited, otherwise built if provisioned on TISUP
TISUP -> GISUP(sipt)	If NPUKK is received in IAM, then it is transited, otherwise built if provisioned on TISUP
ETSI V1 -> GISUP(sipt)	Built if provisioned on the ETSI V1

Table 4 Interworking For NPUKK

Interworking	NPUKK on the outgoing end.
ETSI V2 -> GISUP(sipt)	Built if provisioned on the ETSI V2
GISUP(sipt) -> GISUP(sipt)	If NPUKK is received in IAM, then it is transited, otherwise built if provisioned on GISUP(sipt)
GISUP->GISUP(sipt)	Built if provisioned on the GISUP

61.2.1.7 Translation Verification Tool Support

The TRAVER tool is updated to support the new screening options, KK and UKKCDPN.

Figure 10 on page 1283 and Figure 11 on page 1284, shows the traver output involving KK and UKKCDPN screening, where Bit E is set to 1, hence the CDPN table is skipped.

Figure 10 Example Traver for UKKCDPN,KK screen

```
>traver tr step27isupv2 0033391234 b
TABLE TRKGRP
STEP27ISUPV2 IBNT2 0 NPDGP NCRT STEPDEFAULT 0 ASEQ 0 7848810022
ANSDISC 0 N N N
    N N N N 0 0 N 0 0 0 0 N N N N N N N N N NATL (BCNAME 3_1KHZ) $
TABLE TRKOPTS
STEP27ISUPV2 CCNTLIDX CCNTLIDX ENTRY
TABLE CALLCNTL
ENTRY
    (SCRN (UKKCDPN) ( KK ) (IPI ) (BC ) $)$
PLEASE ENTER VALUE FOR NPUKK:
>PRESENT
PLEASE ENTER VALUE FOR ENTER BIT E:
>BIT_E_1
PLEASE ENTER VALUE FOR SPECIALROUTING INDICATOR
>1
PLEASE ENTER VALUE FOR KUNDENKENNUNG:
>5
 .  . TABLE KKSCRN
 .  . ENTRY 5 KK5 $
PLEASE ENTER VALUE FOR ISDN PREFERENCE INDICATOR:
>preferred
 .  . TABLE IPISCRN
 .  . KK5 PREFERRED KK5_PREFERRED $
PLEASE ENTER VALUE FOR BEARER CAPABILITY:
>speech
 .  . TABLE BCSCRN
 .  . KK5_PREFERRED  SPEECH   KK5_PREFERRED_SPEECH  (CUSTGRP
RUADEFAULT) $
 . TABLE CALLCNTL
 . TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
RUADEFAULT 0 0 0 RUTRK $
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND
DIGCOL
RUADEFAULT NXLA RUADEF NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME RUADEF
TUPLE NOT FOUND
Default from table XLANAME:
RUADEF
    (NET N N 0 N NDGT N N DOD N 69 NPRT_2 NLCA_NILLA_1 NONE $) $ F
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
69 NLCC NONE NT 1 1 NILSFC 0 PX RUAINTL NIL 00 NPRT_10 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
```

Figure 11 Example Traver for UKKCDPN,KK screen (continued)

```
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
RUAINTL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
0033481111
TABLE PXCODE
RUAINTL 00 00 CONT ( PF 2) ( CLASS INTL) ( CONSUME 2) ( XLT CT
RUAXLCT)$
TABLE CTHEAD
RUAXLCT DFLT RTE ( DEST 100)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
33481111
TABLE CTCODE
RUAXLCT 334 334 RTE ( PF 3) ( MM 4 18) ( DEST 14) ( LNET INTERNAT)
( MZONE 3)$
TABLE: CTRTE
KEY:  RUAXLCT   14
 . S RUA14ISUPV2LP
EXIT TABLE CTRTE
TABLE TRIGGRP
DFLTGRP INFOANAL
 . GENTRIG ( CDPN TDP3INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++
DIGIT TRANSLATION ROUTES

1 STEP39ISUPV2          0033491111                  ST

TREATMENT ROUTES.  TREATMENT IS: GNCT

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 12 on page 1285 shows the traver with UKKCDPN screening, with Bit E=0 and the dialed number is in the black list.

Figure 12 Example Traver for UKKCDPN scrn, with Bit E=0

```
>traver tr STEP25ISUPV2 0033361111 b
tABLE TRKGRP
STEP25ISUPV2 IBNT2 0 NPDGP NCRT STEPDEFAULT 0 ASEQ 0 7848810020 ANSDISC
0 N N N
    N N N N 0 0 N 0 0 0 0 N N N N N N N N N NATL (BCNAME 3_1KHZ) $
TABLE TRKOPTS
STEP25ISUPV2 CCNTLIDX CCNTLIDX ENTRY
TABLE CALLCNTL
ENTRY
    (SCRN (UKKCDPN) ( KK ) (IPI ) (BC ) $)$
PLEASE ENTER VALUE FOR NPUKK:
>PRESENT
PLEASE ENTER VALUE FOR ENTER BIT E:
>BIT_E_0
 .  . TABLE CDPNSCRN
 .  . ENTRY (1)
 .  . SUBTABLE CDPNDATA
 .  . 0033361111 0033361111 NO_KEY ( TREAT PDIL)$ $

+++ TRAVER: TREATMENT SET +++
```

61.2.2 Identification procedures for T-ISUP

DTAG specifications enhances the current IDR-IRS functionality for Gateway switch by

- Introducing additional timer T39A
- Additional Identification procedures.

The Timer T39A functionality is covered by the feature A00002908.

This feature covers the additional Identification procedures. DTAG enhances the Identification procedure by adding two new messages.

— NANA (#FF)

— EHZA (#FC)

The procedures are described as below.

61.2.2.1 Procedures for Incoming international Call, terminating on DTAG network (for G -> T and V1 -> T).

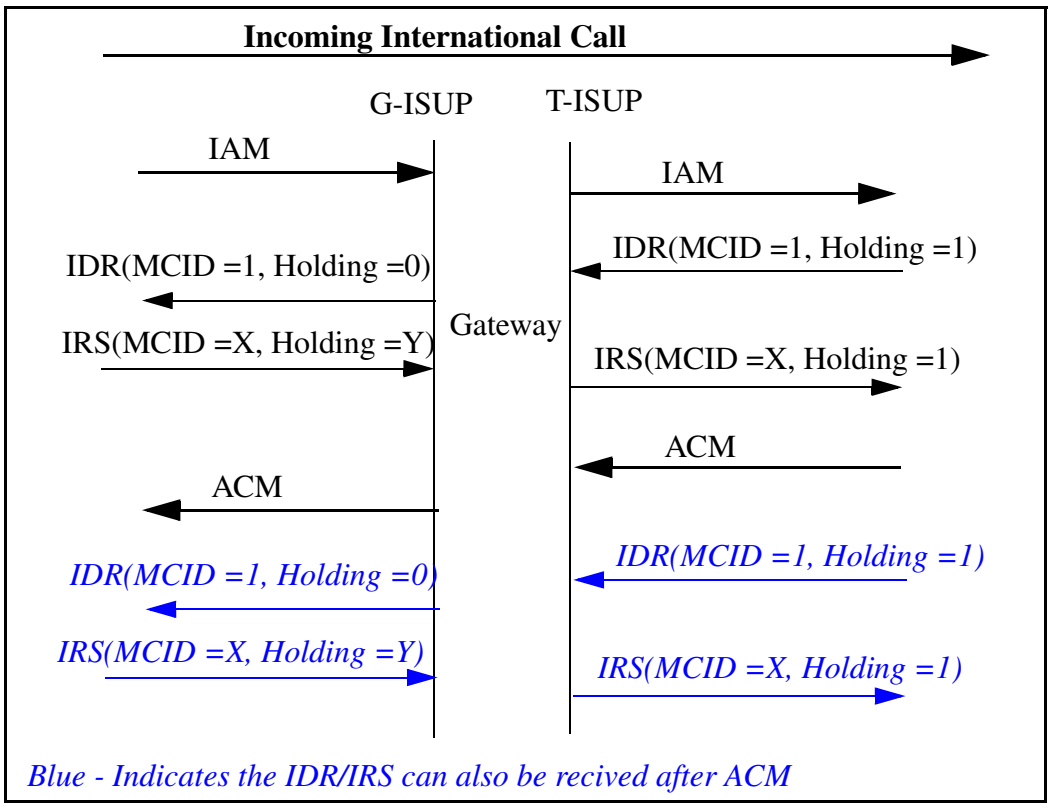
61.2.2.1.1 Activation The enhanced identification procedures are activated by receiving the IDR with Holding bit set to 1. DTAG requires the flexibility that the IDR can be received before or after ACM. The Outgoing IDR on the International gateway will always have the holding Indicator set to zero.

The IRS received from the International network, will be transited to the National network, with Holding Indicator as received in the in IDR. Please

refer to “Figure 13 Transit of IDR-IRS on International Gateway.” on page 1286.

Note: The Timer T39A and the procedures associated with it are not shown in the Figure, to make it simple.

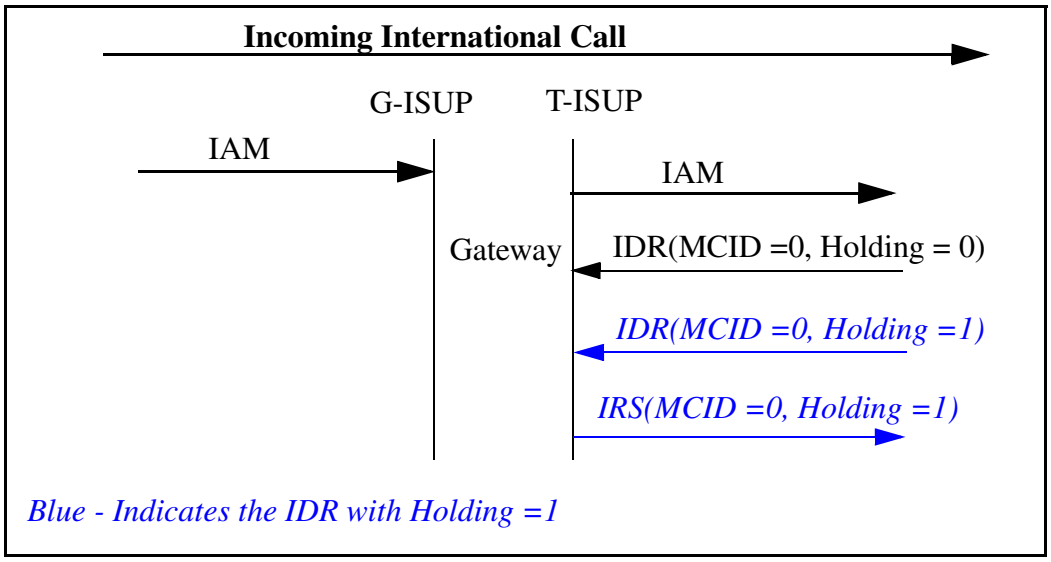
Figure 13 Transit of IDR-IRS on International Gateway.



If the received IDR has MCID indicator set to zero, i.e **MCID not requested** and Holding Indicator set to zero i.e. **Holding not requested** , **then the IDR is discarded and is NOT responded with a IRS.**

If the received IDR has MCID indicator set to zero, i.e **MCID not requested** and Holding Indicator set to one i.e. **Holding requested** , then the IDR is not transited to the International network. **Also the CS2K responds with a IRS message (MCID response Indicator bit set to zero and Holding Bit set to one) and holding procedures are activated on the Avst. Figure 14, "IDR-IRS behavior for MCID Indicator to 1" captures this behavior.**

Figure 14 IDR-IRS behavior for MCID Indicator to 1



In cases where the incoming International call is from ETSI ISUP V1. The IDR received will be responded with IRS, by TISUP and the holding procedures will be activated based on the holding indicator bit.

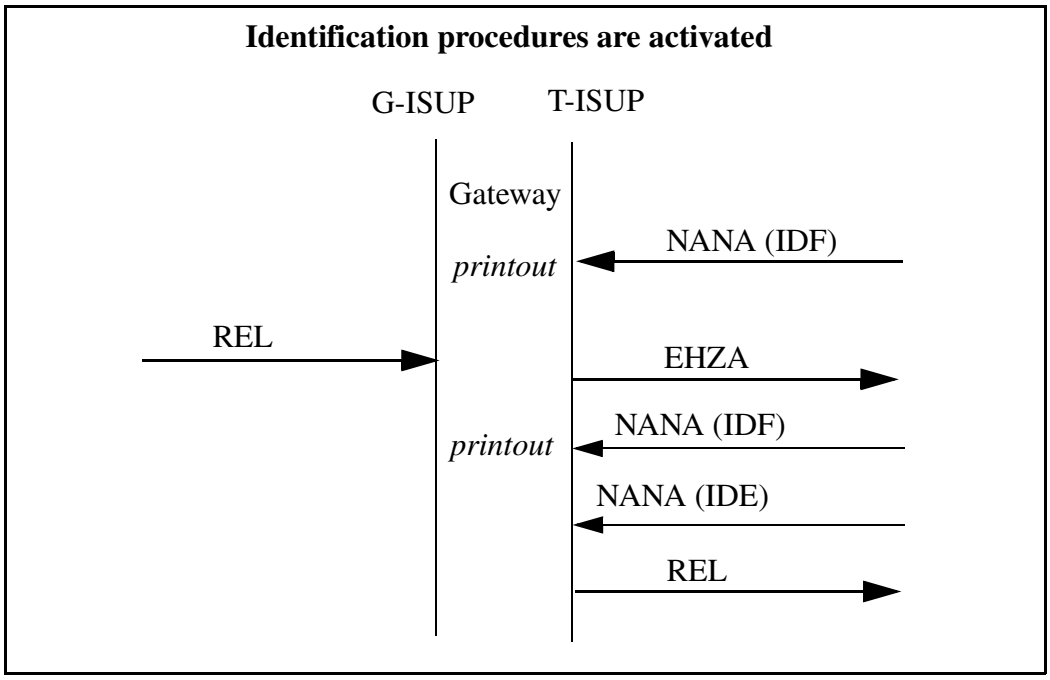
61.2.2.1.2 Behavior for Identification Once the procedure is activated, the NANA message is handled as below.

When a NANA message is received with Message Indicator field in NP.FF set to IDF, the identification data will be printed. The the content of the printout is analogous to the printout of the ETSI MCID service". Hence a new report MCID 600 is added to the MCID log. This log will be generated will be generated on the receipt of the NANA message. The content of the log is as shown in Figure 15, "MCID Log capturing printout for Identification"

Figure 15 MCID Log capturing printout for Identification

```
AVST1_LOG     MCID600 DEC09 18:12:57 5700 INFO IDENTIFICATION DATA
        Calling_Agent  : CKT     STEP36ISUPV2  628
        Called_Agent   : CKT     STEP39ISUPV2  632
        Calling_Number : 7848810036
        Called_Number  : 003349777799
        Date : 09.12.2003
        Time : 18:12:57
```

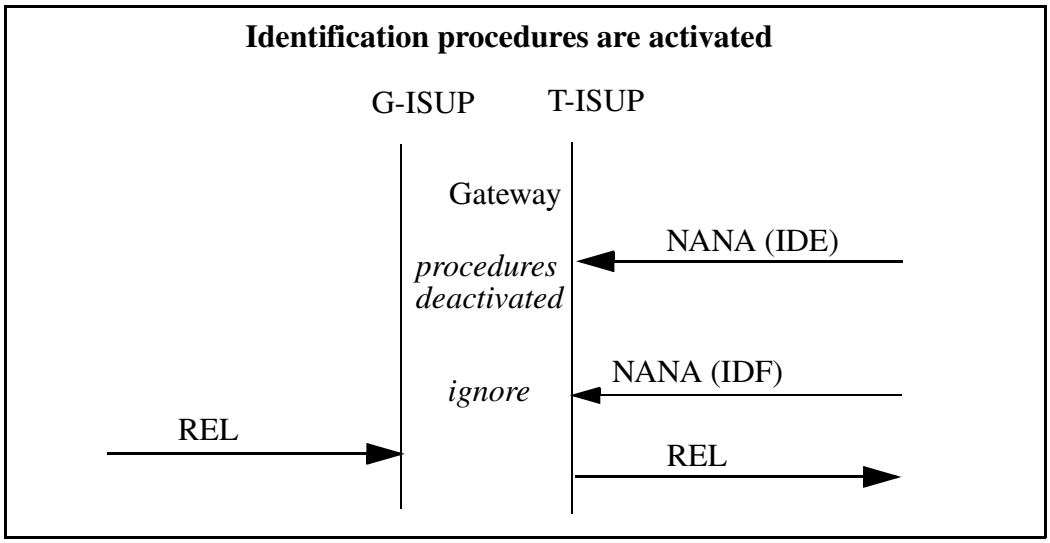
Figure 16 Behavior for Identification.



When Release is received from international side, it is not transmitted to national end. The new EHZA message is sent. The international call leg is disconnected while national leg remains active till NANA(IDE) is received. Any NANA(IDF) is received a printout will be generated as mentioned above. On receipt of NANA(IDE), a release message is sent if an EHZA message is already sent. Please refer to “Figure 16 Behavior for Identification.” on page 1288.

61.2.2.1.3 Deactivation The enhanced identification procedures are deactivated on the receipt of NANA message with the Message Indicator field in NP.FF set to IDE (Identification Ende). Any additional NANA (IDF) and NANA(IDE) message received is ignored.

Figure 17 Deactivation of Identification procedures

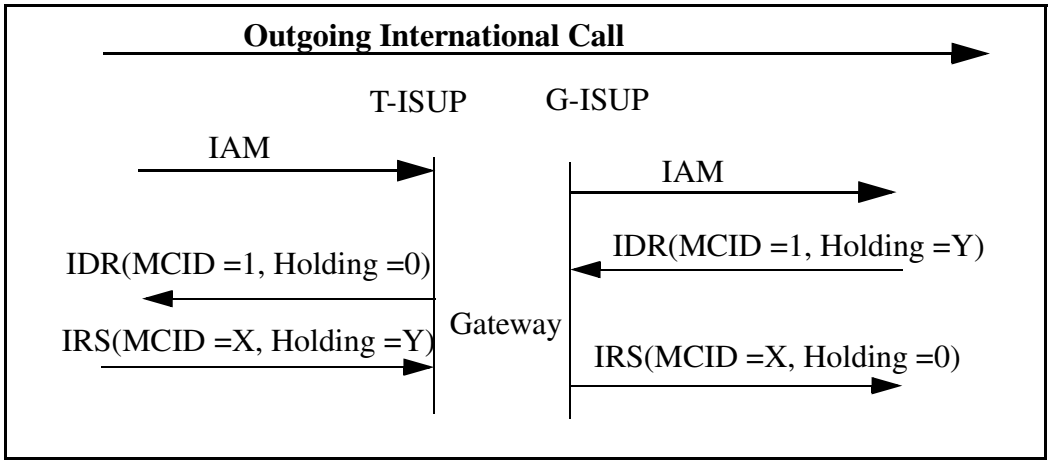


61.2.2.2 Procedures for Outgoing International Call from a DTAG network

For outgoing international calls from a DTAG network, the existing IDR-IRS functionality will be used for identification. no additional capability is being provided.

The holding indicator will be set to set zero when the IDR is transited to the national network and the response IRS will also have the holding bit set to zero, when it is sent on the International network. This is as shown in theFigure 18, "Procedures on outgoing International Gateway."

Figure 18 Procedures on outgoing International Gateway.



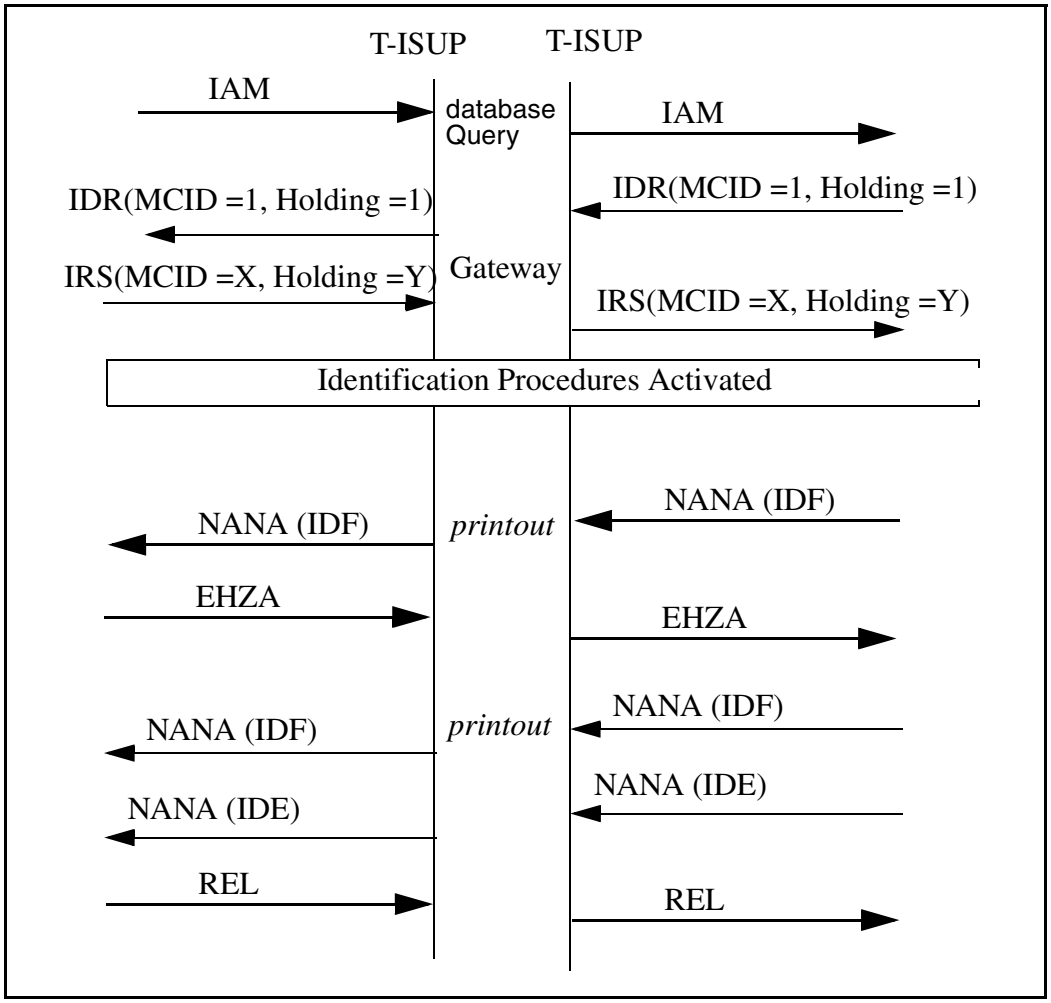
61.2.2.3 Procedures for TISUP - TISUP interworking.

For the procedures for the TISUP-TISUP scenario, Please refer to “Figure 19 .Behavior of TISUP-TISUP interworking.” on page 1290.

Note: The TISUP to TISUP interworking on the AVST is only possible, where the AVST acts as an SSP. Since MCID services are not directly related to the IN queries. Also the early ANM is currently not supported. The procedures described here are considering a normal TISUP -TISUP interworking.

All the messages NANA(IDE), NANA(IDF), EHZA will be transited. Identification procedures are also activated on the switch, NANA(IDF) will cause printout, NANA(IDE) will end the Holding. But these message will be transmitted. There is no release for EHZA.

Figure 19 .Behavior of TISUP-TISUP interworking.



61.2.3 Origination ISC Point Code

DTAG specifies that the origination ISC point code, for an international incoming call, to be captured for statistics purpose. This feature implements the capability to capture the point code and print in a log ISC600

The log is generally generated every 3hrs. It will print the first 480 point code and the count of calls received from that point code respectively.

Additionally, it will also provide a count of all the calls received on the point code. The output of the log based on the point code captured is as below

- For no Calls coming on GISUP to a national trunk

Figure 20 Log for ISC PC for no Calls

```
AVST1_LOG ISC600 NOV28 11:55:28 8900 INFO ISC log report
    Originating ISC point Code captured from NOV-28 11:54 to NOV-28 11:55
    ---------------------------------------------------------------
              No data captured

    ---------------------------------------------------------------
```

- For calls received with number of distinct point codes less than 480.

Figure 21 Log for ISC PC for few calls

```
AVST1_LOG ISC600 NOV28 11:55:28 8900 INFO ISC log report
    Originating ISC point Code captured from NOV-28 11:58 to NOV-28 12:25
    ------------------------------------------------------------------------------------------
    ISCPC Count   ISCPC   Count   ISCPC   Count  ISCPC Count  ISCPC Count
    ------------------------------------------------------------------------------------------
    100    5      150     1       230     1      250    1     16000  1
    16350  1      16400   1
    ------------------------------------------------------------------------------------------
```

- For calls received from distinct PC more than 480.

Figure 22 Log for ISC PC with received point codes more than 480

```
AVST1_LOG ISC600 NOV28 13:44:44 5472 INFO ISC log report
    Originating ISC point Code captured from NOV-28 13:43 to NOV-28 13:44
    ------------------------------------------------------------------------------------------
    ISCPC Count   ISCPC   Count   ISCPC   Count   ISCPC Count   ISCPC Count
    ------------------------------------------------------------------------------------------
    1     5       2       1       5       1       9     1       10    1
    100   5       150     1       230     1       250   1       300   1
    ..........................................

    2001  5       2608    1       3230    1       4250  1       9300  1
    16300 5       16301   1       16302   1       16303 1       16304 1
    ------------------------------------------------------------------------------------------
    PC not captured : 10
    ------------------------------------------------------------------------------------------
```

Note: The figures 18 and 19, shows the point codes and the their count to be left justified in their respective formatting space. In actual log these numbers are right justified.

This functionality is controlled via and Office parameter CAPTURE_ISC_OM, in table OFCENG.

61.2.4 Blocking of Connected Number and Calling Party Number

DTAG requires blocking of connected number and calling party number if the Address Presentation Restricted Indicator is set to “Presentation Restricted”. DTAG also requires the above functionality to be enabled / disabled via a trunk option.

This feature implements the above functionality by creating a new trunk option “BLK_CGPN_CONN” in table TRKOPTS. The option has to be set to “Y” for the functionality to be enabled.

An example of datafill for the option “BLK_CGPN_CONN” in table TRKOPTS is shown below:

Figure 23 datafill in table TRKOPTS

```
TABLE: TRKOPTS
STEP25ISUPV2    BLK_CGPN_CONN     BLK_CGPN_CONN     Y
```

61.3 Hardware Requirements or Dependencies

-NIL-

61.4 Software Requirements or Dependencies

-NIL-

61.5 Limitations and restrictions

61.5.1 Kundenkennung range

The screening frameworks allows up to 8191 indices.

- This implies that there can for each KK, there can be 8191 different routing paths specified. Similarly, for each BC or IPI, there can also be 8191 different routing paths specified.

The total number of customer groups allowed on a switch is 4094.

- This implies that there can only be a total of 4094 different routing systems to be shared between all KK/BC/IPI combinations.

This is not a limitation considering the current scope of the requirement, but would limit the system if the complete range of Kundenkennung is to provisioned.

61.5.2 Holding Indicator Bit

The Holding indicator bit for IRS from GISUP (SIPT) to TISUP, should be transmitted unchanged. This functionality would set it to the received value in IDR message, similar to GISUP (nonsipt) to TSIUP interworking.

61.5.3 SSP procedures

Procedures for Early ANM scenario are not covered.

61.5.4 Holding procedures for Network initiated SUSPEND timeout.

Currently the holding procedure for Network initiated SUSPEND timeout is not supported.

61.5.5 Calling party DN in IRS

The current design sends the Billing DN in the IRS , when we donot have a valid calling number available. This is incompliant with the MCID requirements of the Detusche Telecom.

To satisfy the requirement “It is recommended that the Billing DN is datafilled as $ and Table DEFNUM is NOT datafilled and trunk option DEFNUM is NOT used”

61.6 Interactions

This feature interacts with the screening of Number blocking features, where by the blocked numbers can be overridden with Bit E set to 1.

61.7 Applicable customer facing sections

Fault Management

- Logs __X____
- Alarms _____

Configuration

- Data Schema __X____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters ___X___

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

61.8 Glossary

Term	Explanation
BC	Bearer Capability
CDPN	Called Party Number
CS2K	Call Server 2000
DTAG	Deutsche Telekom AG
G-ISUP	Gateway ISUP
GWC	Gateway Controller
IAM	Initial address Message
IPI	ISDN Preference Indicator
ISC	International Switching Center
MCID	Malicious Call Identifier

NP	National Parameter
T-ISUP	Telekom ISUP
TMR	Transmission Medium Requirement
TRAVER	Translations Verification
UKK	UrsprungsKundenKennung
XLA	Translations

61.9 Appendix

61.9.1 Example Datafill Setup

The first table shows the No sharing of customer group (unoptimized) usage of the screening framework. The following tables provide some examples of the re-use that may occur because of common routing attributes for various IPI/KK/BC combinations. The final table shows the resulting datafill that would satisfy this example. Note that the in the worst-case scenario of this example, 18 customer groups would be required to specify the necessary translations. In the example optimization, only 3 are required because of re-use. Also note that only 2 screening indices were required for the optimized example, while in the unoptimized example, 9 would be required.

Table 5 No sharing of Customer Group

KK	IPI	BC	Resulting Customer Group
Default	Preferred	Speech	C01
		64K Data	C02
	Req	Speech	C03
		64K Data	C04
	Not Req	Speech	C05
		64K Data	C06
A	Preferred	Speech	C07
		64K Data	C08
	Req	Speech	C09
		64K Data	C10
	Not Req	Speech	C11
		64K Data	C12
B	Preferred	Speech	C13
		64K Data	C14
	Req	Speech	C15
		64K Data	C16
	Not Req	Speech	C17
		64K Data	C18

Table 6 KK Sharing

KK	IPI	BC	Resulting Customer Group
Default	Preferred	Speech	C01
		64K Data	C02
	Req	Speech	C03
		64K Data	C04
	Not Req	Speech	C05
		64K Data	C06
A B	Preferred	Speech	C07
		64K Data	C08
	Req	Speech	C09
		64K Data	C10
	Not Req	Speech	C11
		64K Data	C12

Table 7 IPI Sharing

KK	IPI	BC	Resulting Customer Group
Default	Preferred Not Req	Speech	C01
		64K Data	C02
	Req	Speech	C03
		64K Data	C04
A B	Preferred Req Not Req	Speech	C07
		64K Data	C08

Table 8 BC Sharing

KK	IPI	BC	Resulting Customer Group
Default	Preferred Not Req	Speech	C01
		64K Data	C02
	Req	Speech 64K Data	C03
A B	Preferred Req Not Req	Speech	C07
		64K Data	C08

Table 9 Customer Group Sharing

KK	IPI	BC	Resulting Customer Group
Default	Preferred Not Req	Speech	C01
		64K Data	C02
	Req	Speech 64K Data	C03
A B	Preferred Req Not Req	Speech	C01
		64K Data	C02

Table 10 KK Sharing

Initial SCRN Key	KK	KKSCRN Entry	New SCRN Key	IPI	IPISCRN Entry	New SCRN Key	BC	BCSCRN Entry	Resulting Customer Group
SCRN0	Default	No Entry	SCRN0	Preferred	SCRN0 Preferred SCRN1	SCRN1	Speech	SCRN1 Speech C01	C01
							64K	SCRN1 64k C02	C02
				Req	SCRN0 Req C03	N/A	Speech 64K	No Entry	C03
				Not Req	SCRN0 Preferred SCRN1	4 SCRN1			
	A B	SCRN0 A SCRN1	SCRN1	Preferred Req Not Req	No Entry	4 SCRN1			
		SCRN0 B SCRN1	1 SCRN1						

1. KK Sharing: 2 or more KK share the same routing
2. IPI Sharing: 2 or more IPI values share the same routing
3. BC Sharing: 2 or more BC values share the same routing
4. Customer Group Sharing: The same customer group (translations) are used for 2 or more KK/IPI/BC combinations

62: Functional Description (FN): A00003951

This Functional Description (FN) covers the work required to support the i2001 Internet Telephone. The FN also covers the work required to support a common User Interface for the i2001, i2002and i2004.

62.1 Description

The i2001 is a reduced functionality sibling of the i2002 to reduce cost of manufacture it has a smaller screen, fewer buttons and a cheaper build

The i2001 is also a Phase II Unistim Terminal. Currently the CICM supports Phase I Terminals, as part of the scope of this feature, existing support for the i2002 and i2004 Phase I Terminals will be updated to support the new range of Phase II i2002 and i2004's.

Phase 1 terminals will be MD when the Phase II terminals become available so support for the whole range of Phase II terminals (i2001, i2002 and i2004) on the CICM will be required

Table 1 Table 1 i200x Configuration/menu matrix

			Terminal type		
	Function	Sub-options	I2001	I2002	I2004
	Login/Logoff	N/A	✓	✓	✓
	Firmware upgrades	N/A	✓	✓	✓
Options	Audio	Profile	✓	✓	✓
	Display Contrast	N/A	✓	✓	✓
	Feature Keys	Assign	✓	✓	✓
		Label	✓	✓	✓
		Reset	✓	✓	✓
	Language	N/A	✓	✓	✓
	Time	Time Format	✓	✓	✓
		Date Format	✓	✓	✓
		Hours from GMT	✓	✓	✓
		Daylight Saving	✓	✓	✓
	User	Username	✓	✓	✓
		Login Type	✓	✓	✓
		Auto Login	✓	✓	✓
Services	Inbox	Display	✓	✓	✓
		Store	✓	✓	✓
		Clear	✓	✓	✓
		Dial	✓	✓	✓
	Outbox	Display	✓	✓	✓
		Store	✓	✓	✓
		Clear	✓	✓	✓
		Dial	✓	✓	✓
	Directory	Add	✓	✓	✓
		Edit	✓	✓	✓
		Delete	✓	✓	✓
		Dial	✓	✓	✓

62.1.1 Display

The following details apply to the i2001.

- i2001 will have a *32x143* pixel, fully bit-mapped, monochrome, non-grayscale display. This will display 2 lines of 24 5x9 characters.
- The number of Soft labelled feature keys on the i2001 is zero
- Dedicated icon area in the main display area has been removed.
- Dedicated Clock / Calendar area present.
- Dedicated number and context label are present.
- Dedicated down arrow removed.

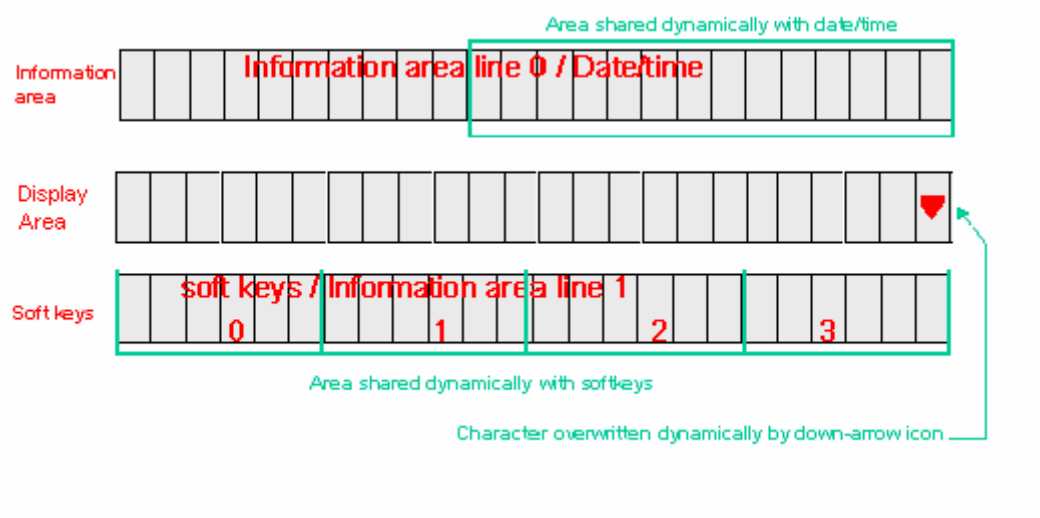


Figure 1 Display layout of i2001

62.1.2 Generic Display Rules

The following rules have been devised for the i200x terminals. These rules have been introduced to allow one common interface across both terminal types and to help avoid issues with Language Translations on soft key strings.

- All strings for menu options should be created with the following rules in mind
  a. Recommended length 12 characters – strings meeting this condition will always be shown in full (both on the information lines and in the context field)
  b. Maximum length 20 character – strings above 12 characters in length and equal to or below 20 characters will be fully displayable in the information line but not in the context field. Long strings in the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.
  c. Strings above 20 characters to be shown:
  — In the information lines will be cropped off to 19 characters and terminated with an ellipsis to indicate they have been cropped.
  — In the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.
- The Login Screen echoes entered digits to information line 0 rather than line 1 (please see Figure 2). The username and passwords entered may be up to a maximum of 15 digits. If the username/password entered is longer than the field space left on the screen (i.e. if the “Username” string is 14

characters and 12 username digits are to be entered), the digits will be scrolled to the left and an ellipsis will be inserted to the left of the username to indicate this (please see example below).

U	S	E	R	N	A	M	E		T	E	S	T	:	.	.	3	4	5	6	7	8	9	0	

- Bottom Soft key labels are set to a maximum of 5 characters with the exception of the last soft key on the screen which may use up to a maximum of 6 characters (please see Figure 2). This is due to a limitation of screen space on the i2001.

Figure 2 i2001 - Login Display

- Soft key labels are limited to a small generic subsection of the previously used soft keys (“Ok”, “Cancel”, “Clear”, “Bkspc”, “Menu”, “Help”, “Yes” and “No”).
- Menu options are selected via a scrollable list (instead of being assigned to a soft key). Scrolling may be carried out using the up and down navigation. This allows menu options to be displayed in strings which may be up to a maximum of 20 displayable characters (see rule 1). This is advantageous for the following reasons:
  - — A greater area makes language translations easier.
  - — A more informative string may be displayed.
- The position within a scrollable list is displayed to the far right hand side of the display. 1 character space is reserved to show scroll position.

- All Menu Options in the scrollable list are numerically indexed with the shortcut key number assigned to that option. The numerical indexes will go from 1 – 9. Options above 9 will have no shortcut assigned/displayed next to the menu option
- A menu option may be selected by either highlighting the option (i2004) or viewing the option (i2002, i2001) and selecting “Ok”. Alternatively the appropriate shortcut key assigned to an option may be selected using the key pad. This will cause the user to jump straight into the menu option required without scrolling.
- All Menu Options are set to a recommended length of 12 characters (so they may be displayed in the context field on the i2004). Please see rule number 1) for further details.
- The Logout option is presented as the first option in the Menu Options List. This will avoid language translation issues on when using a soft key for the same operation.
- All user prompts will be presented on Information line 0 on the display. The maximum length of a prompt is 23 characters. Prompts beyond 23 characters will be cropped down to 22 characters and an ellipsis will be presented as the 23rd character to indicate cropping has taken place. Further text to describe the prompt is viewable on a help screen which is accessed by selecting a “Help” soft key (Please see Figure 3). The help screen presents text to the user by using scrolling pages (Please see Figure 4). The help screen has a maximum number of 255 characters (due to the scrolling functionality). The recommended word size is 24 characters (words exceeding this limit will be word wrapped onto the next line of the display).

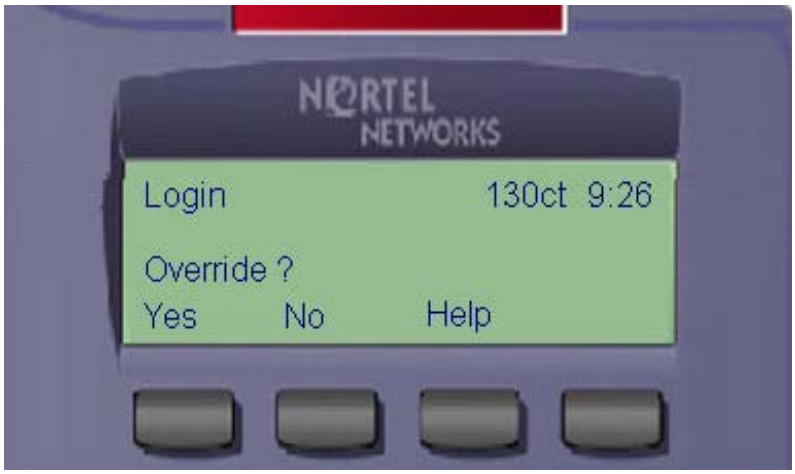


Figure 3 i2001- Override prompt

- User permissions disable

Figure 4 i2001 - Override Help screen

- The Menu system is accessible by either selecting the “Menu” softkey or by selecting the “service” physical key (please see at any time (idle or non-idle).

Figure 5 i2001 - Service key position (used to launch Menu system)

62.1.3 i2001 Display Rules

To show the information required to the user on such a restricted display, the following list of rules have been devised specifically for the i2001. The context-sensitive display that these rules entail are not as intuitive to use as that of the i2004, however there is no choice but to change the position and

visibility of information on the display depending upon context if that information is to be displayed at all.

- The Menu options are selected via a scrollable list.
- The relative position within the list is show to the far right of information line 0 via up and down arrows.

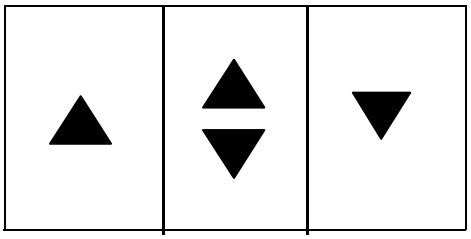


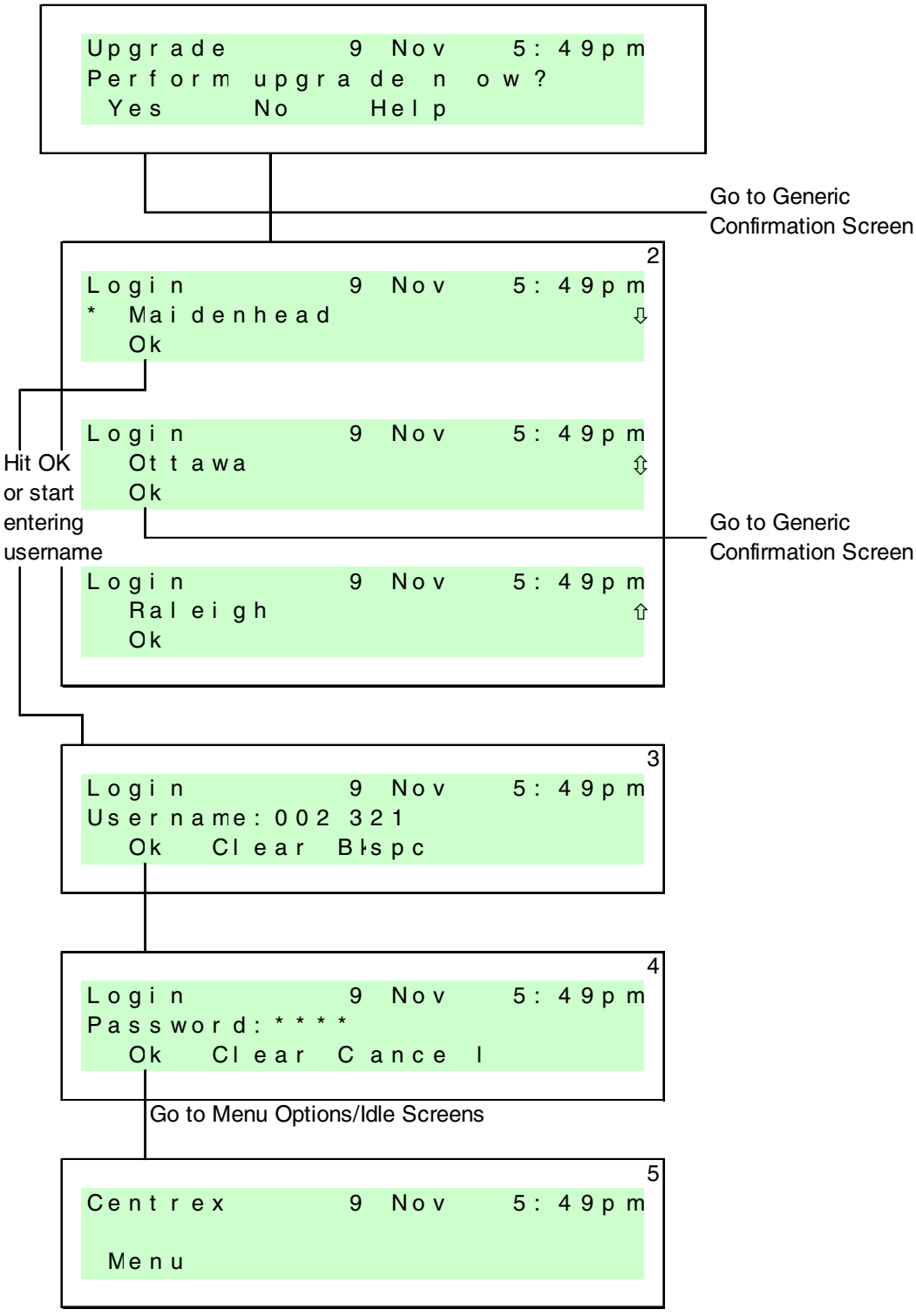
Figure 6 Example of navigation arrows

- Information line 1 is dedicated for the Soft keys.
- Time / Date displayed on context line.

62.1.4 i2001 Menu Map

The following screen representations show what will be presented to the user when logging on to a gateway, and navigating the menu options of the i2001.

62.1.4.1 Login Screens



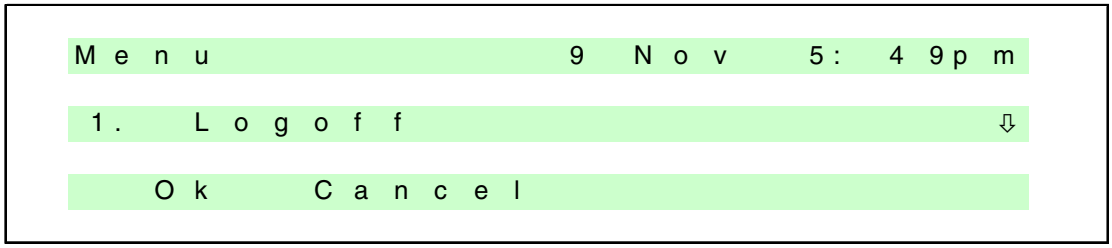
Screen 1 – Only shown if an upgrade is available / required.

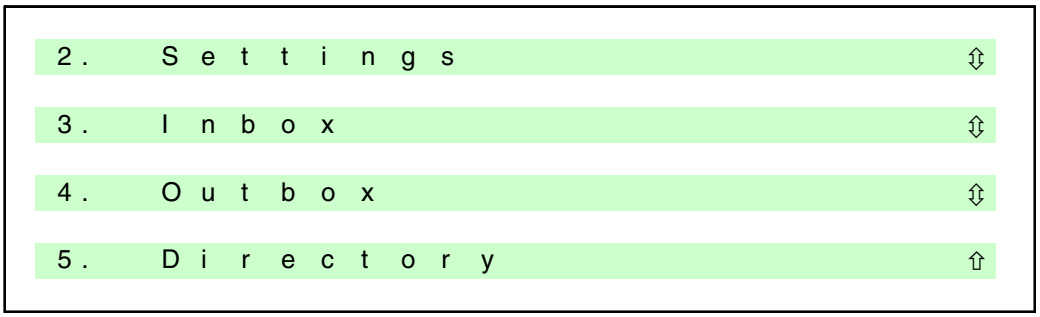
Screen 2 –Selective Gateway Login feature

Screen 2 – A user can either hit “Ok” to accept a gateway to login to, they will then be presented with Screen 3 to login. Alternatively the user may start entering their username digits and this will also accept the currently selected gateway, go to Screen 3 and insert the digit(s) already entered.

Screen 3 – If the username is too long for the display the digits entered will scroll to the left and an ellipsis will be shown to the left of the username to indicate this to the user.

62.1.4.2 Menu Option/Idle Screens



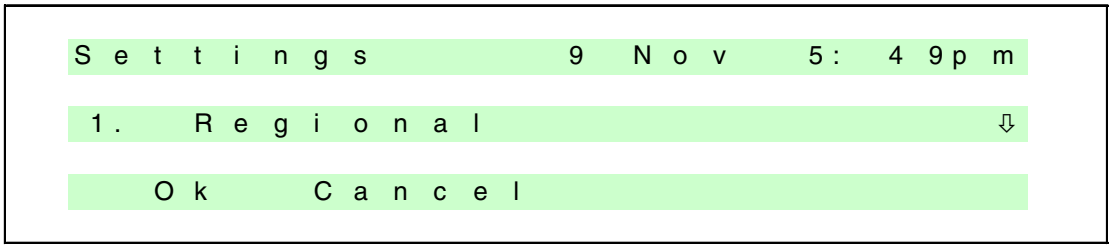


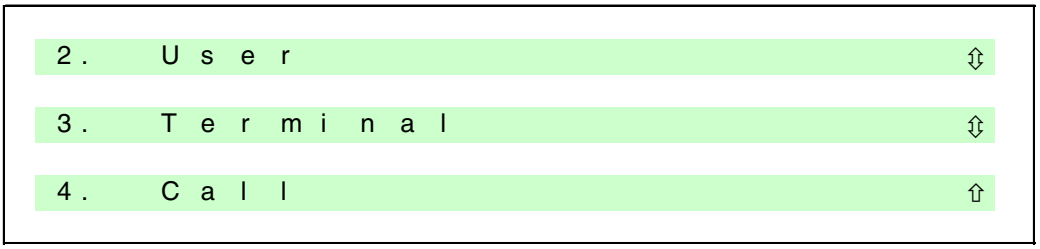
- Menu Option 1: Logoff – a Generic confirmation screen is displayed.
- Menu Option 2: Settings – launches the new i2001 settings menu.
- Menu Option 3: Inbox – Launches the inbox, Inbox is also available via dedicated Inbox key on terminal (i200x). The i2002 will be able to launch the inbox via both the menu and the dedicated key, the i2004 will only be able to access via its existing implementation of the dedicated key.
- Menu Option 4: Outbox – Launches the Outbox, the i2001 does not have a dedicated Outbox key and will only be able to access the Outbox via this

menu system, the i2002 and i2004 terminals will be able to launch the Outbox via the dedicated key. The i2002 will be able to access the Outbox via both the menu and the dedicated key. The i2004 will only access the outbox via the dedicated key.

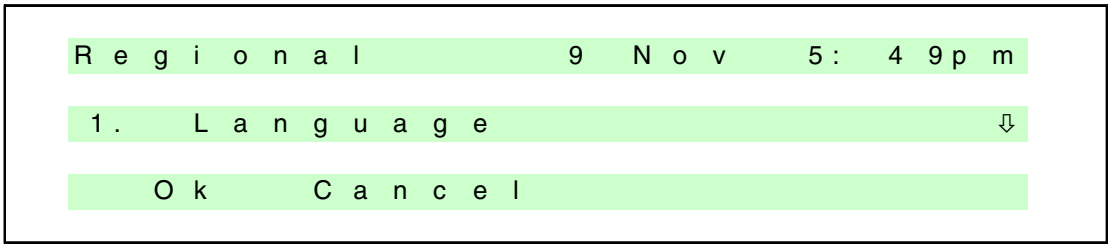
- Menu Option 5:Directory – Launches the directory contact list, the i2001 does not have a dedicated Directory key and will only be able to launch the directory via this menu system, the i2002 and i2004 have dedicated Directory keys to launch the directory

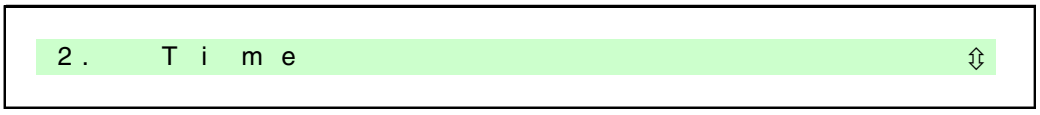
62.1.4.3 Menu Option: Settings



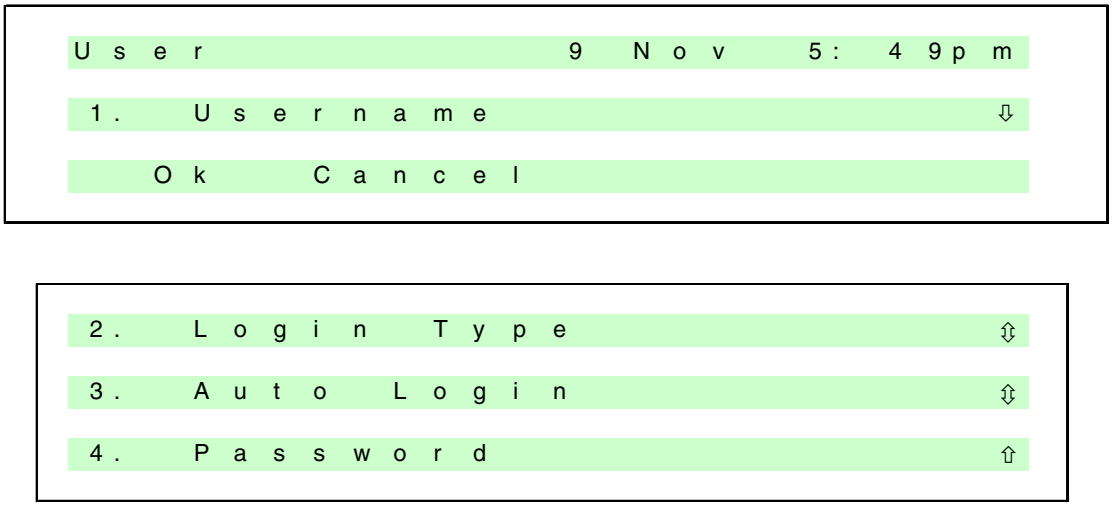


62.1.4.4 Menu Option: Regional Settings



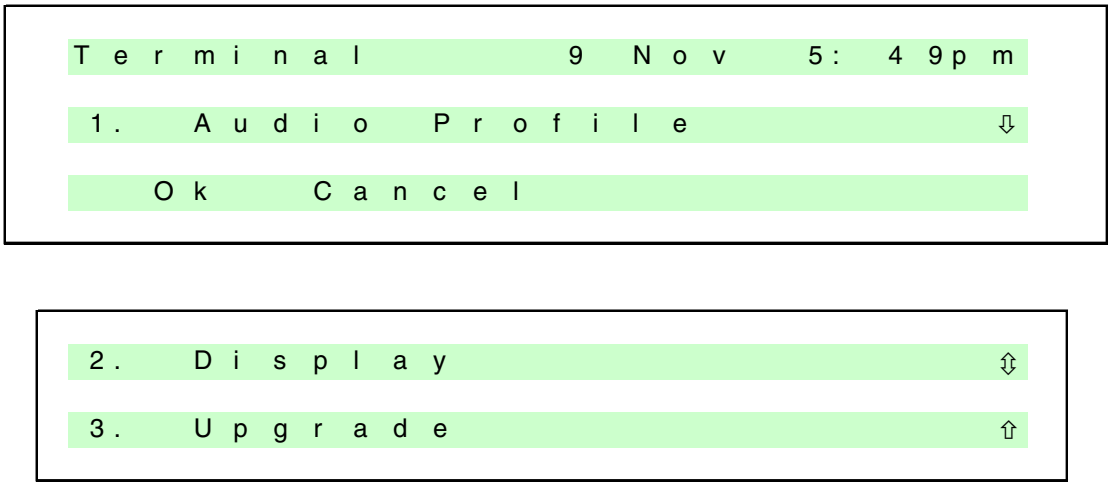


62.1.4.5 Menu Option: User Settings



See section 60.1.4.9 for details of user information screens.

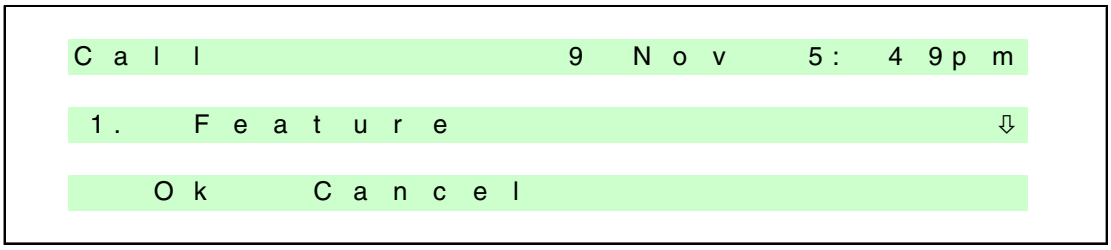
62.1.4.6 Menu Option: Terminal Settings

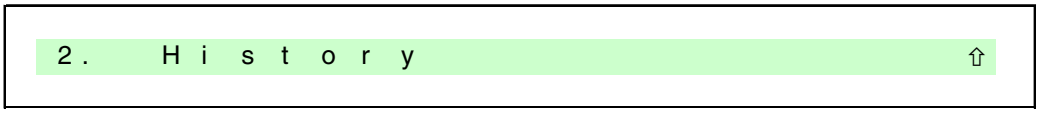


- Terminal Settings Option 1: Launches the Audio Profile menu.

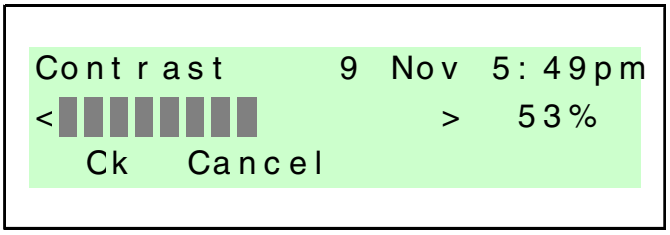
- Terminal Settings Option 2: Launches the display Contrast screen. (2.1.4.8)
- Terminal Settings Option 3: Launches the Upgrade confirmation menu, depending on if an upgrade is available or necessary.

62.1.4.7 Menu Option: Call Settings

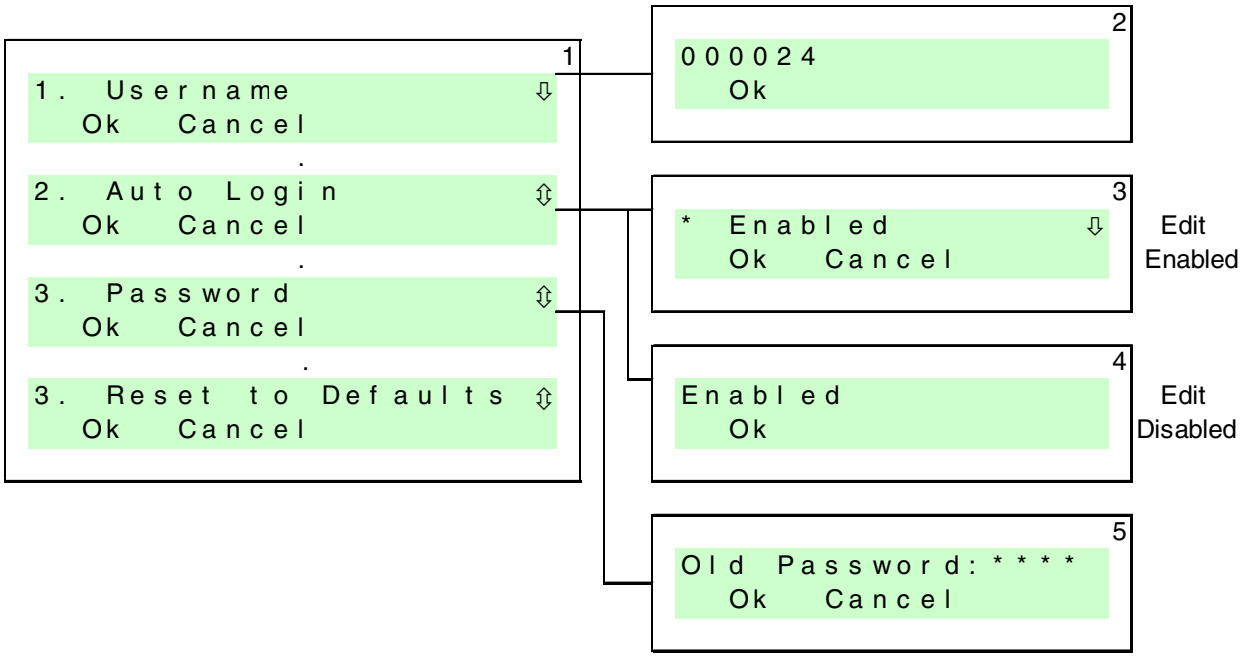




62.1.4.8 Display Contrast Screen



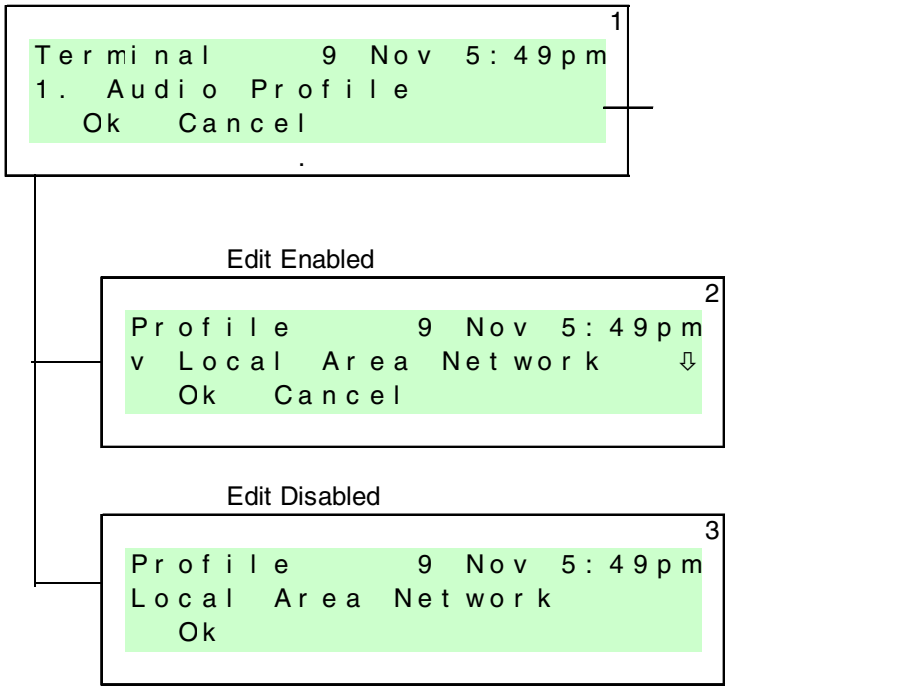
62.1.4.9 User Information Screens



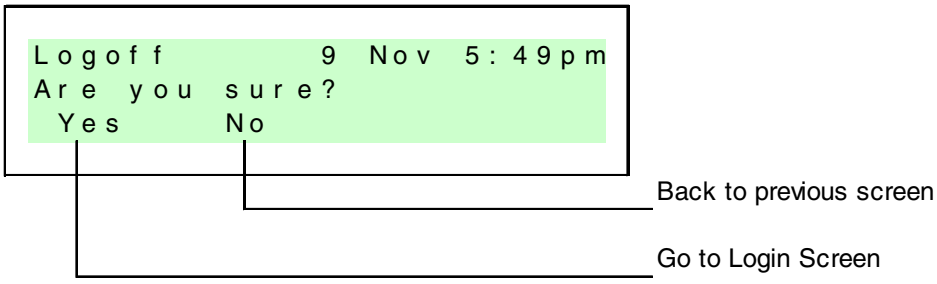
- Screen 3 – The user has permission to edit their Auto Login functionality. The user may enable/disable the feature from this screen.
- Screen 4 – The user has view permission to the Auto Login functionality. The user may only view what their current setting is.

  Note: NOTE: The permissions are configurable via the element manager in the user/user profile settings.

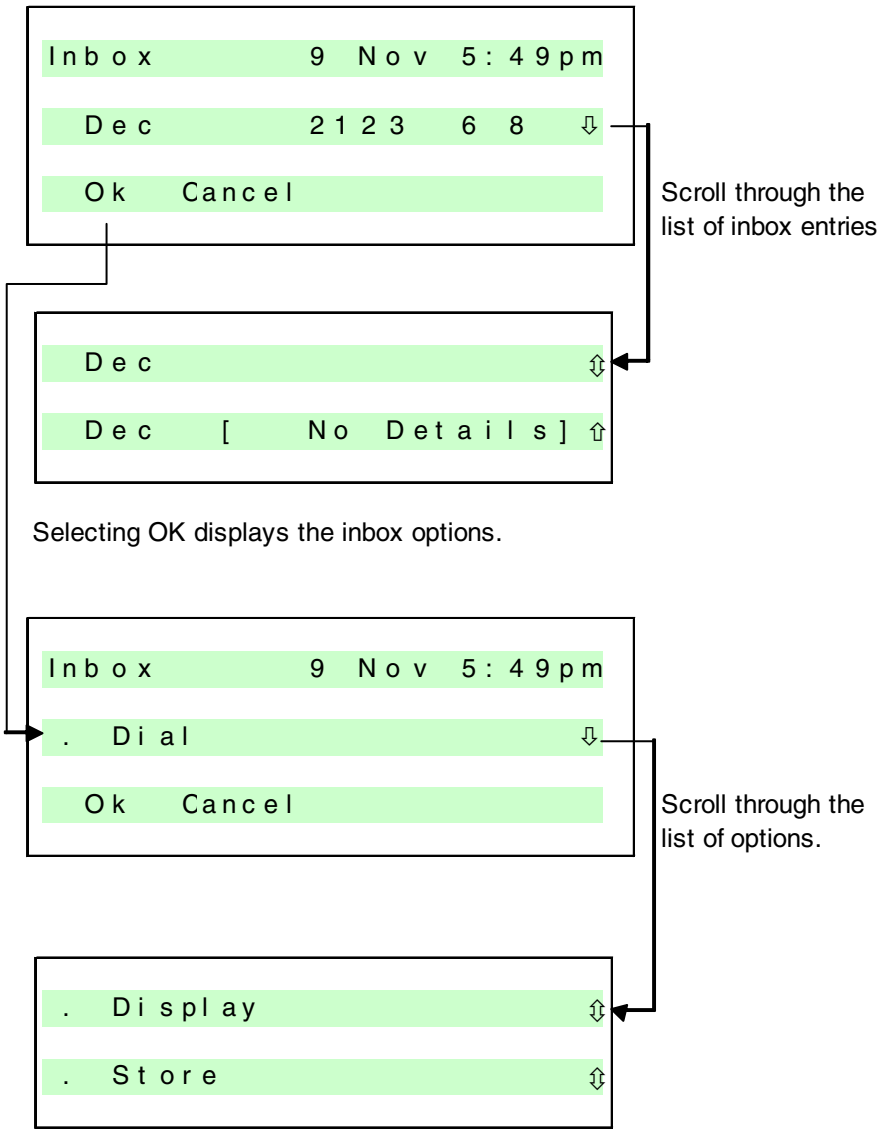
62.1.4.10 Audio Screens



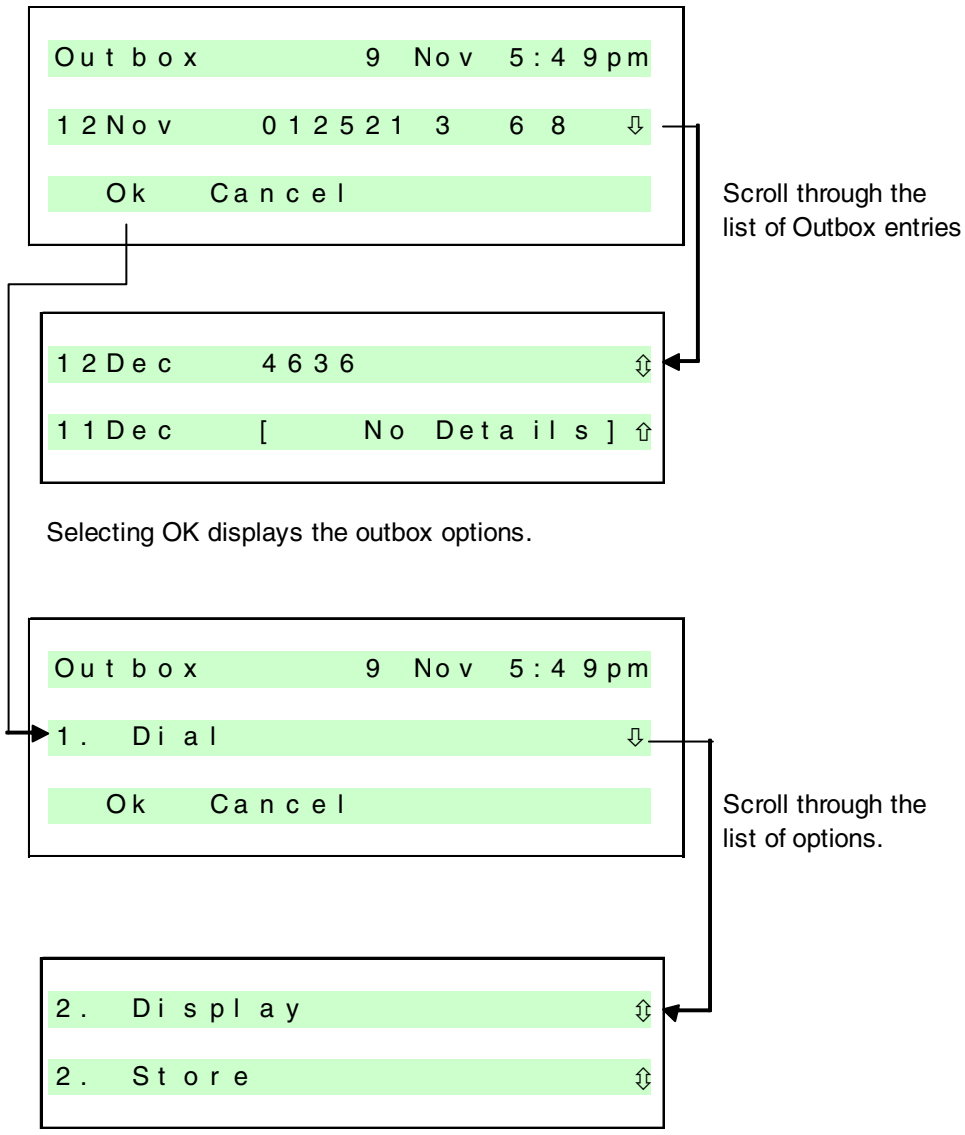
62.1.4.11 Generic Confirmation Screen



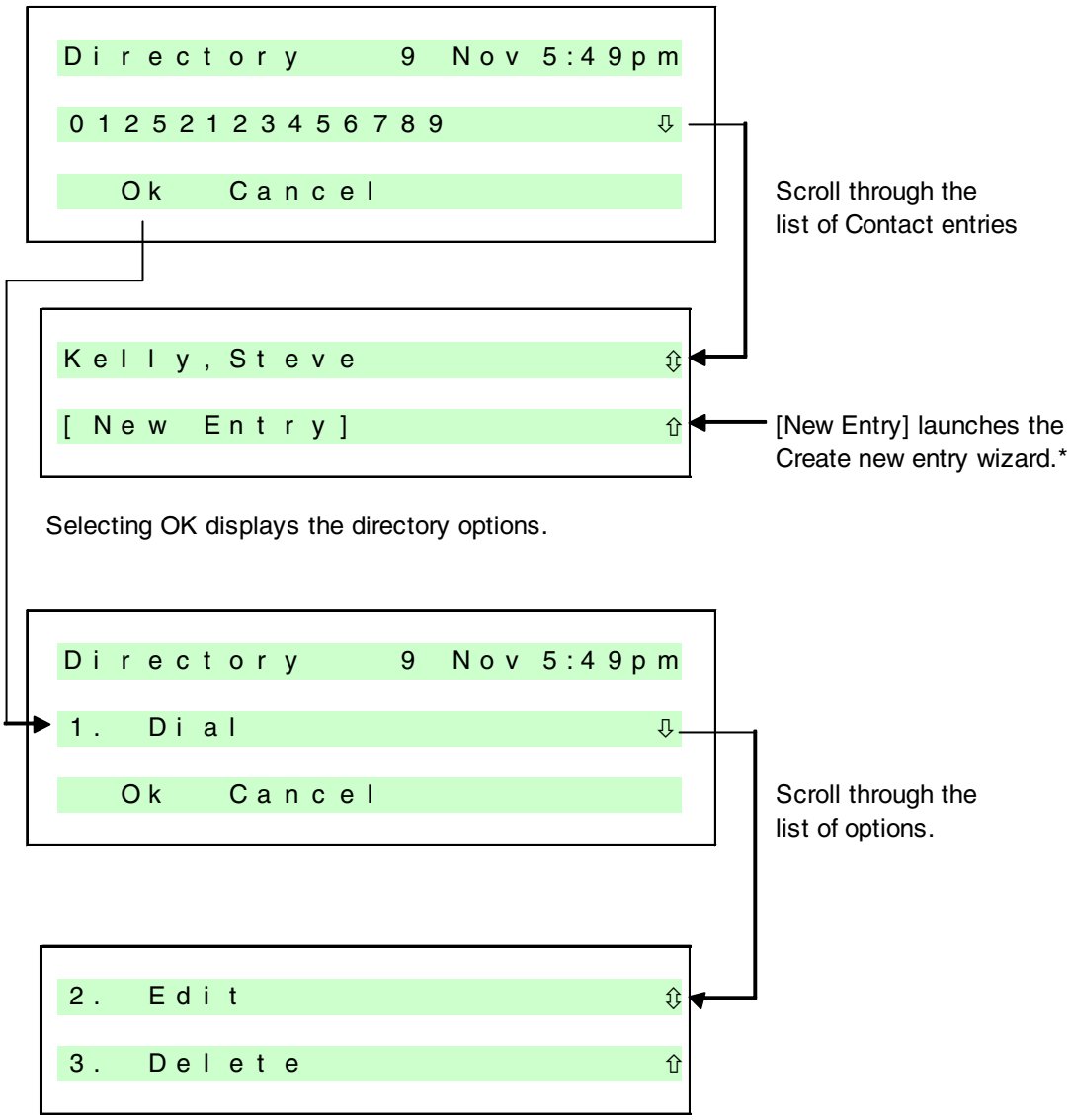
62.1.4.12 Inbox and submenu screens



62.1.4.13 Outbox and submenu screens

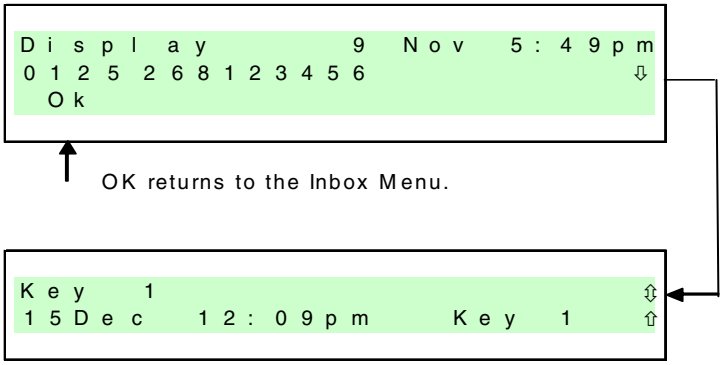


62.1.4.14 Directory display screens

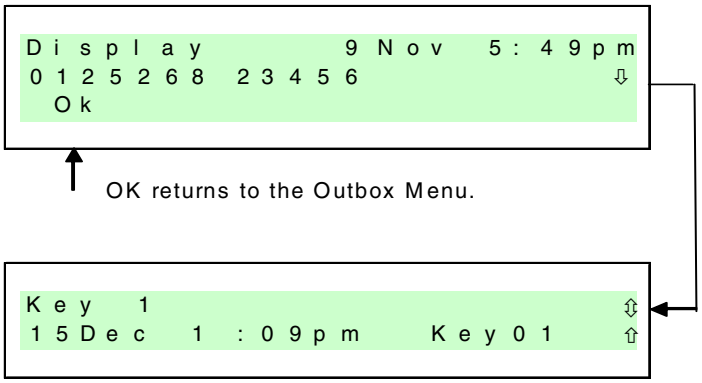


* The [New Entry] option may be ordered to feature at the top of the directory list, so upon entering th directory you will be presented with the first actual entry and press up to select [New Entry]

62.1.4.15 Inbox Display Screen

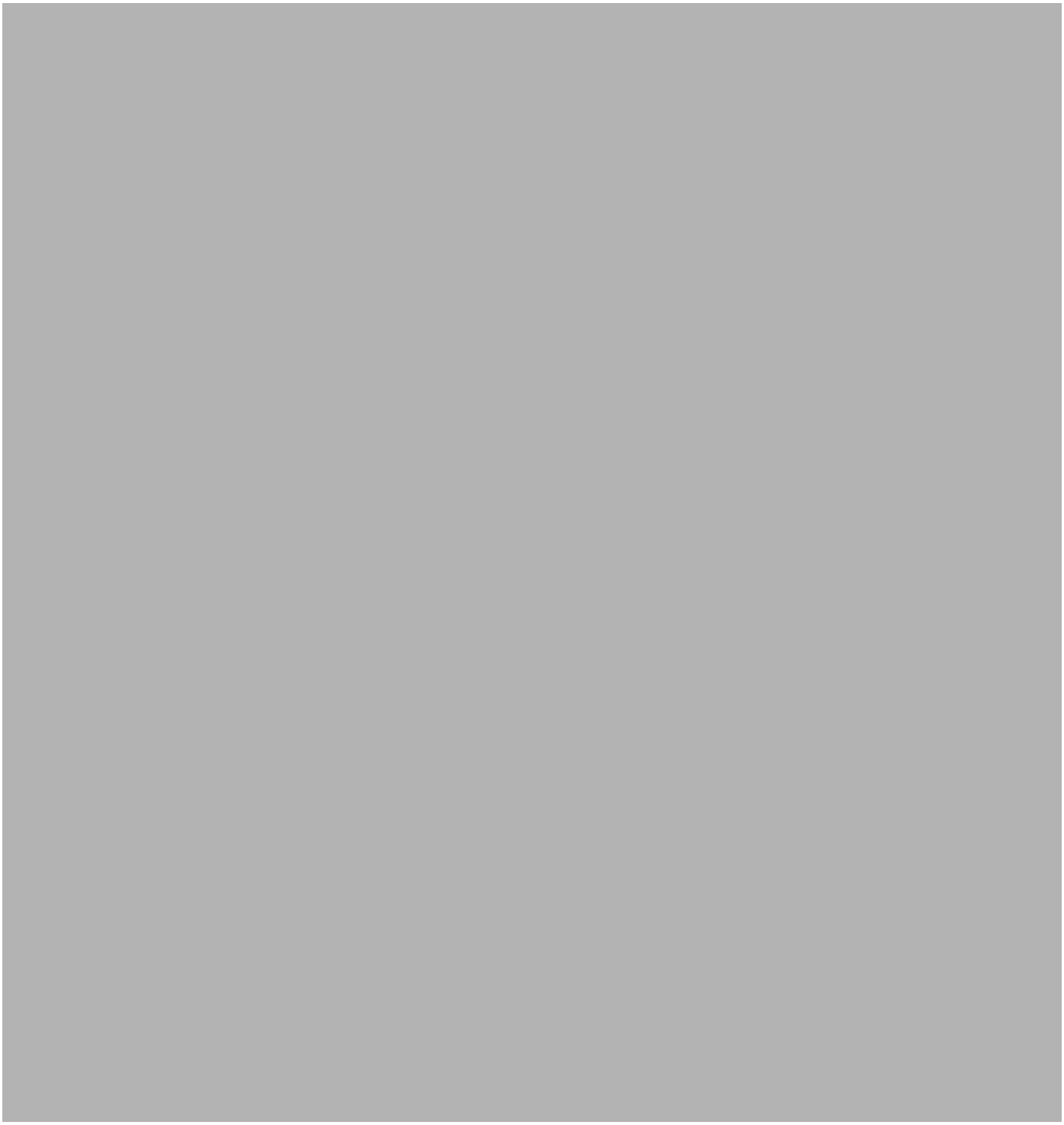


62.1.4.16 Outbox Display Screen



62.1.4.17 Directory Edit screens

62.1.4.18 Time display screens



62.1.4.19 Call History screens

62.1.5 Administration - Element Manager

Figure 7 Screen capture of terminal firmware upgrade page

The administration and configuration of the i2001 terminals will use the same pages which are already provided for the i2004 and i2002 terminals (See Figure 7).

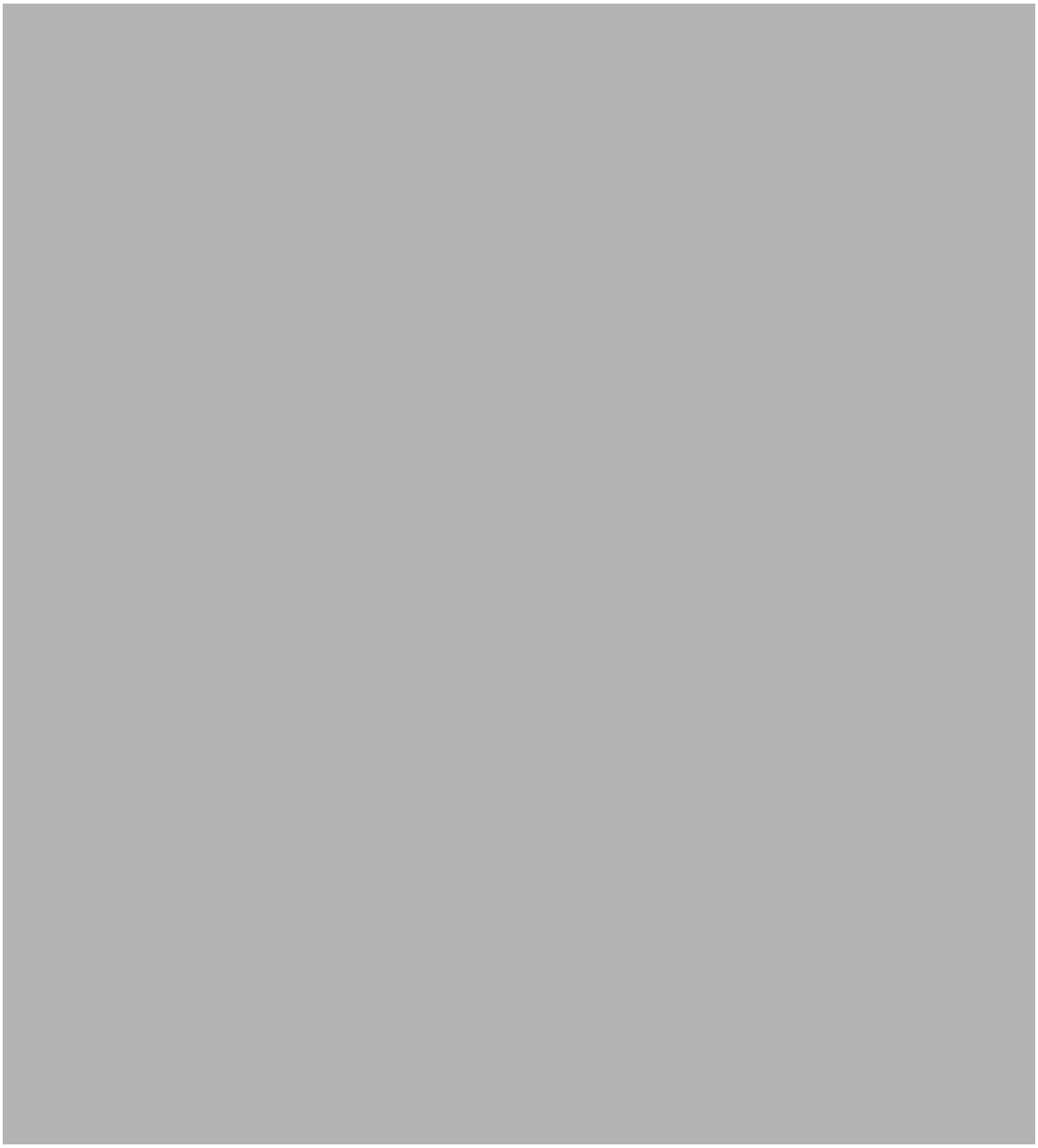


Figure 8 Screen capture of phase 2 terminal firmware upgrade page

User permissions will be editable via the user/user profile pages.

62.2 Interactions

62.2.1 Joint Sessions

The i2001 will only be able to have a joint session with the m6350 Softclient. In this scenario it will always adopt the master position in their master/slave

relationship. In this case, the i2001 will function in the same manner as the i2004.

There will be no support for the i2001 to have a joint session with another i200x.

62.3 Software Requirements or Dependencies

Firmware load *.bin will be used for the development of this feature on the i2001.

62.4 Interactions

This feature will change the existing menu system employed by the i2004 and i2002. Menu options previously displayed on the soft keys will be displayed in the main screen as a scrollable list (using the up and down navigation keys). The Soft keys will only be used for a small sub section of set functions.

The change is beneficial on the i2004 for the support of different languages as longer strings may be used for menu options. Problems had previously been encountered upon translating soft key options which were limited to only 7 characters i.e. a 7 character soft key in English may translate into a 9 character soft key in French which is not easily abbreviated.

62.5 References

63: Functional Description (FN): A00004205

63.1 Feature name

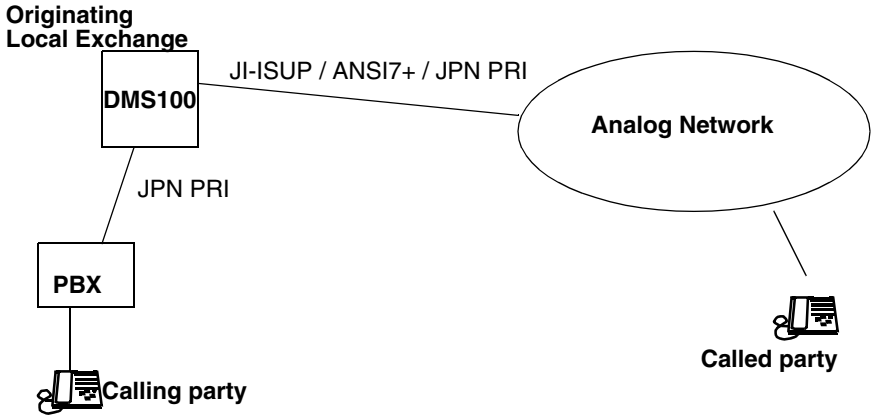
A00004205 - Japan PRI Backward Voice Path Solution

63.2 Description

63.2.1 Introduction

Some PBXs, upon receiving a PROGRESS or an ALERT message with PI#2 (Destination address is non-ISDN) on their Japan PRI interfaces do not open backward direction voice paths. As a result of this, although ring-back tone from destination side is available, PBX subscribers can not hear it. Currently, a PROGRESS message with PI#2 is sent back to the PBX when an ACM message with the pattern described in Section 63.2.2 is received in Japan PRI to Japan Interconnect ISUP(JI-ISUP)/ANSI7+ interworkings. Also currently, an ALERT message with PI#2 is sent back to the PBX when an ALERT message with PI#2 is received in Japan PRI to Japan PRI interworking (1).

Figure 1 Call scenario



The activity “Japan PRI Backward Voice Path Solution (A00004205)” implements in ISN07 the optional addition of a second progress indicator (PI#8: inband info available) to the PROGRESS/ALERT messages sent back to the call originating side like PBX.

Upon receiving the PI#8, the PBXs are expected to open their backward voice paths and resolve the ring-back tone problem described above.

The second PI is only added for the agents given in Figure 1, "Supported Agents and Directions"in the specified direction and it is added only if the switch-based option, that is introduced with activity, is enabled as described in Figure 63.2.3, "Activation of the PI#8 addition".

Table 1 Supported Agents and Directions

From: \ To:	Japan PRIv1	Japan PRIv2
Japan PRIv1	YES	YES
Japan PRIv2	YES	YES
JI-ISUP	YES	YES
ANSI7+(Q764)	YES	YES

Important datafills corresponding to the above interfaces are as follows:

Japan PRIv1
Table LTDEF
ISDN 360 B PRA 15 15 8 7 ***INSPRI V1*** NIL (NOPMD) $

Japan PRIv2
Table LTDEF
ISDN 360 B PRA 15 15 8 7 ***INSPRI V2*** NIL (NOPMD) $

Japan Interconnect ISUP (JI-ISUP)
Table TRKSGRP
2WJIISPAB 0 DS1SIG C7UP 2W N N UNEQ NONE ***Q767*** THRL 0 DMS_NODE N N ***JPN_INTERCONN*** 100_WHITE $ 2WN7 CIC

ANSI7+ ISUP
Table TRKSGRP
2WJPNANSIAB 0 DS1SIG C7UP 2W N N UNEQ NONE ***Q764*** THRH 0 DMS (MBG NONE) $ ANSI2W CIC

In the rest of this document, Japan PRI will refer to both Japan PRIv1 and Japan PRIv2, unless otherwise specified.

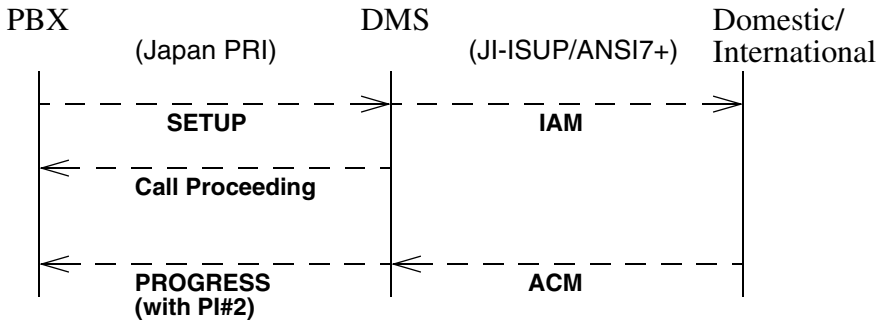
63.2.2 Background

A PROGRESS message with PI#2 is sent back to a JapanPRI trunk upon receiving an ACM message from Japan Interconnect ISUP (JI-ISUP) or ANSI7+ trunk with the following Backward Call Indicators (BCI):

Table 2 Current Backward Call Indicator to Progress Indicator mapping

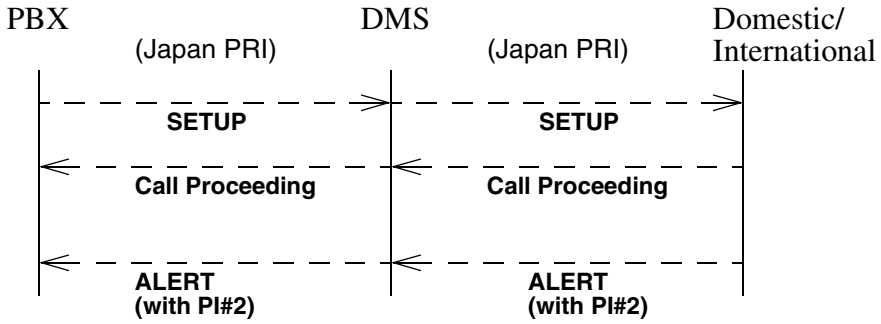
JI-ISUP	Japan PRI
Bit I=0 No interworking encountered Bit M=0 Terminating access is non-ISDN Bit DC=00 No indication	PI#2 (Destination address is non-ISDN)
ANSI7+ ISUP	**Japan PRI**
Bit I=0 No interworking encountered Bit M=0 Terminating access is non-ISDN Bit DC=00 No indication	PI#2 (Destination address is non-ISDN)

Figure 2 Current ACM to PROGRESS mapping



An ALERT message with PI#2 is sent back to a JapanPRI trunk upon receiving an ALERT message with PI#2 from JapanPRI trunk.

Figure 3 Current ALERT to ALERT mapping



63.2.3 Activation of the PI#8 addition

Activation and deactivation of this feature is only available per one DMS100 switch basis.

In order to activate the addition of the PI#8 back to the originating PBXs, ISERVOPT table should be datafilled as follows:

Table 3 ISERVOPT datafill example for JapanPRI option

SOPTSKEY SOPTSVAR
JAPANPRI JAPANPRI Y

The following table displays how datafilling the JapanPRI option will actually take place:

Table 4 Datafilling JapanPRI option in ISERVOPT table

```
>table iservopt
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>japanpri
OPTION:
>japanpri
ALLOW_BACKWARD_VOICE_PATH:
>y
TUPLE TO BE ADDED:
JAPANPRI JAPANPRI Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

63.2.4 Scenarios when PI#8 is not added

When JAPANPRI option in ISERVOPT table is not datafilled or when it is datafilled but ALLOW_BACKWARD_VOICE_PATH is set to ‘N’, the PI#8 will not be added to the PROGRESS/ALERT messages. Therefore in these conditions, ACM to PROGRESS mapping in Japan PRI to JI-ISUP/ANSI7+ interworkings and ALERT to ALERT mapping in Japan PRI to Japan PRI interworkings will be as described in section 63.2.2.

This will be the default behaviour of this feature, in order to prevent changing the existing behaviour after upgrades.

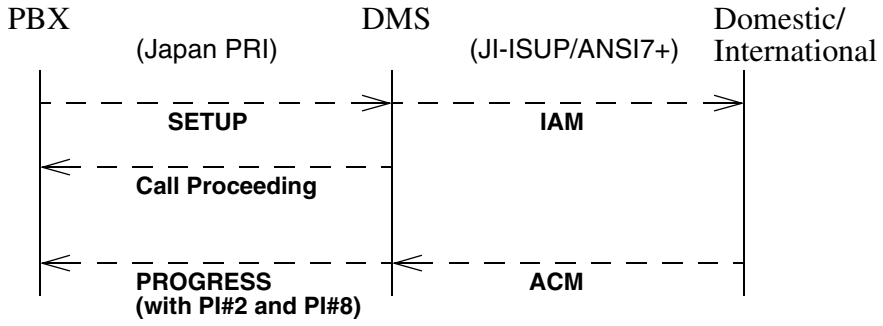
63.2.5 Scenarios when PI#8 is added

If the JAPANPRI option in ISERVOPT table is datafilled and ALLOW_BACKWARD_VOICE_PATH option is set to ‘Y’, then a PROGRESS message with a second PI#8 will be sent back to a JapanPRI trunk upon receiving an ACM message from JI-ISUP or ANSI7+ trunk with the following Backward Call Indicators (BCI):

Table 5 Desired Backward Call Indicator to Progress Indicator mapping

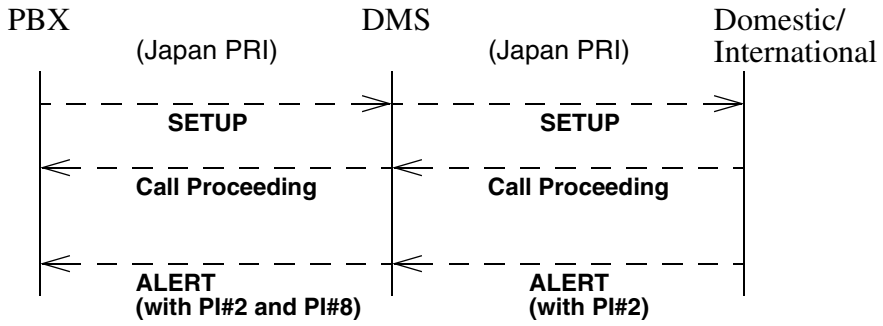
JI-ISUP	Japan PRI
Bit I=0 No interworking encountered Bit M=0 Terminating access is non-ISDN Bit DC=00 No indication	PI#2 (Destination address is non-ISDN) PI#8 (Inband Info Available)
ANSI7+ ISUP	**Japan PRI**
Bit I=0 No interworking encountered Bit M=0 Terminating access is non-ISDN Bit DC=00 No indication	PI#2 (Destination address is non-ISDN) PI#8 (Inband Info Available)

Figure 4 Desired ACM to PROGRESS mapping



If the JAPANPRI option in ISERVOPT table is datafilled and ALLOW_BACKWARD_VOICE_PATH option is set to ‘Y’ then an ALERT message with a second PI#8 will be sent back to a JapanPRI trunk upon receiving an ALERT message from JapanPRI trunk.

Figure 5 Desired ALERT to ALERT mapping



63.3 Hardware Requirements or Dependencies

Not Applicable.

63.4 Software Requirements or Dependencies

Not Applicable.

63.5 Limitations and restrictions

Not Applicable.

63.6 Interactions

Not Applicable.

63.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A

Performance (includes operational measurements) N/A

63.8 Glossary

Term	Description
ACM	Address Complete message in ISUP protocol
BCI	Backward Call Indicator in ACM message
ISDN	Integrated Switched Data Network
ISUP	ISDN User Part
JI-ISUP	Japan Interconnect ISUP
PI	Progress indicator
PRI	Primary Rate Interface

a. **Recommended Reading/References**Cable&Wireless - ISN07 to ISN04 Feature Bridge Back Version, JPN PRI B Voice Path Requirement Specification For Opening the Backward Voice Path (Japan PRI)

b. NIS A220-1 - Japan Primary Rate Interface, Nortel Interface Specification, Standard 09.01, September 1998.

c. NIS A220-2 - Japan PRI, Interworking Description, Standard 02.03, September 1998.

d. ITU-T Recommendation Q-931, ISDN User-Network Interface Layer3 Specification for Basic Call Control

64: Functional Description (FN): A00004503

64.1 Feature name

Calling Party Number Serving Country Code(SCC)

64.2 Description

64.2.1 Notation

The following notations are used throughout the whole document.

Switch: DMS-GSP Switch

Outpulsing/Terminating CLI: Outgoing CGPN

Callp: Call Processing

EISUPV1: ETSI ISUP Version 1

EISUPV2: ETSI ISUP Version 2

64.2.2 Introduction

This document describes the feature ‘Calling Party Number Serving Country Code(SCC))’ which is implemented in GSPISN07 for GSP product(i.e. datafillable on Axxess trunks).

This feature enhances the feature AD9743 by introducing the ability to deactivate the terminating SCC processing for Calling Party Number (CGPN) for ANSI ISUP, ETSI ISUP V1, ETSI ISUP V2, RBTUP and BBTUP agencies.

Terminating SCC processing is controlled via the SCC field of the xxATTR tables (i.e. ISUPATTR, TUPATTR) and applies to both the CGPN and CDPN by removing the country code and changing the CGPN and CDPN Nature of Address (NOA) to National.

With this feature, terminating SCC functionality may be deactivated for the Calling Party Number parameter independent from Called Party Number (CDPN) on a per trunk basis.

64.2.2.1 The background for the requirement

According to the feature for SCC Processing (AD9743), SCC functionality’s aspect is that; when a global carrier switch such as the DMS-GSP is translating calls received from or destined for different countries, it can be difficult to

establish a database of calling numbers due to potential conflicts between each country's number formats. Additionally, when terminating international calls into a certain country, the national dialing plan might require conversion of the called and calling address from international to national formats. The Serving Country Code (SCC) functionality in feature AD9743 is designed to address these issues.

DMS takes off the country code (CC) (implemented in the existing feature AD9743) in the Calling Party Number Parameter in some case and consequently some organizations will delete the CLID when there is no CC or the NOA (nature of address) is set to National or in the worse case, they will reject the call.

This feature introduces the functionality where it is possible to disable the CGPN terminating SCC functionality inside the GSP.

64.2.3 Description of Feature

The feature "Calling Party Number SCC" is implemented in GSPISN07 for GSP product(i.e. datafillable on Axxess trunks).

With this feature, the country code may be always present on the CGPN even when the calls are terminating in country while at the same time have it stripped for the CDPN.

Feature introduces the ability to deactivate terminating SCC processing on the CGPN independently of the CDPN and this is done on a per trunk group basis. Following agencies are supported by this feature:

· ANSI ISUP

· ETSI ISUP V1

· ETSI ISUP V2

· RBTUP

· BBTUP

A new field is introduced in table TRKGRP to provide control for deactivation of terminating SCC processing for CGPN on a per trunk basis.

- the originating Calling Party Number(CG) SCC functionality remains unchanged

- the terminating SCC functionality for CDPN remains unchanged.

A new field in Table TRKGRP is defined to activate/deactivate terminating CGPN SCC processing in order to make terminating CGPN SCC processing independent from terminating CDPN SCC processing. While building up the CGPN in IAM/IAI/INF message this field is checked in order to decide if the terminating SCC processing will be active or not.

- If the field(CGSCCDEA) is set to 'Y' then terminating CGPN SCC processing is deactivated, that is, no SCC processing will be performed on the CGPN, CGPN remaining unchanged from the original received format.
- If the field is set to 'N' then terminating CGPN SCC processing is not deactivated, that is, the existing terminating SCC processing continues to work for CGPN.

This feature provides an optionality for terminating CGPN SCC processing by changing the new field in TRKGRP table. When this boolean field(CGSCCDEA) is set to 'N', the system behaves as it was before this functionality, that is, it performs SCC processing on that trunk (ref. AD9743FN, section 1.4.9.2).

64.2.3.1 Existing Behavior

Below is a background and only a quote for summary for the Feature AD9743. For details please refer to the FN section of that feature.

Feature for SCC processing AD9743 functions as below:

1. Call Origination to the GSP: Convert a received Calling Party Number (CLI) from national to international format before performing any CLI screening (in this way, CLIs can be datafilled for each country). This involves prefixing the SCC and changing the NOA/TON to "International".

2. Call Termination: Convert the Called Party Number from International to National format (thus, stripping the country code and changing the NOA/TON to "National").

3. Call Termination: Convert the CLI to national format by stripping the country code and changing the NOA/TON back to "National".

This feature only enhances the call termination functionality of feature AD9743 mentioned above as the thirs item.

In order to invoke the SCC feature AD9743, only the Serving Country Code(SCC) is datafilled according to trunk's protocol type. The SCC is assigned to a trunk in ISUPATTR, PRIATTR, TUPATTR or CASATTR (only for C5). Below table illustrates the tuples and datafills for the table ISUPATTR.

Table 1 Table ISUPATTR

```
>table isupattr
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISUPATTR
>format pack;lis
ISUPKEY ISUPATTR_DATA SS7ATIDX SCC ECHOSUPR ECHOSELECT
TMRNAME ABCNTL
GLAREVAR DCME ISUP_PREF PI_ROUTING OVLPOUTP CLIOUTP
UNSUPPORTED_PARM OCN_DMI
---------------------------------------------------------------------------
100 ANSI7 NIL THRH 0 N N 0 N N UNEQ NIL NONE CIC N NOVERI N N NIL
FILTER 0
205 EISUPV2 NIL THRH 0 Y INTL Y 0 N N UNEQ NIL NONE CIC N NOVERI N N
NIL
FILTER 0
0 ANSI7 NIL THRH 0 N N 0 N N UNEQ NIL NONE CIC N NOVERI N N NIL FILTER 0
1 EISUPV1 NATIONAL NOVERI NIL THRH 0 Y Y N 0 N N UNEQ NIL NONE CIC N
NOVERI
N N NIL FILTER 0
```

Figure 1 Terminating CGPN SCC Processing according to AD9743

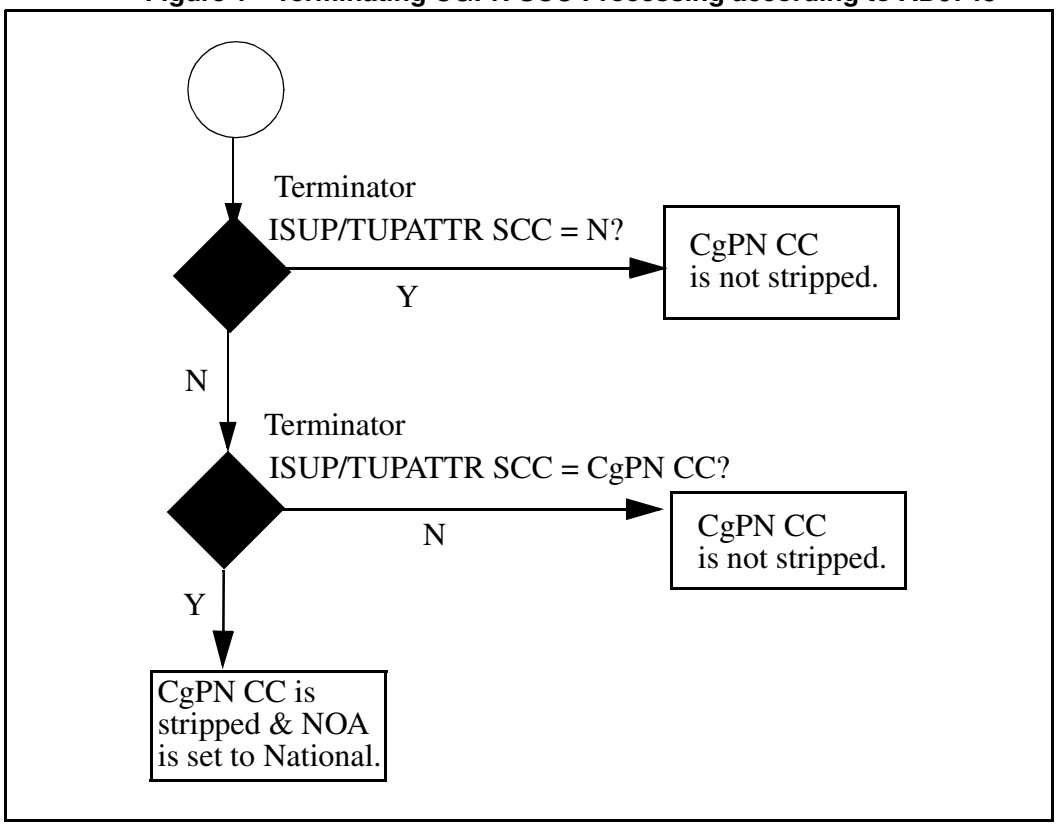


Figure 1 illustrates terminating CGPN SCC processing according to feature AD9743. During termination further processing is needed for an International ANI. If the call is terminating within the same country it originated, then the Country Code from the CGPN needs to be stripped off. To determine if the call is terminating in the same country, the Serving Country Code for the terminating agency in table xxxATTR is compared to the Country Code of the Calling Party Number. If the SCC and CC match then the CC is stripped off from the CGPN and the NOA of the CGPN is set to National. Stripping will not occur if SCC and CC mismatch or if SCC is datafilled as N in table xxxATTR.

In the feature AD9743, the Serving Country Code is a parameter in the tables ISUPATTR and TUPATTR. This field has a NIL option of N if no SCC is datafilled. The range for the SCC parameter is 1 to 3 digits. The SCC is used to create International ANIs out of the incoming Calling Party Number.

64.2.3.2 Functionality Introduced with this Feature

This feature enhances the feature AD9743 by providing an optionality that, for the terminating agents of the supported protocols (ANSI ISUP, ETSI ISUP V1, ETSI ISUP V2, RBTUP, BBTUP) SCC processing for CGPN may be

deactivated according to the new boolean field(CGSCCDEA) in table TRKGRP.

This feature functions for the default CLI being built inside the GSP switch as well.

Below is the TRKGRP table with the new field CGSCCDEA and some examples:

Table 2 Table TRKGRP

```
>table trkgrp
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISUPATTR
>format pack;lis
<line length>:   76 columns can be output per line.
<pack mode>:     Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>:  The first column of output is column 1.
GRPKEY GRPTYP TRAFSNO PADGRP NCCLS GRPINFO
-----------------------------------------
GANSIE1STEP1 AXXESS 0 NPDGP NCIT 2W ODP1 MIDL 16 7 16 16 4 5 4
ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N 1 0 0 0 N N NIL NIL ISUP (NETINFO) $ 0 STD N Y NIL 0 N

GITU1E1STEP1 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 0 0 0 N N NIL NIL ISUP $ 1 STD N Y NIL 0 Y
```

Figure 2 Terminating CGPN SCC Processing introduced by this feature

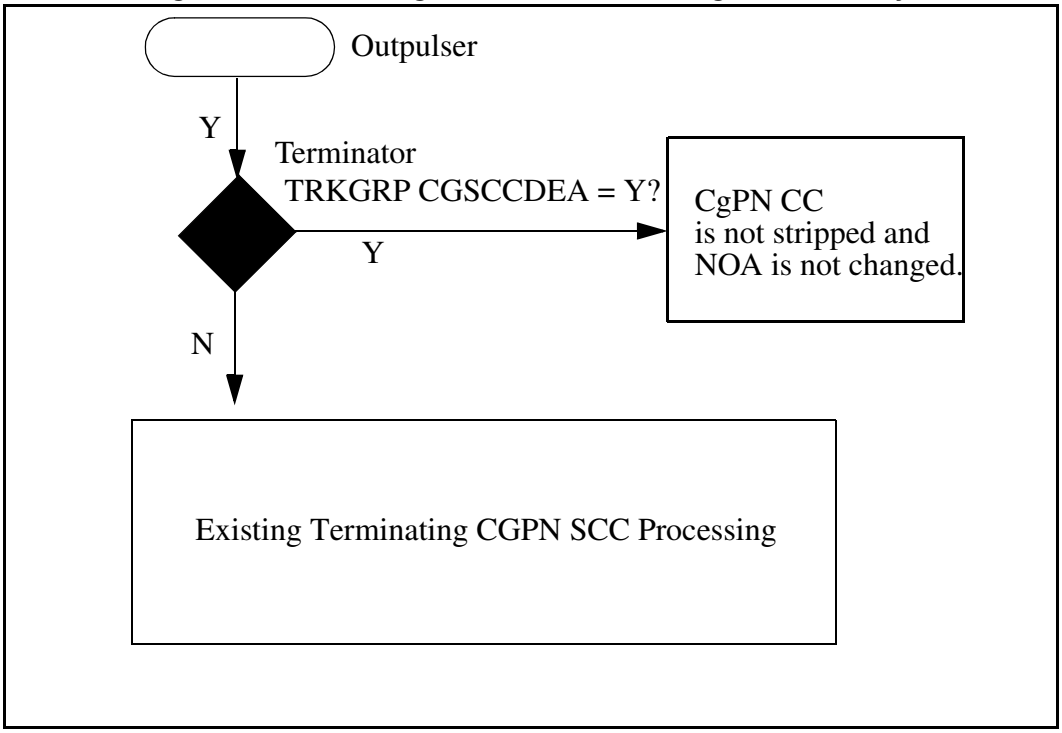


Figure 3 illustrates the terminating CGPN SCC processing introduced by this feature. The new field in table TRKGRP is checked to activate/deactivate terminating SCC processing in order to make terminating CGPN SCC processing independent from CDPN processing.

When building up the outgoing IAM / INF/IAI message this field is checked in order to determine whether the SCC will be stripped off or not.

- If the field is ‘Y’, then there will not be any SCC processing on CGPN and CGPN will be left as it is.
- If the field in table TRKGRP for the terminating trunk agent is ‘N’, then the existing SCC processing will continue to work for CGPN as in the functionality of feature AD9743.

64.2.4 Activation of Feature

This feature is functional for ANSI ISUP, ETSI ISUP V1, ETSI ISUP V2, RBTUP and BBTUP agencies. For the other protocols and variants, this feature is not functional.

The new field will be set to ‘N’ by default for all axxess trunks including incoming, outgoing and two-way trunks. But it will be functional for only outgoing and two-way trunks.

The default value for the newly introduced field ‘CGSCCDEA’ is ‘N’.

CGSCCDEA field can be set to ‘Y’ for only terminating ANSI ISUP, ETSI ISUP V1, ETSI ISUP V2, RBTUP and BBTUP trunks.Please refer to “Limitations/Restrictions“ section of this document for details.

64.2.4.1 New field CGSCCDEA in TRKGRP

To control the SCC processing on per trunk basis, a new boolean field CGSCCDEA is added to TRKGRP table for each trunk having the possible values ‘Y’ representing ‘YES’ and ‘N’ representing “NO’.

Figure 3 Activating/ Deactivating Terminating CGPN SCC Proces

```
>table trkgrp
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos GANSIE1STEP1
GANSIE1STEP1 AXXESS 0 NPDGP NCIT 2W ODP1 MIDL 16 7 16 16 4 5 4
ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N 1 0 0 0 N N NIL NIL ISUP (NETINFO) $ 0 STD N Y NIL 0 N


>pos GANSIE1STEP2
GANSIE1STEP2 AXXESS 0 NPDGP NCIT 2W ODP2 MIDL 16 7 16 16 4 5 4
ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N 1 0 0 0 N N NIL NIL ISUP (NETINFO) $ 0 STD N Y NIL 0 Y
```

As seen from the figure 3, CGSCCDEA field in TRKGRP table is represented as ‘Y’ or ‘N’ and for all axxess trunks it is set to ‘N’ by default.

64.2.4.2 TABLE CONTROL

A new field ’CGSCCDEA’ is introduced for AXXESS trunks in Table TRKGRP.

- The default value of the new field ’CGSCCDEA’ is ’N’ for all trunks
- For ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP trunks CGCCDEA field can be set to ’Y’ to deactivate the terminating SCC processing for CGPN which means for the trunks that have this new field set to ’Y’, Country Code is not going to be stripped off and NOA is not going to be changed while outpulsing the CGPN on the terminating side.

The limitations and restrictions for setting and changing the CGSCCDEA field is mentioned in “Limitations and Restrictions“ section of this document.

64.2.4.3 SIGNALLING:

When a CPGN is received from incoming side with NOA: INTL and SCC code is prefixed in IAM message:

- If the CGSCCDEA is set to ’N’ in Table TRKGRP, ‘terminating CGPN SCC processing’ will work according to feature AD9743; if the SCC prefix in CGPN matches the SCC datafill in TUPATTR/ISUPATTR tables for the outgoing trunk SCC will be stripped off and the NOA will be set to NATL for CGPN in outpulsed IAM message.
- If the CGSCCDEA is set to ’Y’ in Table TRKGRP, CGPN will be outpulsed as received.

When an INR message is received from terminating switch; while outpulsing the CGPN in INF message (if the CGPN to be sent has the NOA INTL and SCC code prefix):

- If the CGSCCDEA is set to ’N’ in Table TRKGRP, terminating CGPN SCC processing will work according to feature AD9743; if the SCC prefix in CGPN matches the SCC datafill in TUPATTR/ISUPATTR tables for the outgoing trunk SCC will be stripped off and the NOA will be set to NATL for CGPN in outpulsed INF message.
- If the CGSCCDEA is set to ’Y’ in Table TRKGRP, CGPN will be outpulsed with NOA INTL and SCC code prefix in INF message.

This functionality is introduced for interworkings which have the terminating side protocols: ETSI ISUP V1, ETSI ISUP V2, ANSI ISUP, RBTUP/BBTUP.

64.3 Hardware Requirements or Dependencies

None.

64.4 Software Requirements or Dependencies

None.

64.5 Limitations and restrictions

This functionality is introduced for interworkings which have the terminating side protocols: ETSI ISUP V1, ETSI ISUP V2, ANSI ISUP, RBTUP/BBTUP.

The new field will be set to ‘N’ by default for all axxess trunks including incoming, outgoing and two-way trunks. But it will be functional for only outgoing and two-way trunks.

As for datafill changes there are some restrictions and limitations:

64.5.1 When attempting to change the value of CGSCCDEA field in table TRKGRP:

For axxess trunks other than ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP, CGCCDEA field CAN NOT be changed to 'Y'.

If the field is attempted to be changed from 'N' to 'Y' for any AXXESS trunks other than ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP, error messages are displayed and modification can not be realized:

- For trunks other than ISUP/TUP:

"CGSCCDEA can be set to Y for ISUP and TUP protocols."

- For ISUP trunks other than ETSI ISUP V1, V2 and ANSI ISUP:

"CGSCCDEA can be set to Y for ISUP trunks datafilled in Table ISUPATTR

as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP."

- For TUP trunks other than RBTUP/BBTUP:

"CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP/BBTUP."

64.5.2 When attempting to change the value of Protocol field in table TRKGRP:

For axxess trunks if the CGCCDEA field is 'Y', the 'Protocol' field in Table Trkgrp cannot be changed to any protocol other than ISUP and TUP.

If the Protocol field is attempted to be changed from ISUP or TUP to any other protocol, an error message is displayed and modification can not be realized.

- For an Axxess trunk with the CGSCCDEA field 'Y' and protocol field ISUP or TUP in table TRKGRP:

"CGSCCDEA can be set to Y for ISUP and TUP protocols."

64.5.3 When attempting to change the value of Protidx field in table TRKGRP:

For axxess trunks if the CGCCDEA field is 'Y', the 'Protidx' field in Table Trkgrp cannot be changed to any index other than the indexes representing the supported variants.

If the Protidx field is attempted to be changed from an index representing a supported variant to any other index of an unsupported variant, an error message is displayed and modification can not be realized.

- For an Axxess trunk with the CGSCCDEA field ‘Y’ and protidx field in table TRKGRP representing a supported variant of ISUP:

“CGSCCDEA can be set to Y for ISUP trunks datafilled

in Table ISUPATTR as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.”

- For an Axxess trunk with the CGSCCDEA field ‘Y’ and protidx field in table TRKGRP representing a supported variant of TUP:

“CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP/BBTUP.”

64.5.4 While adding a new AXXESS trunk in Table TRKGRP:

Following error messages are displayed if the new trunk has the CGSCCDEA field as ’Y’ and the trunk is not a ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP TRUNK.

- For trunks other than ISUP/TUP:

“CGSCCDEA can be set to Y for ISUP and TUP protocols.”

- For ISUP trunks other than ETSI ISUP V1, V2 and ANSI ISUP:

“CGSCCDEA can be set to Y for ISUP trunks datafilled in Table ISUPATTR

as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.”

- For TUP trunks other than RBTUP/BBTUP:

“CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP/BBTUP.”

64.5.5 When CGSCCDEA field is set to ’Y’ :

For any of the trunks ETSI ISUP V1, ETSI ISUP V2 ,ANSI, RBTUP, BBTUP; an error message is displayed under the name of the trunk which has the CGSCCDEA field set to ’Y’ if there is an attempt to change the protocol in ISUPATTR/TUPATTR tables to a value other than ETSI V1, ETSI V2 , ANSI and RBTUP (protocols that do not support CGPN SCC deactivation) and it is not permitted to change the protocol variant in ISUPATTR/TUPATTR tables unless the CGSCCDEA field is changed to ‘N’ for all related trunks.

- “CGSCCDEA field is set to Y in Table TRKGRP”

64.6 Interactions

This feature is an enhancement of the SCC processing function in feature AD9743.

64.7 Applicable customer facing sections

Fault Management N/A

- Logs ___N/A___
- Alarms ____N/A__

Configuration

- Data Schema ____X__
- User Interface ____X__
- Element Management ___N/A___
- Security ___N/A___
- Service Order ___N/A___
- Office Parameters ___X___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ____N/A__

64.8 Glossary

Table 3

Term	Description
ANI	Automatic Number Identification
ANSI	American National Standards Institute
BBTUP	Blue Book TUP
CC	Country Code
CDPN	Called Party Number
CGPN	Calling Party Number
CLI/CLID	Calling Line Identity
ETSI	European Telecommunications Standards Institute
GSP	Global Services Platform
IAI	Initial Address Message with Additional Information
IAM	Initial Address Message
INR	Information Request
ISUP	Integrated Services Digital Network User Part

Table 3

Term	Description
NOA	Nature of Address
ONP	One Night Process
RBTUP	Red Book TUP
SCC	Serving Country Code
TON	Type Of Number
TUP	Telephony User Part

64.9 References

- AD9743 GLOBAL CARRIER SWITCH IN-SWITCH SERVICES

65: Functional Description (FN): A00004563

65.1 Feature name

Activity a00004563: Moroccan ISUP v2 on DMS100

65.2 Description

This activity addresses the following functionality:

1. Introduction of Moroccan ISUP version 2 as a new variant of ETSI ISUP version 2 signaling protocol
2. Support for Moroccan ISUP v2 - Moroccan ISUP v2 interworking
3. Tandem exchange functionality related to the following ISUP messages in a Moroccan ISUP v2 - Moroccan ISUP v2 interworking:
   - Charge (CRG)
   - Information Request (INR)
   - Information (INF)

The Moroccan ISUP v2 is built upon ETSI ISUP v2 BASE variant.

The requirements for Moroccan ISUP v2 are stated in Maroc Telecom Specific Requirements version 1.5.

65.2.1 Introduction of New Variant

The Moroccan ISUP v2 variant is introduced to the DMS. As a result, it is possible to perform calls over a trunkgroup that is datafilled as of Moroccan ISUP v2 variant.

The following is a sample datafill in table TRKSGRP for outgoing (OG), incoming (IC) and two-way (2W) Moroccan ISUP v2 trunks:

Figure 1 Sample TRKSGRP datafill for Moroccan ISUP v2 trunks

```
TABLE: TRKSGRP
SGRPKEY CARDCODE SGRPVAR SGRPVAR
-------------------------------
OGMRISUPV2 0 DS1SIG C7UP OG N N UNEQ NONE Q767 THRH 0 DMS N N
MOROCCO 100_WHITE $ OGN7

ICMRISUPV2 0 DS1SIG C7UP IC N N UNEQ NONE Q767 THRH DMS
MOROCCO 100_WHITE $ ICN7

2WMRISUPV2 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMS N N
MOROCCO 100_WHITE $ 2WN7 CIC
```

Table C7UPTMR is used to datafill the signaling timers applying to a specific trunk subgroup in table TRKSGRP. Table C7UPTMR is not modified by this activity but an example is presented here for completeness.

Figure 2 Sample C7UPTMR datafill for Moroccan ISUP v2 timers

```
TABLE: C7UPTMR

TMRKEY C7UPDIR TMRS OPTIONS
---------------------------
OGN7 OG Q767 15 180 326 60 90 20 180 10 60 10 60 1000 10 120 240 10 $

ICN7 IC Q767 15 180 326 60 90 15 5 15 10 60 10 60 10 60 10 60 10 60
10 60 10 120 240 10 20 4 $

2WN7 2W Q767 15 180 326 60 90 20 15 180 5 15 10 60 10 60 10 60 10 60
10 60 10 60 1000 10 120 240 10 15 20 4 10 $
```

65.2.2 Interworking Support

This activity supports **only** Moroccan ISUP v2 - Moroccan ISUP v2 interworking.

For other interworkings supported by Moroccan ISUP v2, please refer to the following activity documentation:

- a00004563: Line to Moroccan ISUP V2 Interworking
- a00004560: Moroccan ISUP - ISDN Interworking
- a00004557: Moroccan R2 and Interworkings

65.2.3 Supported Messages and Parameters

65.2.3.1 Supported Messages

This activity supports the ISUP v2 messages presented in Table 1, “Supported Messages in Moroccan ISUP v2,” on page 1347”. Please note that the level of support is restricted to **tandem exchange functionality only**.

Table 1 Supported Messages in Moroccan ISUP v2

Message Name	Message Code
Address Complete	#06
Answer	#09
Blocking	#13
Blocking Acknowledgement	#15
Call Progress	#2C
Charge	#31
Circuit Group Blocking	#18
Circuit Group Blocking Acknowledgement	#1A
Circuit Group Reset	#17
Circuit Group Reset Acknowledgement	#29
Circuit Group Unblocking	#19
Circuit Group Unblocking Acknowledgement	#1B
Confusion	#2F
Connect	#07
Continuity	#05
Continuity Check Request	#11
Facility	#33
Facility Accepted	#20
Facility Rejected	#21
Facility Request	#1F
Forward Transfer	#00
Information	#04
Information Request	#03

Message Name	Message Code
Initial Address	#01
Pre-release Information	#42
Release	#0C
Release Complete	#10
Reset Circuit	#12
Resume	#0E
Segmentation	#38
Subsequent Address	#02
Suspend	#0D
Unblocking	#14
Unblocking Acknowledgement	#16
User-to-user Information	#2D

65.2.3.2 Supported Parameters

The set of parameters supported in Moroccan ISUP v2 messages is the same as in ETSI ISUP v2 BASE variant, unless otherwise stated.

The differences with respect to the ETSI ISUP v2 BASE variant are listed in the subsequent tables. Please note that the level of support is restricted to **tandem exchange functionality only** for all parameters.

- A parameter of type “F” is a mandatory parameter for the specified message and has a fixed length as specified in ITU-T Recommendation Q763.
- A parameter of type “V” is a mandatory parameter for the specified message and can have a variable length as specified in ITU-T Recommendation Q763.
- A parameter of type “O” is an optional parameter for the specified message and can have a variable length as specified in ITU-T Recommendation Q763.

Table 2 Supported Parameters in Initial Address Message

Parameter Name	Parameter Type
Message type	F
Nature of connection indicators	F

Parameter Name	Parameter Type
Forward call indicators	F
Calling party's category	F
Transmission medium requirement	F
Called Party Number	V
Calling Party Number	O
Optional Forward call indicators	O
Redirecting number	O
Redirection information	O
CUG interlock code	O
Original Called Number	O
User-to-user information	O
Access transport	O
Generic number	O
Propagation delay counter	O
User teleservice information	O
Service Activation	O
CCBS parameter	O
Generic digits	O
Parameter Compatibility Information	O
Generic notification	O
Location number	O
Hop Counter	O
End of Optional Parameters	O

Table 3 Supported Parameters in Address Complete Message

Parameter Name	Parameter Type
Message Type	F
Backward Call Indicators	F
Optional Backward Call Indicators	O
Cause Indicators	O

Parameter Name	Parameter Type
User-to-User Indicators	O
User-to-User Information	O
Access Transport	O
Generic Notification	O
Access Delivery Information	O
Redirection Number	O
Parameter Compatibility Information	O
Call Diversion Information	O
Redirection Number Restriction	O
End of Optional Parameters	O

Table 4 Supported Parameters in Answer Message

Parameter Name	Parameter Type
Message Type	F
Backward Call Indicators	O
Optional Backward Call Indicators	O
User-to-User Indicators	O
User-to-User Information	O
Connected Number	O
Access Transport	O
Access Delivery Information	O
Generic Notification	O
Parameter Compatibility Information	O
Generic Address	O
Redirection Number	O
Redirection Number Restriction	O
End of Optional Parameters	O

Table 5 Supported Parameters in Call Progress Message

Parameter Name	Parameter Type
Message Type	F
Event Information	F
Cause Indicators	O
Backward Call Indicators	O
Optional Backward Call Indicators	O
Access Transport	O
User-to-User Indicators	O
Redirection Number	O
User-to-User Information	O
Generic Notification	O
Access Delivery Information	O
Parameter Compatibility Information	O
Call Diversion Information	O
Redirection Number Restriction	O
Call Transfer Number	O
End of Optional Parameters	O

Table 6 Supported Parameters in Facility Message

Parameter Name	Parameter Type
Message Type	F
Access Transport	O
Generic Notification	O
Message Compatibility Information	O
Parameter Compatibility Information	O
Call Transfer Number	O
End of Optional Parameters	O

Table 7 Supported Parameters in Connect Message

Parameter Name	Parameter Type
Message Type	F
Backward Call Indicators	F
Optional Backward Call Indicators	O
Connected Number	O
User-to-User Indicators	O
User-to-User Information	O
Access Transport	O
Generic Notification	O
Access Delivery Information	O
Parameter Compatibility Information	O
Redirection Number	O
Generic Address	O
Redirection Number Restriction	O
End of Optional Parameters	O

- The *Charge Message* is nationally defined for Moroccan ISUP v2. The structure of the message is presented in detail in Table 8, “Supported Parameters in Charge Message,” on page 1352. This activity is responsible **only** for the tandeming of the Charge Message in a Moroccan ISUP v2 - Moroccan ISUP v2 interworking.

Table 8 Supported Parameters in Charge Message

Parameter Name	Parameter Type	Parameter Code	Parameter Length
Message Type	F	N/A	1
Tariff Index	O	#FF	3
Pulse Number	O	#FE	3
Parameter Compatibility Information	O	#39	4
End of Optional Parameters	O	#00	1

- The Moroccan ISUP v2 uses the *Information Request* and *Information Messages* as defined in ITU-T Recommendation Q.763. The message formats are included here for convenience only.

Table 9 Supported Parameters in Information Request Message

Parameter Name	Parameter Type
Message Type	F
Information Indicators	F
Call Reference	O
Calling Party Number	O
Calling Party's Category	O
Connection Request	O
Network Specific Facility	O
Parameter Compatibility Information	O
End of Optional Parameters	O

Table 10 Supported Parameters in Information Message

Parameter Name	Parameter Type
Message Type	F
Information Request Indicators	F
Call Reference	O
Network Specific Facility	O
Parameter Compatibility Information	O
End of Optional Parameters	O

65.2.4 Handling of Called Party Number Parameter in IAM

65.2.4.1 Numbering Plan Indicator (NPI) field in CdPn:

- The Moroccan ISUP supports **only** the "ISDN Telephony Numbering Plan" value for the NPI field in the CdPn parameter in an IAM.
- In order to support other values of NPI in the IAM CdPn, the incoming and/or outgoing Moroccan ISUP v2 trunk must be provisioned with the

ALL_NPI option via table *TRKSGRP*. An attempt to receive and/or transmit an IAM with an unsupported NPI value results in the **release** of the call.

65.2.4.2 Nature of Address (NOA) field in the CdPn:

- The Moroccan ISUP supports **only** the following values for the NOA field in the CdPn parameter in an IAM:
  - *Subscriber Number*
  - *National Significant Number*
  - *International Number*
- In order to support other values of NOA in the IAM CdPn, the incoming and/or outgoing Moroccan ISUP v2 trunk must be provisioned with the **ALL_NOA** option via table *TRKSGRP*. An attempt to receive and/or transmit an IAM with an unsupported NOA value results in the **release** of the call.
- In a Moroccan ISUP v2- Moroccan ISUP v2 interworking, the NOA of the CdPn in the outgoing IAM is determined accordking to the **translation class datafill:**

Table 11 Setting CdPn NOA via translation class

Translation Class Datafill	NOA of the Called Party Number in the outgoing IAM
No class datafill **($)**, Intragroup **(IAGRP)**	Same as the CdPn NOA in the incoming IAM
International **(INTL)**, Intercontinental **(ICNTL),** International Operator Assisted **(IOPRA)**	International Number (#04)
National **(NATL)**, Continental **(CNTL)**, Operator Assisted **(OPRA)**, Cellular **(CELL)**	National Significant Number (#03)
Local **(LCL)**	Subscriber Number (#01)
Other classes	Subscriber Number (#01)

65.2.5 Timers

The Moroccan ISUP v2 functionality supports the ISUP timers indicated in ITU-T Recommendation Q.764, “Signalling System No.7 - ISDN user part signaling procedures”.

The timers **not** supported by Moroccan ISUP v2 are listed in Table 12, "Timers not supported by Moroccan ISUP v2":

Table 12 Timers not supported by Moroccan ISUP v2

Timer Name	Associated Functionality	ITU-T Reference
T3	Temporary Trunk Blocking	Q.764, 2.9.9
T29, T30	Congestion Control	Q.764, 2.10.2
T31, T32	ISUP - SCCP signaling	Q.730 1.4.7.3, 1.4.7.4.1, 1.4.7.4.2, 1.4.7.5
T38	Suspend/Resume functionality in an incoming international gateway exchange	Q.764 2.4.1, 2.4.2, 2.4.3
T39	Malicious Call Identification (MCID)	Q.731.7

65.2.6 Supported Call Functionality & Services

This section outlines the functionality & services supported by Moroccan ISUP v2. The level of support is restricted to **tandem exchange functionality only**.

65.2.6.1 Basic Call Capabilities & Procedures

- Speech/3.1 kHz audio
- 64 kbit/s unrestricted
- Compatibility procedure
- Confusion procedure
- Tones and announcements
- MTP pause and resume
- Access delivery information
- Transportation of User teleservice information
- Generic number transfer
- Generic digit transfer
- Generic notification procedure
- Simple Segmentation procedure (IAM only)

65.2.6.2 Supplementary Services

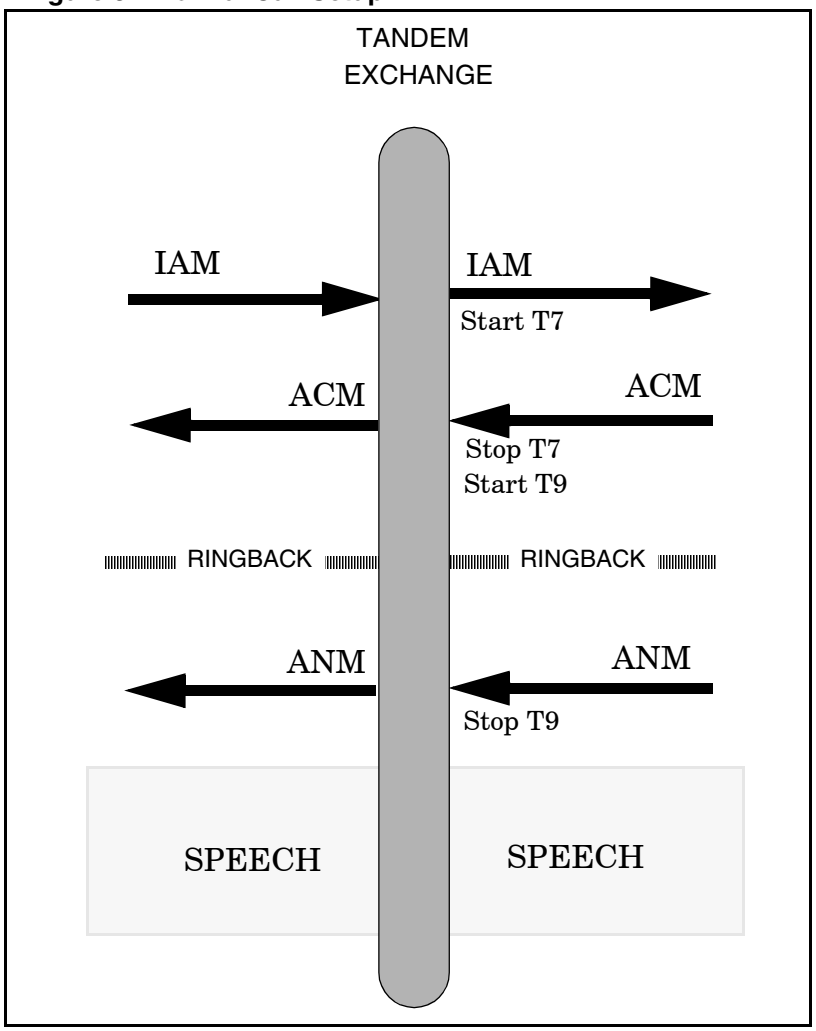
- CLIP/CLIR
- COLP/COLR
- SUB
- TP

- CFU/CFB/CFNR
- CD
- CW
- HOLD
- CONF
- 3PTY
- CUG
- UUS service 1 (implicit)/1 (explicit)/2/3
- ECT
- CCBS
- MCT (CLF)
- MCID

65.2.7 Typical Call Scenarios

65.2.7.1 Normal Call Setup

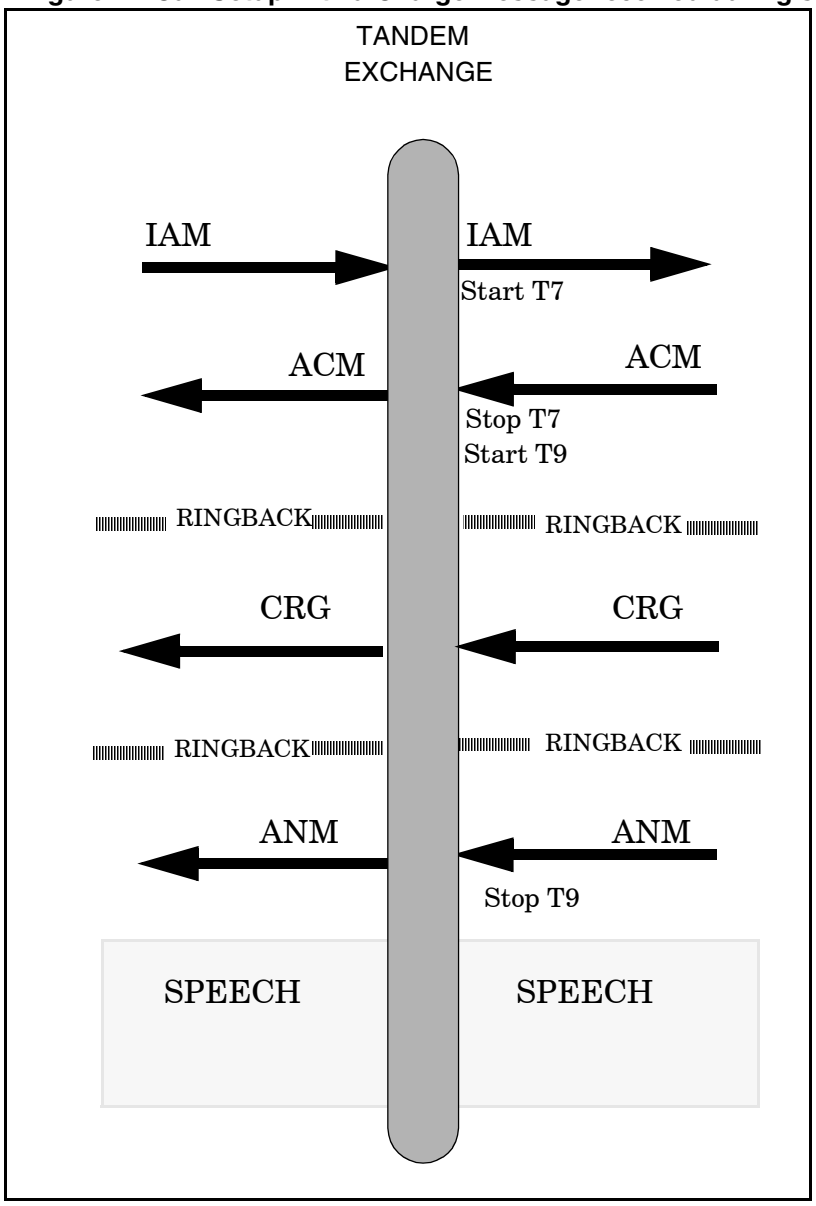
Figure 3 Normal Call Setup



- Timer T7 is started upon sending the IAM, and stopped upon receiving the first backward call setup message (ACM in this case).
- Timer T9 is started upon receiving the ACM, and stopped upon receiving the answer indication (ANM in this case).

65.2.7.2 Call with a Charge Message received during call setup

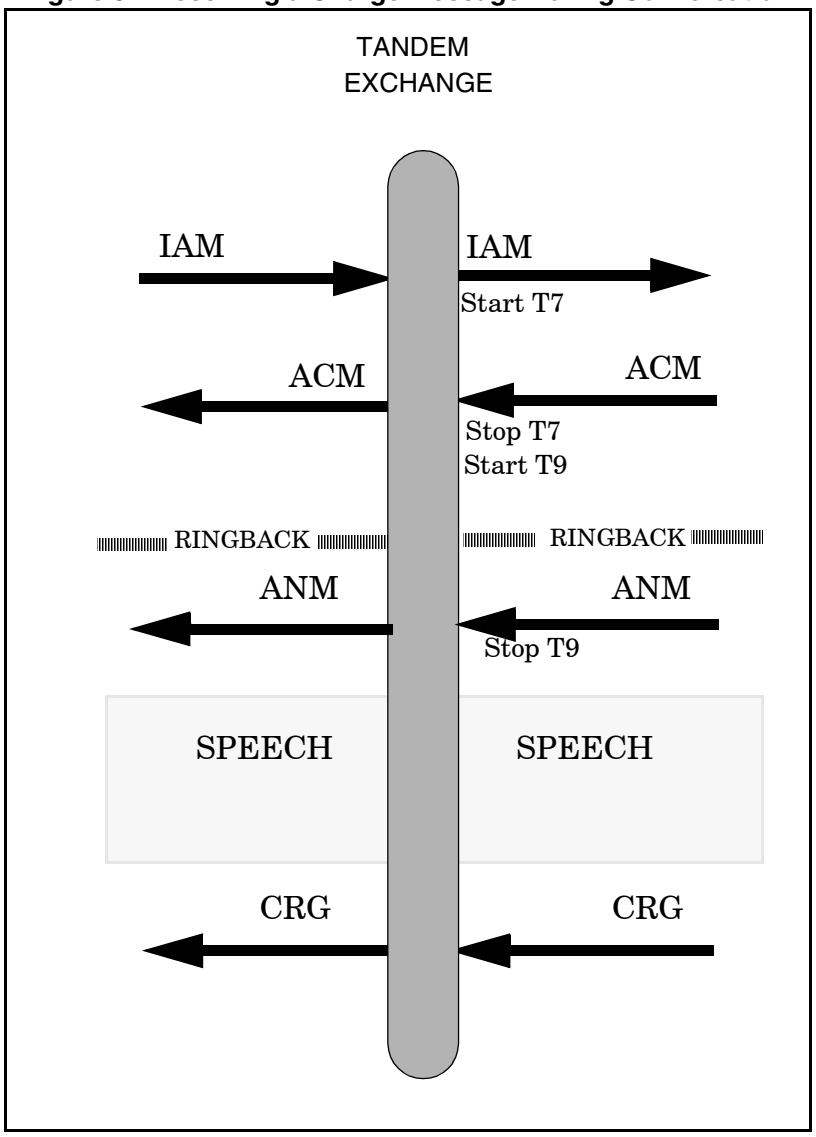
Figure 4 Call Setup with a Charge Message received during setup



- The DMS tandems the CRG message as is.
- No timers specific to CRG message are implemented in the tandem exchange.
- Timers T9 is not impacted by CRG message.

65.2.7.3 Call with a Charge Message received during conversation

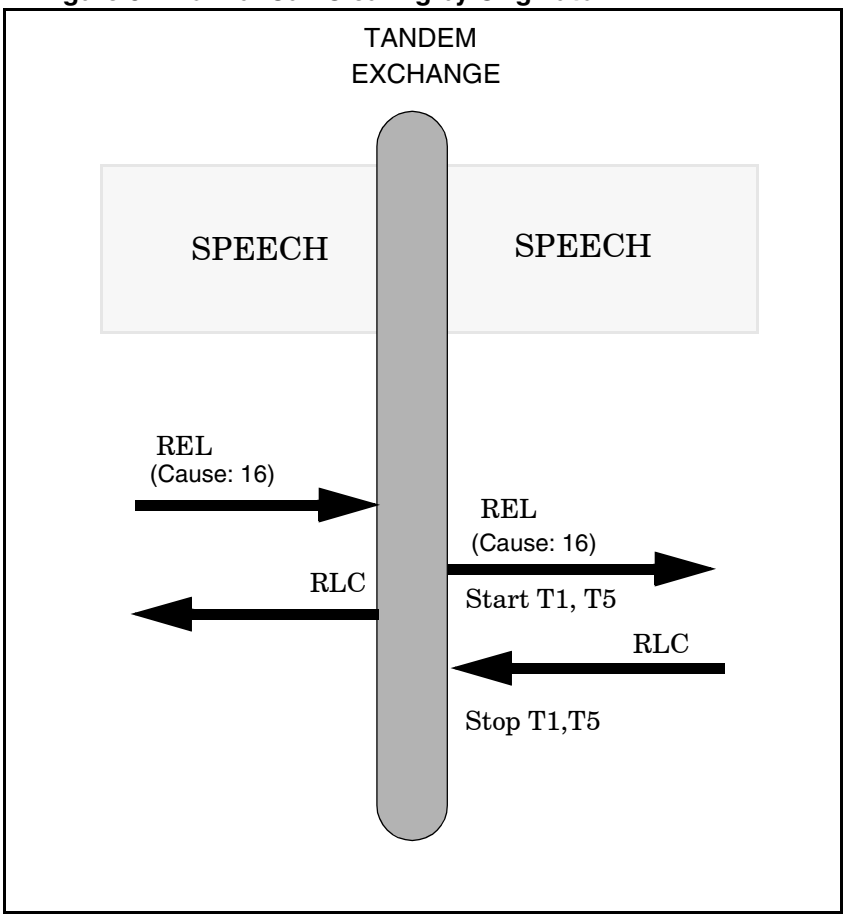
Figure 5 Receiving a Charge Message During Conversation



- The DMS tandems the CRG message as is.
- No timers specific to CRG message are implemented in the tandem exchange.

65.2.7.4 Normal Call Clearing by Originator

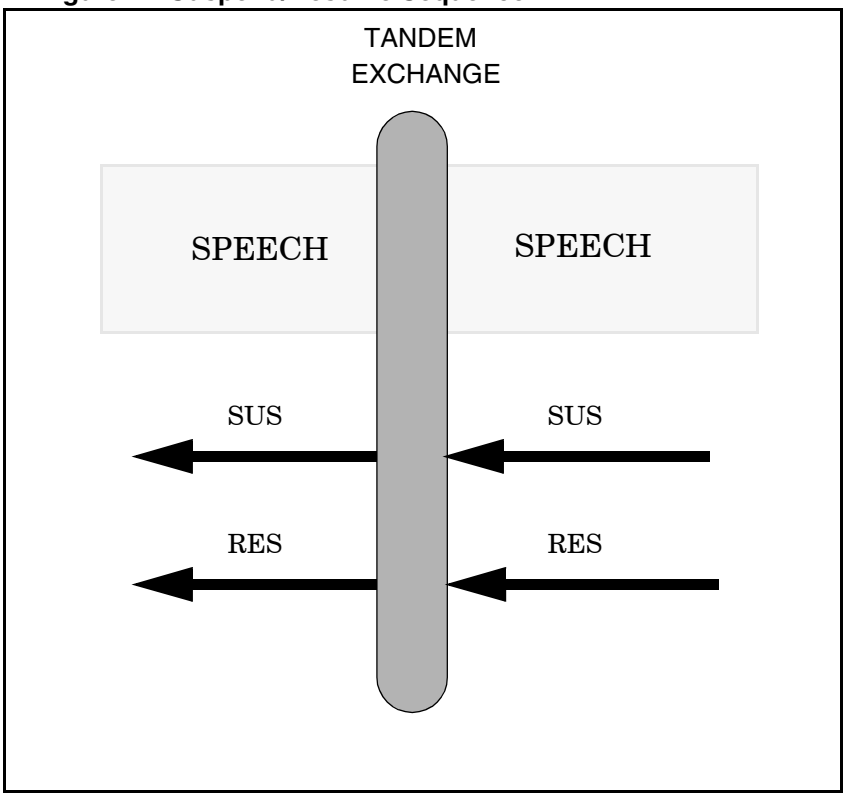
Figure 6 Normal Call Clearing by Originator



- Normal call clearing by the originator is performed using an ISUP REL message with cause 16, “normal call clearing”.
- Upon sending the REL message in an exchange, T1 and T5 timers are started.
- Upon receiving the release completion indication (RLC), the T1 and T5 are stopped in that exchange.

65.2.7.5 Suspend/Resume Sequence (Terminator's Exit)

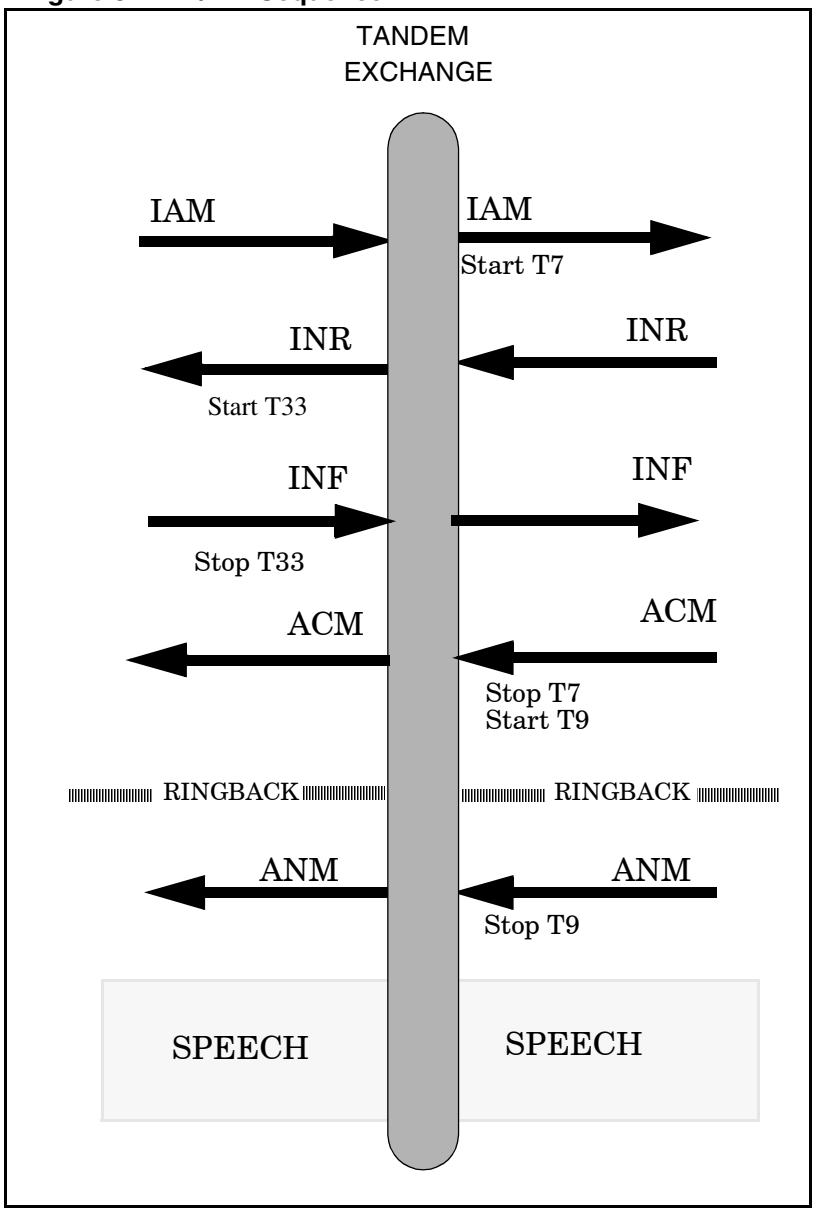
Figure 7 Suspend/Resume Sequence



- The Moroccan ISUP v2 Suspend/Resume functionality is limited to tandeming of SUS and RES messages **only**. **No timers are maintained in the tandem exchange.**

65.2.7.6 Information Request (INR/INF) Sequence

Figure 8 INR/INF Sequence



- The INR/INF sequence is invoked by the terminating exchange to request data from the preceding office(s) which are needed by the terminating exchange to complete the call setup.
- The INR/INF messages are **tandemed** transparently in a Moroccan ISUP v2 - Moroccan ISUP v2 interworking.
- In a Moroccan ISUP v2 - Moroccan ISUP v2 tandem, timer T33 is started upon sending the INR message to the preceding exchange and stopped upon receiving the INF message.

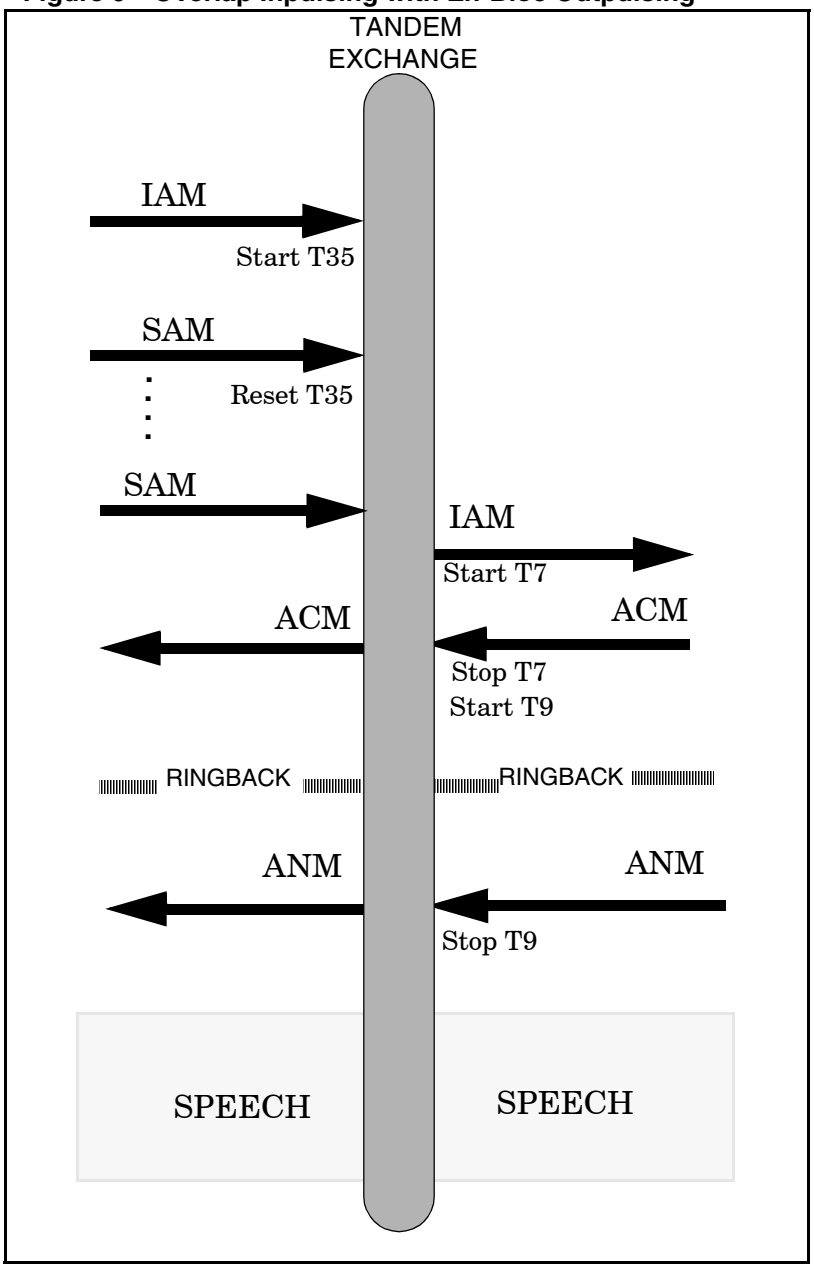
65.2.7.7 Overlap Signaling

- The Moroccan ISUP v2 supports the following overlap signaling procedures:
  - Overlap Inpulsing, en-bloc outpulsing
  - Overlap Inpulsing, overlap outpulsing
- On the inpulsing side, timer T35 is maintained during the receipt of multiple address messages.
- Upon obtaining the minimum address information (i.e. Called Party Number digits) to route the call, the DMS attempts to continue the call setup. The minimum address information needed for routing is determined by the translation datafill.

Note: *In case of overlap inpulsing and en-bloc outpulsing, the translation used for a specific call must ensure that the IAM is not sent too early, i.e. with insufficient CdPN digits, to the succeeding exchange. Otherwise, there is no possibility for tandeming the SAMs that are received after the IAM has been sent, and the call cannot be established due to incomplete address information.*

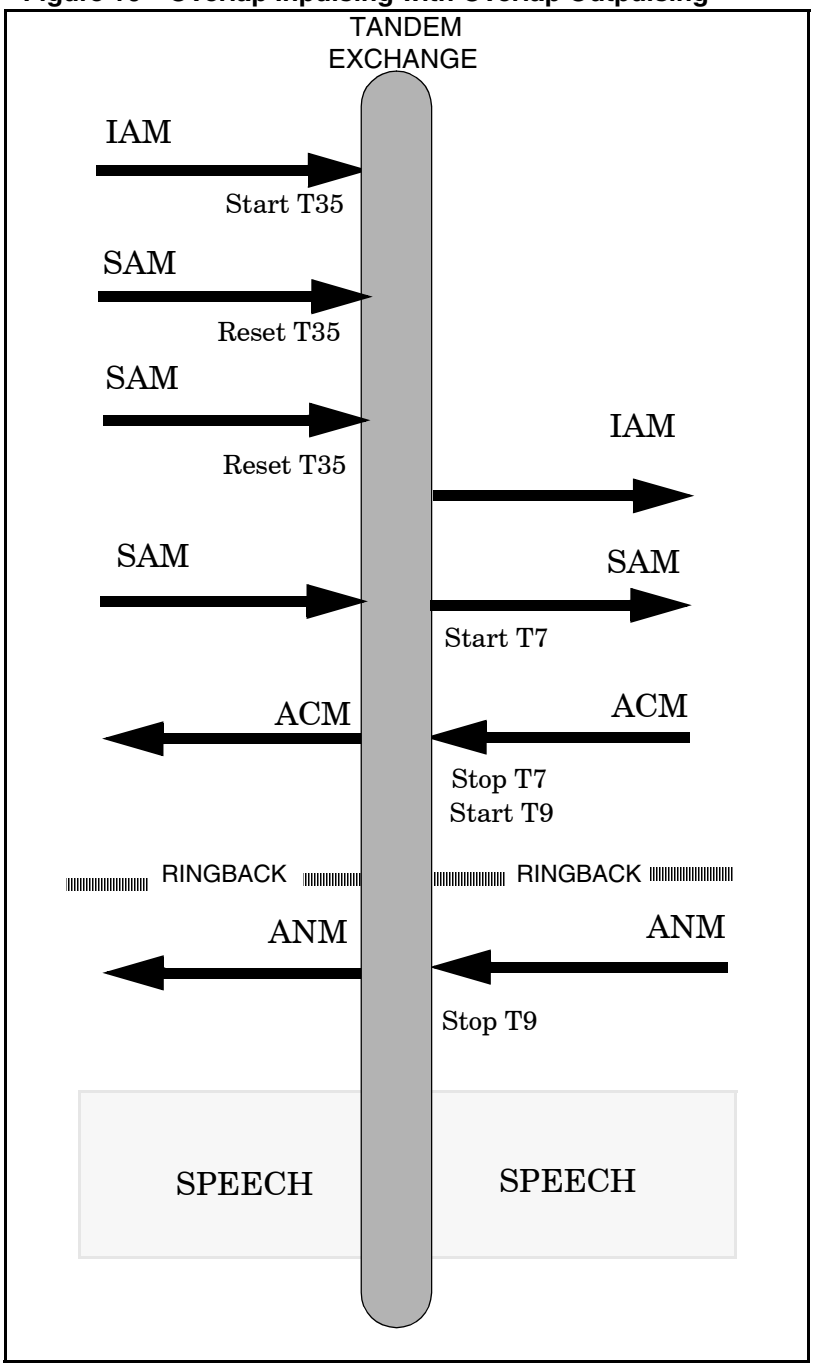
65.2.7.7.1 Overlap Inpulsing with En-Bloc Outpulsing

Figure 9 Overlap Inpulsing with En-Bloc Outpulsing



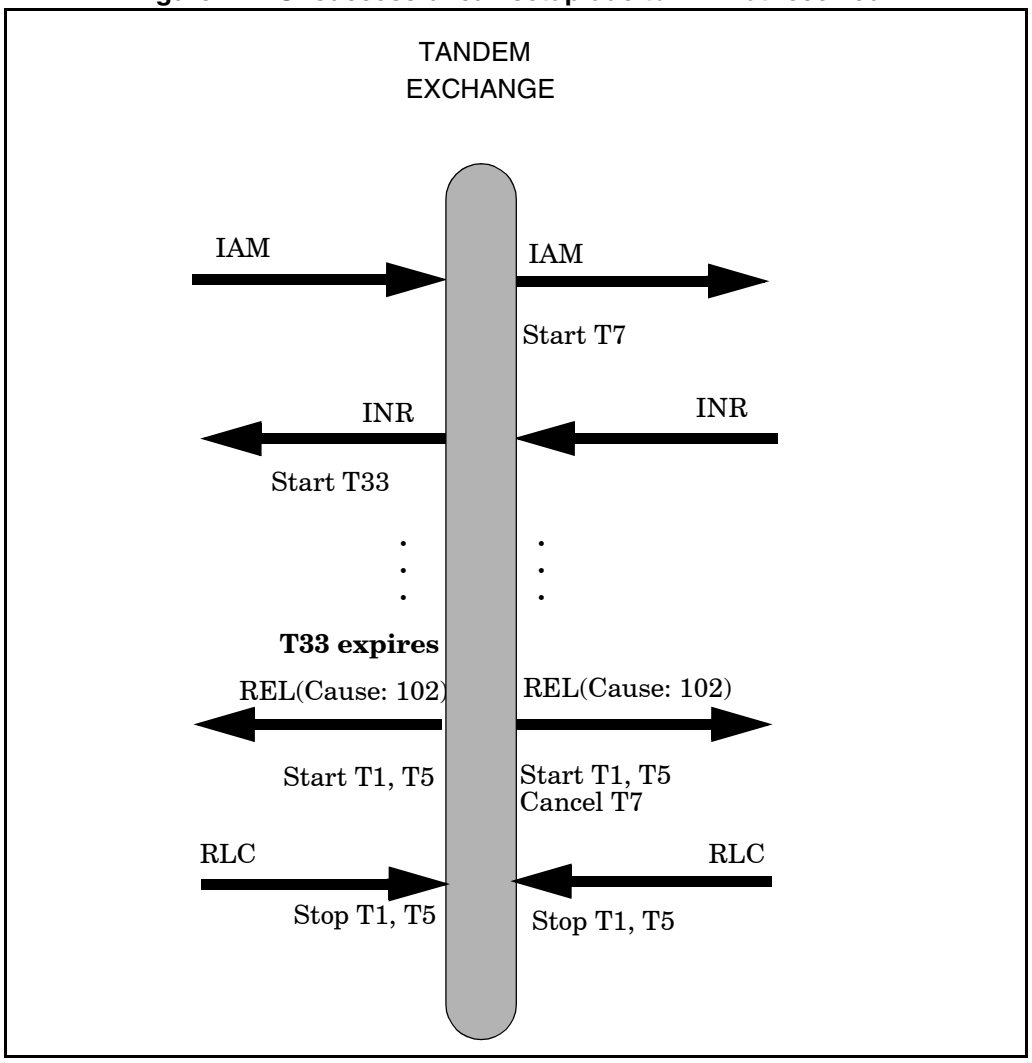
65.2.7.7.2 Overlap Inpulsing with Overlap Outpulsing

Figure 10 Overlap Inpulsing with Overlap Outpulsing



65.2.7.8 Unsuccessful call setup due to INF time-out

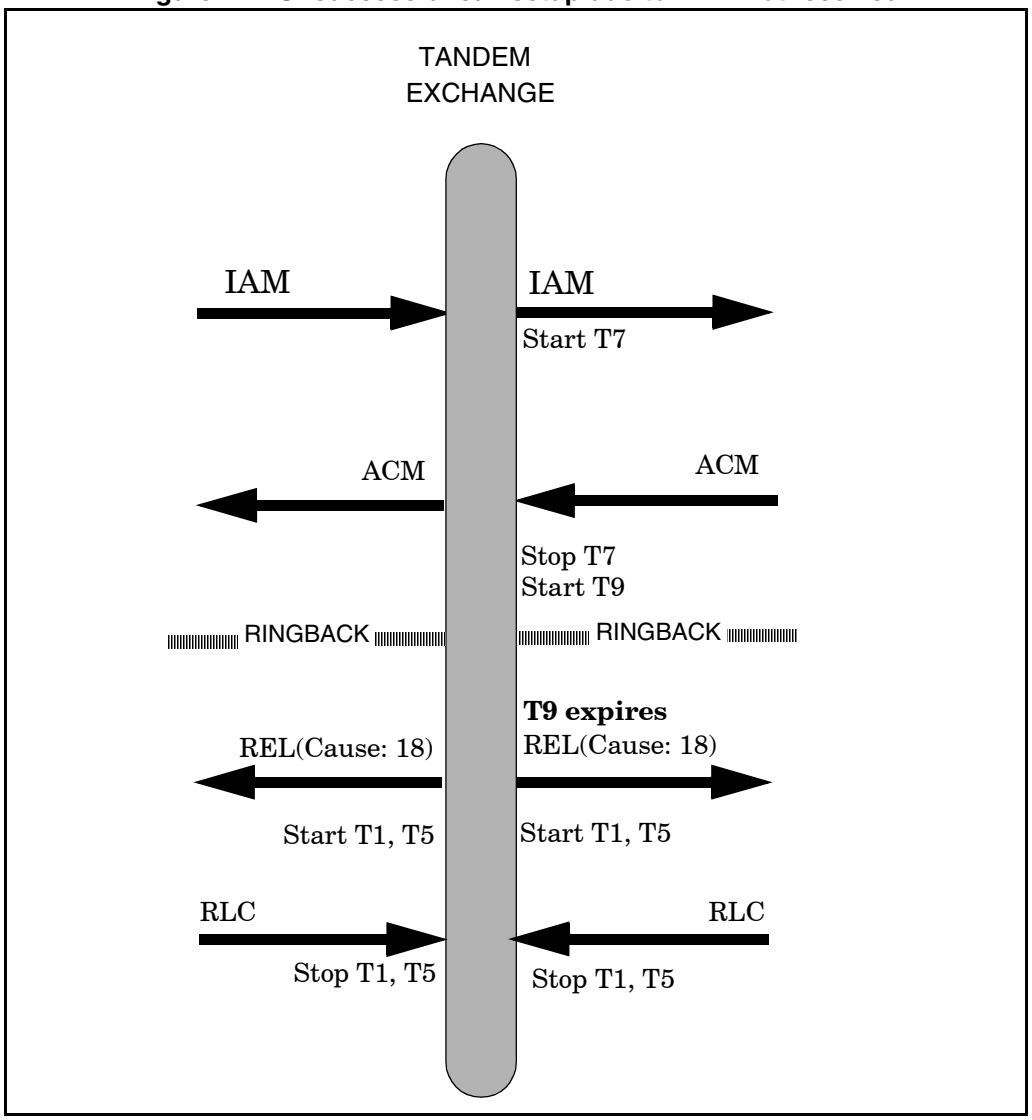
Figure 11 Unsuccessful call setup due to INF not received



- Upon tandeming of the INR message, timer T33 is started.
- If no INF message is received before T33 expiry, the tandem exchange releases the call by sending an ISUP REL message with cause 102, “Recovery on Timer Expiry” in both directions.
- Upon sending the REL message in the tandem exchange, T1 and T5 timers are started.
- Upon receiving the release completion indication (RLC), the T1 and T5 are stopped in that exchange.

65.2.7.9 Unsuccessful call setup due to ANM time-out

Figure 12 Unsuccessful call setup due to ANM not received



- Upon receiving the ACM, timer T9 is started in the tandem exchange.
- If no ISUP ANM is received before T9 expiry, the connection is released in both directions using an ISUP REL message with cause 18, “No user responding”.
- Upon sending the REL message in the tandem exchange, T1 and T5 timers are started.
- Upon receiving the release completion indication (RLC), the T1 and T5 are stopped in that exchange.

65.3 Hardware Requirements or Dependencies

The functionality provided by this activity is supported for **SX05** XPM processors **only**.

65.4 Software Requirements or Dependencies

N/A

65.5 Limitations and restrictions

1. Please refer to the appropriate section of the documentation for possible restrictions/limitations on a specific functional item.
2. Multirate connection types (2x64, 384, 1536 and 1920kbit/s) are **not** supported.
3. Signalling procedures for connection type allowing fallback capability are **not** supported.
4. **No** compatibility procedures are invoked in case of receiving recognized optional parameters with unsupported/unrecognized/spare/reserved values (ITU-T Q.764, 2.9.5.3.3.b).
5. Simple segmentation is supported for the segmentation of the IAM **only**..
6. User part availability control is **not** supported.
7. Propagation delay determination procedure is **not** supported.
8. Echo control procedure is **not** supported.
9. End-to-end signalling Pass along method is **not** supported.
10. End-to-end signalling SCCP Connection Orientated is **not** supported.
11. Simple service activation procedure is **not** supported.
12. Remote operations procedure is **not** supported.
13. Network specific facility procedures is **not** supported.

65.6 Billing

This activity does not implement or modify a functionality related to billing.

65.7 Interactions

N/A

65.8 Applicable customer facing sections

Fault Management

Logs	__N/A___
Alarms	__N/A____

Configuration	
Data Schema	__X_____
User Interface	__N/A____
Element Management	__N/A____
Security	__N/A____
Service Order	__N/A____
Office Parameters	__N/A____
Accounting (includes AMA billing)	__N/A____
Performance (includes operational measurements)	__N/A____

65.9 Glossary

Term	Description
3PTY	3-Party Calling
ACM	Address Complete Message
ANM	ANswer Message
CCBS	Completion of Calls to Busy Subscribers
CD	Call Diversion
CdPn	Called Party Number
CFU	Call Forward Unconditional
CFB	Call Forward Busy
CFNR	Call Forward No Reply
CLIP	Calling Line Identification Presentation
CLF	Calling Line Identification with Flash
CLIR	Calling Line Identification Restriction
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CONF	Conference
CRG	Charge Information
CUG	Closed User Group
CW	Call Waiting
DMS	Digital Multiplex Switch
ECT	Explicit Call Transfer
ETSI	European Telecommunication Standards Institute
HOLD	Call Hold
IAM	Initial Address Message
INF	Information
INR	Information request

ISDN	Integrated Services Digital Network.
ISUP	ISDN User Part
ITU	International Telecommunication Union
MCID	Malicious Call Identification
MCT	Malicious Call Trace
NOA	Nature of Address
REL	RELease message
RES	RESume message
RLC	ReLease Complete message
SAM	Subsequent address
SCCP	Signalling Connection Control Port
SUB	Sub Addressing
SUS	SUSpend message
Tn	Timer n
TP	Terminal Portability
UUS	User to User Signalling
XPM	Extended Peripheral Module

65.10 Recommended Reading/References

1. Maroc Telecom Specific Requirements, High Level, v 1.5
2. AJ4319FN: ETSI ISUP V2 On The DMS100E
3. ITU-T Recommendations Q.763: Signalling System No.7 - ISDN User Part formats and codes
4. ITU-T Recommendations Q.764: Signalling System No.7 - ISDN User Part Signalling Procedures
5. SIM Specification NIS A246-1: ISN04 ETSI ISUP COMPLIANCE

66: Functional Description (FN): A00004565

66.1 Feature name

A00004565 - Line to Moroccan ISUP V2 interworking

A00004551 - Backward Metering For Morocco

66.2 Description

66.2.1 Functional Overview

The activity A00004565 “Line to Moroccan ISUP V2 interworking ” provides line to Moroccan ISUP V2 and Moroccan ISUP V2 to line interworkings. Addition to the ISUP V2 messages, national use messages CRG, INR and INF are supported.

The activity A00004551 “Backward Metering For Morocco” provides backward metering functionality at the originating office for Moroccan ISUP calls. Received metering information in Moroccan ISUP V2 CRG message will be used to meter originating agent with MOG option.

IBN, BRI and V5.2 (IBN, BRI) lines are supported by these activities.

These activities are implemented in ISN07 for TDM.

66.2.2 Feature Description

This feature supports line to Moroccan ISUP V2 and Moroccan ISUP V2 to line interworkings. National use CRG, INR and INF messages are supported by this activity.

66.2.2.1 Line to Moroccan ISUP V2 and Moroccan ISUP V2 to line interworkings

Line to Moroccan ISUP V2 and Moroccan ISUP V2 to line interworking behaviours are same as line to Turkish ISUP V2 and Turkish ISUP V2 to line interworkings. So, for this interworkings please refer to FN section of A59018055.

Also, please refer to FN section of A59012394 (section 2.2.1.4.3. Supported Services for Turkish ISUP V2 and 2.2.1.4.4. Unsupported Services) for supported and unsupported services.

66.2.2.2 INR/INF sequence

During call setup in a Moroccan ISUP V2 - line interworking, the terminating exchange can initiate an INR/INF message sequence to request CPC and/or CLI information from the preceding exchange(s) if one or both of them are not received in the incoming IAM message.

The INR/INF sequence is initiated depending on the datafill in table ISUPSVC.

Default tuples for ISUP variants exist in table ISUPSVC. Default tuples in Moroccan ISUP V2 is shown in Figure 1, "Default Tuple in table ISUPSVC".

Figure 1 Default Tuple in table ISUPSVC

```
>table isupsvc
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISUPSVC
>lis all
TOP
             KEY                                                    SERVICE
-------------------------------------------------------------------------
 MOROCCAN_EIV2   (INR_INF GENERATION_AND_RECEPTION (CGN_REQUESTED)
                   (CPC_REQUESTED) $)$
BOTTOM
>
```

66.2.2.3 Backward Metering Activation and Behaviour

Backward metering information is sent to originating office by a central office with ISUP CRG message to perform metering locally in the originating office.

Two types of CRG message are used by Moroccan ISUP V2 to send backward metering information.

- CRG message which includes tariff index
- CRG message which includes pulse count

There are two types of backward metering provided within this feature according to the used CRG message type:

- ***Local type backward metering:***
  Tariff index is received as backward metering information inside Morocco ISUP V2 CRG message before ISUP ANM/CON message. This tariff index is used for calculating meter counts and updating software meter register of the call locally. Also for hardware metered

lines, pulses are generated according to the MTRTARIFF datafill of received tariff index .

- ***Distance type backward metering:***
  Pulse count is received as backward metering information inside Morocco ISUP V2 CRG messages after ISUP ANM/CON message. This pulse count is accumulated and used for updating software meter register of the call locally. Also for hardware metered lines, received amount of pulse is generated.

The type of backward metering to be performed depends on the reception sequence of the Moroccan ISUP V2 CRG Message

Morocco ISUP calls that will be charged using backward metering is determined via a newly introduced translation option BCKWMTR at the originating office.

BCKWMTR option is added to the OSEL (option selector) field of HEAD and CODE translation tables. BCKWMTR option does not have any subfields. See sample datafill below for PXCODE table.

Figure 2 Sample Datafill in Table PXCODE

```
TABLE: PXCODE
>lis
 XLANAME        FROMD           TOD
                                                              XLADATA
------------------------------------------------------------------
  NETXLA          783           783
CONT (PF 3) (MM 7 7) (CLASS LCL) (XLT OFC OFC783) (LNET INTL)
(MZONE 4) (BCKWMTR) $
>
```

Please note that software metering using local metering datafills is not applied when BCKWMTR is used in translation.

For the calls with BCKWMTR translation option, originating line software and hardware metering is performed using received backward metering information.

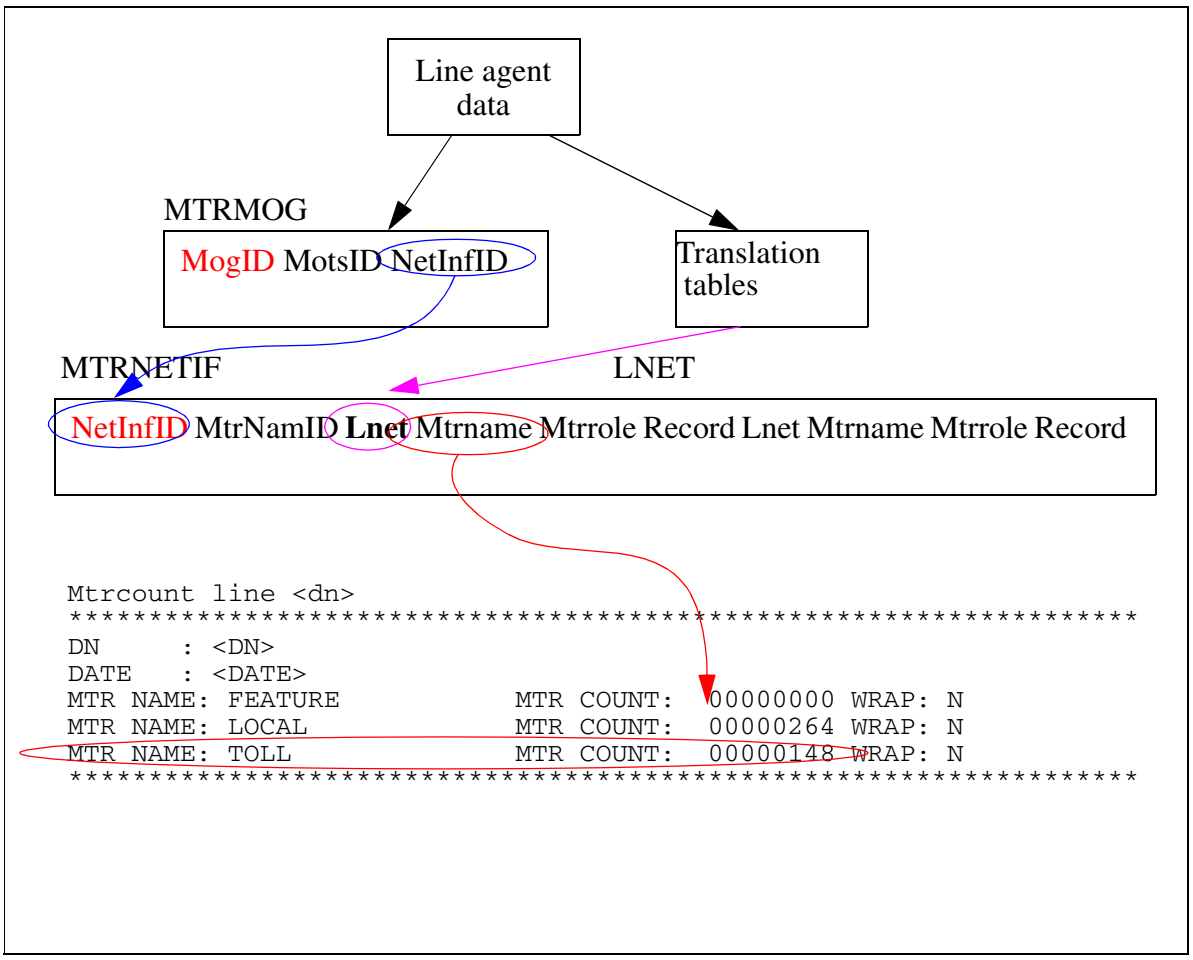
If the below conditions are not met, the call will not be metered by received backward metering information although BCKWMTR option is datafilled:

- Line must have MOG option for line metering
- Line must have SPM/COIN option for line hardware metering
- LNET value must be datafilled in translation tables for both type backward metered call.
- CRG timer must be datafilled in table C7UPTMR.

- Received tariff index must be datafilled in table MTRTARIF for local type backward metered calls.
- A meter name must be datafilled in table MTRNETIF with GENERATE meter role for used LNET.

LNET and MOGID values are used to index the meter name that will be incremented for backward metering call.

Figure 3 Indexing of meter name using LNET and MOGID values



If LNET value is not datafilled in backward metering translation, this missing datafill is reported with an MTR113 log and backward metering is not performed. If MFP parameter in table MTRSYSPM is set to FAIL, the call is sent to treatment otherwise call is not metered for this case.

New MTR logs MTR161 and MTR162 are defined to report backward metering specific failures.

MTR161 log is generated if a matching MTRTARIF tuple could not be found for a received tariff index within Moroccan ISUP V2 CRG message.

If a Moroccan ISUP V2 CRG tariff message with 0 tariff index is received then the call is not charged. Note that, despite 0 tariff index cannot be datafilled in MTRTARIF, it's used as free tariff index by metering system and MTR161 log is not generated for this case.

MTR162 log is generated for two cases:

- When a mismatch occurs between calculated software meter count and reported hardware metering pulse count for local type backward metering
- When a mismatch occurs between received meter count and reported hardware metering pulse count for distance type backward metering

Tariff change over in local office does not take affect for backward metered calls.

If the call is not line to Morocco ISUP V2 interworking then BCKWMTR option in translation is not taken into consideration.

If an ANM,ACM,CON or CPG message with no charge in BCI parameter is received, then the call will not be charged.

Note that, if an ISUP message with no charge in BCI parameter is received during the message sequence, the charge indicator in the following ISUP messages is not taken into consideration by the metering system and the call is not charged. (Examples of this case is ANM/CON/CPG messages with charge in BCI recevied after ACM/ANM/CON message with no charge in BCI parameter).

If AMA record generation with MC 612 is enabled, then pulse count field in ICR records will be updated according to accumulated or calculated backward meter count in software meter register. (originated from s/w metered lines or SPM/COIN lines).

ICR record for a call with BCKWMTR translation will be generated if the originating line has MOG option, LNET is datafilled in translation and a meter name for the used LNET is datafilled in table MTRNETIF with Y in record field.

Note that pulse count value in trunk metering related ICAMA and IAA records will not be updated for backward metering.

66.2.2.4 CRG message

Incoming Morocco specific ISUP V2 CRG message in the originating DMS100 office is handled to support Backward Metering. In backward

metering, central office sends CRG message with meter tariff index or pulse count to local DMS100 office over Moroccan ISUP V2 trunks. Local DMS100 office performs metering procedures according to information in CRG message.

Central office is responsible for CRG message generation. This activity doesn't deal with generation of CRG message. Only handling of incoming CRG message in originating office is covered by this activity.

A new translation option BCKWMTR is introduced by activity A00004551 to mark backward metered calls. Hitting BCKWMTR tuple during translation means that the call needs **backward charging**.

This activity is going to check the existence of the new translation option to decide whether the call needs backward charging in local type backward metering and distance type backward metering.

The metering of originating line is done according to CRG messages coming over Moroccan ISUP V2. There are two types of backward metering: local and distance. In local type backward metering, tariff index is carried in CRG message. In distance type backward metering, pulse count is carried in CRG message.

66.2.2.4.1 CRG message format

This section covers CRG message format on Moroccan ISUP V2 protocol.

The received CRG message should contain one of the following information:

- The metering tariff index during the call establishment phase
- The number of metering pulses during the call

Table 1 CRG message format

Parameter	Type	Code	Length
Message type	M	0011 0001	1
Tariff index	O	1111 1111	3
Pulse number	O	1111 1110	3
Compatibility information	O	0011 1001	4
End of optional parameters	O	0000 0000	1

M : Mandatory

O : Optional

The value range of Parameters:

- Tariff index

0000 0000	No charge
0000 0001	
to	Represents the number of tariff index
1111 1111	

- Pulse number

0000 0000	In use
0000 0001	
to	Represents the incremented pulse count
1111 1111	

- Compatibility information

  Refer to Q.763 for compatibility information

66.2.2.4.2 Local Type Backward Metering

The metering information is sent from distance office (metering exchange, international exchange) and the metering is performed locally in the originating office. This information is received by Moroccan ISUP V2 CRG message which includes tariff index during call set up for local type backward metering.

The status of CRG message for local type backward metering is indicated in the following table.

Table 2 Status of CRG message for local type backward metering

Pulse number	Tariff index	Status
Present	Non present	Invalid

Present	Present	Incorrect
Non present	Non present	Incorrect
Non present	Present	Correct

Actions of the local office for local type backward metering

1. CRG message is received before ANM/CON message (Requirement 1).
2. If the call needs backward charging, and CRG timer is provisioned in table C7UPTMR, all correct CRG messages are reported to CM (Requirement 2).
3. The circuit is reset and the reattempt is performed in case an invalid (CRG message with pulse number) or incorrect CRG message is received as a first backward message after IAM message (Requirement 3).
4. After the first backward message reception during call setup (ACM or correct CRG), if an invalid (CRG message with pulse number) or incorrect CRG message is received, it is ignored (Requirement 4).
5. The CRG message which is received after CPG message is handled and reported to CM (Requirement 5).
6. When ACM, ANM, CON or CPG message is received with “no charge” value for charge indicator in backward call indicator parameter, the received CRG message is ignored.
7. ISUP INFO log (PM189) is generated in XPM to inform the maintenance about the cases numbered 3, and 4 (Requirement 6).

Successful calls for local type backward metering

Refer to Table 2 for the status of CRG message in this subsection. For free calls, central office has the responsibility to send an appropriate CRG message (with index 0) to local DMS. Correct datafill with this index is required on DMS for free charging of the call.

Figure 4 CRG message received before ANM (Req.1)

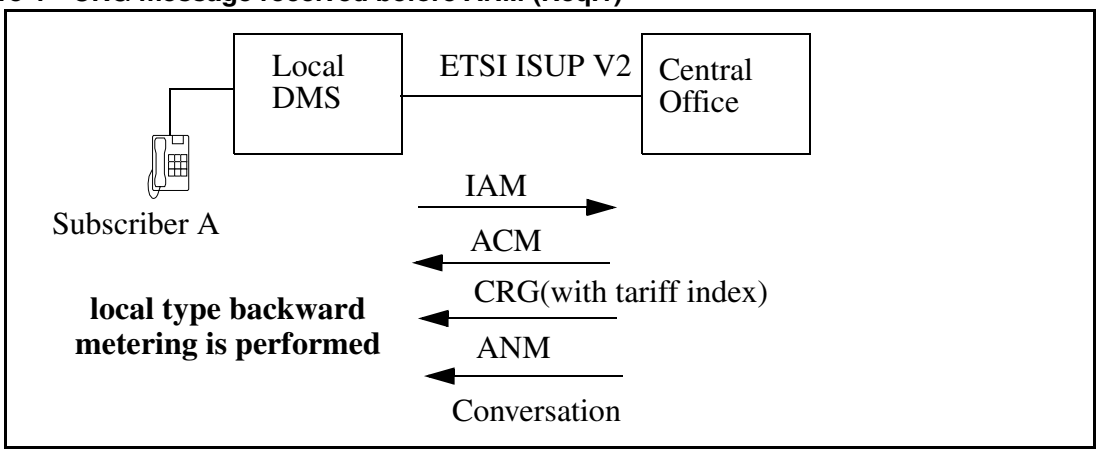


Figure 5 CRG message received before CON (Req.1)

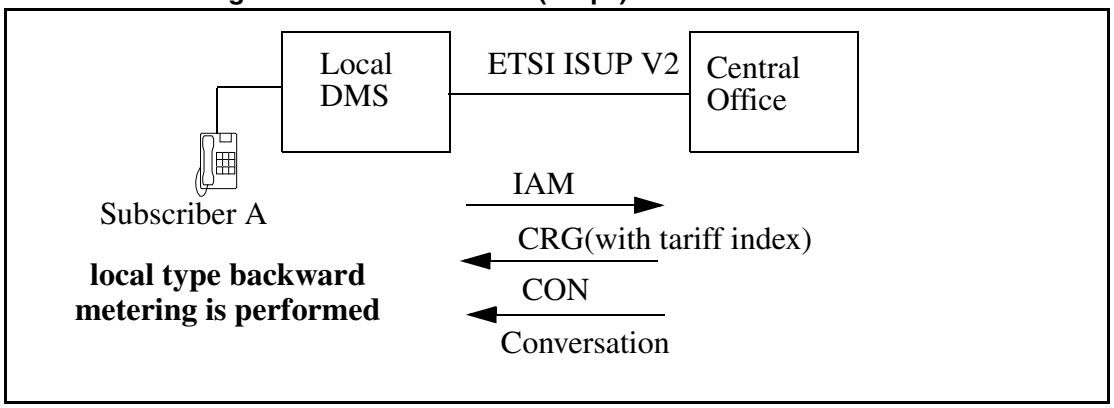


Figure 6 More than one correct CRG message received before ANM (Req. 2)

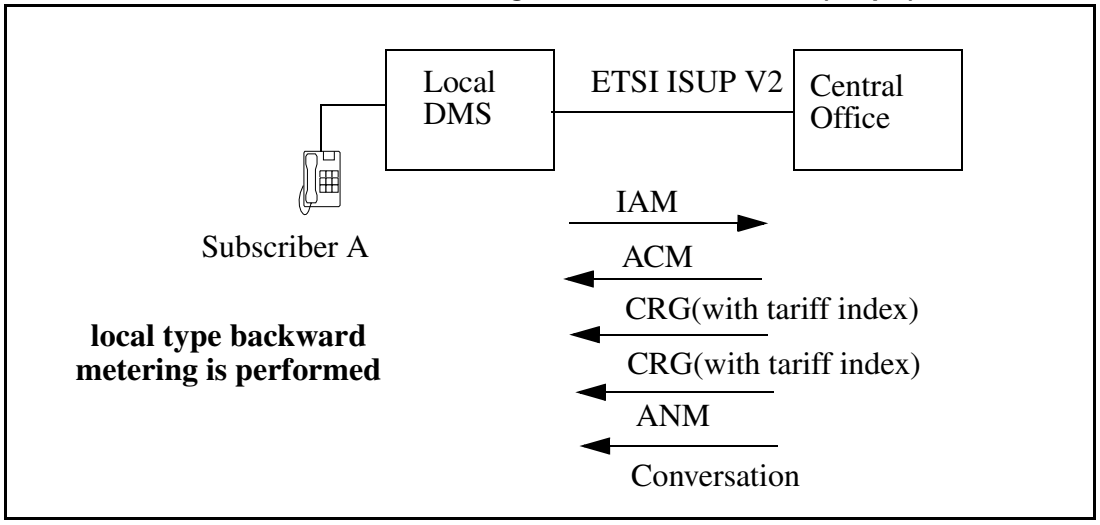


Figure 7 More than one correct CRG message received before CON (Req. 2)

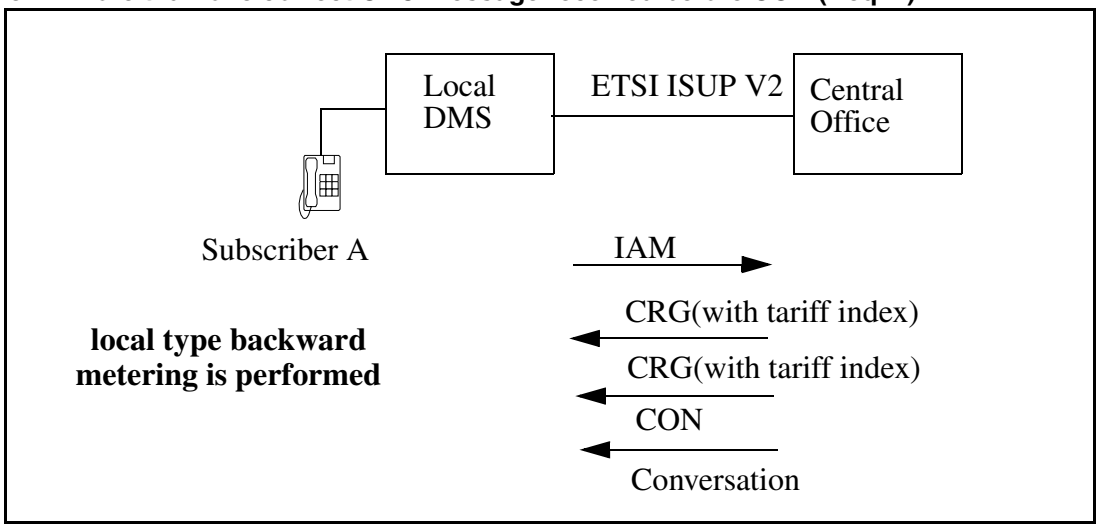


Figure 8 Invalid/Incorrect CRG message after ACM message(Req.4)

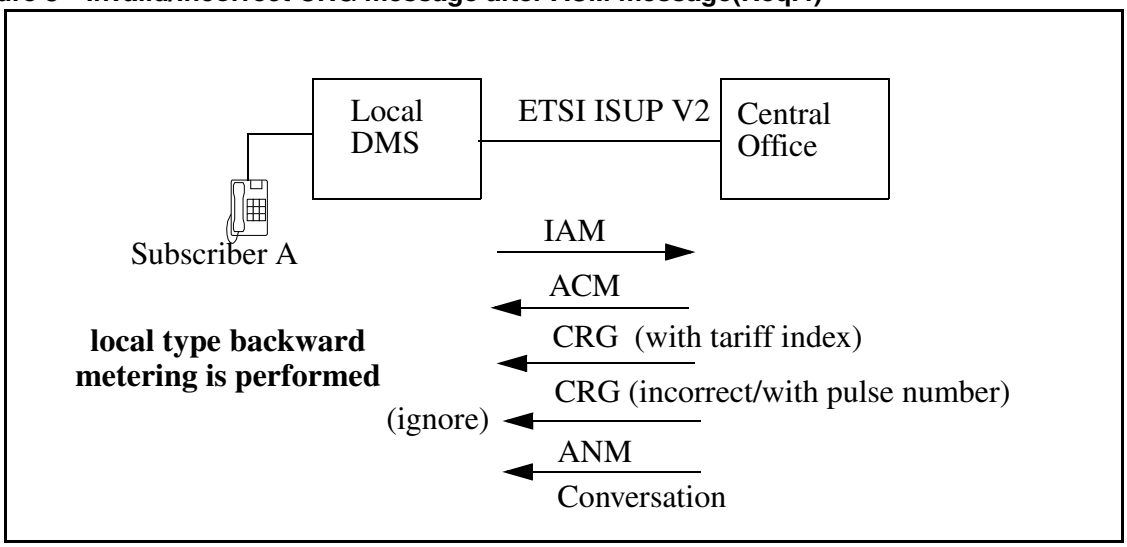


Figure 9 Invalid/Incorrect CRG message after ACM message (Req.4)

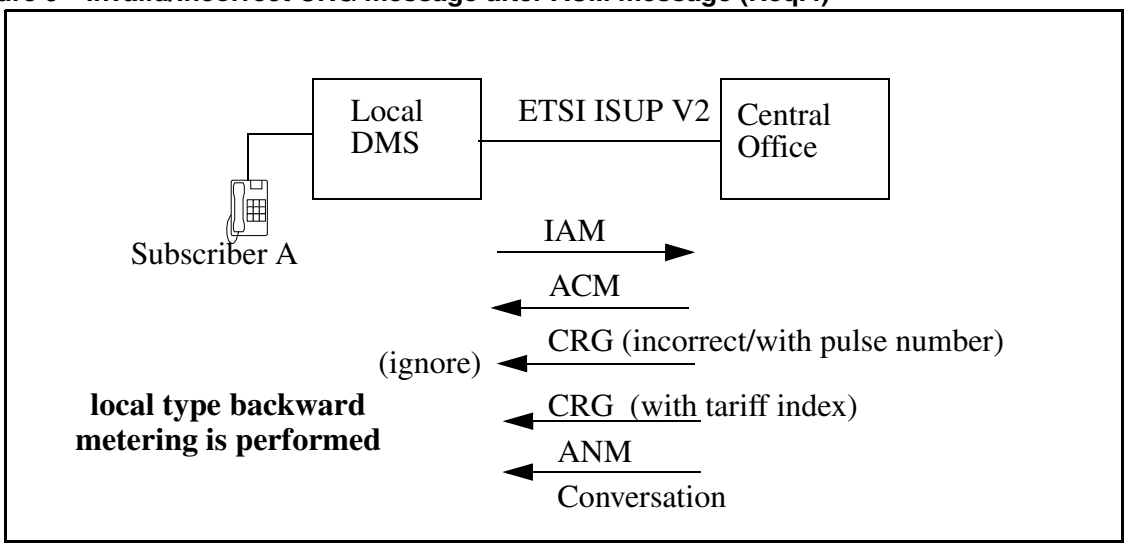


Figure 10 Invalid/Incorrect CRG message after correct CRG message (Req.4)

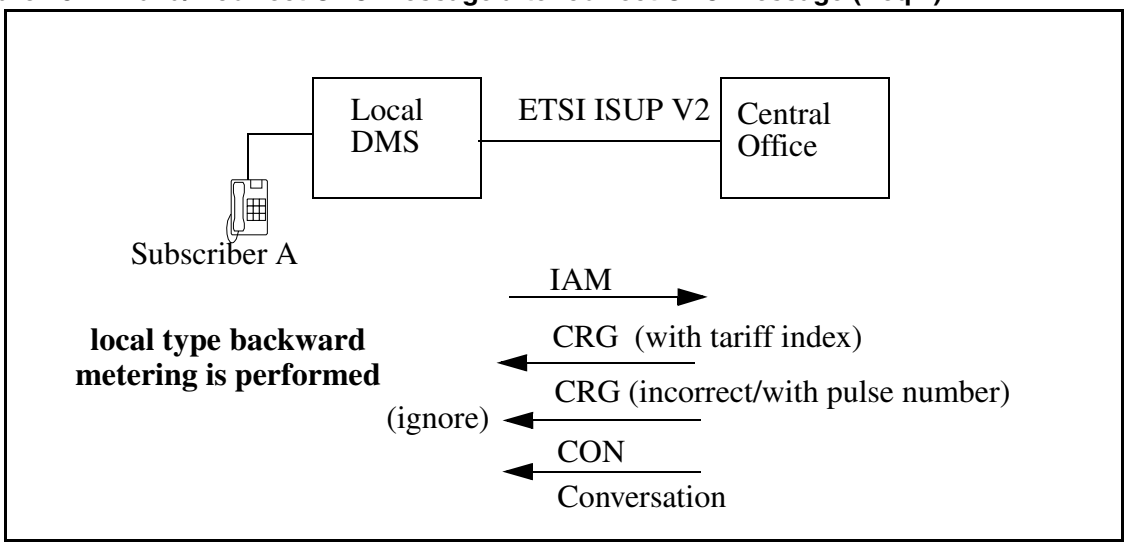
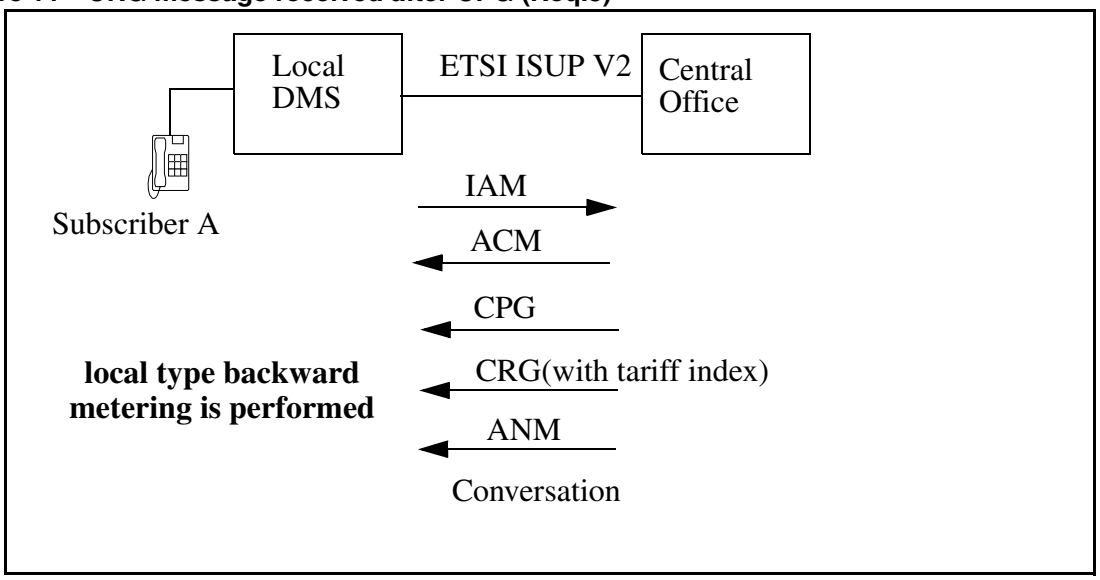


Figure 11 CRG message received after CPG (Req.5)

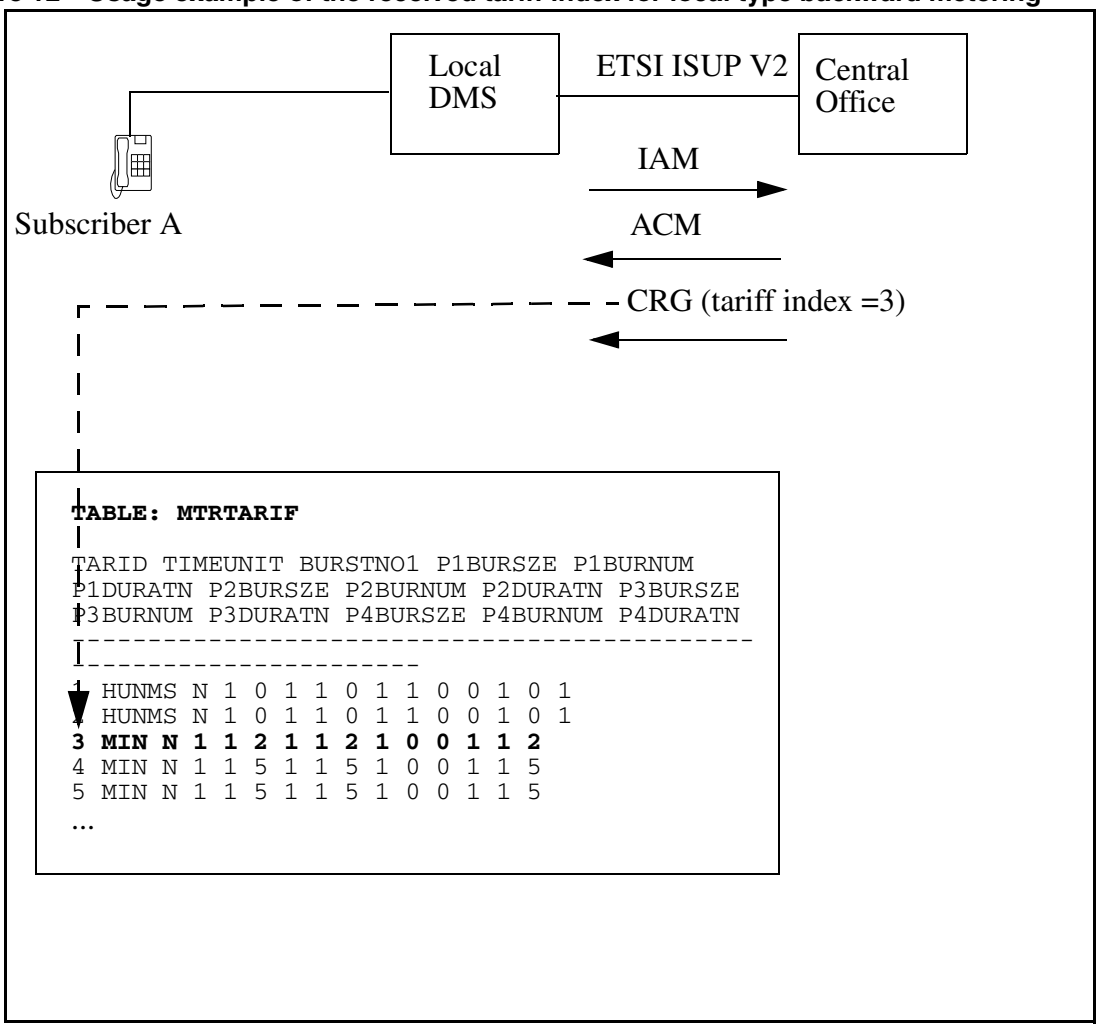


Metering behavior for successful local type backward metering calls:

If the CRG message with a valid tariff index is received, then this index is evaluated by metering system to verify that a corresponding tariff tuple exists in table MTRTARIF. In case more than one CRG message with tariff index is received, the last received tariff index is used by local type backward metering Figure 6, "More than one correct CRG message received before ANM (Req. 2)".

If a related MTRTARIF tuple is found, then this tariff tuple is used for charging the call. Note that tariff index range that can be received within CRG message is 0 to 255 which means MTRTARIF tuples within 256-511 index range cannot be used for local type backward metering.

Figure 12 Usage example of the received tariff index for local type backward metering



For plain subscribers with MOG option, software meters are increased according to the found MTRTARIF tuple.

For SPM/COIN subscribers, pulse generation to the originator is done using the found MTRTARIF tuple.

For MOG subscribers without SPM/COIN, software meters are increased according to the found MTRTARIF tuple.

At the end of the call, an MTR162 log is generated if there is a mismatch between calculated software meter count and reported hardware metering pulse count. In this case calculated software meter counts are used to update software meter registers.

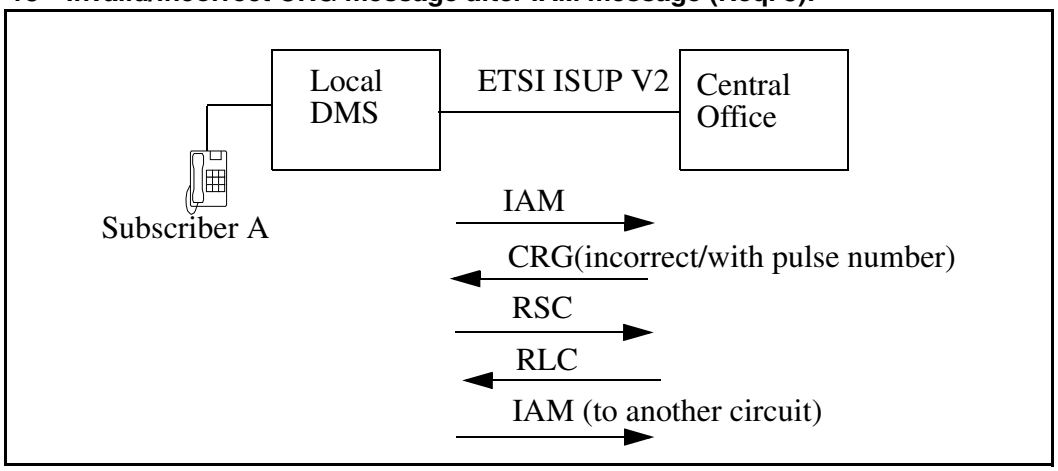
The amount of meter count mismatch which causes MTR162 log generation is determined by the PULMISTH parameter in table MTRSYSPM.

If a corresponding MTRTARIF tuple is not found then an MTR161 log including the received tariff index is generated and the call is not metered. Also the call is sent to treatment and dropped for this case if the MFP parameter in table MTRSYSPM is set to 'FAIL'. If MFP parameter is set to SUCCEED MTR161 log is generated, call is not dropped but not metered.

Unsuccessful calls for local type backward metering

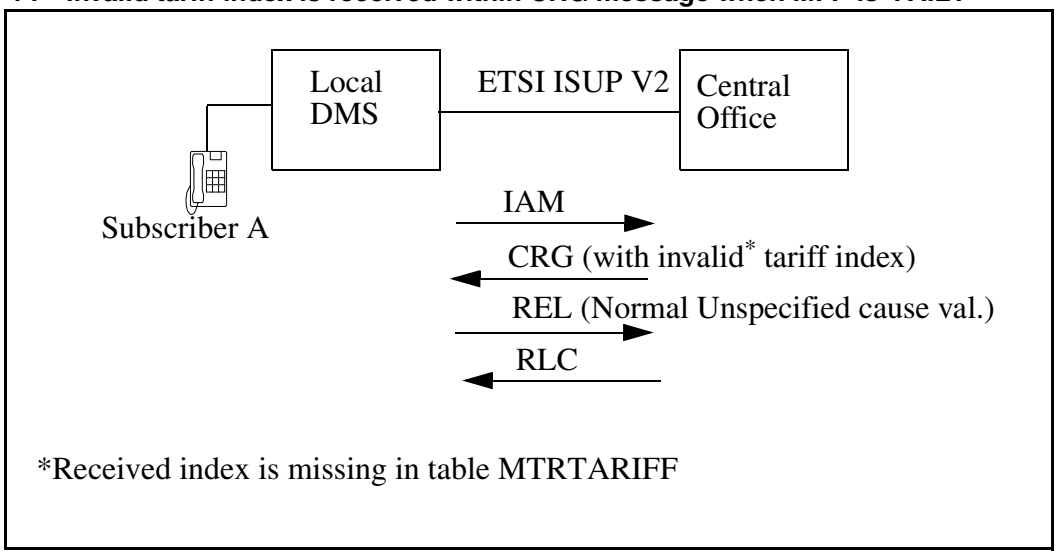
Refer to Table 2 for the status of CRG message in this subsection.

Figure 13 Invalid/incorrect CRG message after IAM message (Req. 3):



Another unsuccessful call scenario for local type backward metering is reception of an invalid tariff index which does not correspond to any MTRTARIF tuple in the local office. If MFP parameter in table MTRSYSPM is set to FAIL, then the call is sent to treatment for this case. Otherwise call is continue but not metered.

Figure 14 Invalid tariff index is received within CRG message when MFP is 'FAIL':



66.2.2.4.3 Distance Type Backward Metering

Central office identifies the charging count and sends this information by CRG message to the local offices during the conversation phase.

The new charge timer is started after receiving of ANM/CON messages to wait for a CRG message at local exchange for the calls that need backward charging. If the new timer is not provisioned in the table C7UPTMR, CRG timer is not started, incoming CRG messages are ignored and not reported to CM.

Table 3 CRG timer values

Minimum value	Maximum Value	Default value
0.5 seconds	4 minutes	20 seconds

The status of CRG message for distance type backward metering is indicated in the following table.

Table 4 Status of CRG message for distance type backward metering

Pulse number	Tariff index	Status
Present	Non present	Correct
Present	Present	Incorrect

Non present	Non present	Incorrect
Non present	Present	Invalid

Actions of the local office for distance type backward metering

1. When ANM/CON message is received, the CRG timer is started for the calls that needs backward charging (Requirement 7).
2. CRG message is ignored and not reported to CM, if CRG timer is not provisioned in table C7UPTMR.
3. CRG timer is stopped when the first correct CRG message is received during conversation (Requirement 8).
4. CRG message is received after ANM/CON message (Requirement 9).
5. All correct CRG messages are reported to CM, if the call needs backward charging, and CRG timer is provisioned in table C7UPTMR (Requirement 10).
6. The circuit is reset and reattempted in case reception of correct (CRG message with pulse number) or incorrect CRG message as a first backward message after IAM message (Requirement 3).
7. The correct (CRG message with pulse number) or incorrect CRG message is ignored if it is received after first backward message (ACM or CRG message with tariff index) during call setup (Requirement 4).
8. Local office ignores the incorrect or invalid (CRG message with tariff index) messages which is received during the conversation (Requirement 11).
9. If local type backward metering is performed for a call, the CRG timer is not started in ANM/CON message. Also received CRG messages during conversation, are ignored (Requirement 12).
10. If no CRG message is received till CRG timer expire, the circuit is released with the cause value timer expiry (Requirement 13).
11. If ACM, ANM, CON, or CPG message is received with "no charge" value for charge indicator in backward call indicator parameter, CRG timer is not started and the received correct CRG messages are not reported to CM (Requirement 14).
12. ISUP INFO log (PM189) is generated in XPM to inform the maintenance about the actions numbered from 6, 7, 8, 9 and 11.

For free calls, ACM,ANM,CON and CPG messages are received with "no charge" value for charge indicator in backward call indicator parameter. In this case received CRG message is not reported to CM.

If charge indicator in backward call indicator parameter is “charge” and a CRG message is received with zero pulse number during conversation, the call is dropped with the cause value Service or option not available. But, if charge indicator is “no charge” then, this CRG message with zero pulse number is ignored.

Successful calls for distance type backward metering

Refer to Table 4 for the status of CRG message in this subsection.

Figure 15 CRG received after ANM (Req. 7,8, and 9)

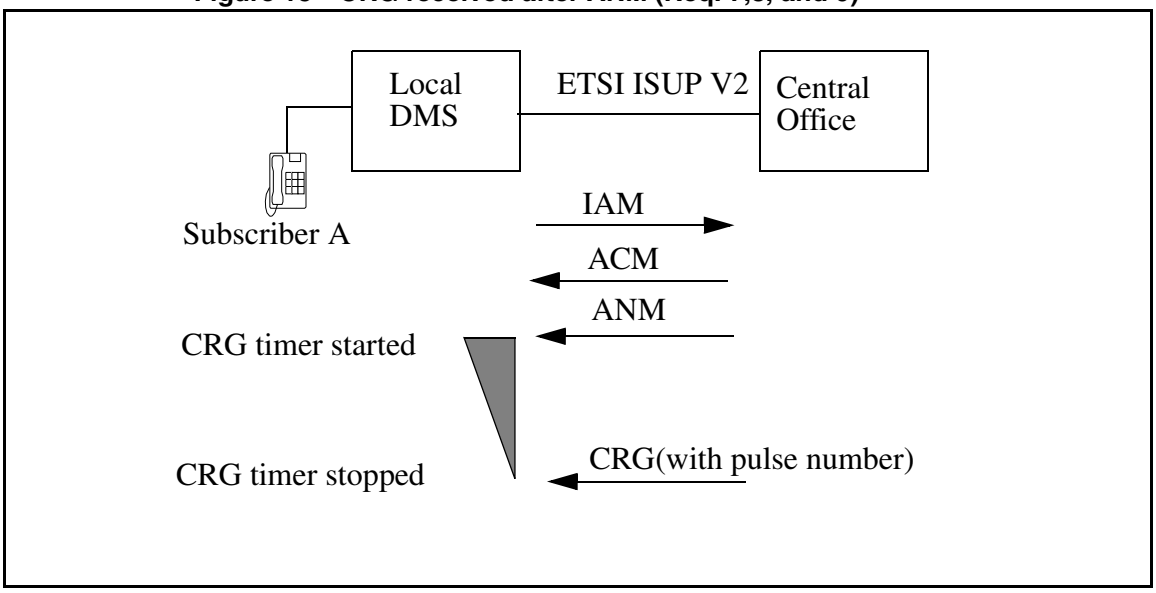


Figure 16 CRG received after CON (Req. 7,8, and 9)

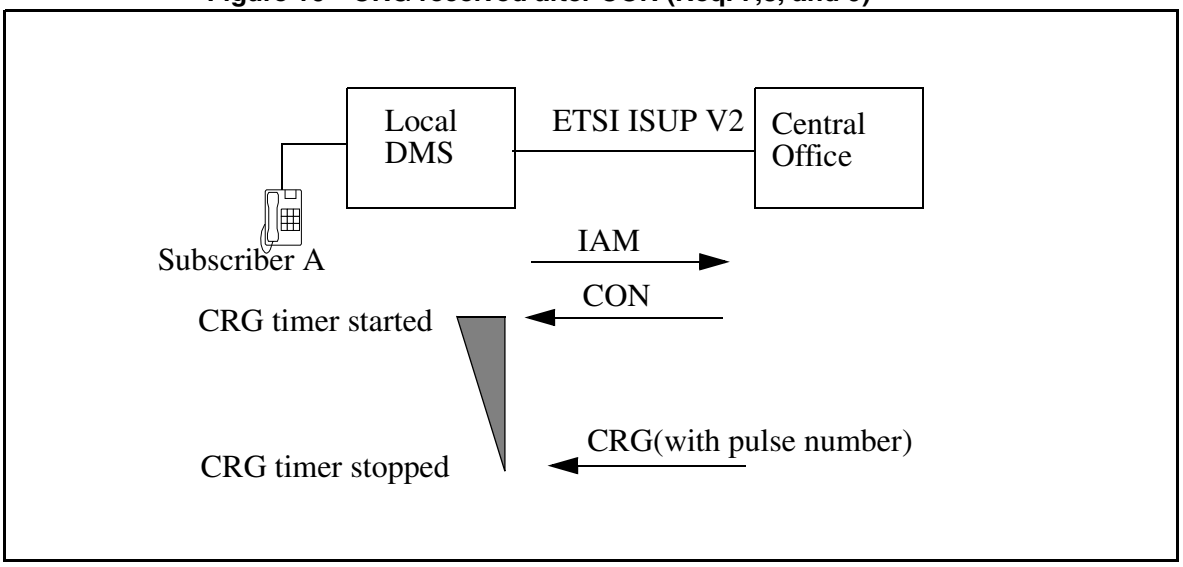


Figure 17 More than one correct CRG received after ANM message (Req.10)

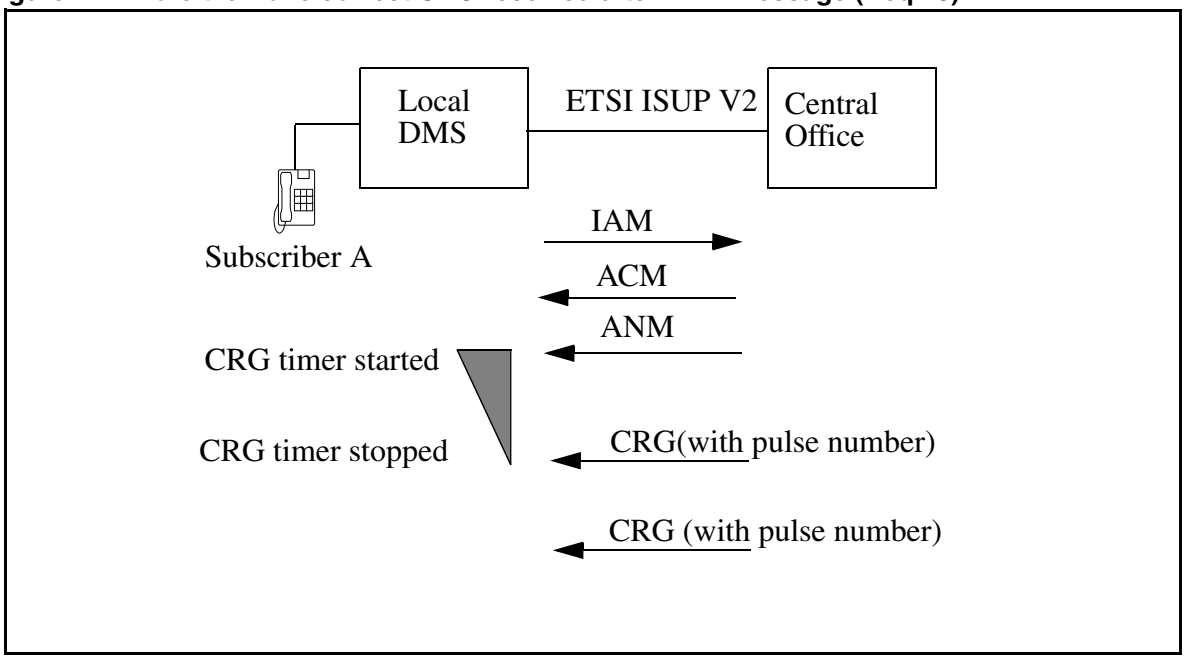


Figure 18 More than one correct CRG received after CON message (Req.10)

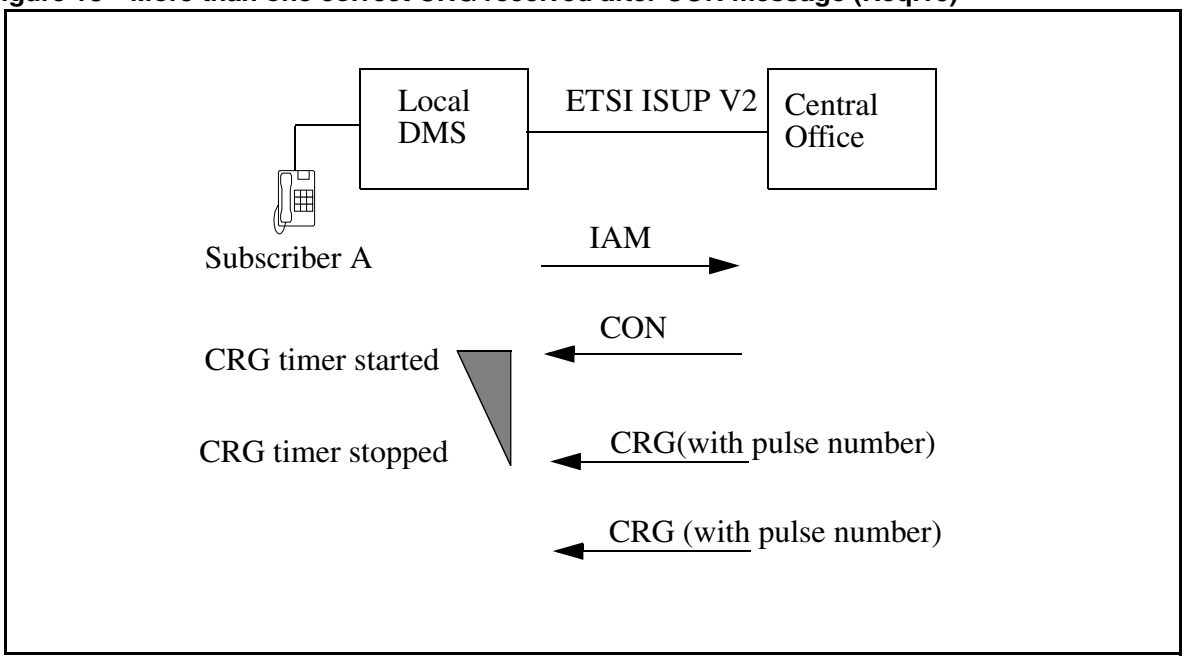


Figure 19 Incorrect/invalid message received during the conversation (Req. 11)

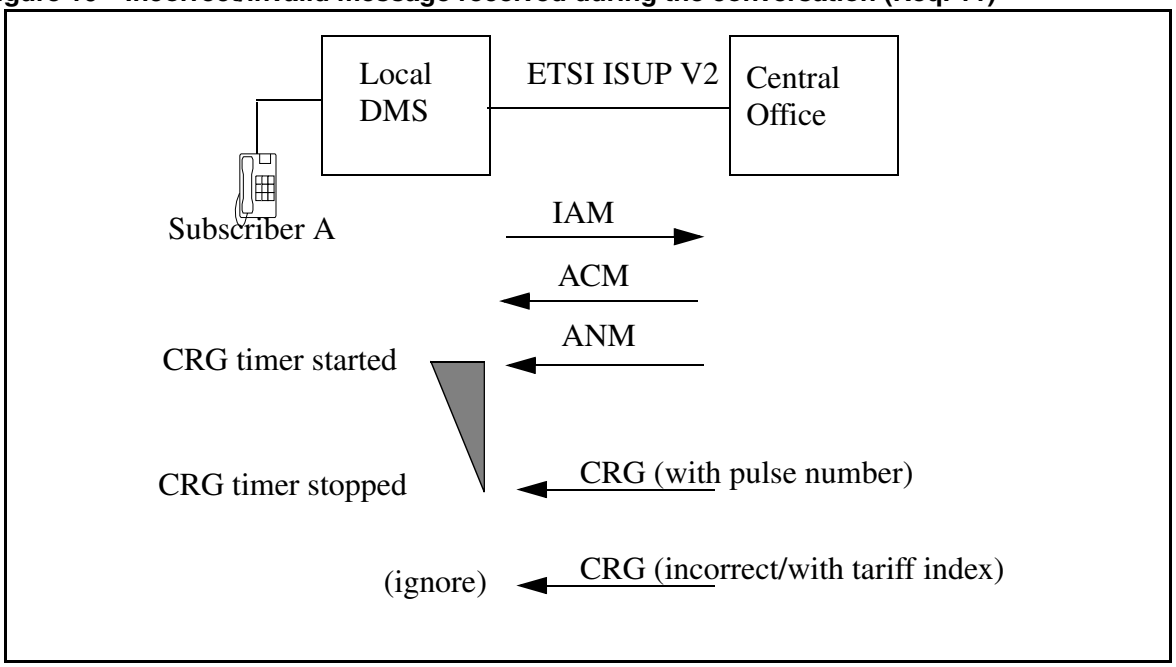


Figure 20 Incorrect/invalid message received during conversation (Req. 11)

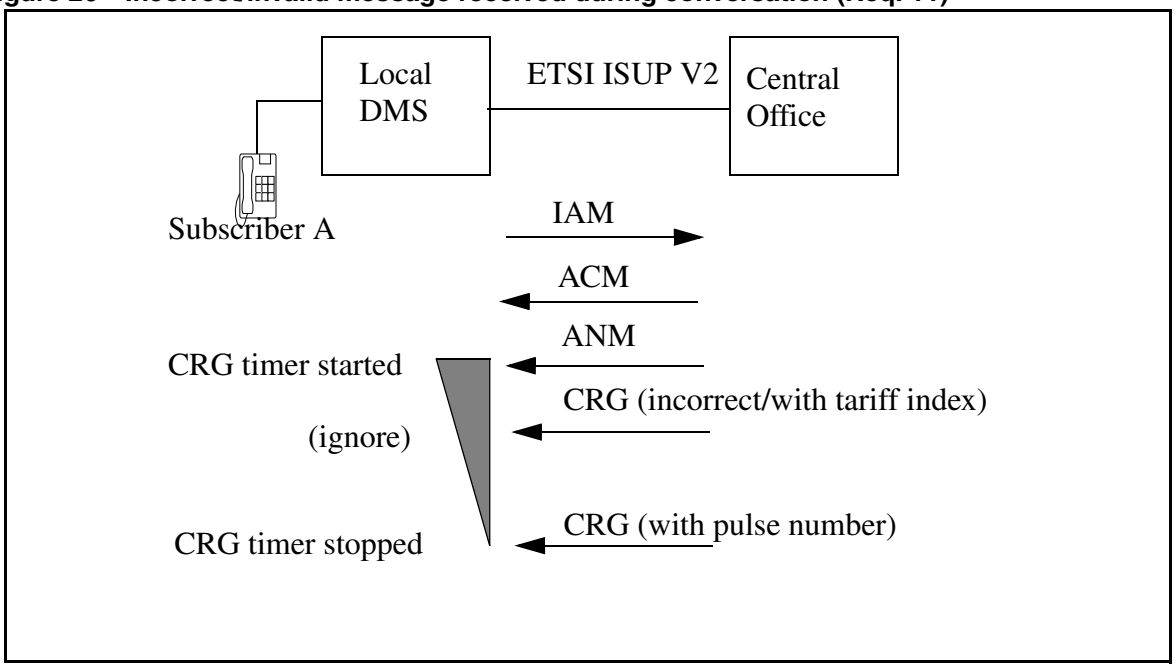


Figure 21 Incorrect/invalid message received during the conversation (Req. 11)

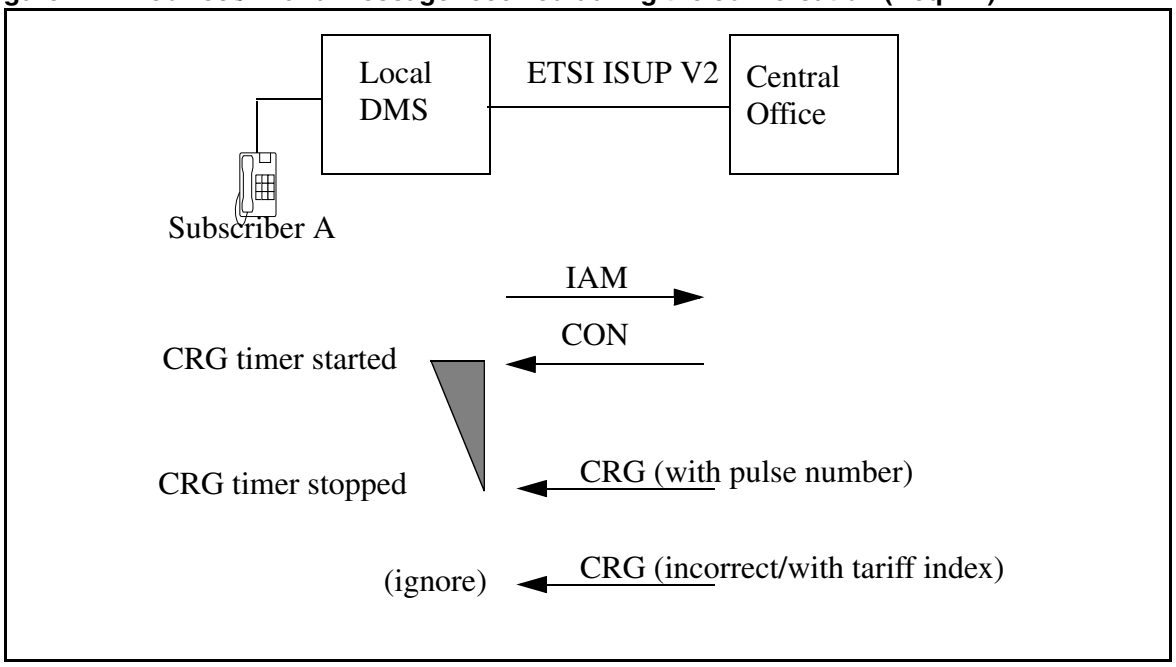


Figure 22 Incorrect/invalid message received before timer expiry (Req. 11)

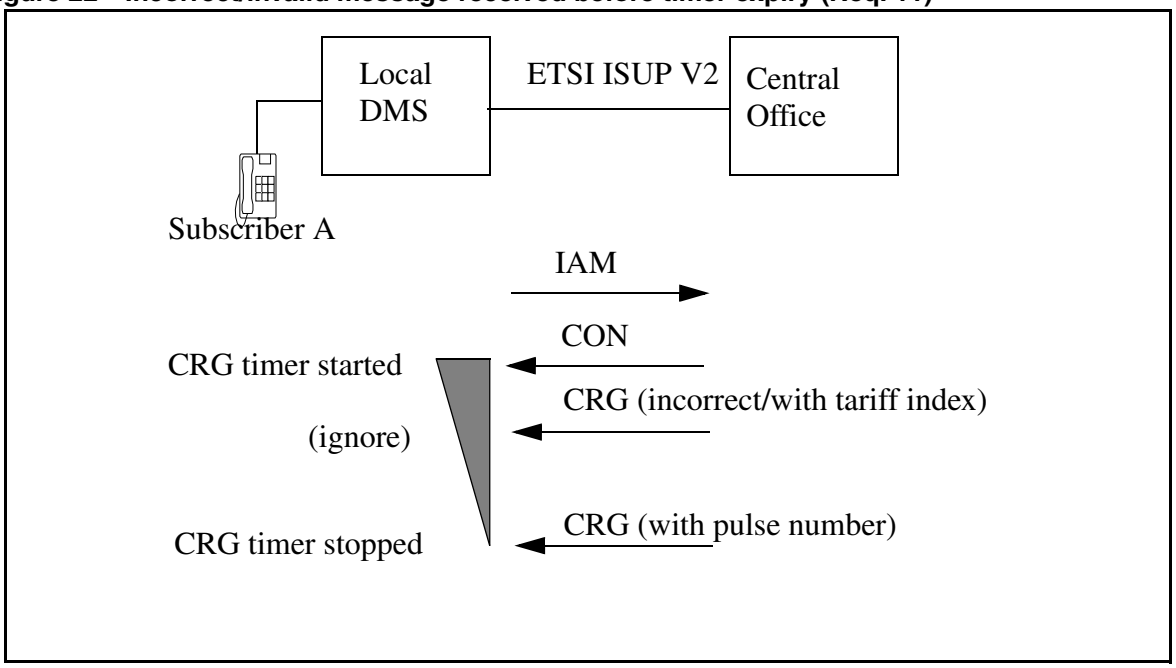


Figure 23 Incorrect CRG received before ANM (Req. 4)

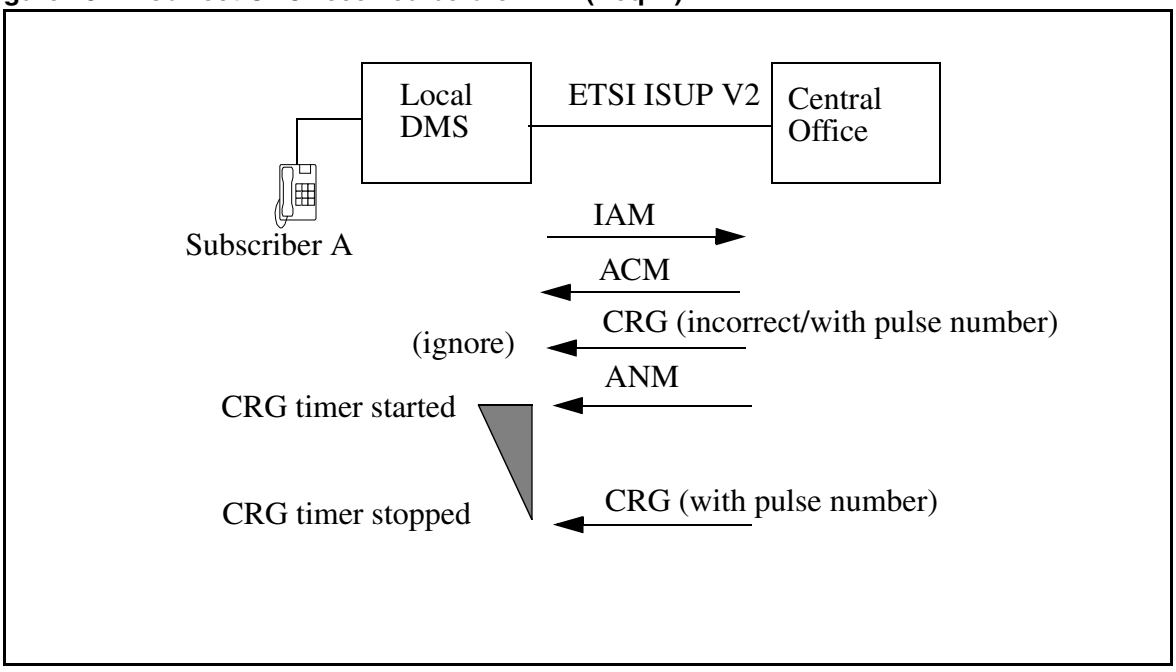


Figure 24 Incorrect CRG received before CON (Req. 4 and 12)

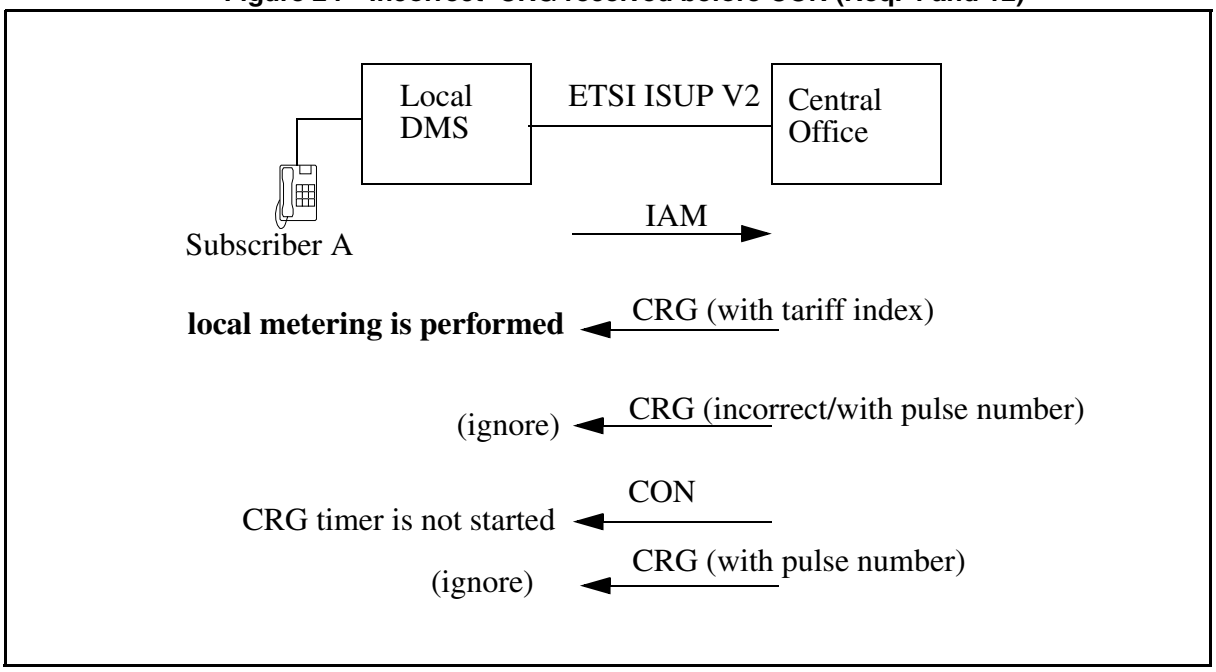


Figure 25 Ignoring CRG message for the local type backward metered call (Req. 12)

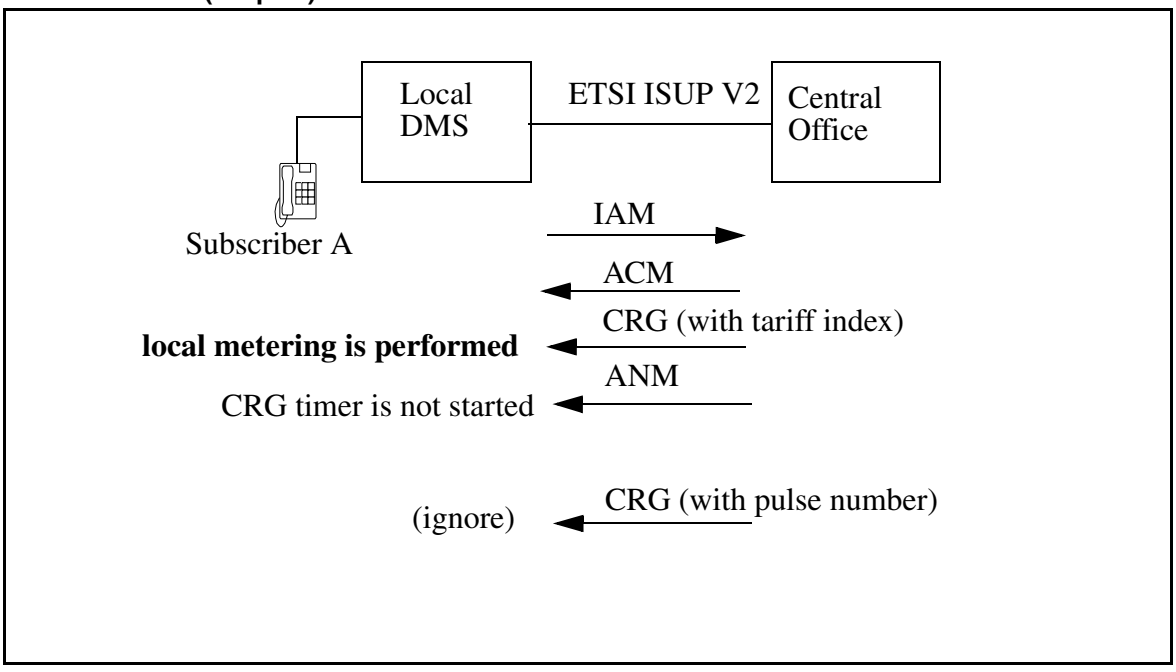


Figure 26 CRG timer according to charge indicator in ACM and ANM (Req. 14)

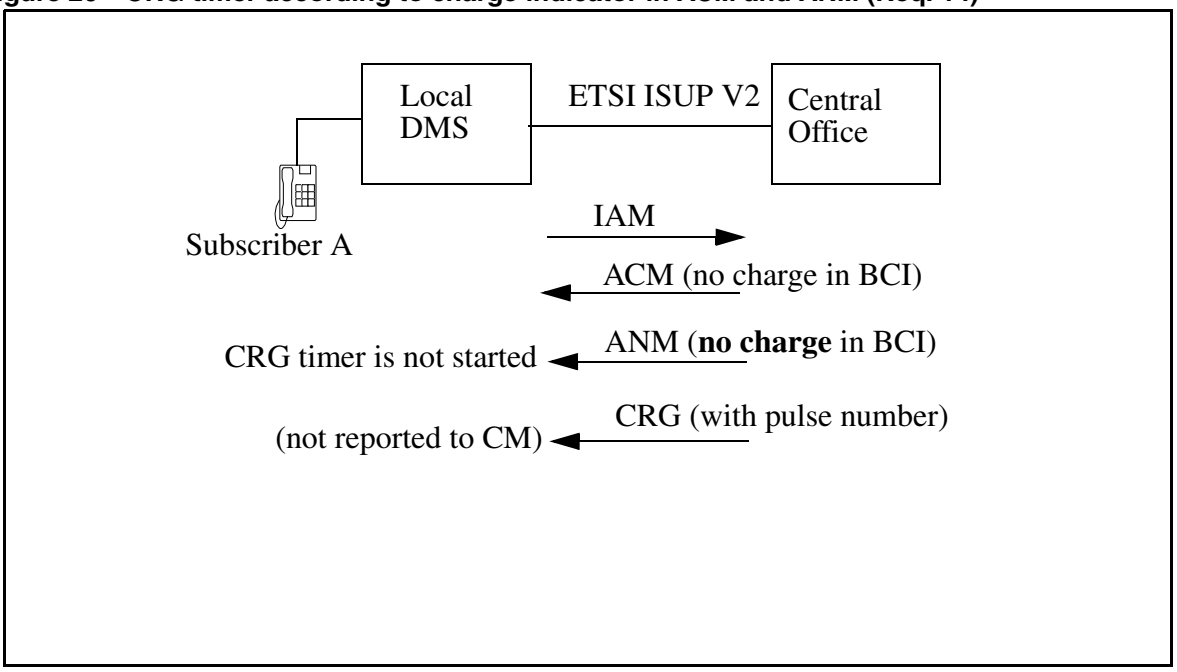


Figure 27 CRG timer according to charge indicator in ACM and ANM (Req. 14)

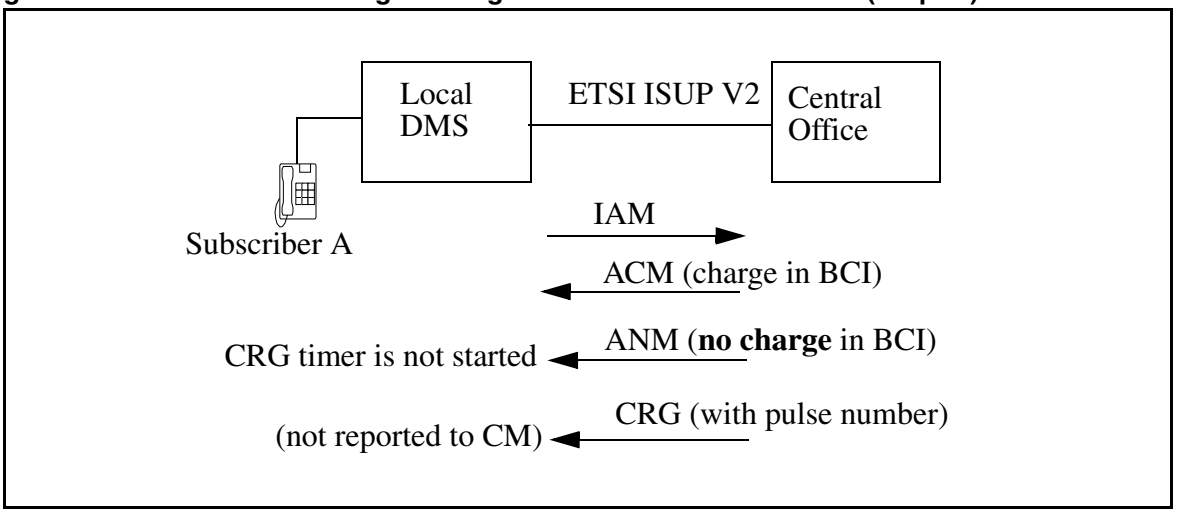


Figure 28 CRG timer according to charge indicator in ACM and ANM (Req. 14)

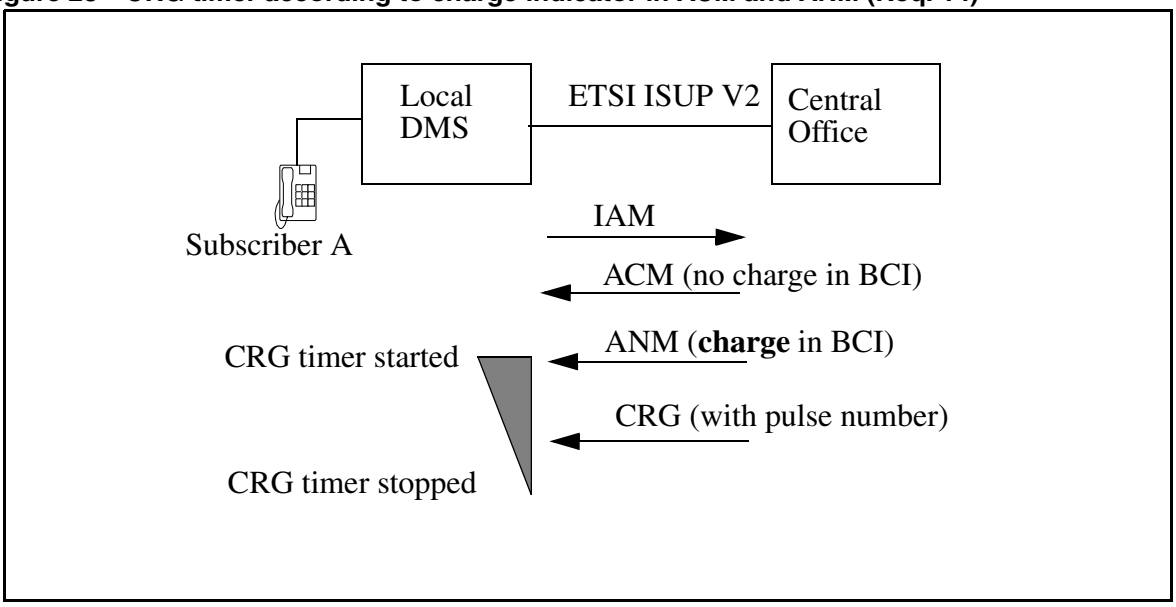


Figure 29 CRG timer according to charge indicator in ACM and ANM (Req. 14)

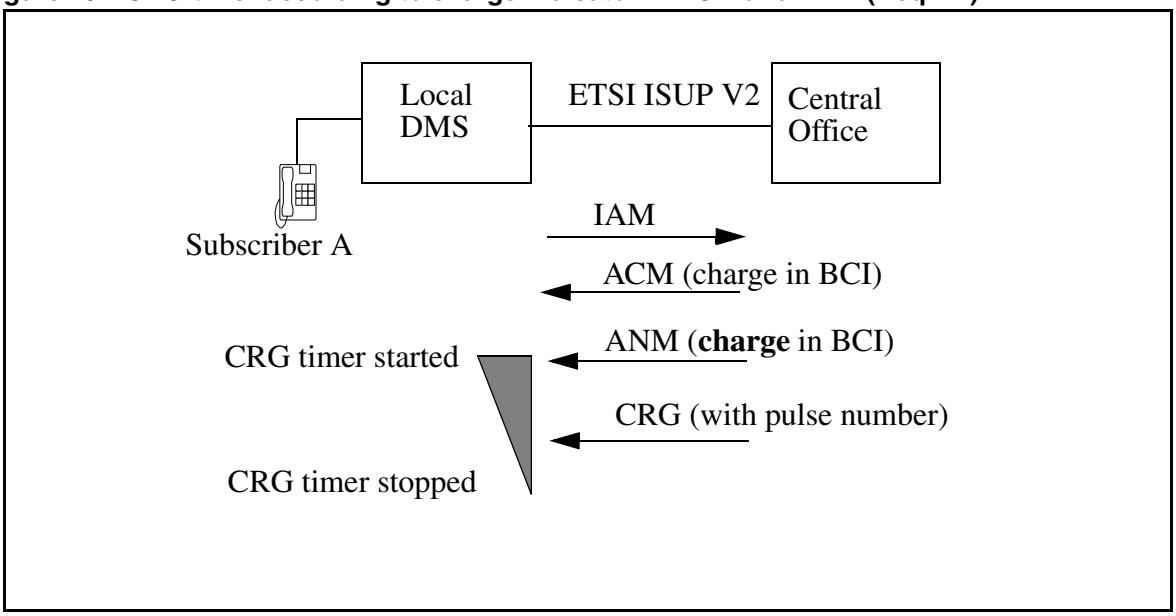


Figure 30 CRG timer according to charge indicator in ACM and ANM (Req. 14)

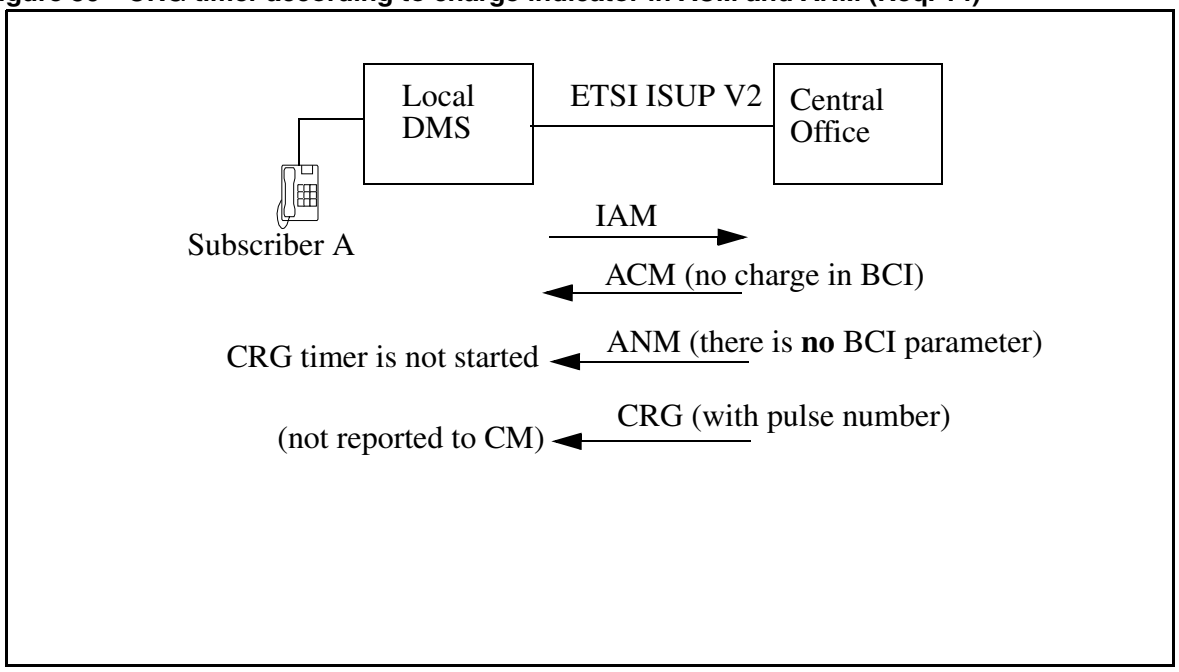
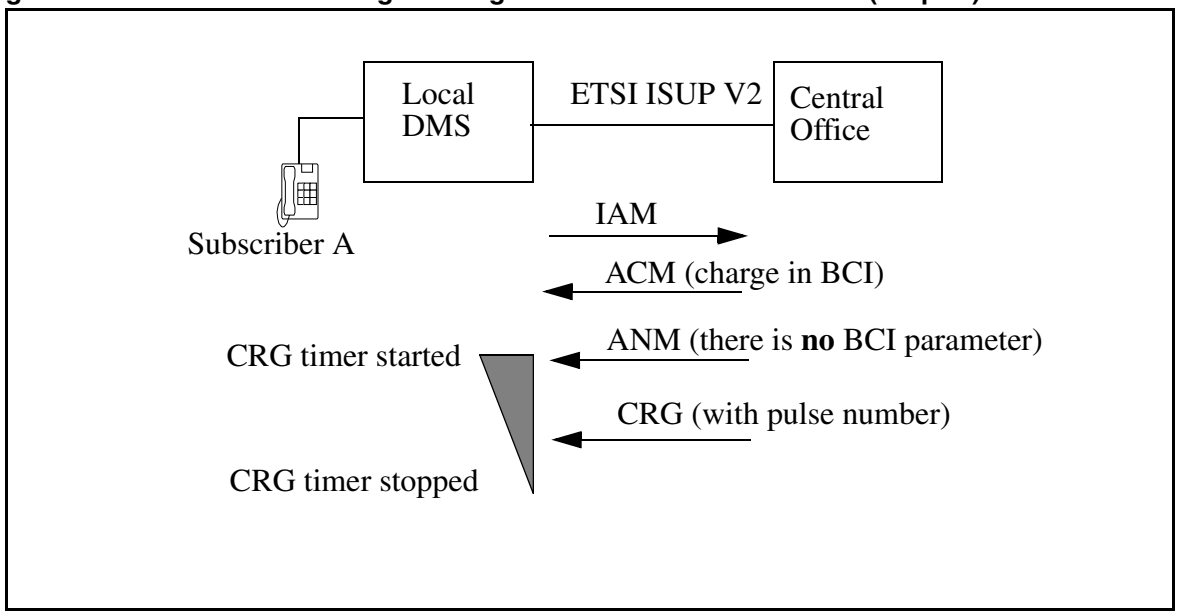


Figure 31 CRG timer according to charge indicator in ACM and ANM (Req. 14)



Metering behavior for successful distance type backward metering calls:

For successful distance type backward metering calls, charging of the originating agent will be done using the total of the received CRG pulse counts up to disconnect stage.

If an ANM, ACM, CON or CPG message with no charge in BCI parameter is received, then the call will not be charged.

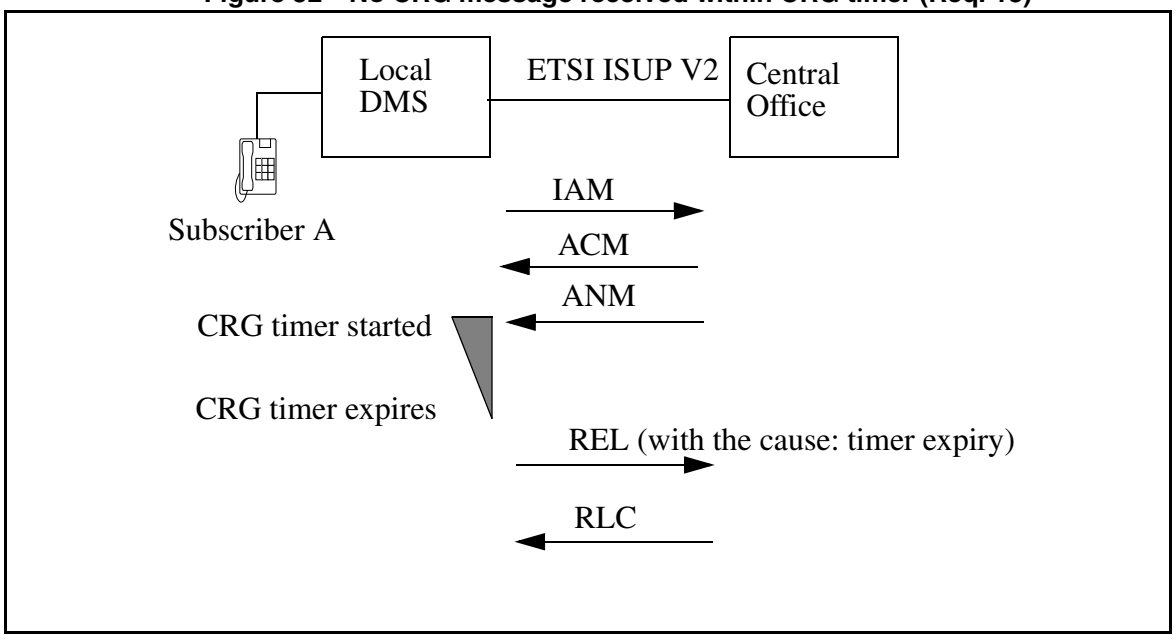
For SPM/COIN subscribers, hardware pulses will be generated for the originating agent using the CRG pulse count received. CRG pulses will be transmitted to originating SPM/COIN line as soon as the CRG message is received.

At the end of the call, if a mismatch occurs between received meter count and reported hardware metering pulse count for the originating line, then an MTR162 log is generated.

Unsuccessful calls for distance type backward metering

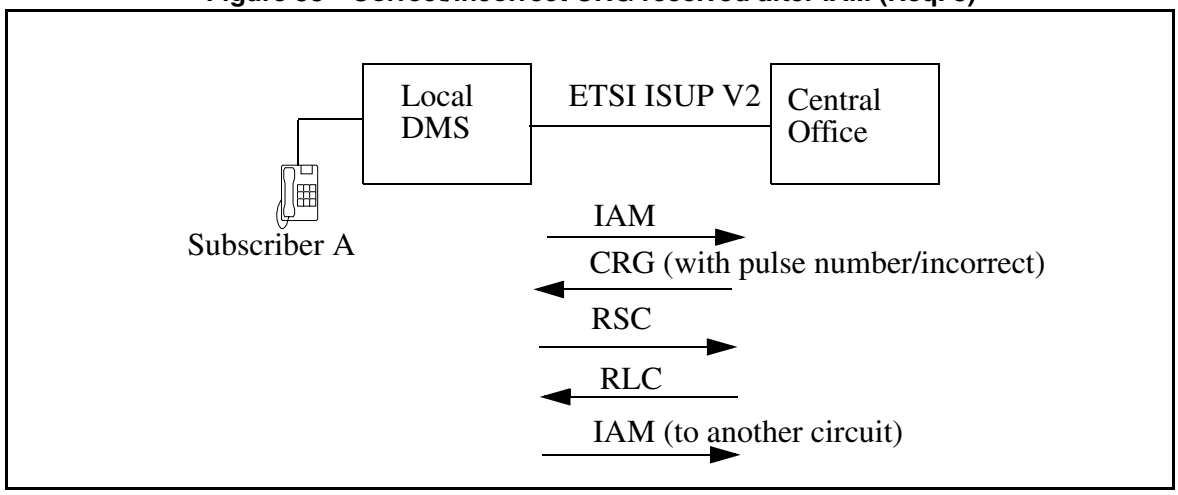
Refer to Table 4 for the status of CRG message in this subsection.

Figure 32 No CRG message received within CRG timer (Req. 13)



If CRG timer is expired after ANM/CON message for distance type backward metered call, call is not metered.

Figure 33 Correct/incorrect CRG received after IAM (Req. 3)



66.2.2.4.4 Charge Timer

The new CRG timer is provisioned in table C7UPTMR. This timer only applies at a local office for line to ISUP interworking. This timer is only started for the calls that need backward charging.

The CRG timer is started after receiving of ANM/CON messages to wait for a CRG message. If ACM and ANM messages are received with "no charge" value for charge indicator in backward call indicator parameter, CRG timer is not started and CRG message is reported to CM.

It is stopped when the first correct CRG message (with pulse number) is received during conversation.

If the new timer is not provisioned in table C7UPTMR, CRG timer is not started, incoming CRG messages are ignored and not reported to CM.

Table 5 CRG timer values

Minimum value	Maximum Value	Default value
0.5 seconds	4 minutes	20 seconds

66.2.2.5 Long Duration Call Interactions with Backward Metering

A call which is active longer than a pre-determined time is identified as a long duration call. For ordinary metered long duration calls, charge count is calculated each time the long duration audit is invoked and software meters of the originator are updated.
Long duration support is available for both local and distance type Morocco backward metering calls.

- For local type backward metering calls, long duration behavior is similar with ordinary metering. Each time the long duration audit is invoked, charge value for the audit period is calculated for the received tariff index, and then software meter of the originator is updated.
- For distance type backward metering calls, pulses are received inside CRG messages. Each time the long duration audit is invoked, received backward metering pulses are accumulated and software meters of the originator are updated with that value.

66.2.2.6 Backward Metering Line Feature Interactions

Backward metering is not supported in complex call scenarios. Feature activations are restricted when it is decided that some part[1] of call is being backward metered.

Controlling FLASH usage defines the behaviour of backward metering in most of IBN CEPT feature interaction scenarios which involves more than one leg (e.g. Call Switching, Three/Six Way Conference, Call Transfer, Call Diversion, Call Waiting, etc).

In ETSI BRI lines, usage of HOLD functionality is allowed with some limitations. Activation of ECT, 3PTY and 6PTY are not allowed if one of call legs is being backward metered.

Call Diversion features are restricted for both IBN and ETSI BRI lines, when 2nd leg is a backward metered call.

Feature interactions of COIN lines are not discussed, since COIN is not compatible with CEPT services (i.e Features that COIN is incompatible with are CWT, CXR, ENQ, CT, CWT, I3WC, I6WC, MDN, MTR, SCR, SPM, 3WC, and VOWDN).

Please note that IGNR_FLSH parameter in table ISERVOPT must be N, in order to enable flash usage of SPM agents.

[1]Any leg in complex call scenarios

IBN and ETSI BRI features, whose existing functionality is changed/limited by this activity are discussed below. Functionality of other features, which are not mentioned in this document, remins tha same.

66.2.2.6.1 Interaction with IBN CEPT Services

Restricting FLASH Usage

Flash usage is not allowed in backward metered calls. So any feature activated by flash (i.e.Call Transfer, 3WC, 6WC, Hold) is not allowed in backward metered calls.

FLASH Activation When Active Call is Backward Metered

Flash usage is not allowed when active call is Backward metered.

Consider the following scenario:

- A (IBN Agent) calls B (A - B Call Backward metered).
- A flashes and takes A-B call on hold (in order to make a new call, or activate a feature, etc.)

Flash is ignored in this case, and A-B call continues.

Backward Metered Call Initiation after FLASH

Initiation of a backward metered call, via flashing during a local type backward metered call, is not allowed. Such calls are routed to treatment when it is decided that call will be backward metered.

Consider the following scenario:

- A (either IBN agent) calls B (A-B Call is not backward metered).
- A flashes (A-B call on hold now), and calls C (A - C call Backward metered).

A - C call is sent to treatment from routing, and A-B call continues when A flashes again. A is given FNAL (LINE138 Log) treatment.

Call Diversion Services (CFU, CFD, CFF, CFU)

Call Diversion feature is not allowed if call is being diverted to a backward metered call. Please note that feature meter count of agent B is incremented for the usage of CFW feature (amount to be incremented is datafilled in MTRFEAT table, by ‘usage’ field), since this scenario is successful in terms of CFW operation, but is blocked by the terminating trunk.

Backward Metering Option on the second (Diverted) Leg

Consider the following scenario:

- B is programmed for being diverted to C (B - C Call Backward metered).
- A calls B.

In this case call diversion is not allowed, and a treatment is applied to A.

Treatment given in this case varies depending on the trunk/line treatment mappings on the first leg (A-B above).

In case

a. A - B is a line to line call, FNAL (LINE 138 Log) treatment is applied to orig agent (A).

b. a trunk (May be either ISUP, R2, PRI etc.) is involved in A - B call, type of treatment being applied to A depends on the treatment and release cause mapping datafills of related trunk. Hence treatment applied here may not be necessarily FNAL treatment. You can find teatment/release cause mappings in related signalling protocol documentation.

Please note that, if type of diversion applied is CFD(Call Forward Do Not Answer), if subscriber B does not answer the call in predefined amount of time (specified by CFDATIM option in table CUSTSTN), call is attempted to be divered to C. This diversion is not allowed since B-C call is backward metered, and B continues ringing[1], since diversion is rejected (general behavior of CFD). In CFD cases, an FNAL(LINE138) LOG might be reported, depending on the signalling protocol (i.e A-B call is line to line, R2, ISUP, PRI, etc).

Backward Metering Option on the first Leg

Consider the following scenario:

- B is diverted to C.
- A calls B (A - B Call Backward metered).

This scenario is not possible since backward metering generation is not supported in current office, only tandeming is supported.

ICWT/CWT (CEPT Call Waiting)

Call Waiting will be restricted since usage of FLASH in backward metered calls has been restricted already, and agent with ICWT/CWT option will not be able to take the call.

Consider the following scenario:

- A has ICWT/CWT option

[1]If B is an ETSIBRI agent, A-B call is taken down too.

- A calls B.
- A - B Call Active (Backward Metered)
- C calls A.

C gets busy tone, and A is not informed about second call request.

The following scenario is not possible since meter pulse generation is not supported in DMS100 MMP Office:

- A and/or B has ICWT/CWT option
- A Calls B.
- A - B Call Active.
- C calls either A or B (A-C Call backward metered).

66.2.2.6.2 Interaction with ETSI BRI Services

ETSI HOLD

The existing functionality of ETSI HOLD service is not affected, except that **silent tone**[1] is given to the held party if a backward metered call is taken hold.

Consider the following scenario for ETSI BRI agents:

- A (ETSI BRI Agent) calls B (A - B Call Backward metered).
- A holds A-B call.

A - B call is held, and B is applied silent tone. Now a new call can be initiated from A, and subscriber can turn back to A - B call via HOLDing the active call.

ECT (Explicit Call Transfer)

Call Transfer is not allowed if any of legs is a backward metered call.

Consider the following scenario for ETSI BRI agents:

- A(ETSI BRI Agent with ECT option) - B call is active (A - B call backward metered, and A is the originator).
- A - C call (any call) is on hold.

A attemts to transfer B - C, and call transfer is not allowed.

Call Transfer is rejected again, if backward metered call was on HOLD and call transfer was requested from the other leg.

3PTY (Three Way Conference)

[1] instead of HOLD announcement/tone

3PTY is not allowed, if ETSI BRI agent (who is the controller of conference) is the originator of a backward metered call on any leg (might be either HELD or IDLE leg).

Consider the following scenario:

- A (ETSI BRI agent with 3PTY option).
- A - B call is on HOLD. (A-B call backward metered and A is the originator).
- A - C call is active, and A requests 3PTY.

3PTY is not allowed, and conference is not established. Calls on both legs are preserved, and A might switch between calls via HOLD.

3PTY is again rejected if 3PTY is requested from the backward metered leg in the above scenario.

6PTY (Six Way Conference)

Initiation of 6PTY is not allowed if the controller is the originator of current backward metered call.

- A (ETSI BRI Agent with ECONF option).
- A - B call is active and backward metered.
- A attemts to initiate a 6 way conference, and conference request is rejected.

Also, addition of a backward metered call to an existing conference is not allowed.

A (ETSI BRI Agent with ECONF option), and is the controller of the ongoing conference.

- A takes the conference on HOLD, and initiates A-B call (backward metered).
- When B answers the call, A attempts to add A-B leg to the conference.
- Request of A for addon leg is rejected.

Call Diversion Services

Behavior of call diversion services for ETSI BRI lines in backward metered calls are as described in the Call Diversion Section for IBN lines.

66.3 Hardware Requirements or Dependencies

These activities are supported

- only for SX05 PDTC

- only for SX05 GPP and QPO load
- MX77 (development will be done) PLGC and OLG load
- SX05 (only for basic sanity tests will be done) PLGC, QGI loads.

66.4 Software Requirements or Dependencies

None

66.5 Limitations and restrictions

- If more than one pulse count is received in CRG message, generation of all received pulses to SPM/COIN lines is not guaranteed for distance type backward line hardware metering.
- Maximum supported CRG message rate is 1 message per 0.52 seconds for distance type backward line hardware metering.
- In case CRG timer is not datafilled in C7UPTMR local software metering is done instead of backward metering.
- Trunk software metering is not supported for Morocco ISUP V2.
- Retranslation scenarios are not supported in Morocco ISUP V2 backward metered calls, similar to existing metering functionality.

66.6 Interactions

None

66.7 Applicable customer facing sections

Fault Management	
Logs	X
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A

Performance (includes operational measurements) N/A

66.8 Glossary

None

66.9 Recommended Reading/References

c. Maroc Telecom Specific Requirements, High Level, v 1.5

d. A39005695: ETSI ISUP V2 Backward Metering for Morocco

e. TA0600: Backward Metering in Morocco Network

f. ITU-T Recommendation Q763: Signalling System No.7 - ISDN User Part Formats and Codes

g. A00004563 : Moroccan ISUP V2 on DMS100

h. A00004551 : Backward Metering for Morocco

i. A59012394 : Turkish ISUP V1/V2

j. A59018055 : Turkish ISUP V2 - Line interworkings

k. A59007794: Line Hardware Metering Base

l. DMS-100 MMP Metering Guide -NTP 297-9051-020

67: Functional Description (FN): A00004743

67.1 Feature name

Activity ID: A00004743

Title: Line originations CLI modification through CALLCNTL in ISN07

67.2 Description

67.2.1 Background

Customers wants the ability to send a different CLI dependent on the dialed digits and calling digits for their ONE NUMBER service.

All ONE NUMBER VoIP lines have a real DN (original DN) that is datafilled on the call server and a virtual DN (new CLI), where the original DN is changed into the new CLI when the called number is in a special range.

Features A59028780 and A59033687 (from MMP15 and tested in Succession ISN loads) provide a capability through table CALLCNTL and related tables to perform CLI modification based on the called number and calling number. These features work well in a trunk to trunk scenario.

The translations can also be applied in line originated calls (line to trunk and line to line) correctly. However, the CLI presented at the terminating display or in the outgoing message of the trunk terminating call, is not modified, and remains as the original CLI, but the Orig Open Digs in AMA log is the modified CLI.

This feature enhances the capability in ISN07 to modify the CLI based on called number and calling number (through table CALLCNTL) for IBN line originating calls. And this feature also provides a datafillable ability to control whether the modified CLI or original CLI is put into the Orig Open Digits field of AMA record.

67.2.2 Detail description

67.2.2.1 CLI for display

Following scenarios are supported by this feature.

- For IBN line -> IBN line calls, the modified CLI is presented at the CLASS display if the CLI needs to be changed to the virtual DN.

  Note: In order to active this function, CND tuple for ETSI variant must be added in table ISERVOPT (please refer to Figure 1), and the called party must be with CND/DDN option.

Figure 1 Datafill example in table ISERVOPT

```
TABLE: ISERVOPT
>lis
SOPTSKEY SOPTSVAR
-----------------
CND CND ETSI RS15 N N DEFAULT
```

- For IBN line -> ETSI V2 BASE ISUP trunk calls, the modified CLI is sent in the outgoing IAM if the CLI needs to be changed to the virtual DN.
- For IBN line -> ETSI PRI trunk calls, the modified CLI is sent in the outgoing SETUP message if the CLI needs to be changed to the virtual DN.

As to how to datafill the CLI modification through table CALLCNTL, please refer to features A59028780 and A59033687 for detail.

67.2.2.2 CLI in Orig Open Digs field of AMA log

BILLCLI, a new option in subtable CGPNDATA of table CGPNSCRN and subtable CDPNDATA of table CDPNSCRN, is introduced by this feature to control which CLI is put into the Orig Open Digs field of AMA log.

The modified structure of subtable CGPNDATA of table CGPNSCRN is as below:

Figure 2 Structure of subtable CGPNDATA of table CGPNSCRN

```
TABLE: CGPNSCRN CGPNSCRN: CGPNDATA
>ran
 1 FROMDIGS          EDIG_DIG_REG
 2 TODIGS            EDIG_DIG_REG
 3 CGPNINDX          THIRTY_TWO_CHAR_VECTOR
 4 CCOPTION          CALLCNTL_OPTION_VECTOR
 5 CGPNOPT           CDGPNSCRN_OPTION_VECTOR
LOGICAL TUPLE TYPE: CGPNDATA_LOG_TUPLE
>ran 5
 5 CGPNOPT           CDGPNSCRN_OPTION_VECTOR
TYPE IS CDGPNSCRN_OPTION_VECTOR VECTOR OF UP TO 2 MULTIPLES WITH
       CDGPNSCRN_OPTIONS      {CONTINUE, BILLING_CLI} REFINEMENTS:
        {CONTINUE}              MULTIPLE WITH
             CONSUME            {0 TO 31}
        {BILLCLI}              MULTIPLE WITH
             CLI                {ORIG, MODIF}
```

The modified structure of subtable CDPNDATA of table CDPNSCRN is as below:

Figure 3 Structure of subtable CDPNDATA of table CDPNSCRN

```
TABLE: CDPNSCRN SCRN_PROVIDER12: CDPNDATA
>ran
 1 FROMDIGS          EDIG_DIG_REG
 2 TODIGS            EDIG_DIG_REG
 3 CDPNINDX          THIRTY_TWO_CHAR_VECTOR
 4 CCOPTION          CALLCNTL_OPTION_VECTOR
 5 CDPNOPT           CDGPNSCRN_OPTION_VECTOR
LOGICAL TUPLE TYPE: CDPNDATA_LOG_TUPLE
>ran 5
 5 CDPNOPT           CDGPNSCRN_OPTION_VECTOR
TYPE IS CDGPNSCRN_OPTION_VECTOR VECTOR OF UP TO 2 MULTIPLES WITH
        CDGPNSCRN_OPTIONS       {CONTINUE,BILLCLI} REFINEMENTS:
        {CONTINUE}              MULTIPLE WITH
             CONSUME            {0 TO 31}
        {BILLCLI}              MULTIPLE WITH
             CLI                {ORIG, MODIF}
```

A datafill example in subtable CGPNDATA of table CGPNSCRN is as below:

Figure 4 Datafill example in table CGPNSCRN

```
TABLE: CGPNSCRN CLISCRN: CGPNDATA
>lis
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT
----------------------------------------
106602 106602 RETURN (DIGMAN CGPN 2) $ (BILLCLI ORIG) $
```

A datafill example in subtable CDPNDATA of table CDPNSCRN is as below:

Figure 5 Datafill example in table CDPNSCRN

```
TABLE: CDPNSCRN CLISCRN: CDPNDATA
>lis
TOP
FROMDIGS TODIGS CDPNINDX CCOPTION CDPNOPT
----------------------------------------
106602 106602 RETURN (DIGMAN CGPN 0) $ (BILLCLI MODIF) $
```

When BILLCLI is *ORIG*, the Orig Open Digs in AMA log is the original CLI if the CLI has been modified through table CALLCNTL; When BILLCLI is *MODIF*, it is the modified CLI.

Note: This function is applied to line and trunk originating calls.

For line originating calls with the CFW service on the called party, if BILLCLI is *ORIG*, the Orig Open Digs field in the first AMA log is set to original calling number whereas the filed in the other AMA logs are set to original called number.

If the option is not datafilled, AMA log is not impacted by this feature.

67.3 Hardware Requirements or Dependencies

N/A

67.4 Software Requirements or Dependencies

N/A

67.5 Limitations and restrictions

N/A

67.6 Interactions

67.6.1 IBN line to IBN line calls

- The CLI from SCP overrides the modified CLI through table CALLCNTL, i.e. the SCP CLI is displayed on the phone.
- The modified CLI is not manipulated through DN reverse translation.

67.6.2 IBN line to ETSI V2 ISUP trunk calls

- The CLI from SCP overrides the modified CLI through table CALLCNTL, i.e. the CLI from SCP is sent in the outgoing IAM.
- The IN DEFNUM overrides the modified CLI through table CALLCNTL, i.e. the IN DEFNUM is sent in the outgoing IAM.
- The manipulation of CLI through CLIOUTP or CLGDMI option on the outgoing trunk overrides this feature's functionality, i.e. the CLI manipulated by those options is sent in the outgoing IAM.

67.6.3 IBN line to ETSI PRI trunk calls

- The CLI from SCP overrides the modified CLI through table CALLCNTL, i.e. the CLI from SCP is sent in the outgoing SETUP message.
- The manipulation of CLI through CLIOUTP or CLGDMI option on the outgoing trunk overrides this feature's functionality, i.e. the CLI manipulated by those options is sent in the outgoing SETUP message.

67.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	Y
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	N/A
Accounting (includes AMA billing)	N/A

Performance (includes operational measurements) N/A

67.8 References

1. A59028780 -- Call Control and Universal Screening

2. A59033687-- Call Control and Universal Screening -phase II

68: Functional Description (FN): A00004750

68.1 Feature name

Even Bit Inversion(EBI) Support on DTCO2.

68.2 Description

The intent of this activity is to download even bit inversion feature to DTCO2s Downloading is enabled/disabled by means of a datafillable entity.

We would normally do not require this feature for DTCO2s. This feature is only needed for some specific scenarios described in the following sections:

68.2.1 Background Information

Currently, EBI for PLGC and PDTC (DTCO) is defined by features AE0385 ’EBI - CC SUPPORT’ and AE0334 ‘EVEN BIT INVERSION’. GSP/GMP customers were complaining about bringing the CCS7 links on the DTCO2s into service while they are making changes in BIT_INVERSION field of table LIUINV to make the bit inversion compatible with the far-end datafill.

For example, the customers would like to set the BIT_INVERSION field in LIUINV to Even Bit Inversion (EBI) to make it compatible with the far-end setting. When the customer brings the CCS7 link into service, the link drops into SYStem Busy (SYSB) state and never recovers unless they change the bit inversion to a suitable setting (e.g: No Bit Inversion (NBI)).

Basically, the customer has two offices, one with DTCO and the other with DTCO2 carrying a CCS7 link in between but the link cannot be bring into service when they made an equivalent bit inversion setting in LIUINV.

Customer indicated that they do not have this problem when they move the CCS7 link to a DTCO from DTCO2.

68.2.2 Root-Cause

Basically, the problem is due to bit conversions done on the network side due to the setting of TYPE_OF_NETWORK parameter in table OFCENG.

The two offices in question have different TYPE_OF_NETWORK settings. Namely, one office containing MMP load has the setting of INTERNATNL and the other containing GSP/GMP load has the setting of NORTH_AMERICA.

The TYPE_OF_NETWORK parameter is introduced to DMS by the activity AE0385 - EBI CC Support. Based on the network type selection, it does a

conversion on the network side. For example for a PCM30 voice carrier where no conversion is done on the P-side, the bit stream is converted to “CCITT A-Law + EBI A-Law companding” for a setting of INTERNATNL in the network side. However, for a NORTH_AMERICA setting, this conversion is “True data + ABI Inverted Data” in the network side.

The reader is referred to FN section of activity AE0385 for a detailed explanations of the bit conversions based on the TYPE_OF NETWORK.

The reader is also referred to DS section of the same document for the datafill details of this activity.

Neverthless, the GSP/GMP office in question is configured as NORTH_AMERICA type_of_network. This parameter should only be datafilled during the office setup and should not be changed thereafter.

On the other hand, the DTCOs can be added an NT6X44EA optional card in the LTCINV datafill to download the EBI support onto it. Hence the DTCOs can work with the far-end as expected.

The reader is referred to activity AE0385 for a detailed description of NT6X44EA usage.

Unlike the DTCOs, the DTCO2s cannot be datafilled NT6X44EA optional card and therefore the EBI information cannot be downloaded to DTOC2s.

68.2.3 The Solution

In order to overcome this problem, the EBI support should be downloaded to DTCO2s.

A fix has been submitted into TL20 stream to download EBI support to DTCO2s, however, this update may bring new problems as stated in the following section.

68.2.4 Potential Problems of the TL20 fix

Consider an office which has CCS7 links on some of DTCO2 and their associated bit inversion fields in LIUINV are not compatible with the far-end (as in our case, the near-end is NBI and far-end is EBI). Right after an ISN07 upgrade, the DTCO2s may be re-started to download the static data (performing and kind of PM WARM or COLD swact, or a PM REX swact or BSY/RTS of whole PM or a RELOAD RESTART of CM).

As there is no control of the fix submitted into TL20, the EBI feature is downloaded to DTCOs which ultimately impacts the bit inversion and hence causes CCS7 link outages.

To prevent such outages, the customers are expected to change their LIUINV bit inversion datafills and make it compatible with the far-end.

68.2.5 The Ultimate Solution

Ultimately, the fix in TL20 has no control on the downloading of EBI support feature to DTCO2s. Therefore, adatafillable switch should be defined on CM to enable/disable the functionality provided by the fix.

68.3 Feature Descripton

EBI is defined by features AE0334 and AE0385. AE0334, Even Bit Inversion feature enables the time switch card (NT6X44EA) the ability to provide PCM conversions(A-Law, Mu Law, EBI conversion) on per channel basis. This feature uses AE0385, EBI-CC Support Feature which provides Central Control Software in the International DMS-100F Switches. Within an International Network all data is EBI'd and all voice is A-law companding. The conversions required between PCM at the lines or trunks, and PCM within the network is done by peripheral's timeswitch card NT6X44EA.

The reader is referred to activities AE0334 and AE0385 for a wider understanding of how bit inversion is handled within the internal network for different type of networks.

The type of network is determined by the office parameter TYPE_OF_NETWORK in table OFCENG. Please refer to activity AE0385 for a description of this parameter.

Unlike the DTCOs where the even bit functionality is downloaded by adding NT6X44EA in LTCINV, the DTCO2's are not allowed to datafill NT6X44EA, hence does not have the ability to download even bit support feature.This activity, as in NT6X44EA, downloads the EBI support feature into DTCO2s by adding a new optional attribute to table LTCINV.

The following table is clone from AE0385 and it shows how bit inversions are done for voice and data in the internal network for different values of TYPE_OF_NETWORK setting.

In the table below the following symbols are used

A : CCITT A-Law

Ai : A + ABI Inverted CCITT A-Law

Ae : A + EBI A-Law Companding (EBI'd CCITT A-Law)

U : CCITT U-Law

Ui : U + ABI Inverted CCITT U-Law

Ue : U + EBI EBI'd CCITT U-Law

OBI : Odd Bit Inversion

Table 1 Network/Carrier Type/Voice Law/Conversion Matrice for a defined link.

Network Type	Carrier Type	Voice Law	Voice Conversion	Data Conversion
INTERNATIONAL	PCM30	A-LAW	NO CONVERSION	NO CONVERSION
INT.	PCM30	MU-LAW	Ae<-->Ue	NO CONVERSION
INT.	DS1	A-LAW	OBI	OBI
INT.	DS1	MU-LAW	Ae<-->Ui	OBI
A-LAW	PCM30	A-LAW	OBI	OBI
A-LAW	PCM30	MU-LAW	Ai<-->Ue	OBI
A-LAW	DS1	A-LAW	NO CONVERSION	NO CONVERSION
A-LAW	DS1	MU-LAW	Ai<-->Ui	NO CONVERSION
NORTH AMERICA	PCM30	A-LAW	Ui<-->Ae	OBI
NORTH AMERICA	PCM30	MU-LAW	OBI	OBI
NORTH AMERICA	DS1	A-LAW	Ui<-->Ae	NO CONVERSION
NORTH AMERICA	DS1	MU-LAW	NO CONVERSION	NO CONVERSION

68.3.1 New Optional Attribute Definition in LTCINV Table for EBI Activation

This activity adds a new optional attribute, namely, "EBI" in table LTCINV.

When it is added into a DTCO2 tuple in LTCINV, it downloads EBI support feature to DTCO2 during static data download. LIUINV table should be compatible with the far end setting.

The reader is referred to Data Schema section of this activity to have a sample datafill.

68.4 Hardware Requirements or Dependencies

This feature is designed for DTCO2s.

68.5 Software Requirements or Dependencies

None.

68.6 ONP Requirements

This activity is a follow-up activity for a fix (which uncontrollably downloads EBI support to DTCO2s) made in TL20 timeframe and is intended to eliminate possible CCS7 link failures during/after an ISN07 upgrade.

Without this activity being deployed in TL20, the EBI support feature is downloaded to DTCO2 during a static data download due to PM REX or PM SWACT or CM RELOAD RESTARTs right after an ISN07 upgrade and ultimately, bit inversion in the internal network is changed and hence cause a CCS7 link outage if the bit inversion field in the associated LIUINV tables are not made compatible with the far-end bit inversion settings (for example, near-end is set to NBI and far-end is set to EBI). In these circumstances, the customer may require to set the LIUINV bit inversions correctly.

However, this activity addresses this issue to overcome such problem that may occur right after an ISN07 upgrade.

68.7 Limitations and restrictions

None.

68.8 Interactions

None.

68.9 Applicable customer facing sections

Fault Management	
Logs	_N/A__
Alarms	_N/A__
Configuration	
Data Schema	__X____
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__

Service Order __N/A__

Office Parameters __N/A___

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

68.10 Glossary

Term	Description
CCS7	Comman Channel Signalling #7
DTCO	Digital Trunk Controller Offshore
DTCO2	Reduced Footprint DTCO
EBI	Even Bit Inversion
OBI	Odd Bit Inversion
A Law	A system of companding used in European and International switching systems
U-law	A system of companding used in North American switching systems.
PLGC	Peripheral Line Group Controller
PCM	Pulse Code Modulation

69: Functional Description (FN): A00004931

69.1 Feature name

Indian ISUP Act A00004931

69.2 Description

This activity addresses the ability to support Indian ISUP. Indian ISUP is on the CS2K IP solution. It is available on the International Succession Product.

The Indian ISUP is based on following international standards:

ETSI standard ETS 300 356-1 to -12 and -14 to -19 (February 1995): ISDN User Part (ISUP) Version 2 for the international interface

ETSI standard ES 201 296, V1.1.2 (1998-09) (ISUP Signalling aspects of charging)

The primary difference between Indian ISUP and ETSI ISUP V2 baseline is the modification of some of the existing additional parameters within the supported message set of ETSI ISUP base and additional parameters with Indian ISUP specific format.

Following interworkings will be covered by this activity:

to ETSI ISUP V2

to ANSI ISUP

to Indian ISUP

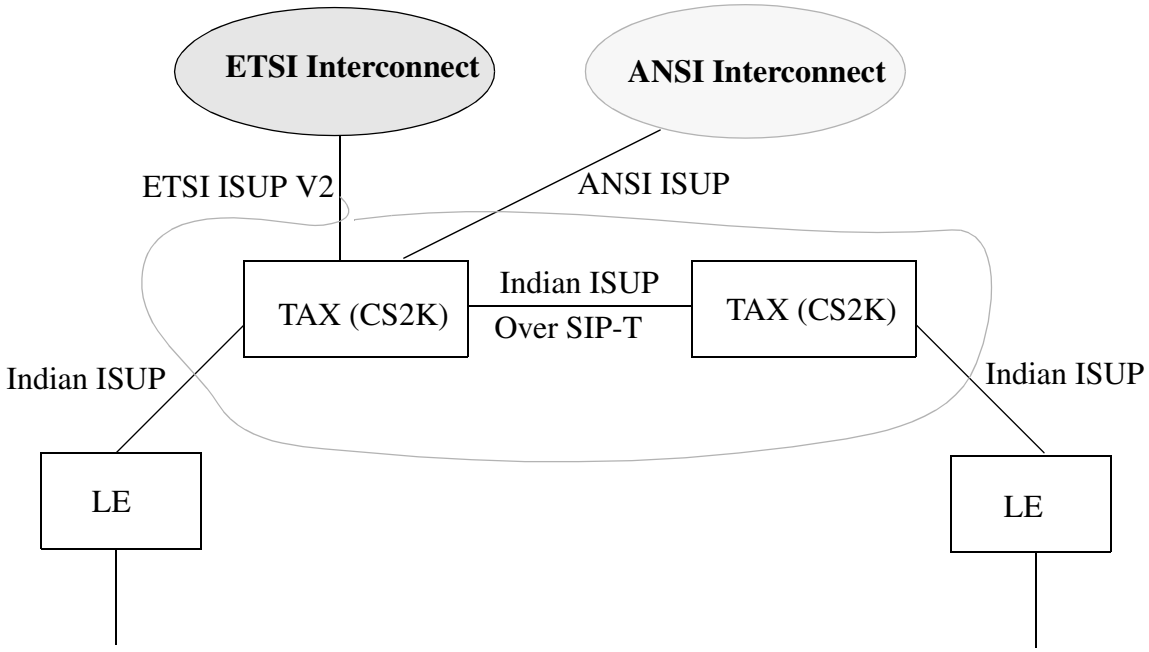
The following table indicates which protocols will be tested using SIP-T

Table 1 SIP-T Usage

Protocol	SIP-T	non-SIP-T
ISUP V2	X	X
Indian ISUP	X	X

The following figure illustrates the planned CS2K configuration for Indian ISUP.

Figure 1 CS2K Configuration for Indian ISUP



The following additional timers shall be provided as detailed by the specification for Indian ISUP, rest of timers shall be used as defined for ETSI ISUP V2.

UI SUS Control timer - Initiated when controlling exchange receives SUS (user) message and terminated upon receipt of resume message. At expiry the release procedure is initiated.

Congestion handling short - Initiated when congestion indication is received. At expiry the new congestion indication will be taken into account.

Congestion handling long - Initiated when congestion indication is received. At expiry the traffic is restored by one step.

Response to Call Reference release - Initiated when response to request of end to end connection establishment is sent and terminated at the receipt of the first end to end message from remote end. At expiry end to end message is allowed to be sent.

69.2.1 Indian ISUP datafill

This activity provides the ability to datafill Indian ISUP variant in table TRKSGRP. An example of this datafill in TABLE TRKSGRP is as shown below:

Table TRKSGRP

99ATMC42IT2 0 DS1SIG C7UP 2W N N EXTERNAL NONE Q767 THRH 0 DMSETSI N Y **INDIA 100_WHITE** $ ETSI2W CIC

'100_WHITE' indicates that the variant is based on ETSI ISUP V2.**'INDIA'** marks the specific variant based on 100_WHITE.

69.2.2 Indian ISUP signalling

69.2.2.1 General

This section describes the supported messages and parameters. The description within this section is based on ETSI ISUP V2 specification and Indian ISUP specification.

69.2.2.2 Messages

The following set of tables describes the messages and the parameters that these messages will/will not supported in Indian ISUP.

Table 2 ISUP Address Complete Message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
ACM	Message type	Y	Mandatory
	Backward call indicators	Y	Mandatory
	Optional backward call Indicators	Y	Optional
	Cause indicators	Y	Optional
	User-to-user indicators	Y	Optional
	User-to-user information	Y	Optional
	Generic notification indicator	N	-
	Transmission medium used	N	-
	Access transport	Y	Optional
	Access delivery information	Y	Optional

Table 2 ISUP Address Complete Message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
	Redirection number	Y	Optional
	Parameter compatibility information	Y	Optional
	Call diversion information	Y	Optional
	Service Activation	N	-
	Redirection number restriction indicator	Y	Optional
	Echo control information	Y	Optional
	End of optional parameters	Y	Optional

Table 3 ISUP Answer Message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
ANM	Message type	Y	Mandatory
	Backward call indicators	Y	Optional
	Optional backward call indicators	Y	Optional
	User-to-user indicators	Y	Optional
	User-to-user information	Y	Optional
	Connected number	Y	Optional
	Access transport	Y	Optional
	Access delivery information	Y	Optional
	Generic notification indicator	N	-
	Parameter compatibility information	Y	Optional
	Backward GVNS	N	-
	Call history information	N	-
	Generic number	N	-
	Remote operations	N	-
	Transmission medium used	N	-
	Redirection number	Y	Optional

Table 3 ISUP Answer Message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
	Service activation	N	-
	Echo control information	Y	Optional
	Display information	N	-
	Redirection Number Restriction Indicator	Y	Optional
	End of optional parameters	Y	Optional

Table 4 Blocking/Unblocking message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
BLO UBL	Message type	Y	Mandatory

Table 5 Blocking/Unblocking acknowledgment message

Message	Parameter	Supported on Indian ISUP	Optional/ Mandatory
BLA UBA	Message type	Y	Mandatory

Table 6 Call progress message

Message	Parameter	Support on Indian ISUP	Optional/ Mandatory
CPG	Message type	Y	Mandatory
	Cause indicators	Y	Optional
	Call reference	N	-
	Backward call indicators	Y	Optional
	Optional backward call Ind.	Y	Optional
	Access transport	Y	Optional

Table 6 Call progress message

Message	Parameter	Support on Indian ISUP	Optional/ Mandatory
	User-to-user indicators	Y	Optional
	Redirection number	Y	Optional
	User-to-user information	Y	Optional
	Generic notification indicator	N	-
	Transmission medium used	N	-
	Access delivery information	Y	Optional
	Parameter compatibility information	Y	Optional
	Call diversion information	Y	Optional
	Service activation	N	-
	Call transfer number	N	-
	Echo control information	Y	Optional
	Connected number	Y	Optional
	Backward GVNS	N	-
	Generic Number	N	-
	Call history information	N	-
	Redirection number restriction indicator	Y	Optional
	End of optional parameters	Y	Optional

Table 7 Charge Information Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CRG	Message type	Y	Mandatory
	Charge Band	Y	Mandatory
	Message compatibility information	Y	Mandatory
	End of optional parameters	Y	Mandatory

Table 8 Circuit Group Blocking Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CGB	Message type	Y	Mandatory
	Circuit group supervision message type indicators	Y	Mandatory
	Range and status	Y	Mandatory

Table 9 Circuit Group Blocking Acknowledgement Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CGBA	Message type	Y	Mandatory
	Circuit group supervision message type indicators	Y	Mandatory
	Range and status	Y	Mandatory

Table 10 Circuit Group Reset Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
GRS	Message type	Y	Mandatory
	Range and status	Y	Mandatory

Table 11 Circuit Group Reset Acknowledgement Message(status subfield not present)

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
GRA	Message type	Y	Mandatory
	Range and Status	Y	Mandatory

Table 12 Circuit Group Unblocking Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CGU	Message type	Y	Mandatory

	Circuit group supervision message type indicators	Y	Mandatory
	Range and status	Y	Mandatory

Table 13 Circuit Group Unblocking Acknowledgement Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CGUA	Message type	Y	Mandatory
	Circuit group supervision message type indicators	Y	Mandatory
	Range and status	Y	Mandatory

Table 14 Confusion Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CFN	Message type	Y	Mandatory
	Cause Indicator	Y	Mandatory
	End of optional parameter	Y	Optional

Table 15 Connect Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CON	Message type	Y	Mandatory
	Backward call indicators	Y	Mandatory
	Optional backward call indicators	Y	Optional
	Backward GVNS	N	-
	Connected number	Y	Optional
	User-to-user indicators	Y	Optional
	User-to-user information	Y	Optional
	Access transport	Y	Optional
	Network specific facility	N	-
	Generic notification Indication.	N	-
	Remote Operation	N	-

	Transmission medium used	N	-
	Echo control information	Y	Optional
	Access delivery information	Y	Optional
	Call history information	N	-
	Parameter compatibility information	Y	Optional
	Redirection number	Y	Optional
	Service activation	N	-
	Generic number	N	-
	Redirection number restriction	N	-
	End of optional parameters	Y	Optional

Table 16 Continuity Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
COT	Message type	Y	Mandatory
	Continuity indicators	Y	Mandatory

Table 17 Continuity Check Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
CCR	Message type	Y	Mandatory

Table 18 Identification Request Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
IDR	Message type	Y	Mandatory
	MCID request indicators	Y	Optional
	Message compatibility information	Y	Optional
	Parameter compatibility information	Y	Optional
	End of optional parameters	Y	Optional

Table 19 Identification Response Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
IRS	Message type	Y	Mandatory
	MCID response indicator	Y	Optional
	Message compatibility information	Y	Optional
	Parameter compatibility information	Y	Optional
	Calling party number	Y	Optional
	Access transport	Y	Optional
	Generic number	N	-
	Charge Party ID	N	-
	End of optional parameter	Y	Optional

Table 20 Information Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
INF	Message type	Y	Mandatory
	Information indicators	Y	Mandatory
	Calling party's category	Y	Optional
	Calling party number	Y	Optional
	Call reference	N	-
	Connection request	N	-
	Parameter compatibility information	N	-
	Network specific facility	N	-
	End of optional parameters	Y	Optional

Table 21 Information Request Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
INR	Message type	Y	Mandatory
	Information request indicators	Y	Mandatory
	Call reference	N	-
	Network specific facility	N	-
	Parameter compatibility information	N	-
	End of optional parameters	Y	Optional

Table 22 ISUP Initial Address Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
IAM	Message type	Y	Mandatory
	Nature of connection Ind.	Y	Mandatory
	Forward call indicators	Y	Mandatory
	Calling party's category	Y	Mandatory
	Transmission medium requirement	Y	Mandatory
	Call reference	Y	

	Called party number	Y	Mandatory
	Transit Network Selection	Y	Optional
	Calling party number	Y	Optional
	Optional forward call indicators	Y	Optional
	Closed User Group interlock code	Y	Optional
	Connection Request	Y	Optional
	Original called number	Y	Optional
	User-to-user information	Y	Optional
	Access transport	Y	Optional
	User service information	Y	Optional
	User-to-user indicators	Y	Optional
	Generic number	N	-
	User service information prime	N	-
	Network specific facility	N	-
	Generic Digits	N	-
	Originating ISC point code	Y	Optional
	Remote operation	N	-
	User teleservice information	Y	Optional
	Parameter compatibility information	Y	Optional
	Generic notification	N	-
	Service activation	N	-
	MLPP precedence	Y	Optional
	Transmission medium requirement prime	N	-
	Location number	N	-
	Forward GVNS	N	-
	CCSS	N	-
	Network management controls	Y	Optional
	Circuit assignment map	N	-
	Correlation ID	Y	Optional
	SCF ID	Y	Optional

	Hop counter	Y	Optional
	Call diversion treatment indicators	Y	Optional
	Call offering treatment indicators	Y	Optional
	Called IN number	Y	Optional
	Collect call request	Y	Optional
	End of optional parameters	Y	Optional

Table 23 Release Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
REL	Message type	Y	Mandatory
	Cause indicators	Y	Mandatory
	Redirection number	Y	Optional
	Redirection Indicator	Y	Optional
	Access transport	Y	Optional
	Signaling Point Code	Y	Optional
	User-to-user information	Y	Optional
	Automatic congestion level	Y	Optional
	Network specific facility	N	-
	Access delivery information	Y	Optional
	Parameter compatibility information	Y	Optional
	User-to-user indicators	N	-
	Display information	N	-
	Remote operations	N	-
	End of optional parameters	Y	Optional

Table 24 Release Complete Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
RLC	Message type	Y	Mandatory
	Cause Indicators	Y	Optional

	End of optional parameters	Y	Mandatory

Table 25 Reset Circuit Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
RSC	Message type	Y	Mandatory

Table 26 Resume Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
RES	Message type	Y	Mandatory
	Suspend/Resume Indication	Y	Mandatory
	Call reference	N	-
	End of optional parameters	Y	Optional

Table 27 Suspend Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
SUS	Message type	Y	Mandatory
	Suspend/Resume Indication	Y	Mandatory
	Call reference	N	-
	End of optional parameters	Y	Optional

Table 28 Segmentation Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
SGM	Message type	Y	Mandatory
	Access transport	Y	Optional
	User-to-user information	Y	Optional
	Message compatibility information	Y	Optional
	Generic Digits	N	-
	Generic notification	N	-
	Generic number	N	-

	End of optional parameter	Y	Optional

Table 29 Subsequent Address Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
SAM	Message type	Y	Mandatory
	Subsequent number	Y	Mandatory
	End of optional parameters	Y	Optional

Table 30 Unblocking Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
UBL	Message type	Y	Mandatory

Table 31 Unblocking Acknowledgement Message

Message	Parameters	Supported in Indian ISUP	Optional/ Mandatory
UBA	Message type	Y	Mandatory

69.2.2.3 Parameter that are getting effected for INDIAN ISUP

The following sections describes the existing ETSI ISUP message parameters that will be enhanced/restricted or if the parameter is new in the existing message.

69.2.2.3.1 IAM parameters

CPC (Calling Party Category):

The format of Calling Party Category is as shown below:

8	7	6	5	4	3	2	1
Calling Party's Category							

In addition to all the Calling Party Categories defined in ITU-T recommendation Q.763 the following categories will be supported over Indian ISUP:

00001001 - National Operator with Trunk offer

11100001 - Operator with trunk offer

11100000 - CCB Subscriber

11100010 - Interception Operator

11100011 - Subscriber with Home meter

11100100 - PABX

11100101 - PABX with priority

11100110 - Line test desk

TMR (Transmission Medium Required):

The format of Transmission Medium Required is as shown below:

8	7	6	5	4	3	2	1
Transmission Medium Required							

In the TMR parameter defined in ITU-T Q.763, The following values will not be used for Indian ISUP:

00000100 to 00000101

00000111 to 00001010

00010000 to 00101010

USI (User Service Information):

The format of User Service Information is as shown below:

	8	7	6	5	4	3	2	1
1	ext.	Coding standard		Information transfer capability				
2	ext.	Transfer mode		Information transfer rate				
2a	Rate multiplier							
3	ext.	Layer ident.		User information layer 1 protocol				
4	ext.	Layer ident.		User information layer 2 protocol				
5	ext.	Layer ident.		User information layer 3 protocol				

NOTE 1 – Octet 2a is required if octet 2 indicates multirate (64 kbit/s base rate); otherwise, it shall not be present.

NOTE 2 – Octets 3, 4, 5 or any combination of these octets may be omitted. Octet 3 may be extended as described in Recommendation Q.931.

The codes listed below are reserved and are not provided:

01 to 11 - Coding Standard

10001 and 11000 - Information Transfer Capability

10001 to 10111 and 11000 - Information Transfer Rate

00010, 00100, 00101, 00110 and 00111 - User information Layer-1 protocol identification

69.2.2.3.2 ACM, ANM, CPG parameters

BCI (Backward Call Indicators):

The format of Backward Call Indicator is as shown below:

	8	7	6	5	4	3	2	1
1	H	G	F	E	D	C	B	A
2	P	O	N	M	L	K	J	I

The parameter ‘Backward Call Indicator’ is defined in ITU-T Recommendation Q.763, The following bit fields are reserved and will not be used:

Bit DC - 10 (Binary Value)

69.2.2.3.3 INF parameters

Information Indicators:

The format of Information Indicators is as shown below:

	8	7	6	5	4	3	2	1
1	H	G	F	E	D	C	B	A
2	P	O	N	M	L	K	J	I

The parameter ‘Information Indicators’ is defined in ITU-T recommendation Q.763, The following bit value is fixed:

Bit H - Always set to 0

69.2.2.3.4 REL, CPG, ACM parameter

Cause Indicator:

The format of Cause Indicator is as shown below:

	8	7	6	5	4	3	2	1
1	ext.	Coding standard		Spare	Location			
2	ext.	Cause value						
3								
.	Diagnostic(s) (if any)							
.								
n								

NOTE – Octet 3 to 3n may be omitted or repeated, e.g. 3' to 3'n.

The parameter ‘Cause Indicator’ is defined in ITU-T recommendation Q.763, The following bit value is fixed:

Coding Standard - 01 to 11

Location - 0001, 0101 and 0111

69.2.2.3.5 CRG parameter

Charge Band:

Please refer FN for Act A00004933.

69.2.3 Supplementary services supported by Indian ISUP

The ETSI V2 supplementary services will be directly inherited by Indian ISUP. The following will be the list of supplementary services that will be supported over Indian ISUP.

Direct Dialing-In (DDI)

Multiple Subscriber Number (MSN)

Calling Line Identification Presentation (CLIP)

Calling Line Identification Restriction (CLIR)

Connected Line Identification Presentation (COLP)

Connected Line Identification Restriction (COLR)

Malicious Call Identification (MCID)

Call Forwarding Busy (CFB)

Call Forwarding No Reply (CFNR)

Call Forwarding Un-conditional (CFU)

Call Waiting (CW)

Call Hold (HOLD)

Three Party Service (3PTY).

69.2.4 Interworking

The interworking of Indian ISUP with ETSI ISUP V2 and ANSI ISUP has been supported. The section below describes the message mapping and parameter mapping between Indian ISUP and ETSI ISUP, and Indian ISUP and ANSI ISUP respectively.

69.2.4.1 Message mapping

69.2.4.1.1 Indian ISUP to ETSI ISUP interworking

All messages except national specific messages of Indian ISUP will be supported by ETSI ISUP.

69.2.4.1.2 Indian ISUP to ANSI ISUP interworking

Received ANSI7+ Message	Indian ISUP (Gen/Rx)	Generated ANSI7+ Message
Forward Set-Up Messages		
IAM	IAM	IAM
	SAM	
Backward Set-Up Messages		
ACM	ACM	ACM
CPG	CPG	CPG
ANM	CON	ANM
Call Supervision Messages		
ANM	ANM	ANM

REL	REL	REL

69.2.4.2 Parameter mapping

All the parameter mapping from Indian ISUP to ETSI ISUP, and Indian ISUP to ANSI ISUP follows the same framework as ETSI ISUP to ETSI ISUP interworking except the ones listed below

Table 32 Indian ISUP to ETSI ISUP (V2) Interworking

S. No.	Indian ISUP	ETSI ISUP V2
1	Cause Indicator	Cause Indicator
2	Backward Call Indicator	Backward Call Indicator
3	Information Indicator	-
4	Calling Party Category	Calling Party Category
5	Transmission Media Request	Transmission Media Request
6	USI	USI
7	Circuit Group Supervision Message type	-
8	Redirection Information in REL Message	-
9	Automatic Congestion Level in REL Message	Automatic Congestion Level in REL Message
10	Redirection Number in REL Message	-
11	Call Reference (Only in IAM)	Call Reference (Only in IAM)
12	Display Information	-
13	Connected number in CPG message	-
14	Correlation ID in IAM Message	-

15	Call Diversion Treatment Indicator	-
16	Charge Band	-
17	Message Compatibility Information in CRG Message	-
18	Transit Network in IAM Message	-

Table 33 Indian ISUP to ANSI ISUP Interworking

S. No.	Indian ISUP	ANSI ISUP
1	Cause Indicator	Cause Indicator
2	Backward Call Indicator	Backward Call Indicator
3	Information Indicator	Information Indicator
4	Calling Party Category	Calling Party Category
5	Transmission Media Required	USI
6	USI	USI
7	Circuit Group Supervision Message Type	Circuit Group Supervision Message Type
8	Redirection Information in REL Message	Redirection Information in REL Message
9	Automatic Congestion Level in REL Message	-
10	Redirection Number in REL Message	Redirection Number in REL Message
11	Call Reference (only in IAM)	Call Reference (only in IAM)
12	Display Information	-

13	Connected Number in CPG Message	-
14	Correlation ID in IAM Message	-
15	Call Diversion Treatment Indicator	-
16	Charge Band	-
17	Message Compatibility Information in CRG Message	-
18	Transit Network in IAM Message	-

69.3 Hardware Requirements or Dependencies

Not Applicable

69.4 Software Requirements or Dependencies

Not Applicable

69.5 Limitations and restrictions

- Only Indian ISUP to Indian ISUP/ETSIV2/ANSI trunk interworkings will be supported.
- With respect to Lines, only Indian ISUP to IBN line interworking will be supported.
- Transit Network Selection parameter is supported only for transit call scenarios.
- Diagnostics of Cause Indicator parameter in REL message will be removed only when there are no optional parameters in the REL message
- Call Reference Parameter shall only be supported for IAM
- Display Information Parameter will not be supported

69.6 Interactions

Since Indian ISUP is based on ETSI ISUP V2 this feature interacts with the base implementation of ETSI ISUP V2.

69.7 Applicable customer facing sections

Fault Management

Logs	__N/A___
Alarms	__N/A___
Configuration	
Data Schema	___Y___
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

69.8 Glossary

Term	Description
ACM	Address Complete Message
ACC	Automatic Congestion Control
ACL	Automatic Congestion Level
ANM	Answer Message
BCI	Backward Call Indicators
CGBA	Circuit Group Blocking Acknowledgement message
CFB	Call Forwarding Busy
CFN	Call Forward Number
CFNR	Call Forwarding No Reply
CFU	Call Forwarding Un-conditional
CLIR	Calling Line Identification Restriction
CLIP	Calling Line Identification Presentation

Term	Description
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CPC	Calling Party Category
CPG	Call Progress message
CW	Call Waiting
DDI	Direct Dialing-In
ETSI	European Telecommunications Standards Institute
HOLD	Call Hold
IAM	Initial Address Message
ISUP	ISDN User Part
MSN	Multiple Subscriber Number
MCID	Malicious Call Identification
MMI	Man Machine Interface
RLC	Release Complete message
REL	Release message
TMR	Transmission Medium Requirement
USI	User Service Information
3PTY	Three Party Service

69.9 References

[1] BSNL Specification No. S/CCS-02/03. JAN 2000

[2] ITU-T Q.763 Formats and Codes of the ISDN User Part of Signalling System No. 7.

[3] ITU-T Q.764 Signalling System No. 7 - ISDN User Part Signalling Procedures

[4] Indian ISUP requirement document A00004931

70: Functional Description (FN): A00004933

70.1 Feature name

A00004933- Indian ISUP Charging

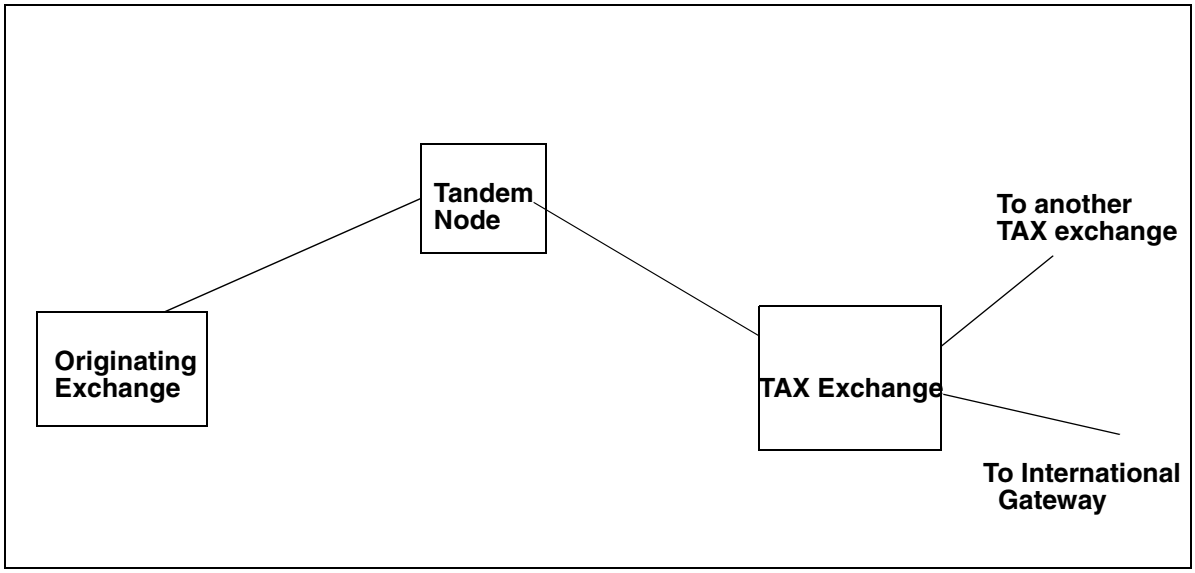
70.2 Introduction

70.2.1 Overview:

In this feature we are dealing with following points

- Charge Band Table.
- CDP node functionality.
- CGP node functionality.
- Exception condition on receipt of Charging message.
- Tandem/interworking node functionality.
- Generation of AMA record.

Figure 1 Network Diagram in Indian scenario



70.2.1.1 Charge Band Table:

Charge Band Tables are used to calculate the pulses for charging in Indian Market. These tables have relationship between the CBN and pulse duration. For Indian Market, CDP is the TAX exchange and CGP is the Local exchange.

70.2.1.1.1 Charge Band Parameter:

CBN parameter is national parameter for Indian ISUP which has following structure

Parameter	Type	Length(octets)	Code(hex)
Message Type	F	1	31
charge band	O	3	
parameter code			FF
parameter length			01
Charge band number			
message compatibility information	O	3	38
end of optional parameter	O	1	00

Message compatibility information need to be supported in the CRG message. The format of the message compatibility information parameter field is shown in table below

8	7	6	5	4	3	2	1
Instruction Indicator							

The instruction indicator has following subfields:

bit

A Transit at intermediate exchange indicator.

According to the Indian ISUP Charging specification it should have the value 0 for transit interpretation.

B Release call indicator.

According to the BSNL specification it should have value 1 which means release call, 0 value is used for do not release call.

C Send notification indicator.

Should have the value 0 which means do not send notification according to the specification.

D Discard message indicator.

According to the BSNL specification it should have value 0 which means do not discard the message (pass on).

E Pass on not possible indicator.

It has value 0 which means release call. Value 1 means discard information.

F/G Broadband/narrowband interworking indicator.

00 value to be used, meaning spare. The extension indicator defines if information continues through the next octet or not. It has a value 1 which means Last octet.

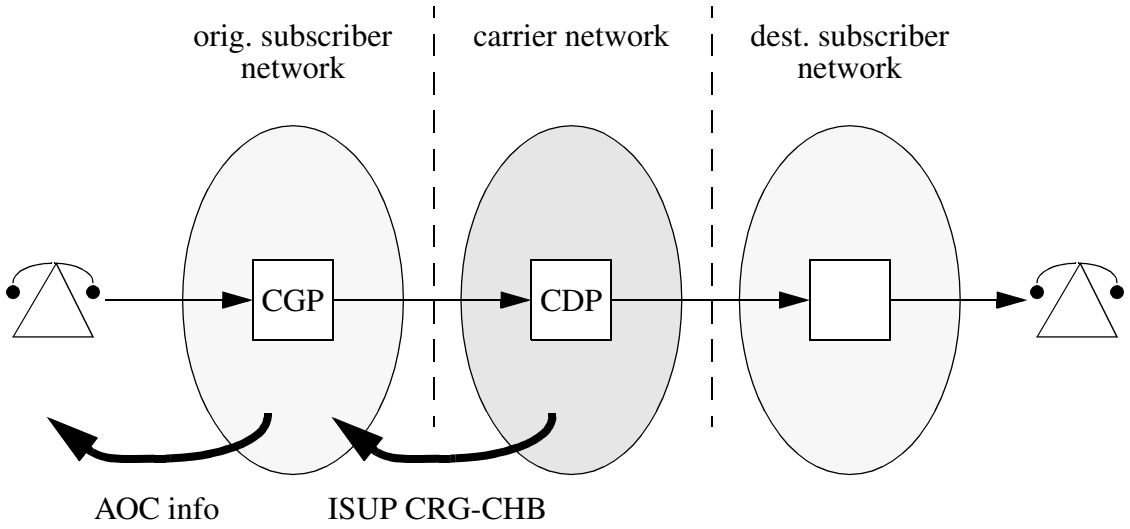
70.2.1.2 Charge Determination point functionality:

This feature provides the capabilities for the determination of charging related information between a charge determination point (CDP) and a charge generation point (CGP) which all may be located in multiple networks or on same network.

Main function of CDP is to determine charge Band number and generation of CRG message. The charge generation point is an exchange where the charging information received from the network is converted into a format that is delivered to the actual subscriber.

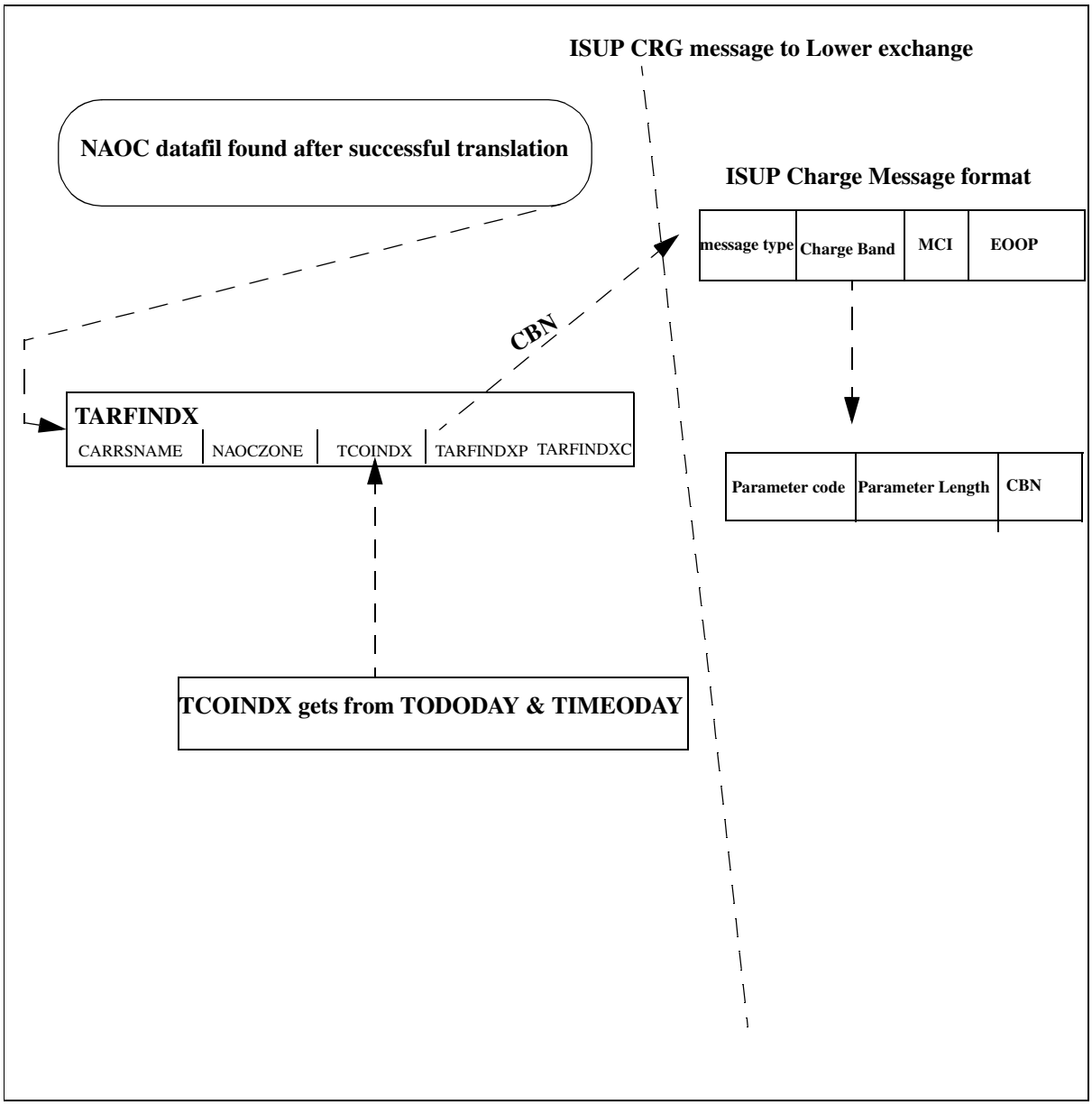
The following diagram shows a simple scenario where this functionality is needed and the location where the CDP (exchange to determine the tariff, send it over ETSI ISUP trunks) and CGP (receiving and processing OLE) reside during the call.

Figure 2 Network AOC support for Indian ISUP Charging



For this NAOC call, the charge determination point (CDP) is located in the carrier network and the charge generation point (CGP) is located in the originating subscriber network. At CDP the charge band number is calculated and send in ISUP CRG message to CGP which uses this information to get the tariff information with the existing charge band table. ISUP charge message is generated for all calls pre ACM at the TAX node. CRG message contains the national specific Charge Band Parameter. Charge Band Parameter contains CBN. The calculation of CBN at the TAX node is done according to the Time of the Day, Type of the call and day of the week. At the outgoing trunk, if NAOC datafill is found after successful translation, then the TARFINDXP indices in the table TARFINDX is taken and is treated as CBN. This CBN number is put in the filled of CRG message along with message compatibility and sent to the CGP. More details are provided later in the datafill section.

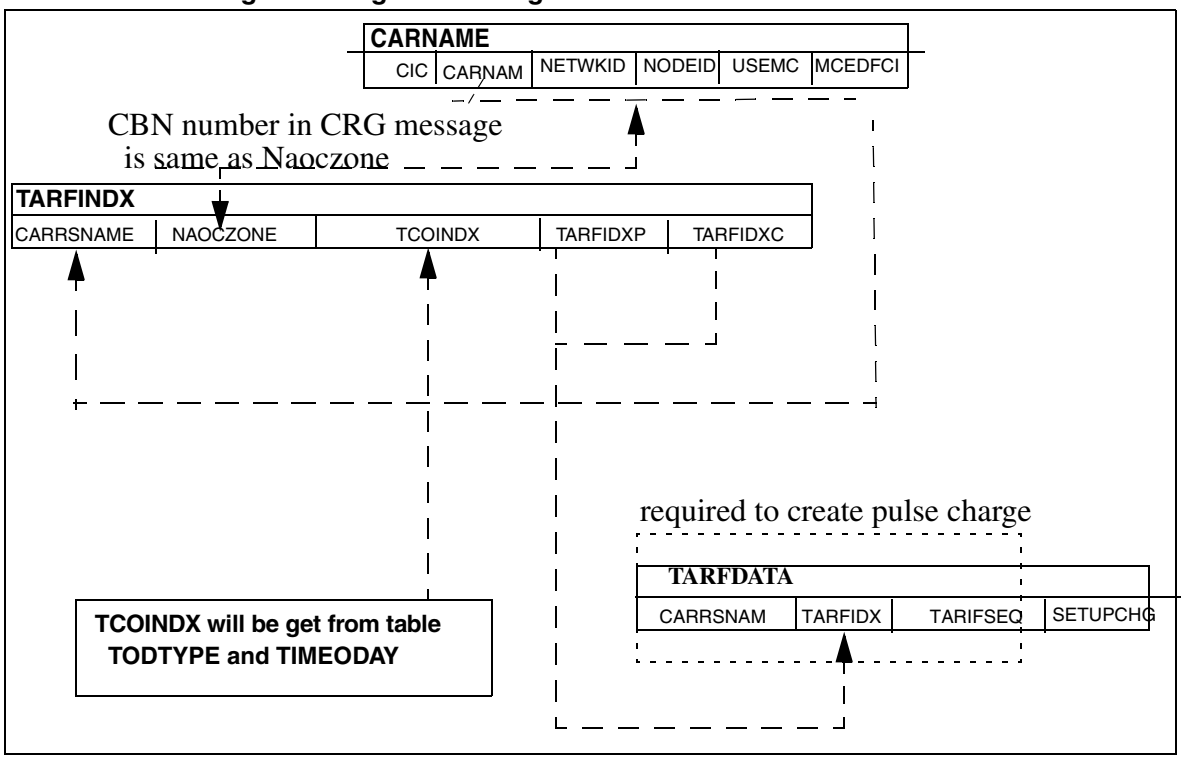
Figure 3 Figure showing table used in CDP and ISUP CRG-CHB format



70.2.1.3 Charge generation point functionality :

On CGP, Charge Band Number received in the CRG message will be used to determine tariff. Table SERVZONE has two keys SERVDN and NAOCZONE. SERVDN can be interpreted by the originating DN whereas the NAOCZONE is same as the CBN received in CRG message. The output of the table will be the CARRSNAM. In the table TARFINDX the keys are CARRSNAM, NAOCZONE, and TCOINDX. TCOINDX is interpreted from TIMEODAY and TODHEAD. The output of the table will be TARFIDXP (for preselect call) or TARFIDXC (for per call). TARFINDX output (tarfindxp and tarfindxc) is used in table TARFDATA to get the charge rate. Table CARRSNAME should be datafilled with charges of one pulse.

Figure 4 Figure showing Tables used at CGP



70.2.1.4 Exception condition on receipt of CRG message:

CS2K will release the call if any of the following cases will occur. These are the exception cases and only in certain scenario when it will occur the call will be released with proper cause value.

70.2.1.4.1 The charge band number received is not in the charge band table: The IAM message will be sent from the LE to the TAX. The tandem (or intermediate) exchange will pass the IAM message to the TAX exchange. ISUP CRG message will be sent to the LE. If the LE find the CBN number in the charge message as corrupted or not in the datafil the call will be released with the cause value 111. Fig 6 gives the diagramatic view of the scenario.

70.2.1.4.2 CRG is not received before ANM/ CON : IAM message for a call is sent to the TAX. If there is any intermediate exchange in between which will pass the IAM message to TAX. If for any reason or for any error condition the CRG nessage is not sent befor the ANM or CON message to LE, the LE will release the call with cause value 111. The diagramatic view of the scenario is shown below.

70.2.1.4.3 When the originating or interworking exchange receives an incorrect CRG message.

Figure 5 Figure showing CRG-CHB received is corrupted

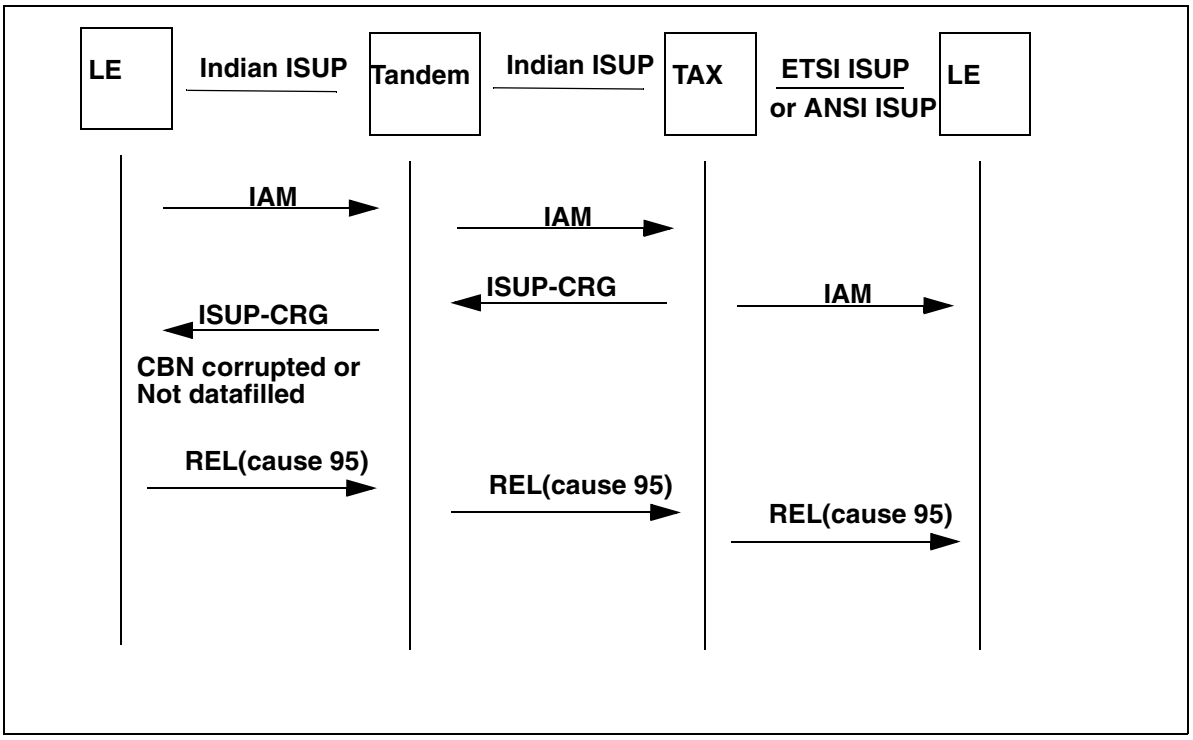


Figure 6 Figure showing no CRG-CHB received

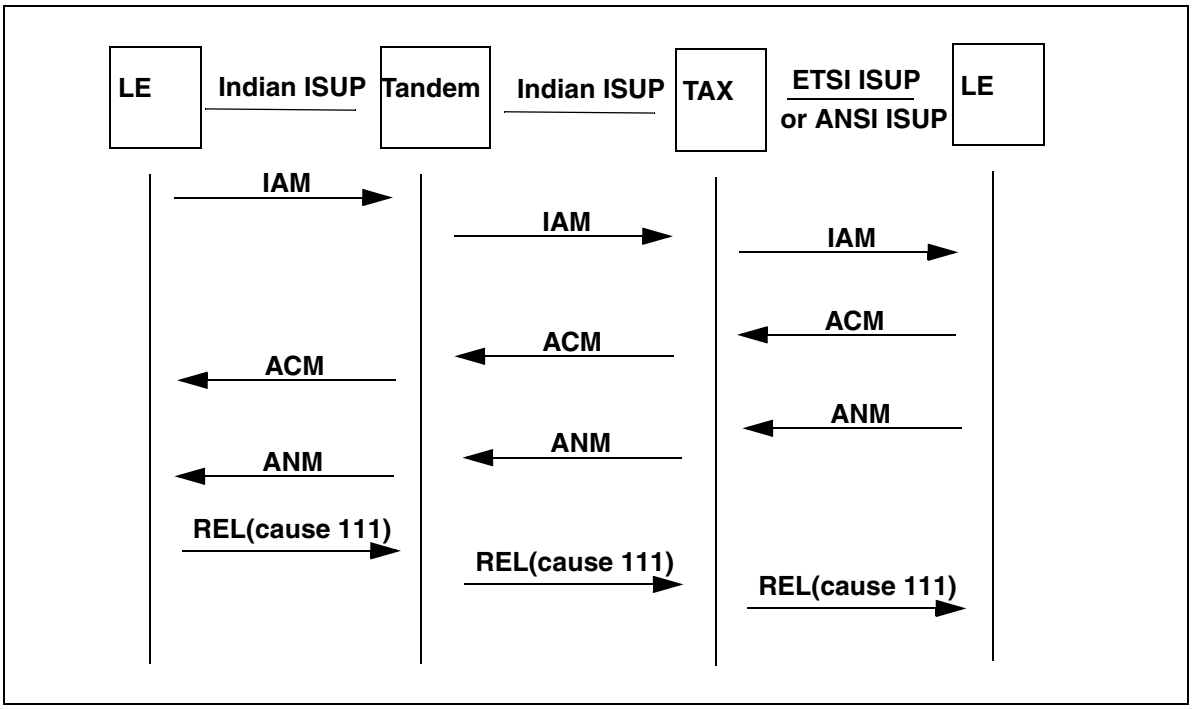
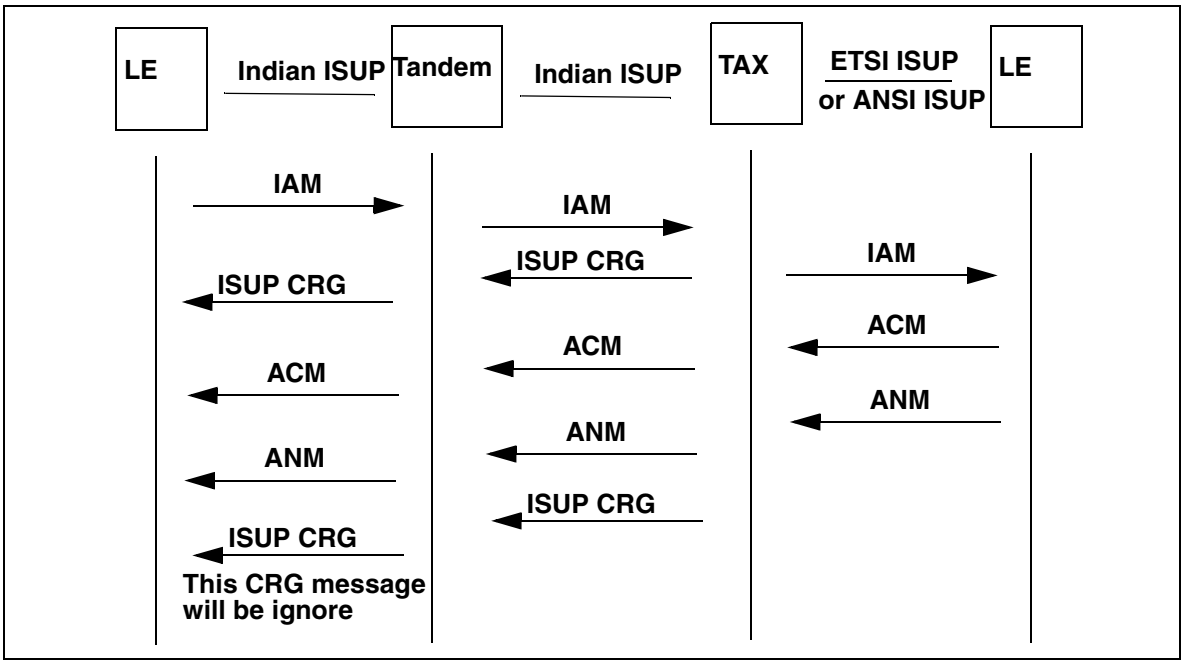


Figure 7 Figure showing CRG-CHB received after call established



70.2.1.5 Internetworking node functionality:

In case when Indian ISUP CRG message has to pass to Indian ISUP internetworking, the TAX exchange will generate the CBN and send the CRG message.

In case when Indian ISUP to ETSI ISUP the tax will send the CRG message to the originating exchange.

In case of ETSI ISUP to Indian ISUP the internetworking node need not send any CRG message. Same applies for ANSI ISUP and Indian ISUP internetworking.

Figure 8 Indian ISUP <-> ETSIISUP

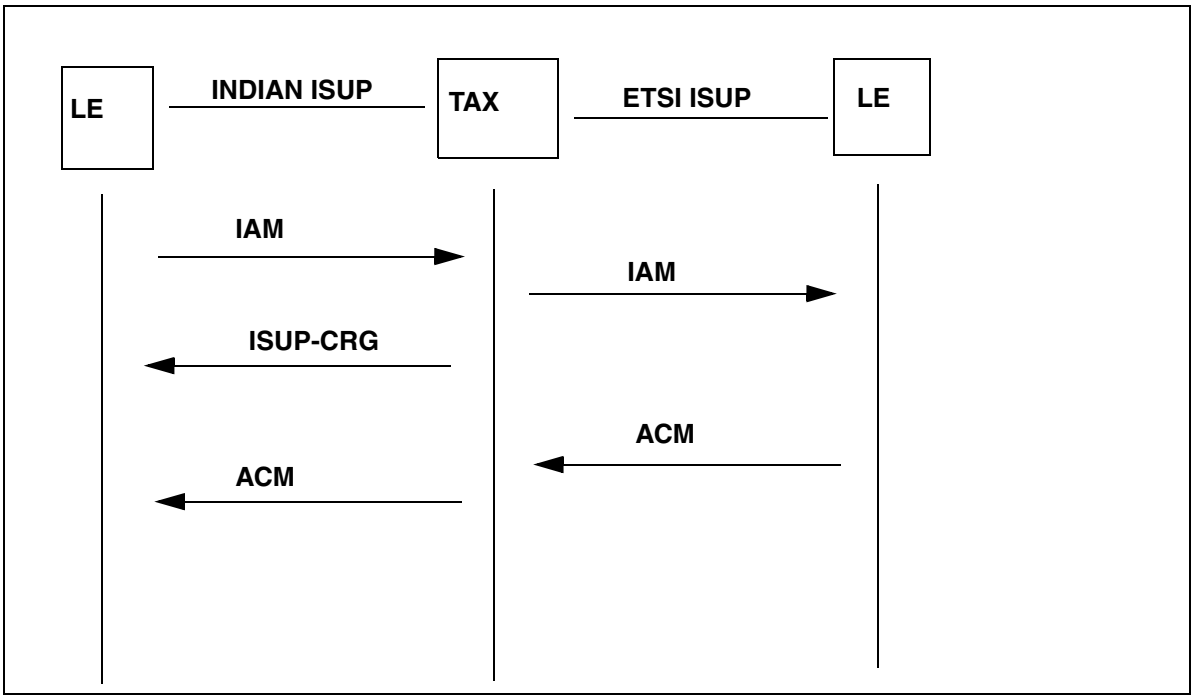


Figure 9 Indian ISUP <-> ANSI ISUP

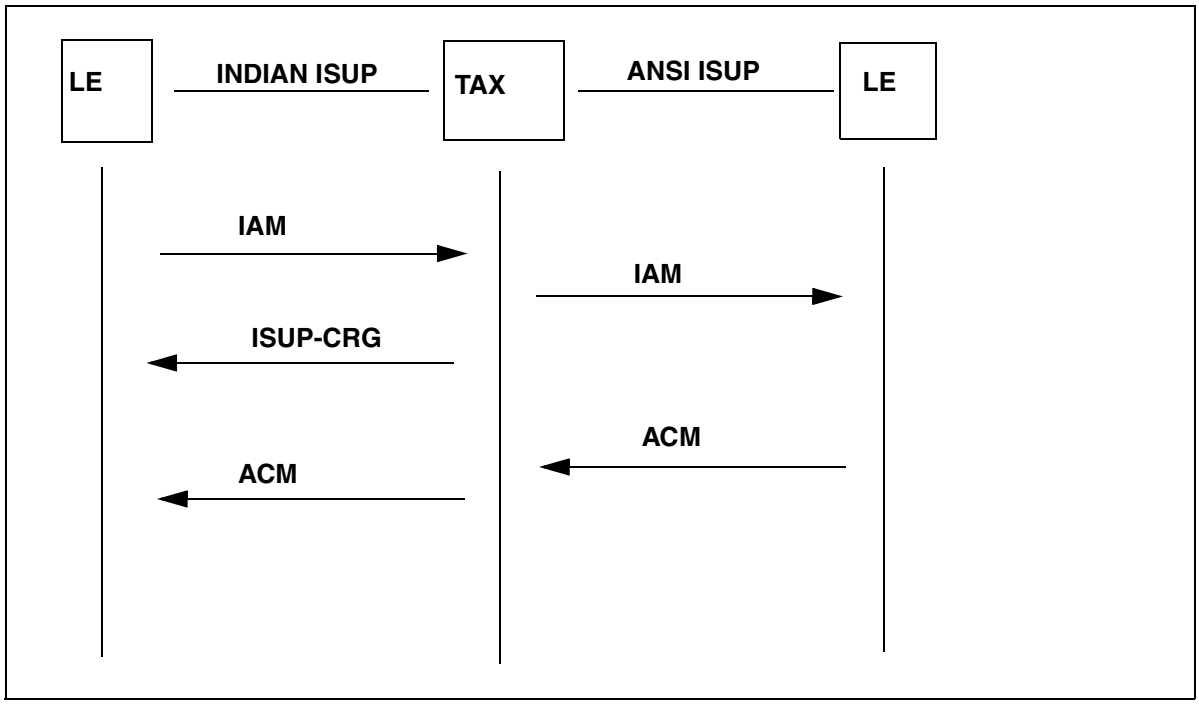


Figure 10 ETSI ISUP <-> Indian ISUP

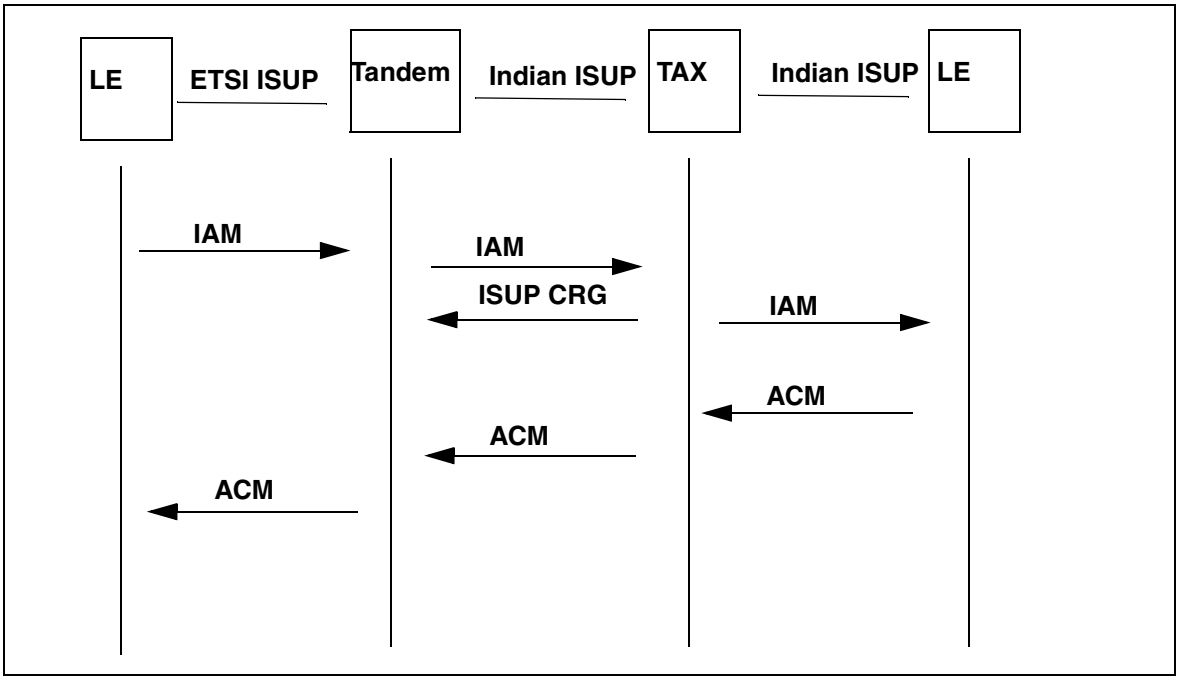
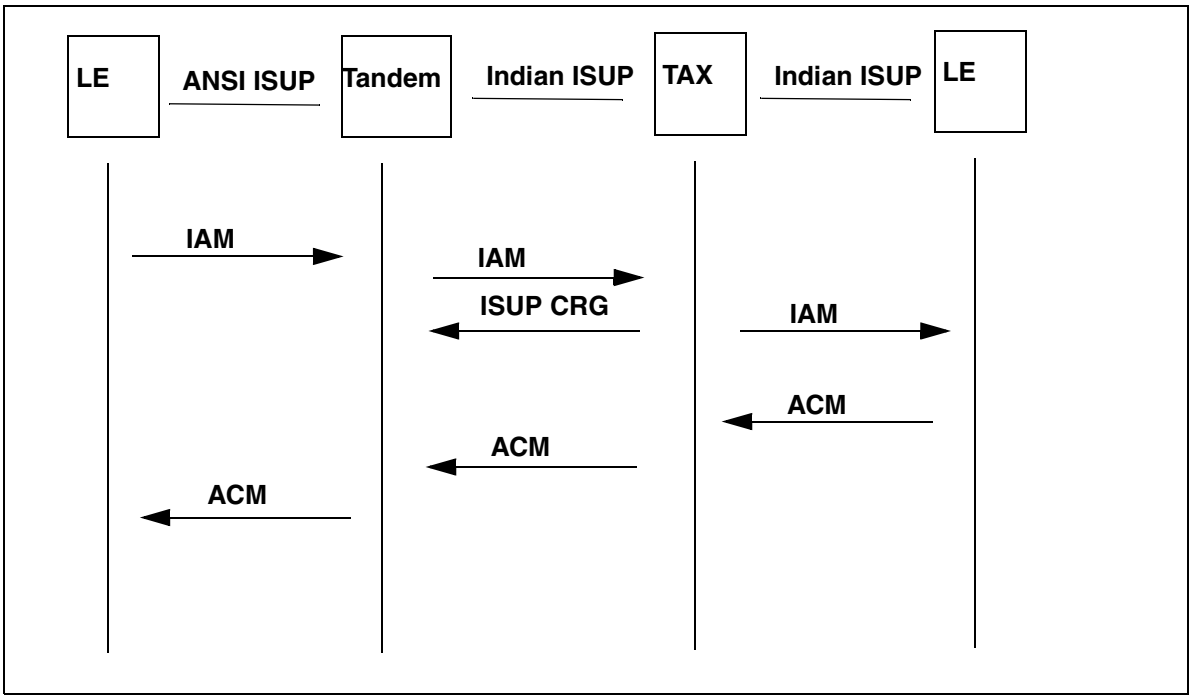


Figure 11 ANSI ISUP <-> Indian ISUP



70.2.1.6 Generation of AMA record:

Indian ISUP has requirement to generate the AMA record for the call. AMA record is generated according to the Time of day, Day of week and Holiday.

In the Local exchange (i.e CGP) a new option **Capt_Charge_Band_Number** should be selected and AMASEL should be made ON to generate AMA record.

```
>table amaopts
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>format pack; lis all;.
TOP
OPTION                          SCHEDULE
-------------------------------------------------------------------
Capt_Charge_Band_Number         ON
```

For the CDP the option Capt_Charge_Band_Number is set to OFF condition.

70.3 Background

70.3.1 NAOC

Network **A**dvice **O**f **C**harge (NAOC) implements the tariffing of calls between different exchanges. It can operate

- in a single carrier environment, where tariffs are sent between different nodes within the same carrier's network. This is the case addressed by the current activity.

For more information Refer act id A00002637 page 36, 37

70.4 Datafill

Datafill is done by entering the keyword NAOC following by one of the zoning classes **NATL, SERV** in the **PXHEAD/PXCODE** tables as listed below. This activity provide changes to the way how NAOC has to be provisioned.

70.4.1 The Translation Option:

After an ISUP IAM message is received and all the parameters inside it are decoded (Calling Party Number and Called Party Number) the translation tables are traversed.

This option has many possible sub-options: **natl**, **serv** are two of them. Each of the two sub-options are discussed separately.

The naoc translation option should only be datafilled if you want to configure the exchange as CDP. Datafilling this option on the wrong node may result in more than one CDP for the call, which can cause undesirable results at the CGP. At the CGP the NAOC option is not to be filled.

a) NAOC sub-option: NATL

If this translation selector/sub-option is encountered during the translation of the call, the call is assumed to be a National call. This means the call does not cross any international boundaries, and is a regular subscriber to subscriber call. In order to define which calls are National calls, they must be datafilled in the translation tables with the **naoc** selector, with the **natl** sub-option. The zone class is then set to **national,** and the NAOC Indian ISUP process begin to access the zoning/tariff database.

```
table natlzone;
>format pack; lis all;
<line length>: 76 columns can be output per line.
<pack mode>: Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>: The first column of output is column 1.
TOP
ONDC NATLRNGE
-------------
2 (0 1) $
```

b) Indian ISUP NAOC sub-option: SERV

If this translation selector/sub-option is encountered during the translation of the call, the call is assumed to be an International call. This means the destination number is outside the originators international boundary, and it is a regular subscriber to subscriber call. In order to define which calls are international calls, they must be datafilled in the translation tables with the **naoc** selector, with the **serv** sub-option.

```
table servzone;
>format pack; lis all;
<line length>:   76 columns can be output per line.
<pack mode>:     Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>:  The first column of output is column 1.
TOP
SERVDN  NAOCZONE CARRSNAME   DISCINDX  FREECALL
---------------------------------------------
 222             23         RES63         $       405             N
```

70.4.1.1 Table PXHEAD:

PXHead table in CDP is to be filled with NATL, INTL or SER but at CGP PXHEAD is not to be datafil.

TABLE PXHEAD

TYPEPX DFLT CONT (CLASS NATL) (AMAXLA MANTEST) (XLT PX K4PSTN) (NAOC NATL)

70.4.1.2 Table PXCODE

TABLE PXCODE
TYPEPX 43 43 CONT (NAOC NATL) $

70.4.1.3 Table TRKOPTS:

TABLE TRKOPTS
add etsiv2og ISUPSVC ISUPSVC mykey
add etsiv2ic ISUPSVC ISUPSVC mykey
add etsiv2og OFFNET_CARRID OFFNET_CARRID 1041
add etsiv2ic OFFNET_CARRID OFFNET_CARRID 1041

70.4.1.4 Table PCIXLA:

TABLE PCIXLA
add 1041 PRESELECT 4 $ $ XLARTE PX TYPEPX PRESELRTE 8 $

70.4.1.5 Table OFCENG

TABLE OFCENG
PRESELECT_DEFAULT_CARRIER 1041
ENABLE_METERING Y

70.4.1.6 Table CARNAME

```
>table carname;format pack;lis all;
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: CARNAME
<line length>:   76 columns can be output per line.
<pack mode>:     Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>:  The first column of output is column 1.
TOP
CIC CARNAM NETWRKID NODEID USEMCE MCEDFLT MCEOVR
------------------------------------------------
1041 NAOC 0 0 N CALL_BY_CALL USE_CALL_BY_CALL
```

70.4.1.7 Table NATLZONE

ONDC NATLRNGE
---
add 211 (0 1) (195 2) (205 3) (220 2) (230 1) $

70.4.1.8 Table RESNAME

```
>table resname;format pack;list all;
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: RESNAME
<line length>:   76 columns can be output per line.
<pack mode>:     Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>:  The first column of output is column 1.
TOP
RESNAM CIC MCEOVR
-----------------
RES63 1041 USE_CALL_BY_CALL
BOTTOM
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RESNAM:
>res63
CIC:

MCEOVR:
>USE_CALL_BY_CALL
```

70.4.1.9 Table DNSCRN

```
TABLE DNSCRN
add  8206001 (CARRSNAM RES63)
```

70.4.1.10 Table TARFINDX

```
TABLE: TARFINDX
CARRSNAM NAOCZONE TCOINDX TARFIDXP TARFIDXC
------------------------------------------
TOP
CARRSNAM NAOCZONE TCOINDX  TARFIDXP  TARFIDXC
--------------------------------------------------
  RES63       1      1          72       73
  RES63       1      2          72       73
  RES63       1      3          72       73
  RES63       1      4          72       73
  RES63       1      5          72       73
  RES63       1      6          72       73
  RES63       1      7          72       73
  RES63       1      8           1        1
```

70.4.1.11 Table TARFDATA

```
add RES63 73 (300 -2 0 N) $ 1 0 0 N
add RES62 73 ( 3-2 0 N) $ 1 0 0 N
```

70.4.1.12 Table TODHEAD

```
TODNAME TODTYPE DAYTYPES
-----------------------------------------------
add RES63 NAOC 3 (weekday) (weekend) $
```

70.4.1.13 Table DAYOWEEK

```
 TODNAME WEEKDAY DAYTYPE
-----------------------------------------------
add RES63 MON WEEKDAY
 add RES63 TUE WEEKDAY
 add RES63 WED WEEKDAY
 add RES63 THU WEEKDAY
 add RES63 FRI WEEKDAY
 add RES63 SAT WEEKEND
 add RES63 SUN WEEKEND
```

70.4.1.14 Table TIMEODAY

```
TODNAME DAYTYPE TIME DATA
-------------------------------------------
add RES63 weekday 0 0 NAOC 1
add RES63 weekday 2 0 NAOC 6
add RES63 weekday 3 0 NAOC 7
add RES63 weekday 8 0 NAOC 2
add RES63 weekday 12 0 NAOC 3
add RES63 weekday 18 0 NAOC 4
add RES63 weekday 0 0 NAOC 5
```

70.5 Hardware Requirements or Dependencies

This feature does not add any additional hardware requirements and dependencies on top of those one used for NAOC and PCA or for the features that NAOC/PCA do interact with.

70.6 Software Requirements or Dependencies

This feature requires the following features do be activated by SOC:

- ***NETK0019*** Network AOC
- ***NETK0024*** Network AOC Tariff
- ***NETK0028*** CGP Network AOC

SOC option name:	NETK NETWORK AOC Tariff
SOC option title:	NETK NETWORK AOC Tariff
SOC option control type:	code/state

New SOC option?	Yes
SOC option order code	NETK0024
Option defined in DRU:	WT
Affected products:	-

NAOC tariff information is required, since this activity reuses the ***NAOC*** functionality. NAOC datafill including the NAOC tables and translation options have to be set up in a appropriate way.

70.7 Limitations and restrictions

70.8 Interactions

None

70.9 Applicable customer facing sections

Fault Management
Logs _____
Alarms _____
Configuration
Data Schema _____
User Interface _____
Element Management _____
Security _____
Service Order _____
Office Parameters _____
Accounting (includes AMA billing) _____
Performance (includes operational measurements) _____

70.10 NAOC and PCA history

Figure 12 Overview of the NAOC and PCA development

Type	Stream	Activity	ACTID	Description of Reference

NAOC	MMP12	SIM	ND0076	*German Network-AOC Support over ISUP*, Issue AA03, Version: Pre 1.1, PLS MDIVDOC module: *ND0076*.
			ND0035	*AOC for NLOs Strategic Interface Management (SIM)*, Issue AA03, Release: ISSUE 2.7, PLS MDIVDOC module: *ND0035*.
		Feature	59007987	*ETSI ISUP - Network AOC (CDP+CGP)*, Issue AA25, PLS FMDOC module: *network_aoc_etsi_isup.*
			59008229	*ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)*, Issue AA67, PLS FMDOC module: *naoc_etsi_isup_tariff_db_tco.*
		Feature	59007780	*Network AOC CGP Function*, Issue AA18, PLS FMDOC module: *A59007780*.
	MMP13		59012308	*ETSI ISUP Network AOC - analog enhancement,* Issue AA15, PLS FMDOC module *A59012308 (TDM onlly)*
			59012315	*ETSI ISUP Network AOC - V5.2 enhancement,* Issue AA02, PLS FMDOC module *A59012315*
		Feature	59013775	*Network AOC: Integrated CGP and CDP,* Issue AA27, PLS FMDOC module: *A59013775.*
	ISNH03		59032878	*NAOC on PRI,* Issue AA05, PLS FMDOC module: *A59032878.*
PCA	SN04		59034497	*Payment ceiling for Succession Intl. Cable IP,* Issue AA32, PLS FMDOC module: *A59034497.*
	SN05		59039121	*NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD,* Issue AA30, PLS FMDOC module: *A59039121.*
NAOC	SN06		89007454	*NAOC German Regulatory Enhancements,* Issue AA17, PLS FMDOC module: *A89007454.*
PCA			89007461	*Payment Ceiling Regulatory Enhancements,* Issue AA40, PLS FMDOC module: *A89007461.*
NAOC	SN06.2		A00001927	*Line Hardware Metering,* Issue AA03, PLS FMDOC module: *A00001927.*
			A00002625	Full Line HW Metering / Billing Complianodule, Issue AA01, PLS FMDOC, module: *A00002625.*
			A00002738	*PCA SW Metering Billing Compliance,* Issue AA05, PLS FMDOC module: *A00002638.*

70.11 Glossary

Term	Description
AOC	Advice of Charge
AOCRG	Add-On Charge
APM	Application Transport Message
APP	Application Transport Parameter
BCD	Binary Coded Digit
BRI	Basic Rate Interface
CCB	Call Condense Block
CCS7	Common Channel Signalling System No. 7
CDN	Called Party Directory Number
CDP	Charge Determination Point
CGN	Calling Party Directory Number
CGP	Charge Generation Point
CFBP	Call Forward Busy Programmable
CFBF	Call Forward Busy Fix
CFDP	Call Forward Don’t Answer Programmable
CFDF	Call Forward Don’t Answer Fix
CFF	Call Forward Fix
CFU	Call Forward Universal Programmable
CIC	Carrier Identification Code
CLF	Calling Line Identification with Flash
CLID	Calling Line Identification
CONT	Translation Option - Continue
CRGA	Charging Acknowledgment
CRGT	Charging Tariff
CRP	Charge Registration Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000

CSP	Carrier Selection Parameter
ECT	Explicit Call Transfer
ELN	Essential Line
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
MEB	Metering Extension Block
MMP	Multi Market Platform
NAOC	Network Advice of Charge
NDC	National Destination Code
NLO	New Licensed Operator
NP	Number Portability
ODP	Open Dial Plan
OLE	Originating Local Exchange
PCA	Payment Ceiling Advice
PVG	Passport Voice Gateway
PRI	Primary Rate Interface
RTE	Translation Option - Route
SIE	Service Interaction Environment
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol - Telephony
SNP	Service Number Portability
TNB	Teilnehmernetzbetreiber (German for network, where the CGP is located)
UXLA	Universal Translations
VBD	Voice Band Data
VNB	Verbindungsnetzbetreiber (German for network, where the CDP is located)
XLA	Translations

70.12 References:

- Indian ISUP spec NO. S/SCS-02/03. JAN 2000
- A00002909 - Telekom ISUP (T-ISUP)
- A00003007 - AMA enhancements for DTAG Intl GW
- A00004933 - INDIAN ISUP Charging
- A59008229 - NAOC_ETSI_ISUP_TARIFF_DB_TCO ETSI ISUP - NETWORK AOC TARIFF AND TIME
- A00004931 - Indian ISUP
- Q763(9/97) - Signaling System No 7- ISDN User Part general function of messages and signals.
- TEC specification Q.764
- A00002637- NAOC Trunk Metering Enhancements

71: Functional Description (FN): A00004981

71.1 Feature name

GWC-EM Internet Transparency VCAC provisioning support for CentrexIP gateways - Activity ID A00004981

71.2 Description

Activity A00002512 introduces VCAC in the SN07 timeframe. VCAC introduces Limited Bandwidth Links(LBLs) to the SESM (network panel) AND a topological hierarchy that links LBLs and NATs to form a tree of 'internet transparency middleboxes'. These devices are sent to the small lines GWCs via the

GWC-MIDDLE-BOX-MIB and
GWC-MIDDLEBOX-RSRCUSAGE-MIB (the resource usage of the LBL)

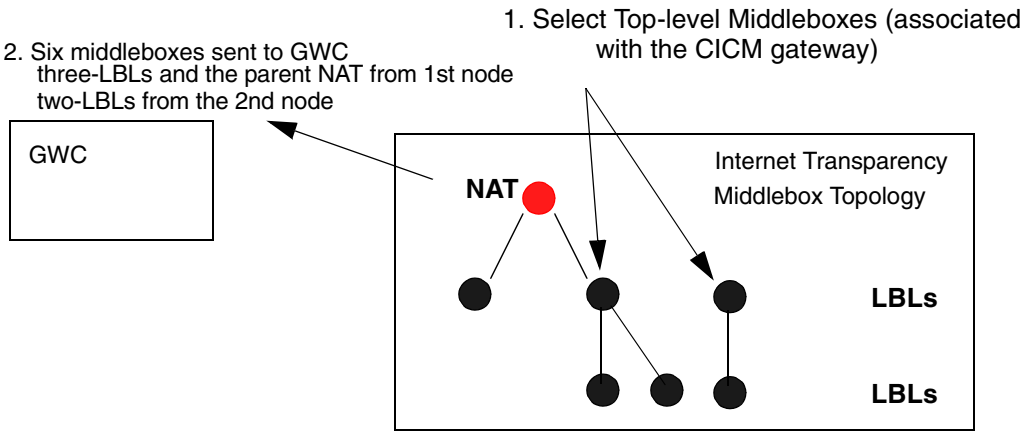
The model for this download of data has been designed for the "fixed-lines" IAD deployment, and occurs when the gateway is associated to an adjacent-middlebox.

This solution is to allow VCAC to function correctly for CICM gateways because unlike the small-lines IAD solution the CICM gateways resides in the TSP (succession) domain. The CICM **gateway** does not "fit" the concept of an "adjacent middlebox". The Adjacent middlebox will always be = 0 (<none>).

CICM users login to the CICM terminals, this sends a message to the GWC. In SN07 this message will contain the "discovered" adjacent middlebox of the terminal/endpoint. The CallP ITA function will then "look-up" this middlebox in the GWC static tables. For a more comprehensive problem definition please refer to the DID for this activity.

This solution allows the user to provision a set of root (top-level) middleboxes, allowing the GWCEM to send all the underlying middleboxes to the GWC. Ensuring that when a CICM user logs in, the middlebox will be available on the GWC, see figure 1.

Figure 1 CICM gateway : Multiple root middlebox provisioning



This feature provides the following functionality (from the OSS and GWCEM - GUI):

- Provision a set of root middleboxes (a maximum of 5) per CICM gateway.
- Change the current provisioning of root middleboxes against provisioned CICM gateways.
- Display/Query the root middleboxes that are provisioned against a CICM gateway.

71.3 Hardware Requirements or Dependencies

No new hardware is required or introduced by this feature. The application components provided by this feature execute as part of the SESM.

71.4 Software Requirements or Dependencies

Dependencies:

- A00002512 VCAC provisioning for the GWCEM
- A00003568 E911 support will allow the CICM endpoints adjacent middlebox to be sent to the GWC when the user logs into the gatway.
- A00002739 GWC Call-P for the VCAC functionality.

71.5 Limitations and restrictions

- The GWC has a limit of 2000 middleboxes.

- Internal counting limits the provisioning of gateways onto the same GWC as the associated chain of LBLs (they must be provisioned onto one GWC). This needs to be made clear in the engineering guidlines, and will be blocked by code to stop the user from completing such provisioning steps.
- A limit of 5 Root Middleboxes can be provisioned against a gatway.
- The CentrexIP users cannot roam outside of their provisioned “enterprise” area, and expect VCAC to function.

71.6 Interactions

The following existing GUIs have been modifed (refer to the Configuration section of this feature):

- Associate Media Gateway Dialog
- Change Gateway Dialog
- Gateway Provisioning Panel

The following existing XML commands have been modified:

- AssocMG
- ChangeRootMiddleBoxes
- QueryMG

The on-line help facility will be updated with information on the use, syntax and valid values for all the above modifications/additions.

71.7 Applicable customer facing sections

Fault Management	
Logs	_N/A_
Alarms	_N/A_
Configuration	
Data Schema	**_X_**
User Interface	**_X_**
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_

Accounting (includes AMA billing) _N/A_

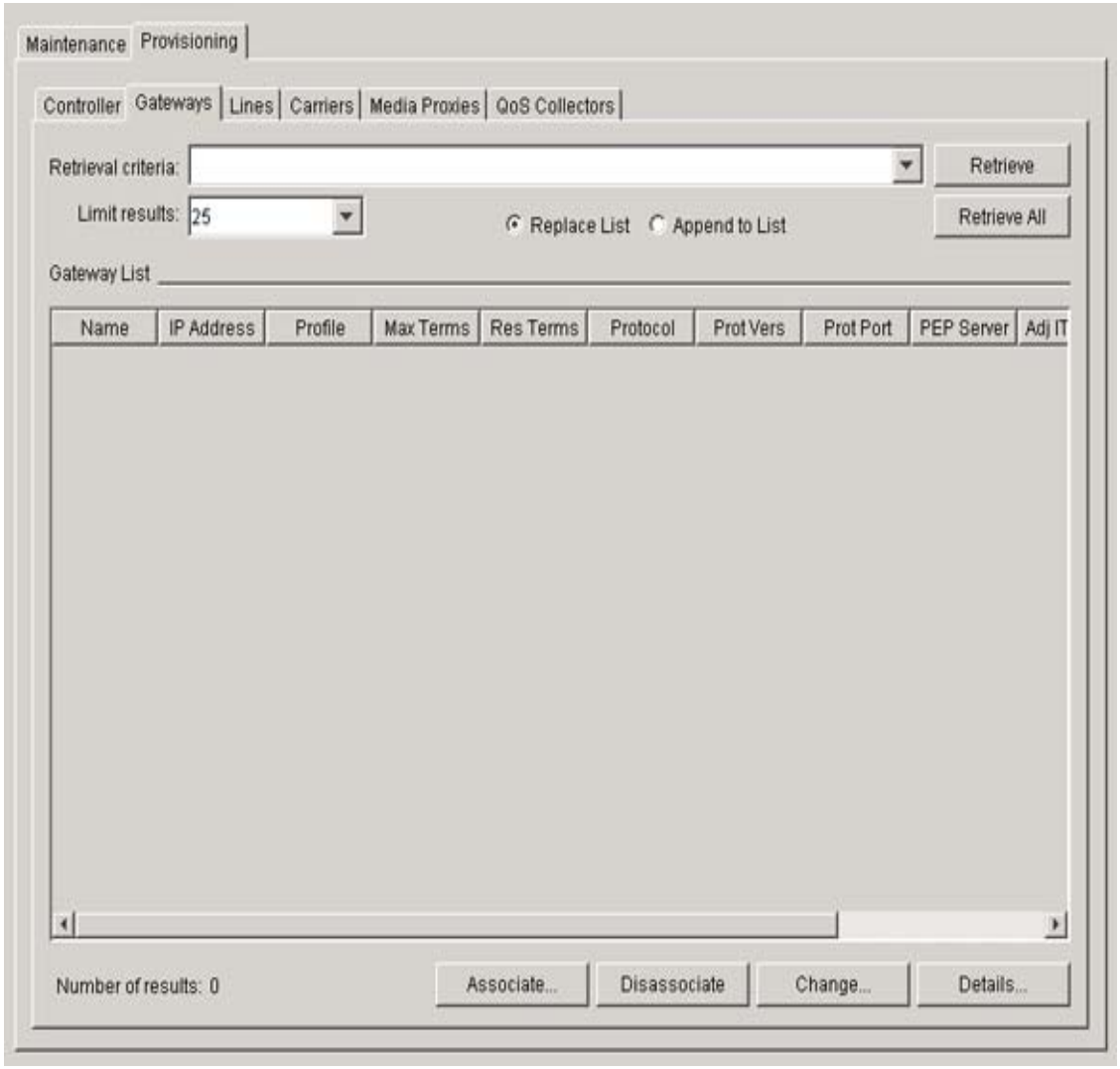
Performance (includes operational measurements) _N/A_

71.8 GWC-EM GWC Provisioning

The GWC-EM has been modified to display the rootMiddleboxes that are provisioned against the CICM gateways.

71.8.1 GUI Client : The Gateways panel

Figure 2 The GWC-EM Gateways Panel



71.9 Gateway Provisioning changes

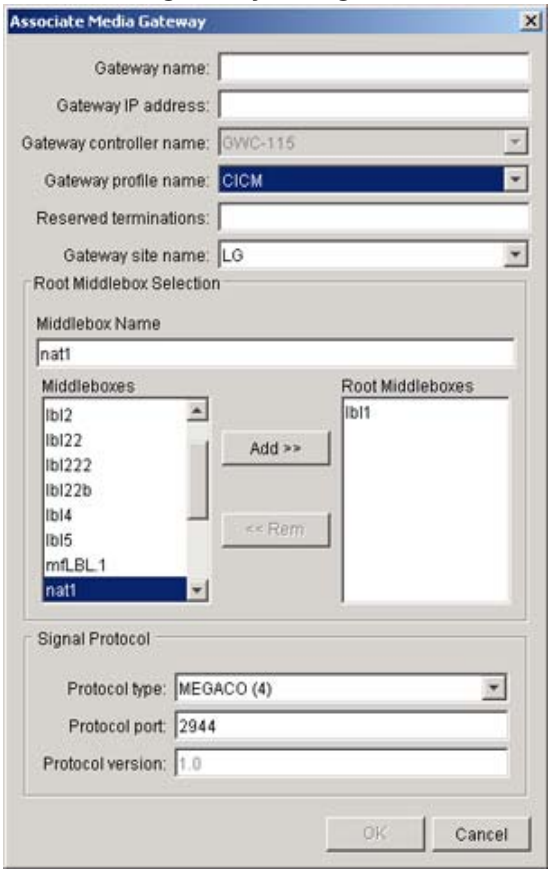
The association of a CICM gateway(or other future Roaming user style gateways) to a GWC has been modified to allow the user to provision a set of root middleboxes (0..5 only). Already provisioned gateways can also be changed to have a different set of (or none) root middleboxes.

71.9.1 GUI Client

71.9.1.1 Associate gateway GUI

The Associate gateway dialogue has been modified to display a new internet transparency panel, this occours when a CICM gateway has been selected. The user may optionally select upto 5 root middleboxes to associate with the CICM gateway, these are selected to define the roaming area where VCAC will function for the CICM users/endpoints. The root middlebox selection process is controlled from within the Root middlebox selection area, this is the same for either the Associate gateway or the Change gateway commands.

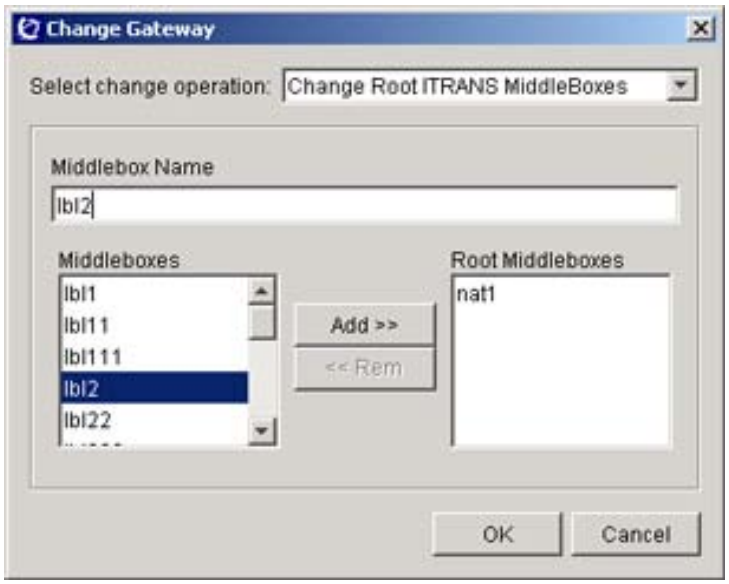
Figure 3 Associate gateway dialogue



71.9.1.2 Change Gateway GUI

The change gateway Root Middleboxes dialogue has been created to allow the user to modify (or remove) the Root Middleboxes associated with an already provisioned CICM gateway.

Figure 4 Change gateway RootMiddleboxes dialogue



71.9.1.3 Root Middleboxes Details

Figure 5 Root Middlebox details can be displayed by selecting the details button.

71.9.2 XML Interface

The AssocMG and QueryMG interface has been modified to allow/display (0..5) root middleboxes. A new interface ChangeRootMiddleboxes has been added to the ItransIf code .If any request is unsuccessful, an error message is returned as described in Appendix B.

71.9.2.1 AssocMG command

Figure 6 XML command AssocMG

```
<?xml version="1.0" encoding="UTF-8"  ?>
 <CommandList>
  <Command>
   <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
     <assocMG usn="1" version="1.0">
      <Parameters>
         <mgUIName>MGBOBXML.5</mgUIName>
         <mgProfileName>CICM</mgProfileName>
         <mgIpAddr>22.33.44.56</mgIpAddr>
         <mgProtocolType>4</mgProtocolType>
         <mgProtocolVersion>1.0</mgProtocolVersion>
         <mgProtocolPort>2944</mgProtocolPort>
         <gwcUIName>GWC-113</gwcUIName>
         <reservedTerminations>5</reservedTerminations>
         <rootMiddleboxName1>NAT1</rootMiddleboxName1>
         <rootMiddleboxName2>NAT2</rootMiddleboxName2>
         <rootMiddleboxName3>NAT3</rootMiddleboxName3>
         <rootMiddleboxName4>NAT4</rootMiddleboxName4>
         <rootMiddleboxName5>NAT5</rootMiddleboxName5>
      </Parameters>
     </assocMG>
   </Methods>
  </Command>
</CommandList>
```

71.9.2.2 QueryMG command

Figure 7 XML command for queryMG (No change)

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
     <queryMG usn="1" version="1.0">
      <Parameters>
        <mgUIName>MGBOBXML.5</mgUIName>
      </Parameters>
     </queryMG>
    </Methods>
  </Command>
</CommandList>
```

Figure 8 XML response for queryMG

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods><queryMG usn="1" version="1.0">
<ReturnData>
<Row>
        <mgUIList>bobcicm.1</mgUIList>
        <mgIpList>43.43.22.11</mgIpList>
        <callServerId>CS2K1_MAID</callServerId>
        <gwcUIName>GWC-113</gwcUIName>
        <svcTypeList>0</svcTypeList>
        <nodeName>LG    033</nodeName>
        <engrEndPoints>123</engrEndPoints>
        <protType>megaco</protType>
        <protVersion>1.0</protVersion>
        <protPort>2944</protPort>
        <profileName>CICM</profileName>
        <rootMiddleboxName1>NAT1</rootMiddleboxName1>
        <rootMiddleboxName2>NAT2</rootMiddleboxName2>
        <rootMiddleboxName3>NAT3</rootMiddleboxName3>
        <rootMiddleboxName4>NAT4</rootMiddleboxName4>
        <rootMiddleboxName5>NAT5</rootMiddleboxName5>
        </Row><RC>0</RC><MsgTxt>Query of a Single MG
        was successful</MsgTxt>
</ReturnData>
</queryMG>
</Methods>
</Response>
</CommandList>
```

71.9.2.3 ChangeRootMiddleboxes command

Figure 9 XML command for ChangeRootmiddleboxes

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeRootMiddleboxes usn="1" version="1.0">
      <Parameters>
          <MGname>bobcicm.1</MGname>
          <rootMiddleboxName1>NAT1</rootMiddleboxName1>
          <rootMiddleboxName2>NAT2</rootMiddleboxName2>
      </Parameters>
     </changeRootMiddleboxes>
    </Methods>
  </Command>
 </CommandList>
```

71.10 Authorization for Commands

The security for the GUI Client and OSSgate interface includes support for permission or ‘Authorization’ levels for commands. Each command is assoicated with one or more user groups. In order to execute a command, a user must belong to at least one of the assoicated user groups. The user groups assoicated with the new commands associated with this feature are specified in the table below.

Table 1 NEW Internet Transparency Commands Authorization

Command	User Group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
ChangeRootMiddleboxes	X	X			
Display Gateway Root Middlebox details	X	X	X	X	X

71.11 Upgrade

When upgrading the GWCEM to SN07 when CICM gateways are present in the Network:

It is necessary to (i) set the Call Agent ID and then (ii) update the IDs for all enterprises (NATs) on a CICM to new IDs **prior** to upgrading the CICM Gateway.

Hence the recommended order for upgrade is as described below:

Upgrade Procedure

1. Upgrade GWCEM to SN07.
2. Set Call Agent ID in GWCEM. This causes all existing middlebox ids to be upgraded to the SN07 format.
3. Upgrade the GWC to SN07 (this may also be done after step 5).
4. Upgrade CICM EM to SN07
5. On the CICM EM, using the provided interface, retrieve the middlebox IDs for all NATs from GWCEM. This will update the NAT information stored in the CICM EM with the new SN07 format middlebox ids.
6. Upgrade CICMs to SN07. CICM upgrade from SN06.2 to SN07 will be done by adding SN07 CICM to GWC and migrating users across to new CICM. The SN07 CICM will have the new format middlebox IDs. All terminals will re-login as part of this upgrade, hence all get new format IDs associated with them in the CICM.

71.12 Glossary

Term	Description
GUI	Graphical User Interface
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
NAT	Network Address Translation
LBL	Limited Bandwidth Link
VCAC	Virtual Connections Admission Control

71.13 Appendix A: XML validation schemas

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

                                                                                <!--
*****************************************************************************
********************** -->
 <!-- * Define AssocMG Method Parameters -->
                                                                                <!--
*****************************************************************************
********************** -->
 <xsd:complexType name="assocMGMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="assocMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="assocMGParamsType">
  <xsd:sequence>
   <xsd:element name="mgUIName" type="NoSpaceNameType" />
   <xsd:element name="mgProfileName" type="NoSpaceNameType" />
   <xsd:element name="mgIpAddr" type="IPAddressType" />
   <xsd:element name="mgProtocolType" type="MGProtocolType" />
   <xsd:element name="mgProtocolVersion" type="xsd:decimal" />
   <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" />
   <xsd:element name="mgSiteName" type="MGSiteNameType" minOccurs="0" />
   <xsd:element name="gwcUIName" type="GWCNameType" minOccurs="0" />
   <xsd:element       name="reservedTerminations"       type="ReservedTerminationsType"
minOccurs="0" />
   <xsd:choice minOccurs="0">
    <xsd:element name="pepServerName" type="xsd:token" />
    <xsd:element name="itransMiddleboxName" type="xsd:token" />
   <xsd:element name="rootMiddleboxName1" type="NoSpaceNameType" />
</xsd:choice>
 <xsd:element name="rootMiddleboxName2" type="NoSpaceNameType" minOccurs="0" />
  <xsd:element name="rootMiddleboxName3" type="NoSpaceNameType" minOccurs="0" />
  <xsd:element name="rootMiddleboxName4" type="NoSpaceNameType" minOccurs="0" />
  <xsd:element name="rootMiddleboxName5" type="NoSpaceNameType" minOccurs="0" />
  </xsd:sequence>
 </xsd:complexType>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
```

```
            xml:lang="en" >

                                                                                <!--
*****************************************************************************
********************** -->
 <!-- * Define changeRootMiddleboxes Method Parameters -->
                                                                                <!--
*****************************************************************************
********************** -->
 <xsd:complexType name="changeRootMiddleboxesmethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="changeRootMiddleboxesparamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="changeRootMiddleboxesparamsType">
  <xsd:sequence>
   <xsd:element name="MGname" type="NoSpaceNameType" />
    <xsd:element name="rootMiddleboxName1" type="NoSpaceNameType" />
   <xsd:element name="rootMiddleboxName2" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName3" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName4" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName5" type="NoSpaceNameType" minOccurs="0" />
</xsd:sequence>
 </xsd:complexType>
```

71.14 Appendix B: Error codes and messages

Table 2 Return codes when command is unsuccessful

Cause of error	Return code	Example return messages
The Media Gateway hasn't got a ITransRoam service type in its profile	16	The use of Root Middle Box name(s) is invalid. The Gateway does not support this internet transparency service.
The GWCEM has failed the provisioning method.	21	GWCEM failed to associate the MG with the GWC, Reason the number of distinct Middleboxes used gwc *[gwc id]* exceeds the limit of 2000 per GWC

Cause of error	Return code	Example return messages
Incorrect command version in query	301	Unsupported version
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error
Unable to change RootmiddleboxNames because of a database error occurred	303	Database error occurred during setting of Root MiddleboxNames
Unable to add/change RootmiddleboxNames because of invalid input data	304	Cannot set RootMiddleboxName because VCAC internal counting constraint hit. LBLs must be on one GWC.
User is not a member of any of the user groups allowed to perform this action	501	Insufficient permissions to perform this operation
General SAX parser exceptions	None	caught ParserEx,Reason: Caught SAXException trying to parse xml-Details:org.xml.sax.SAXParseException: Element type "rootMiddleboxName6" must be declared.>

71.14.1 Example Return Messages

Error message example:

```
<?xml version="1.0" encoding="UTF-8"  ?>
 <CommandList>
  <Command>
   <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
     <assocMG usn="1" version="1.0">
      <Parameters>
       <mgUIName>MGBOBXML.5</mgUIName>
       <mgProfileName>CICM</mgProfileName>
       <mgIpAddr>22.33.44.56</mgIpAddr>
       <mgProtocolType>4</mgProtocolType>
       <mgProtocolVersion>1.0</mgProtocolVersion>
       <mgProtocolPort>2944</mgProtocolPort>
       <gwcUIName>GWC-113</gwcUIName>
       <reservedTerminations>5</reservedTerminations>
```

```
      <rootMiddleboxName1>NAT1</rootMiddleboxName1>
      <rootMiddleboxName2>NAT2</rootMiddleboxName2>
      <rootMiddleboxName3>NAT3</rootMiddleboxName3>
      <rootMiddleboxName4>NAT4</rootMiddleboxName4>
      <rootMiddleboxName5>NAT5</rootMiddleboxName5>
    </Parameters>
   </assocMG>
  </Methods>
 </Command>
</CommandList>
<?xml version="1.0" encoding="UTF-8" ?><CommandList><Response><Interface>cs2kCfgMgrIf</
Interface><Methods><assocMG usn="1" version="1.0"><RC>21</RC><MsgTxt>GWCEM failed to associate the MG with
the GWC, Reason is The Root Middlebox : NAT1 does not exist  </MsgTxt></assocMG></Methods></Response></
CommandList>
```

Success message example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList><Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
<assocMG usn="1" version="1.0">
<ReturnData><Row>
<gwcUIName>GWC-113</gwcUIName>
<gwcIpAddr>47.165.172.76</gwcIpAddr>
<mgNodeName>LG    00 1</mgNodeName>
</Row><RC>0</RC>
<MsgTxt>The MG was successfully associated with a GWC</MsgTxt>
</ReturnData>
</assocMG>
</Methods>
</Response></CommandList>
```

71.15 Appendix C: XML Commands: description of method parameters

71.15.1 Parameter definitions

- **encoding??**
- **version** - The version refers to the version of the method or operation - e.g., the changeRootMiddleboxNames operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.
- **ReturnCode value**- A numeric value indicating the result of the attempted operation (see Table 3, for range and definitions of each possible value). TYPE *string*.
- **Return code text**- Appropriate text that describes the result of the operation. TYPE *string*.

- **rootMiddleboxName1(1..5)** - The Middlebox name(s) of the root node middlebox(es) that encompasses the enterprise network that the CICM gateway operates with.. TYPE *NoSpaceNameType* .(32 character token without spaces, see xsd definitions in Appendix A.)

71.15.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **AssocMG** - Method to associate a gateway to the CS2K. This method has the following NEW parameters: (only NEW ones described, see standard documentation for the other definitions).

- Input data:

– usn

– version

– rootMiddleboxName1 (Optional, Cannot be included as well as itransMiddleboxName or pepServerName) - defines the 1st RootMiddlebox for this gateway.

– rootMiddleboxName2 (Optional, Cannot be included as well as itransMiddleboxName or pepServerName) - defines the 2nd RootMiddlebox for this gateway.

– rootMiddleboxName3 (Optional, Cannot be included as well as itransMiddleboxName or pepServerName) - defines the 3rd RootMiddlebox for this gateway.

– rootMiddleboxName4 (Optional, Cannot be included as well as itransMiddleboxName or pepServerName) - defines the 4th RootMiddlebox for this gateway.

– rootMiddleboxName5 (Optional, Cannot be included as well as itransMiddleboxName or pepServerName) - defines the 5th RootMiddlebox for this gateway.

- Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

2. **QueryMG** - Method that gets the gateway information from a CS2K. This method has the following NEW Output parameters: (only NEW ones described, see standard documentation for the other definitions) :

- Output data:

– rootMiddleboxName1 - defines the 1st RootMiddlebox for this gateway.

– rootMiddleboxName2 - defines the 2nd RootMiddlebox for this gateway.

– rootMiddleboxName3 - defines the 3rd RootMiddlebox for this gateway.

– rootMiddleboxName4 - defines the 4th RootMiddlebox for this gateway.

– rootMiddleboxName5 - defines the 5th RootMiddlebox for this gateway.

–

3. **changeRootMiddleboxes** - Method that changes the rootMiddleboxes for a given gateway. This method has the following parameters:

- Input data:

– usn

– version

– MGname indicates the gateway that this change command is for.

– rootMiddleboxName1 - defines the 1st RootMiddlebox.

– rootMiddleboxName2 - (Optional) defines the 2nd Root Middlebox.

– rootMiddleboxName3 - (Optional) defines the 3rd Root Middlebox.

– rootMiddleboxName4 - (Optional) defines the 4th Root Middlebox.

– rootMiddleboxName5 - (Optional) defines the 5th Root Middlebox.

- Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

72: Functional Description (FN): A00005164

72.1 Feature name

ACT.A00005164 - Russia ISUP V2+ on CS2K .

72.2 Description

This activity provides the capability to support Russia ISUP V2+ introduced by the activity ACT.A00000937 on succession product line. This is done by porting the functionality of existing TDM MMP19 feature with actid ACT.A00000937 into the ISN07 load.

The purpose is to enable CS2K with ISN load to directly interconnect to existing Russia network.

In this activity, the interworkings of only the following agents are verified:

- Russia ISUP V2+ to/from Russia ISUP V2+
- Russia ISUP V2+ to/from IBN/V5.2 lines
- Russia ISUP V2+ to/from ETSI PRI
- Russia ISUP V2+ to/from Russia ISUP V2+ over SIP-T

ACT.A00000937 addresses only the ability to support IBN to/from Russia ISUP V2+, and Russia ISUP V2+ to/from Russia ISUP V2+ interworkings. Other Russia specific functionalities, such as ISDN interworkings, new subscriber categories, subscriber category based authentication, etc., are implemented in MMP20 time frame with the following features:

- ACT.A00001923 - “CIS Subscriber Categories”
- ACT.A00001929 - “Russian ISUP - ISDN Interworkings”
- ACT.A00002100 - “ISUP-R-2000 Operator Call on Busy Subscriber (Toll Break In) Support”.

This activity verifies the functionality provided with these activities (for supported interworkings).

Russia requires a distinct ringing when a call request is received from toll exchange over Russia ISUP V2+ trunks. This functionality is out of the scope of this activity.

For the differences between Russia ISUP V2+ vs. ETSI ISUP V2 BASE variant, please refer to **ISUPR2000** in FMDOC library. Additionally, “ISDN

User Part (ISUP) Technical Specifications For the National Network of Russia" includes the Russia requirements for ETSI PRI interworkings.

72.3 Hardware Requirements or Dependencies

None.

72.4 Software Requirements or Dependencies

None.

72.5 Limitations and restrictions

Following interworkings are not verified with this activity:

— ETSI ISUP V2 BASE to/from Russia ISUP V2+

— BRI to/from Russia ISUP V2+

All limitations and restrictions indicated in the FN documents of ACT.A00000937, ACT.A00001923, ACT.A00001929, and ACT.A00002100 are also applicable in this activity.

In ACT.A00002100, Russia specific call waiting tone was applied to the operator, when an operator calls a busy subscriber over Russia ISUP V2+ trunks.

On TDM, in order to be able to apply the Call Waiting Tone to the operator over Russia ISUP V2+ trunk, a special CWT trunk was defined on MTM device which has 3X68AB/ 3X68AC card on it. However, this hardware is not available on CS2K, therefore, standard ring-back tone is applied to the operator in TBI.

Russia requires a distinct ringing when a call request is received from toll exchange over Russia ISUP V2+ trunks. This functionality is out of the scope of this activity.

72.6 Interactions

All interactions provided in the FN documents of ACT.A00000937, ACT.A00001923, ACT.A00001929, and ACT.A00002100 are also applicable, and are verified in this activity.

72.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface __X__

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

72.8 Glossary

Term	Description
CIS	Commonwealth of Independent States
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ETSI	European Telecommunications Standards Institute
PRI	Primary Rate Interface
BRI	Basic Rate Interface
SIP-T	Session Initiation Protocol Tandeming

72.9 References

- A00000937 - “Russia ISUP V2+ - Phase.1” in FMDOC library
- A00001923 - “CIS Subscriber Categories” in FMDOC library
- A00001929 - “Russian ISUP - ISDN Interworkings” in FMDOC library
- A00002100 - “ISUP-R-2000 Operator Call on Busy Subscriber (Toll Break In) Support” in FMDOC library
- ISUPR2000 in FMDOC library

73: Functional Description (FN): A00005802

73.1 Feature name

A00005802, *SPM COMPANDING LAW PROVISIONING.*

73.2 Description

This feature allows an OC3-SPM p-side companding to be a provisionable option to either Mu-law or A-law, instead of the current architecture which always assumes that the p-side companding to be Mu-Law. This feature also provides for a provisionable Bit Inversion Option to either EBI or ABI, instead of basing it from the OFCENG parameter TYPE_OF_NETWORK

SPM p-side voice companding and bit inversion option is controlled by datafill. This datafill is done in table MNNODE, and is downloaded to the SPM through DDM framework. The c-side companding law will remain unchanged and will be determined from TYPE_OF_NETWORK parameter.

This feature supports OC3-SPM of the DMSCP class. No other variants of SPMs are currently supported.

The p-side companding law and bit inversion option introduced in table MNNODE will have default values such that the current system behavior can be maintained. The default values are determined as follows -

- Over an upgrade from a load without this feature, the default values for p-side companding in table MNNODE will be determined by type of DMSCP SPM (OC3 or STM). The default value of companding for OC3-SPM will be Mu-Law and for STM-SPM it will be A-law in this case.
- For a new SPM that is to be added, if it is desired that the SPM maintain the current system configuration, the field in MNNODE must contain '**$**'. If the craftsperson enters the companding law and bit inversion option in table MNNODE, it is assumed that the set defines the required configuration.. Also in addition, while the craftsperson datafills MNCKTPAK, a warning message will be displayed if the p-side companding in MNNODE is different from current system behavior for that RM type, and if this is not desired, p-side companding in table MNNODE has to be changed before proceeding. If the craftsperson wishes to continue it is assumed that this is desired, and if the craftsperson does not wish to continue, tuple addition in table MNCKTPAK is aborted and p-side companding must be changed by craftsperson in table MNNODE before proceeding.

For examples refer to “Supplementary Information” in the Configuration section of this feature.

Changes to Companding Law and Bit inversion Option in MNNODE are allowed only on an OOS SPM that is in MANB or OFFL state. This is to allow the transfer to data to the local through bulk DDM download.

73.3 Hardware Requirements or Dependencies

None.

73.4 Software Requirements or Dependencies

None.

73.5 Limitations and restrictions

- If TYPE_OF_NETWORK is changed over a restart, the companding law and bit inversion option present in MNNODE must be verified if they are in desired configuration. The craftsperson has to manually change the companding and Bit Inversion values of the SPM nodes if necessary. There will be no report or warning to indicate this.
- This feature allows SPM_OC3 to have all possible combinations of Companding Law and Bit-Inversion options. In table MNNODE, default value of COMPOPT ($) is suggested unless a specific combination of Companding Law and Bit-Inversion values are required. This feature is mainly targeted at CDMA network with SBS connected to SPM-OC3.
- To ensure good voice quality of the call, all components in the voice path of the call should have compatible Companding Law and/or Bit-Inversion values. Voice quality may be seriously affected if the Companding Law and/or Bit-Inversion values are not compatible.
- Forcustomer using SBS, the desired and supported configurations are:
  - **Default:** OC3-SPM: $ SBS: mu_law (it is equivalent to OC3-SPM: A_law+EBI: a_law for International type_of_network; and equivalent to OC3-SPM: Mu_law+ABI, SBS: mu_law for NA type_of_network)
  - OC3-SPM: A_law + ABI, SBS: a_law

73.6 Interactions

None.

73.7 Applicable customer facing sections

Fault Management

Logs _N/A__

Alarms	_N/A__
Configuration	
Data Schema	__X___
User Interface	_N/A__
Element Management	_N/A__
Security	_N/A__
Service Order	_N/A__
Office Parameters	_N/A__
Accounting (includes AMA billing)	_N/A__
Performance (includes operational measurements)	_N/A__

73.8 Glossary

SPM	Spectrum Peripheral Module
DMSCP	Digital Multiplex Switch Call Processor
RTS	Return To Service
MNNODE	Managed Network NODE
MNCKTPAK	Managed Network Circuit Pack
NA	North American
INTL	International
DDM	Data Distribution Manager
BSY	Busy
PRSM	Post Release Software Management
IOAU	Input / output Audit

73.9 Recommended Reading/References

a. SPM Settable Companding - Software FRS Version 2.0

74: Functional Description (FN): A00006001

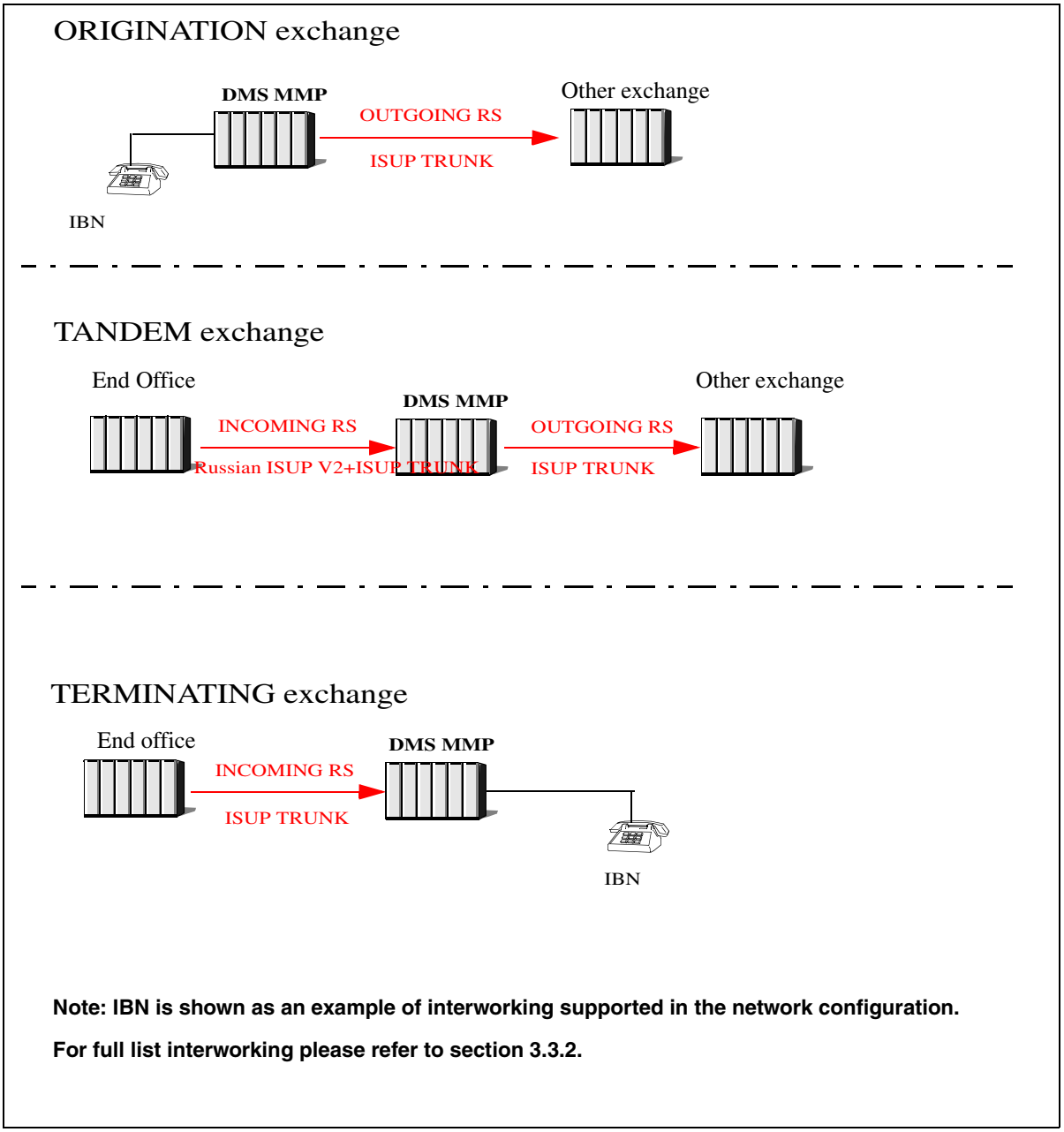
74.1 Feature name

AT.A00006001 - RUSSIAN ISUP AND TONES FOR INTERNATIONAL SPM

74.2 Overview

Figure 1 below shows the basic network configuration for Russian ISUP V2+ on DMS-MMP.

Figure 1 Russian ISUP V2+ Network Configuration



Note: IBN is shown as an example of interworking supported in the network configuration.

For full list interworking please refer to section 3.3.2.

This activity will mainly concentrate on what needs to be done to support Russian Isup V2+ on SPMs along with the interworking with other supported lines and trunks. After studying the different activities (as listed below) done to support Russian ISUP V2+ on PDTCs with DMS-MMP switch the following functional areas are needed to support Russian ISUP V2+ on SPMs.

74.3 Description

This activity introduces functionality to enable the DMS MMP to support the Russian V2+ variant using the SPM STM-1 peripheral. Russian ISUP V2+ is a variant of the ETSI ISUP V2 protocol and is dependent on the ETSI ISUP implementation within the SPM. The ETSI ISUP V1 and V2 protocol is provided in the SPM by activity A59012154: ETSI ISUP V1/V2 Base support for STM-1 access on the DMS MMP, in the MMP13/SP13 release.

This activity addresses the ability to support basic calls:

i. Line(IBN)-Russian ISUP V2+n ISUP on DMS MMP originating exchange

ii. Russia ISUP-Russia ISUP on DMS MMP tandem exchange

iii. Russia ISUP-Line(IBN) on DMS MMP terminating exchange

Note: Listed above are the basic call scenarios. There are a set of interworking supported by this activity. For full details, please refer to section 3.3.2.

The functionality currently available on the DMS MMP for Russian ISUP V2+, provided by PDTCs remain unchanged by this activity. Unless explicitly stated, the SPM implementation is equivalent to that of the PDTC in the XPM implemented by the activities

- ACT.A00000937 - Russian ISUP V2+ - Phase.1.
- ACT.A00000945 - CIS Tones and Cadences
- ACT. A00000943 - CIS Subscriber Line Parameters
- ACT.A00002033 - Russian ISUP-IBN Line Interworking
- ACT.A00002034 - Russian ISUP-V5.2 Interworking
- ACT.A00001929 - Russian ISUP-ISDN Interworking
- ACT.A00001923 - CIS Subscriber Categories
- ACT.A00002100 - ISUP_R_2000 Operator Calls on Busy Subscribers(TBI)
- ACT.A00001921 - CIS Toll Call Ringing
- ACT.A00002172 - SOSM: PROVISIONING
- ACT.A00002173 - SOSM: X.25 MESSAGING & CONNECTION
- ACT.A00002178 - SOSM : CALLP & SERVICE INTERACTIONS
- ACT. A59033579 - Downloadable Tones for SPMs

Russian ISUP V2+, defined in Russian 2000 requirements document, is based on ETSI ISUP V2. ISUPR2000.AB01 version document in FMDOC will be the requirements used to develop this activity.

This activity on STM1 SPM implements the following Russian ISUP V2+ requirements on DMS MMP switches for call processing :

- Definition of Russian ISUP V2+
- Basic Russian ISUP V2+ call scenarios
- Basic Russian ISUP V2+ call termination
- Russian specific ISUP messages (CCL, RNG)
- Handling of ISUP messages (FAC, CRG)
- Modifications in mandatory and optional signalling parameters such as
    iv. Called Party Number - Nature of Address Ind.,
    v. Nature of Connection Ind.- Satellite Ind.,
    vi. Backward Call Ind. - Called Party's Category Ind. and
    vii. Backward Call Ind. - Echo Control Device Ind.
- Handling calling party categories (CPC) for Russian ISUP V2+
- Handling IDR/IRS-INR/INF messages
- Enhancement of ISUP timers: T5, T13, T15, T17, T19, T21, T23
- Support for trunk offering (TBI) procedures at tandem exchanges for backward compatibility.
- Russian Tones and Cadences support

A summary of the activities that are required in SPM STM1 are given in table below.

Table 1 Activities Requirement for A00006001

Activities	Title	SPM	Core	DT	PV
ACT.A00000937	Russia ISUP V2+ - Phase.1	**Y**	**Y**	**Y**	**Y**
ACT.A00000945	CIS Tones and Cadences	N	N	N	Y
ACT.A00000943	CIS Subscriber Line Parameters	N	N	N	Y
ACT.A00002033	Russian ISUP-IBN Line Interworking	N	N	N	Y
ACT.A00002034	Russian ISUP-V5.2 Interworking	N	N	N	Y
ACT.A00001929	Russian ISUP-ISDN Interworking	N	N	N	Y
ACT.A00001923	CIS Subscriber Categories	N	N	N	Y

Table 1 Activities Requirement for A00006001

Activities	Title	SPM	Core	DT	PV
ACT.A00000937	Russia ISUP V2+ - Phase.1	**Y**	**Y**	**Y**	**Y**
ACT.A00002100	ISUP_R_2000 Operator Calls on Busy Subscribers(TBI)	N	N	N	Y
ACT.A00001921	CIS Toll Call Ringing	N	N	N	Y
ACT.A00002172	SOSM: PROVISIONING	N	N	N	Y
ACT.A00002173	OSM: X.25 MESSAGING & CONNECTION	N	N	N	Y
ACT.A00002178	SOSM : CALLP & SERVICE INTERACTIONS	N	N	N	Y
ACT. A59033579	Downloadable Tones for SPMs	N	Y	Y	Y

Notes: SPM, Core: Yes/No implies that this activity does/does not have any core or Local SPM-STM1 changes to support the activities listed in the table.

Notes: DT, PV: Yes/No implies that this activity does/does not have testing efforts to support the activities listed in the table.

Notes: DT testing Y or N is determined based on the software chagnes required as part of this activity in Core or SPM. For eg., there are no core or local SPM changes required to support the activity A00002100. Hence there is no DT/IT required for this activity to test the feature A00002100 supported in MMP20 (iSN07).

74.3.1 New ISUP Variant

This activity defines a new ISUP V2 variant in SPM STM1. This variant is based on the architecture of ETSI ISUP V1 and ETSI SUP V2 on SPM-STM1.

74.3.2 Basic and Interworking Call Scenarios

This activity addresses the ability to support basic calls:

1. Line(IBN) - Russian ISUP - Line(IBN)
2. Line (IBN) - Russia ISUP - Russia ISUP - Line (IBN)

Other Interworking supported are:

3. V5.2-on GPP -> Russian ISUP V2-on SPM -> V5.2-on GPP
4. ISDN BRI Line -> Russian ISUP V2-on SPM -> ISDN BRI Line
5. Line -> ETSI PRI -> Russian ISUP V2-on SPM -> ETSI PRI on SPM -> Line
6. Operator calls on Busy subscriber (Toll Break In)

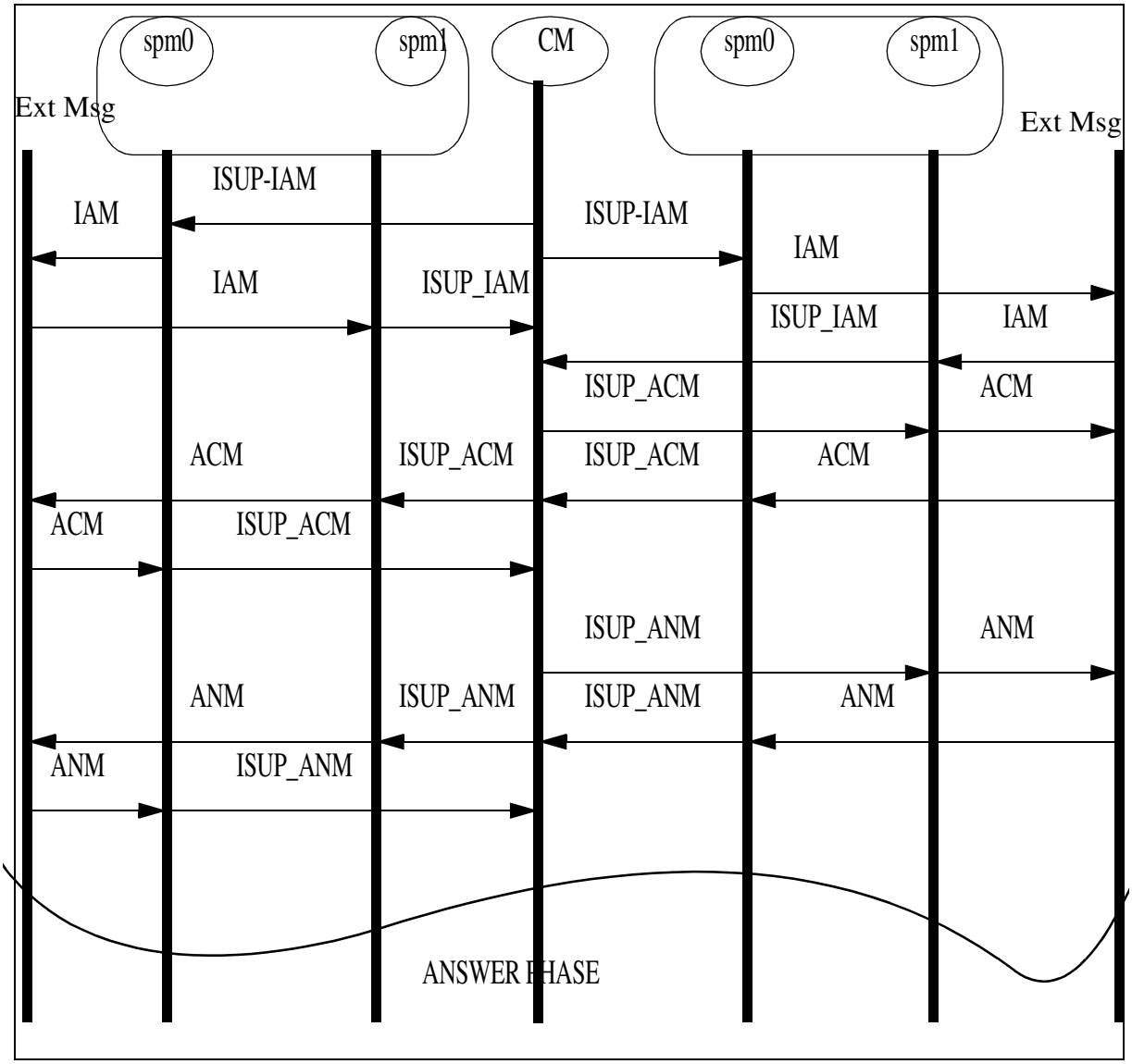
Russian ISUP variants will be configured on SPM STM1(orginal actid - A00000937). This interworking will be developed and design tested to support on SPM-STM1.

Note: **There are two activities identified as part of TBI service. The first original activity is A00000937. This will be supported in SPM-STM1 with necessary software changes. The second activity is A00002100. There were no software changes required in PDTC to support A00002100 activity (ISUP_R_2000 Operators calls on Busy Subscribers). Hence this SPM activity (A00006001) will not introduce any software changes to support too. Therefore A00006001 will not perform any DT/IT testing for A00002100.**

74.3.3 Basic Call

A basic call flow diagram with the ISUP messages on the set-up phase of the call for the scenario (Line -> Russian ISUP V2+ -> Line) is shown in Figure 2, "Basic Call Scenario : Message flow Diagram".

Figure 2 Basic Call Scenario : Message flow Diagram



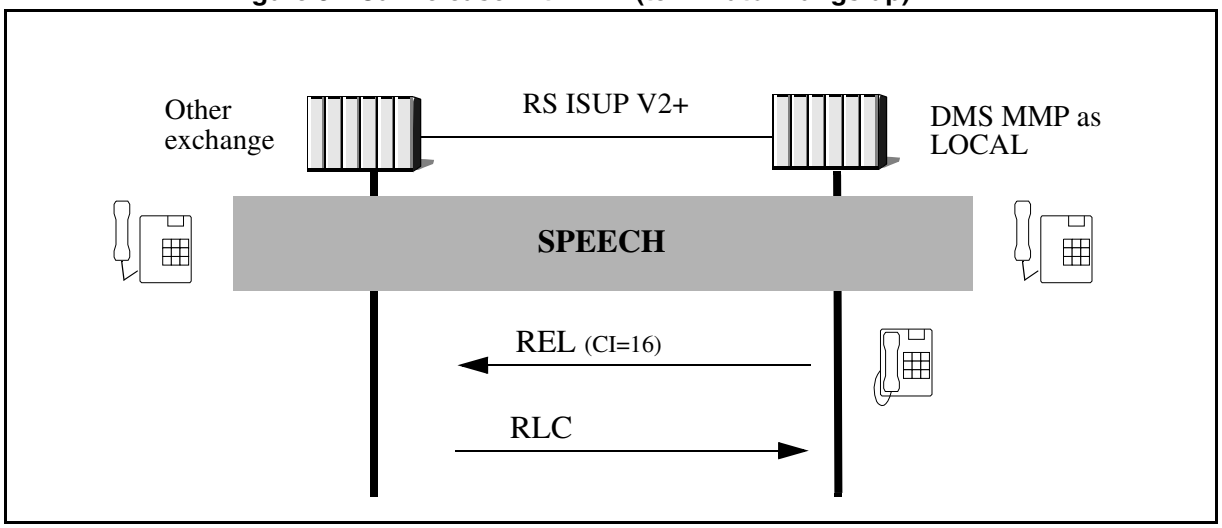
74.3.3.1 Call Termination

When called subscriber on-hooks, REL message will be sent instead of SUS message as required by interworking specifications. Additionally, re-answer is not supported in Russia network, thus, when network initiated SUS message is received over Russia ISUP V2+ trunks at an originating exchange, DMS MMP will release the call immediately with REL (CI=16).

User initiated SUS messages will be ignored by both originating and terminating exchanges, but they will be transmitted at tandem.

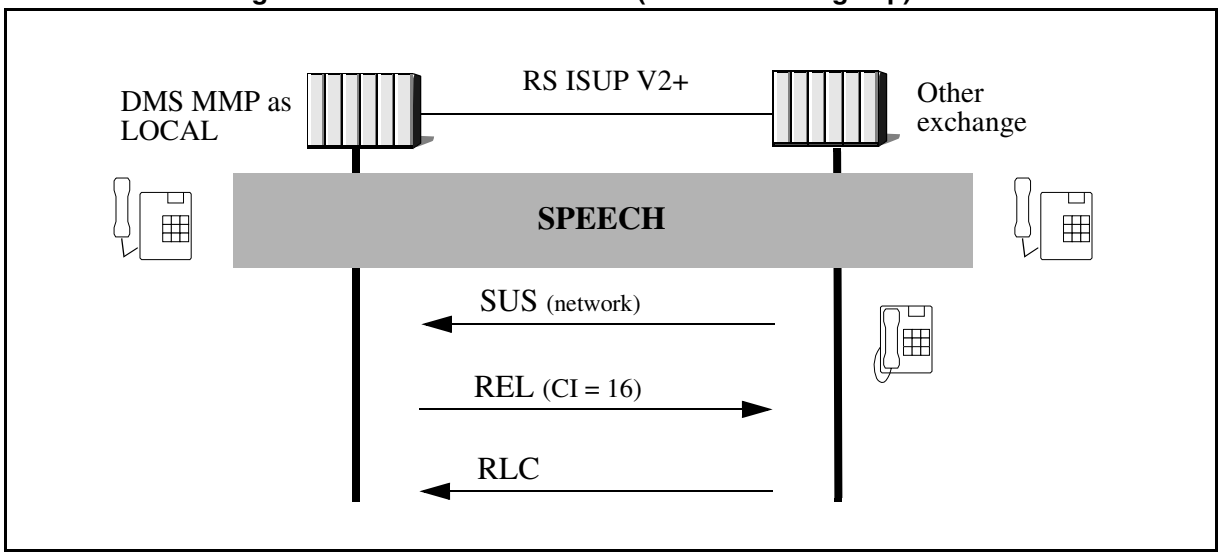
When a called subscriber on-hooks, REL message is sent instead of SUS message as required by interworking specifications. Please refer to Figure 3.

Figure 3 Call release with REL (terminator hangs up)



If network initiated SUS message is received at an originating DMS MMP exchange, REL with "Normal Call Clearing" cause is sent back (instead of starting T6 timer), as given in Figure 4, since Russia ISUP V2+ trunks does not support re-answer in automatic calls.

Figure 4 Call release with SUS (terminator hangs up)



Additionally, T6 timer is not started at DMS MMP tandem exchanges when network initiated SUS message is received.

Originating and terminating DMS MMP exchanges ignore user initiated SUS messages received over Russia ISUP V2+ trunks instead of starting T2 timer.

When REL message is received over Russia ISUP V2+ trunks at terminating DMS MMP exchange, a datafillable treatment can be applied to the terminating subscriber. This functionality can be achieved by datafilling Y for the office parameter FLEXIBLE_FAIL_CAUSE_TO_TRMT_MAP in table OFCENG.

The disconnect treatment, which will be applied to the terminating agent, should be datafilled in table FAILMSG where FLEXIBLE_FAIL_CAUSE_TO_TRMT_MAP is datafilled as "Y". Example datafill of FAILMSG table (for CI=16 (normal call clearing) - Russia ISUP V2+ to line interworking) is given in Figure 5.

Figure 5 Example FAILMSG datafill

```
INPUTMSG MAPTO LOG RESULT
------------------------------------------------------------
Q767 NORMCLR OTHERWISE N TREAT RODR
```

If FLEXIBLE_FAIL_CAUSE_TO_TRMT_MAP parameter in table OFCENG is datafilled as N, DMS MMP applies disconnect timeout treatment (DISC), by default, to the terminating subscriber for all release causes.

Upon reception of REL message over the incoming Russia ISUP V2+ trunk, DMS MMP applies the specified treatment (DISC or datafilled treatment) to the terminating subscriber after a certain time interval. This time interval can be determined by datafilling the office parameter FLEXIBLE_DISCONNECT_TIMER in table OFCENG. The duration of the interval (in seconds) is 2,5 times the parameter value. FLEXIBLE_DISCONNECT_TIMER should be datafilled as "0", if it is required to apply disconnect treatment immediately after REL message is received.

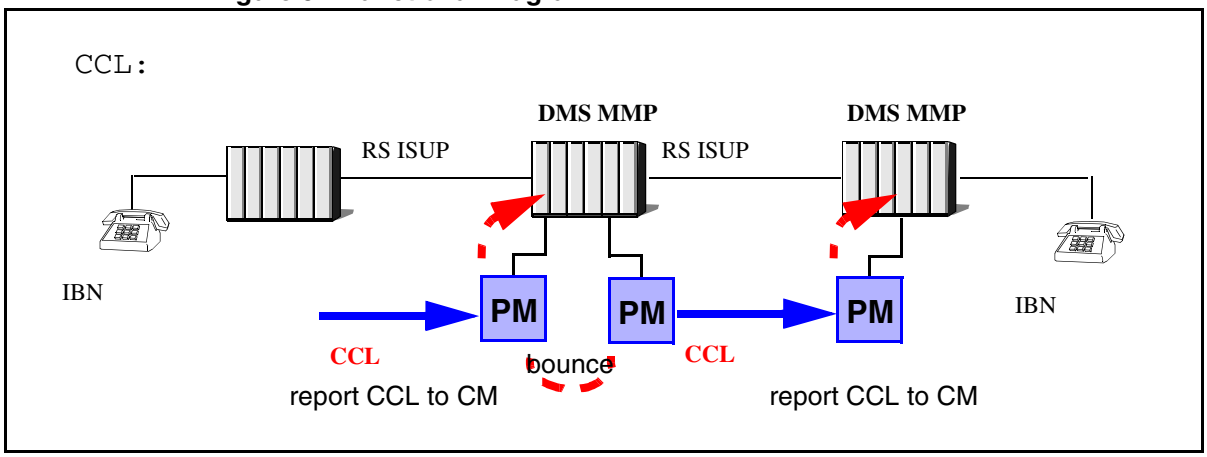
74.3.4 New Russia Specific ISUP Messages on SPM STM1

As part of this activity there are two new message types supported in SPM which are required by Russia specifications: CCL and RNG.

Other required messages are all existing ISUP messages, and are supported by DMS MMP and SPM-STM1. The list of required messages and parameters for Russia ISUP V2+ is available in ISUPR2000 in FMDOC library.

74.3.4.1 Calling Line Clear (CCL)

Figure 6 Functional Diagram



In this activity, following items will be implemented for CCL message:

- Definition of the CCL message.
- Formatting of the CCL message.
- Handling CCL message in SPM (Originating, Tandem and Terminating exchanges)

Note: CCL requirement for this activity is based on ISUPR2000.AB01

74.3.4.1.1 Definition of CCL Message

Calling line clear message (CCL) is a forward message sent instead of RELease signal in malicious call hold (MCH). It is used to provide 'called control disconnection type'. Hold indicator is not supported by the Russia ISUP V2+, instead CCL message is used.

Figure 7 The CCL message template

*NEW	MESSAGE TYPE	1111 1100

Mandatory fixed parameter

74.3.4.1.2 DMS MMP as Originating Exchange

Generation:

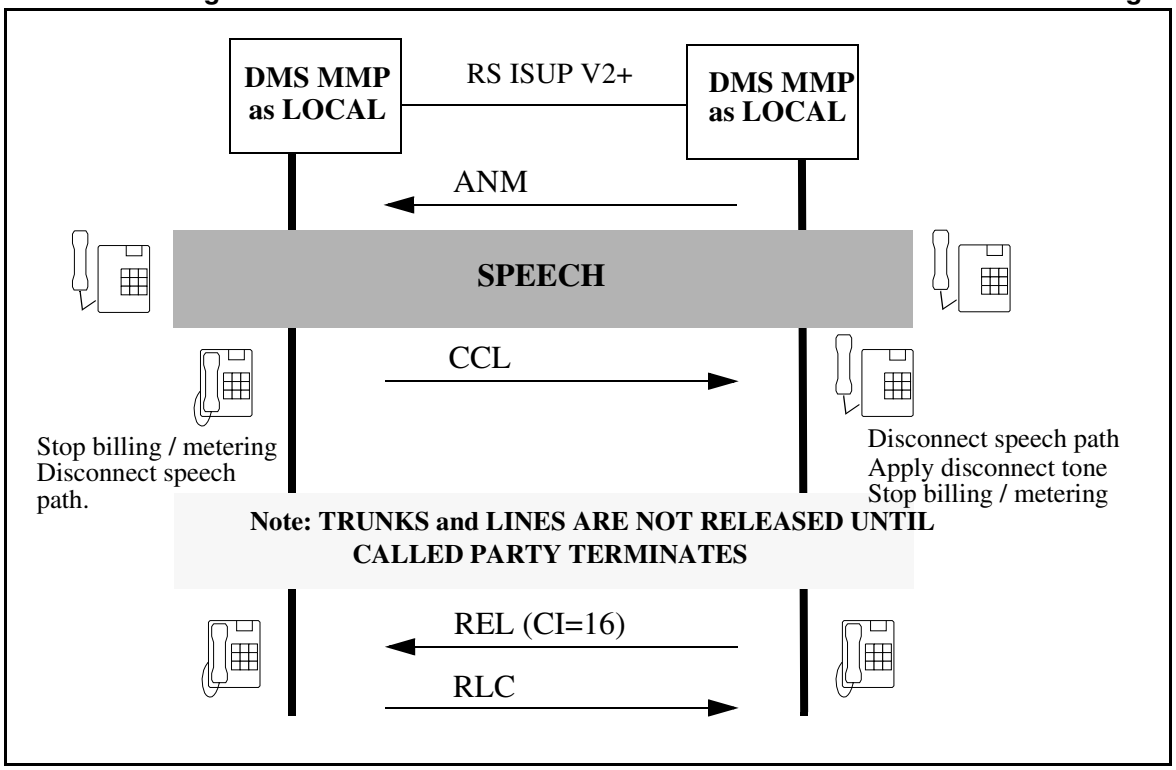
Upon calling subscriber's on-hook during a conversation, DMS MMP sends CCL message **if CALLCTRL option is datafilled within corresponding tuples of translation tables (XXHEAD / XXCODE) with CALLED value**. Otherwise REL is sent. **In called controlled calls,**

billing and metering of the call stops when originator terminates the call.

There are 4 possible scenarios for the originating DMS-MMP Generation:

Scenario 1: CCL Generation at Originating Exchange
Call releases with CCL at Originating DMS MMP Exchange upon calling subscriber's on-hook. Refer to Figure 8. If not datafilled with CALLCTRL option, REL will be sent. This will be a normal Call release scenario.

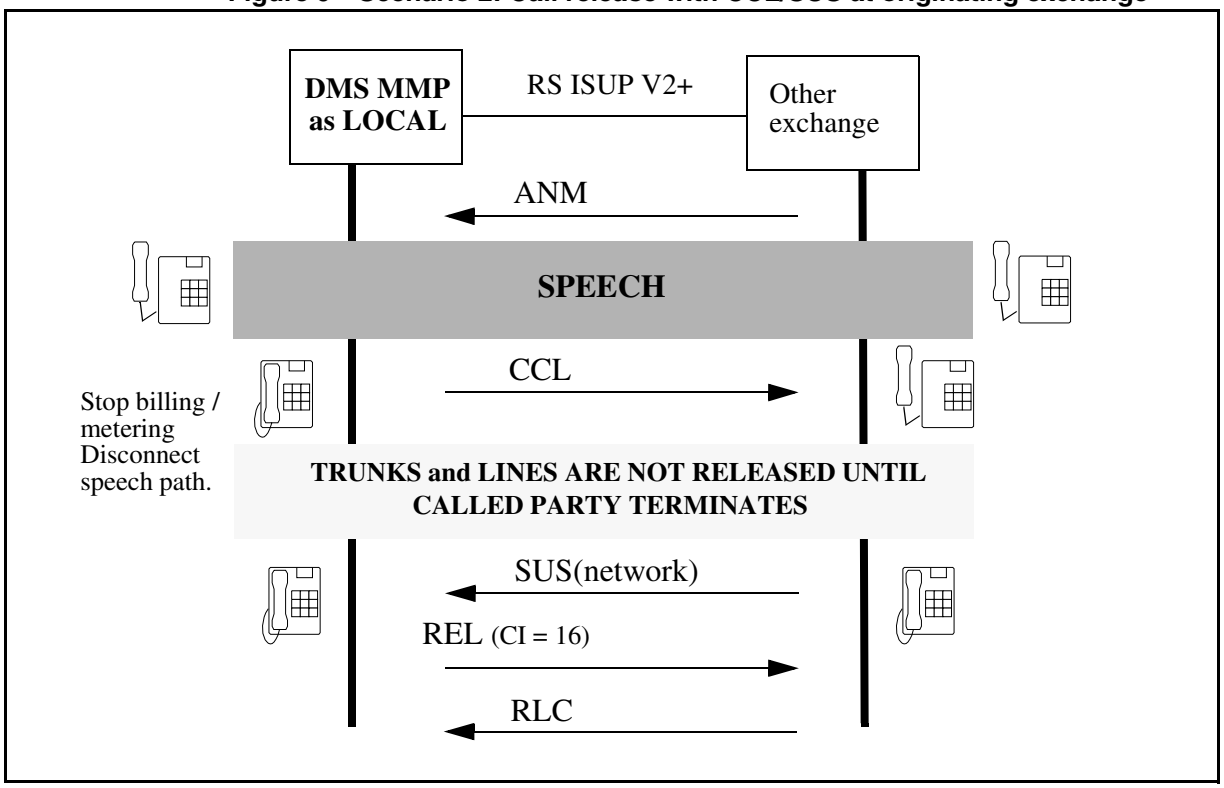
Figure 8 Scenario 1: Call release with CCL/REL at ORIG and TERM exchanges



Scenario 2: CCL Generation at Originating Exchange, Other Exchange Sending SUS

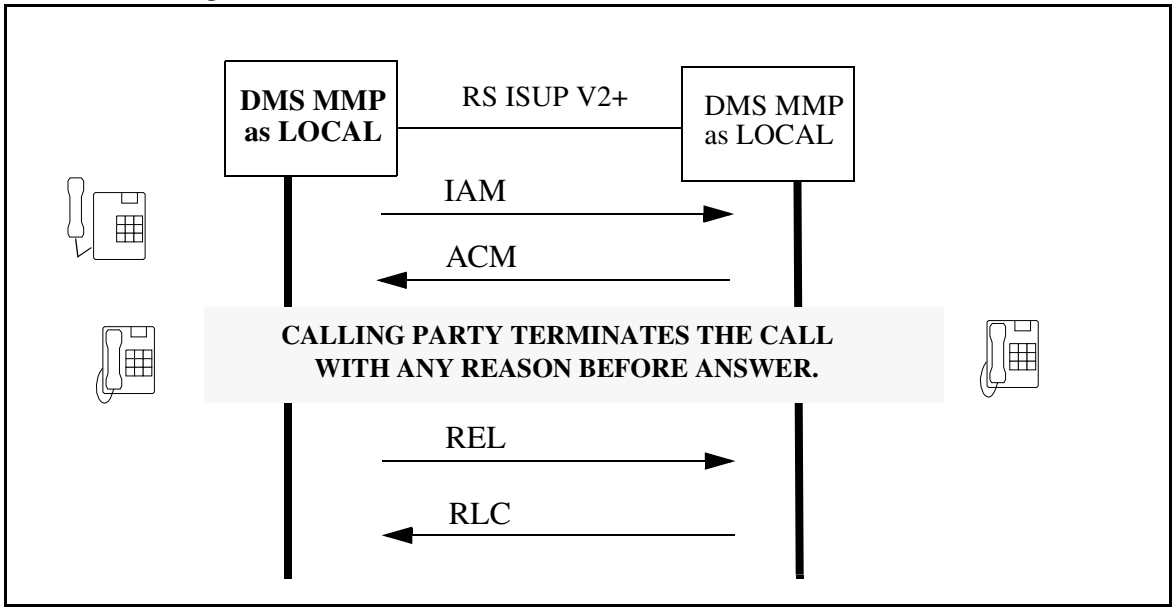
Call release with generating CCL and receiving SUS at Originating DMS-MMP exchange.

Figure 9 Scenario 2: Call release with CCL/SUS at originating exchange



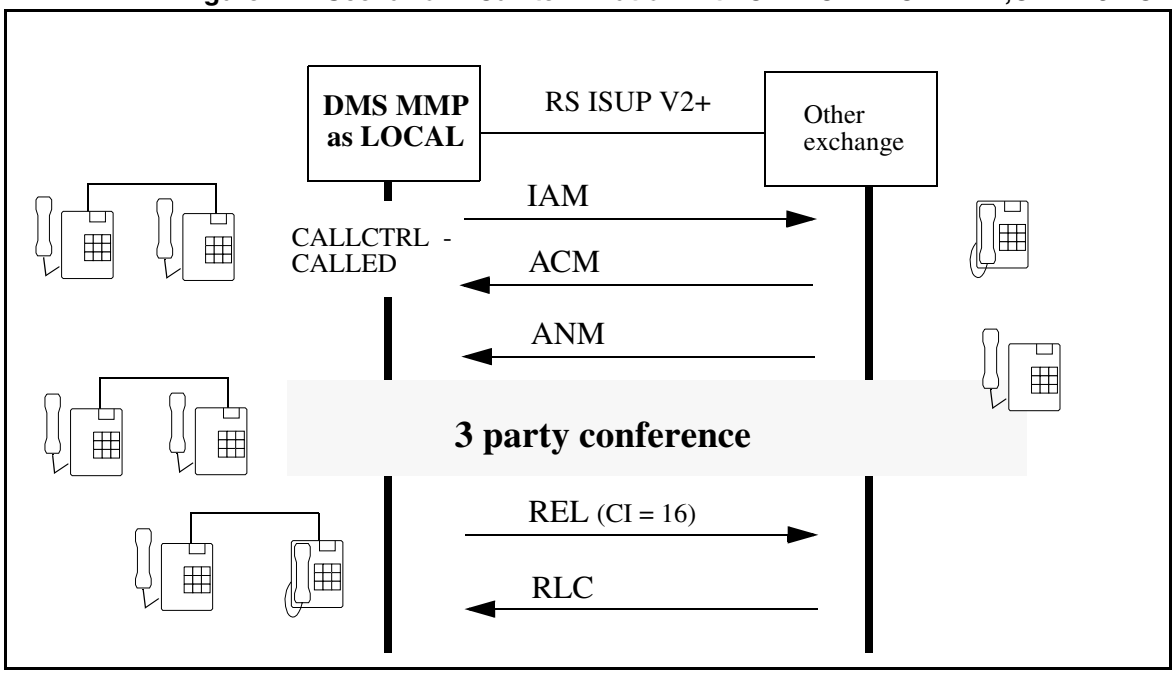
Scenario 3 : Call release with REL from Originating DMS MMP Exchange

Figure 10 Scenario 3:Call release with REL.



Scenario 4: Call termination on Originating DMS MMP Exchange with CALLCTRL-CALLED and CEPT-I3WC.

Figure 11 Scenario 4: Call termination with CALLCTRL-CALLED,CEPT-I3WC

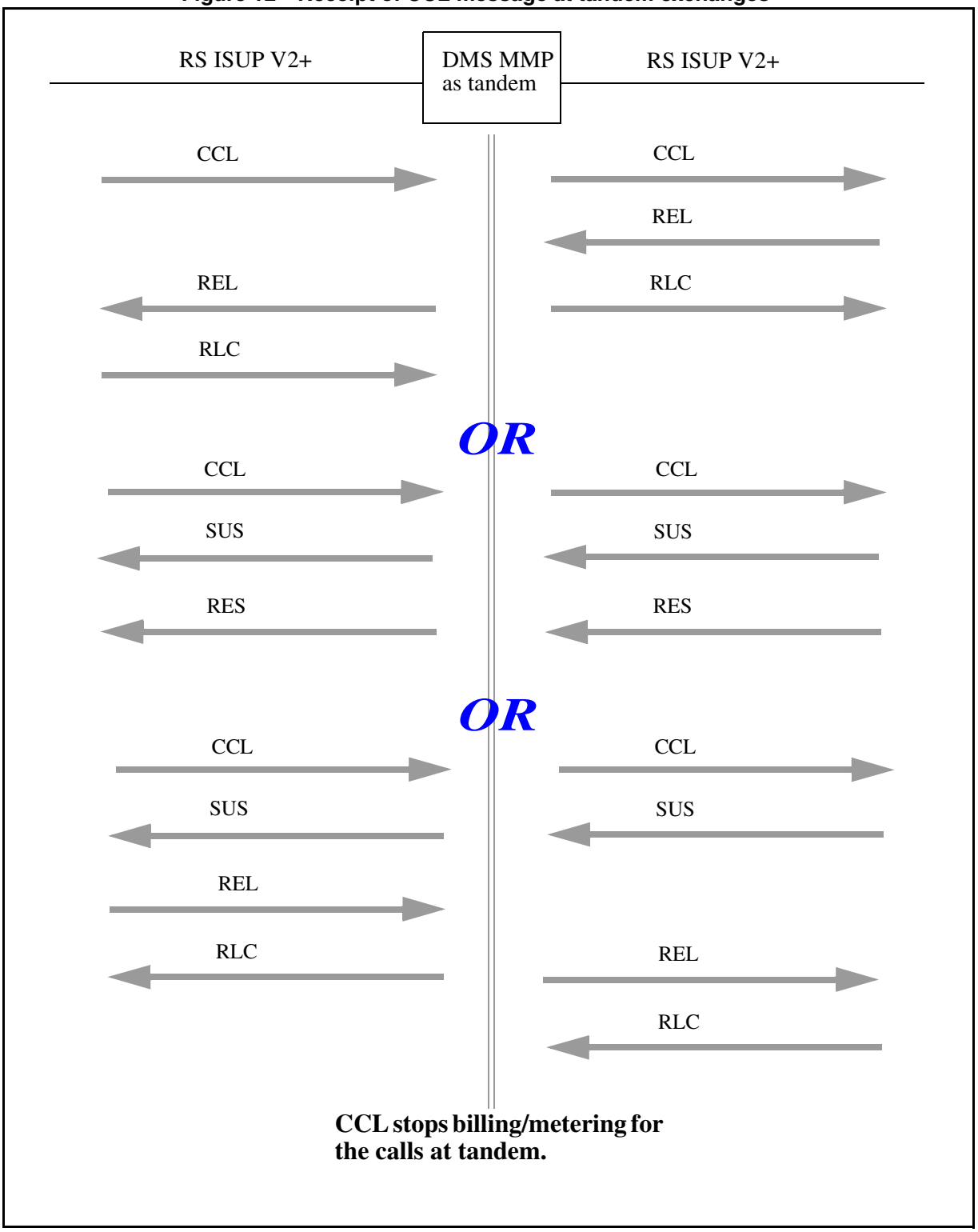


74.3.4.1.3 DMS MMP as a Tandem Exchange

DMS MMP transmits CCL message without changing any of its parameters. **CCL message stops billing and metering of the call at tandem exchanges.** There are 3 possible scenarios on a tandem exchange. These 3 scenarios will be supported on DMS-MMP with SPM-STM1 peripheral. (Figure 12)

SUS and RES messages, which are received at tandem after CCL, are transmitted without modification.

Figure 12 Receipt of CCL message at tandem exchanges



74.3.4.1.4 Reception

DMS MMP stops billing/metering, disconnects speech path, and applies reorder (RODR) treatment to the terminating IBN agent, after CCL message is received, as given in Figure 13. Clearing the call depends on the called subscriber's action after receiving CCL message.

With the use of CCL message, this activity supports called party control functionality, as given in Russia requirements, **only for IBN** subscribers which are routed to Russia ISUP V2+ trunks. **Called party control is not supported for line-to-line calls, and other Russia ISUP V2+ interworkings.**

CCL message, and called party control applies only in basic calls. Calls subject to called-party control shall have the following call transfer related services denied:

— Call Hold

— Call Transfer

— Call Waiting

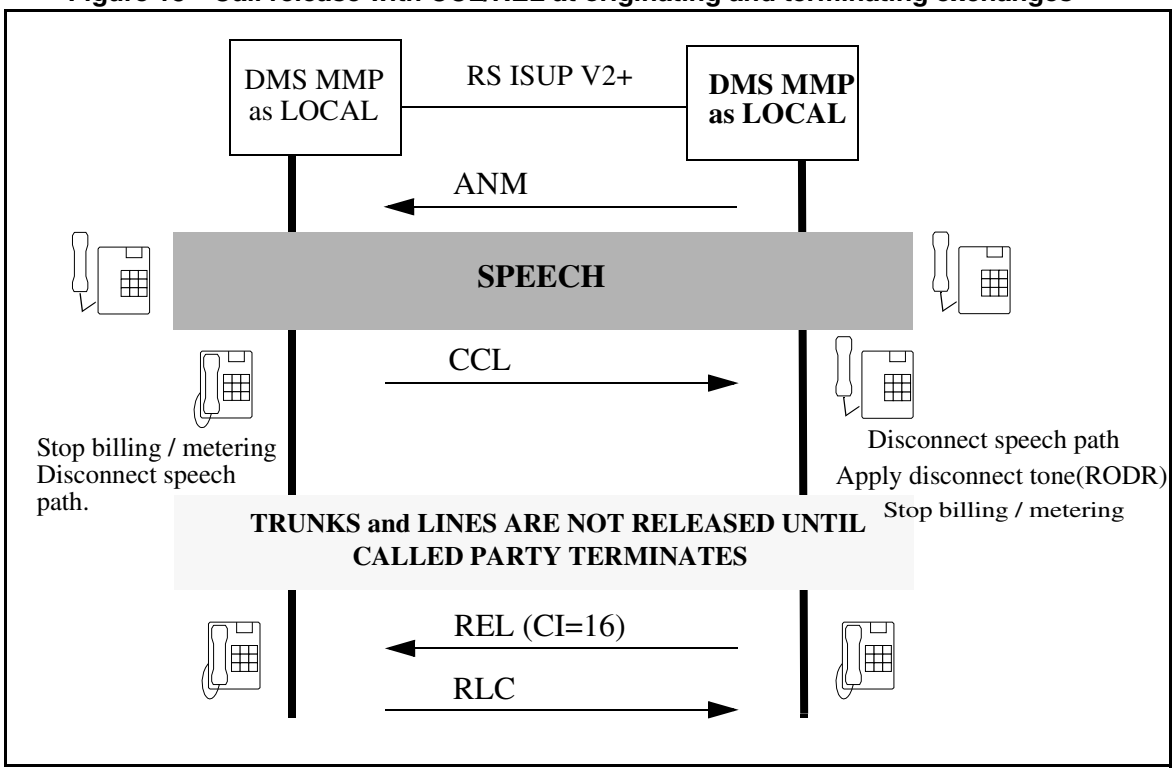
— 3-Way Calling

— 6-Way Calling

Originating subscribers are not allowed to FLASH within called party controlled calls, after the call is answered.

Additionally, called-party control is not supported within multi party calls. In multi party calls, where CALLCTRL-CALLED translation option is introduced after the first call is established, the call transfer related feature shall override called party control as given in Figure 13.

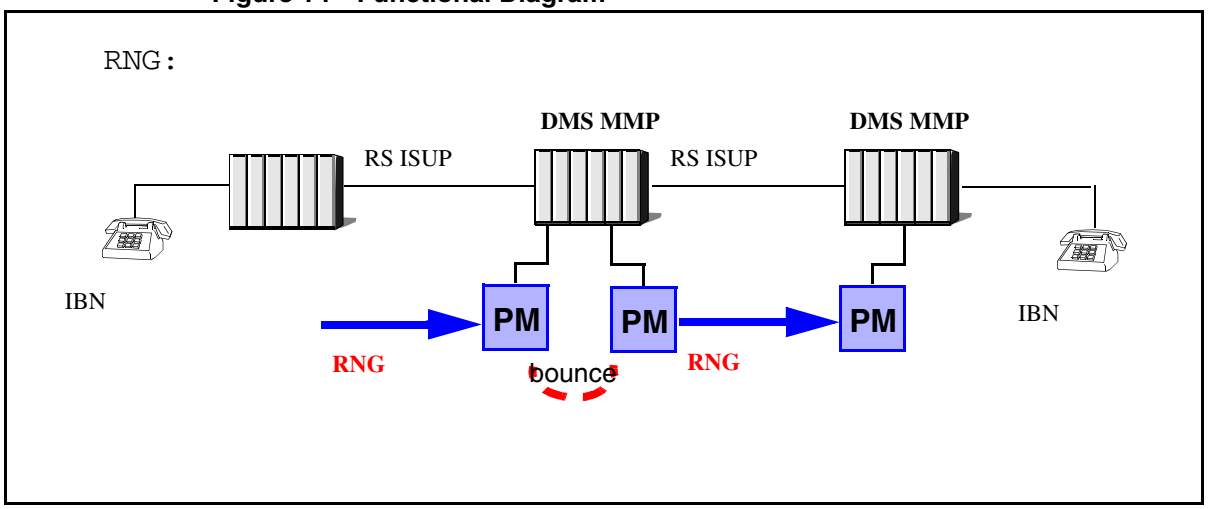
Figure 13 Call release with CCL/REL at originating and terminating exchanges



The scenarios, where called subscribers - of called-party controlled calls - involve in complex calls (I3WC, I6WC, ICT, CFX ...etc), are not supported by this feature.

74.3.4.2 Ring (RNG) Message

Figure 14 Functional Diagram



In this activity, following items will be implemented for RNG message on SPM:

- Definition of the RNG message.
- Formatting of the RNG message.
- Handling RNG message in SPM (Originating, Tandem and Terminating exchanges)

  Note: RNG is used for Backward Compatibility.

74.3.4.2.1 Definition of RNG Message

Ring message (RNG) is a forward signal sent from an operator-connected exchange towards the line-connected exchange.

Figure 15 RNG Message Template.

*NEW	MESSAGE TYPE	1111 1111
*	POINTER TO START OF OPTIONAL PART	0000 0000

Mandatory fixed parameter

- *Generation:*

  In Russia network, RNG message is generated only during a semi automatic call in case of operator's re-ring. Since DMS MMP does not support operator positions, this message will not be generated.

- *Tandem:*

  DMS MMP forwards RNG message without changing any of its parameters.

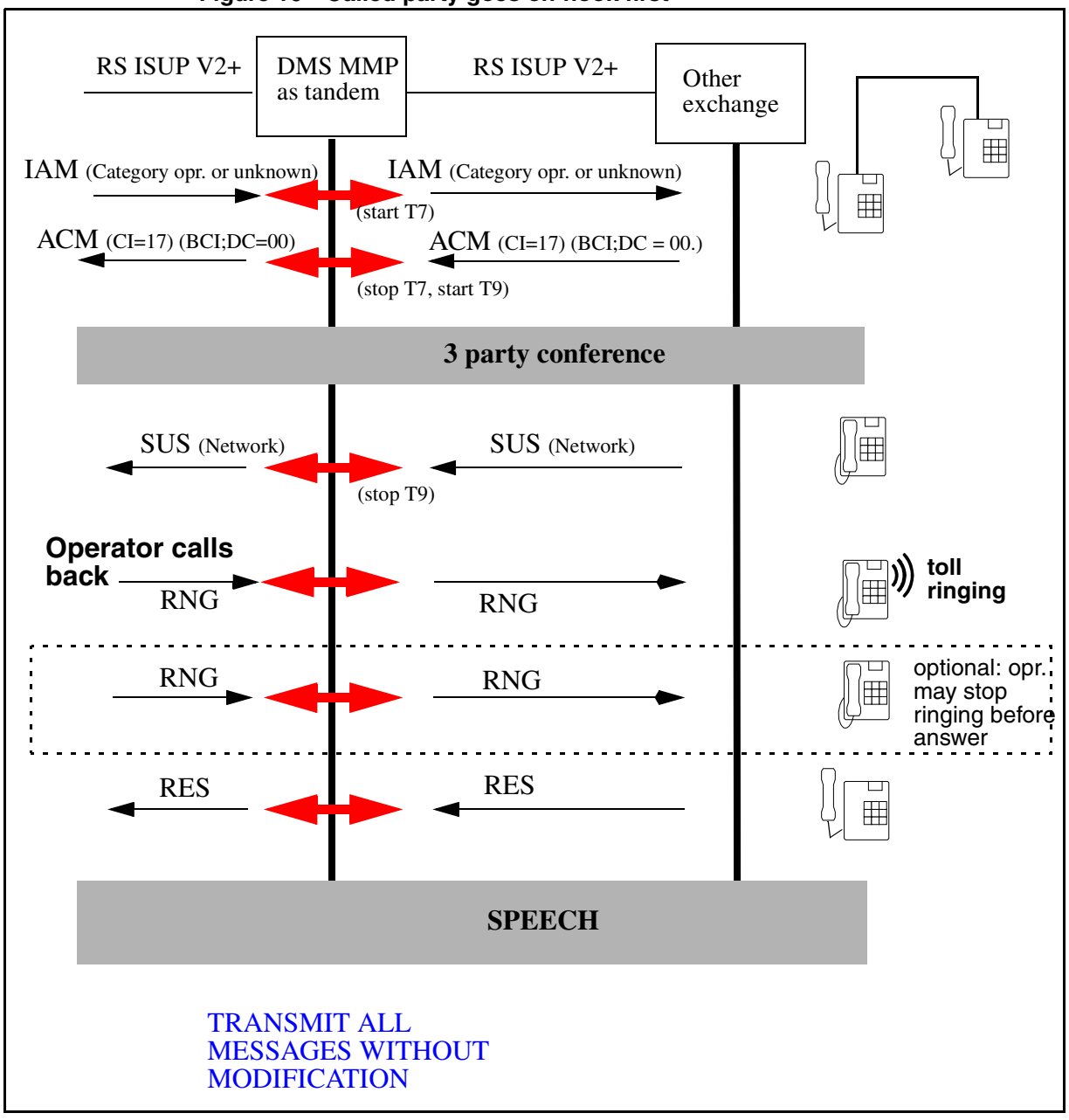
- *Reception:*

  This message was previously being used in Russia network for TBI service (Old TBI). However, within ISUPR2000.AB01 specifications, it is indicated that CWT will be used instead of TBI, thus it is not required to process RNG message. DMS MMP ignores RNG message when it is received at terminating exchange.

  Note: Please note, Old TBI refers to Backward Compatibility for TBI service. Wherever necessary the document will refer the Backward compatibility TBI service to Old TBI

As indicated above, DMS MMP can only receive RNG message within TBI scenarios. TBI scenario at tandem -where RNG message is received- is given in Figure 16 below.

Figure 16 Called party goes on-hook first



RNG message is supported only for the scenarios similar to Figure 16, at tandem switches. If RNG message is received after ACM and ANM at an originating or terminating DMS MMP switch, it will be ignored.

If ISUP_RNG is received in forward direction in operator calls after ACM or ANM at tandem nodes, it will be transmitted unchanged, but it will not be processed. If RNG is received in a non-operator call after ACM or ANM, it will be ignored even at tandem.

In other scenarios (i.e. RNG received after IAM) DMS MMP behaves as described in Q764.2.9.5.1-”Handling of Unexpected Messages”.

For more details on the possible RNG messages on tandem, please refer to section 3.3.5 on Toll Break In (TBI).

74.3.5 Toll Break In (old TBI) Support in SPM STM1

In Russia network, toll operators can establish calls to busy subscribers using TBI feature with ISUP-R-1994 signalling.

DMS MMP does not support TBI feature as an originating or terminating exchange.

Operator calls are distinguished from other calls via CPC parameter in IAM. Possible CPC can be:

- Unknown (#00)
- National Operator (#09)
- Semiautomatic call, categoryI - OCCI (#F1)
- Semiautomatic call, categoryII - OCCII (#F3)
- Semiautomatic call, categoryIII- OCCIII (#F5)
- Semiautomatic call, categoryIV- OCCIV (#F7)

There are 4 possible scenarios in order to support TBI.

RNG message is supported only for the scenarios similar to Figure 17 at tandem switches. If RNG message is received after ACM and ANM at an originating or terminating DMS MMP switch, it will be ignored.

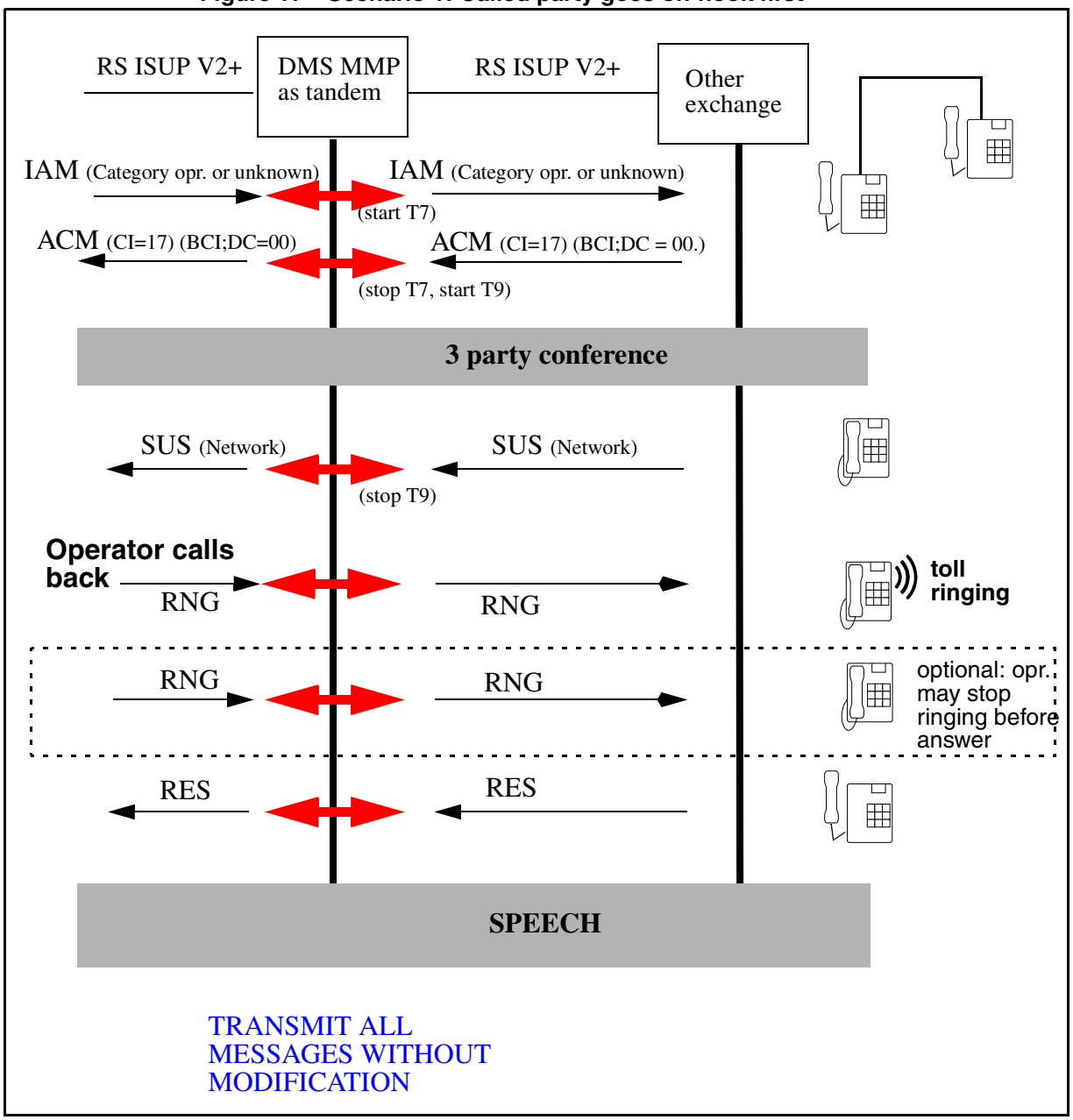
If ISUP_RNG is received in forward direction in operator calls after ACM or ANM at tandem nodes, it will be transmitted unchanged, but it will not be processed.

If RNG is received in a non-operator call after ACM or ANM, it will be ignored even at tandem.

In other scenarios (i.e. RNG received after IAM) DMS MMP behaves as described in Q764.2.9.5.1-”Handling of Unexpected Messages”.

Scenario 1: Line -> Russian ISUP V2+ -> Russian ISUP V2+ -> Line: Called Subscriber busy in TBI - called party goes on-hook (hangs up) first

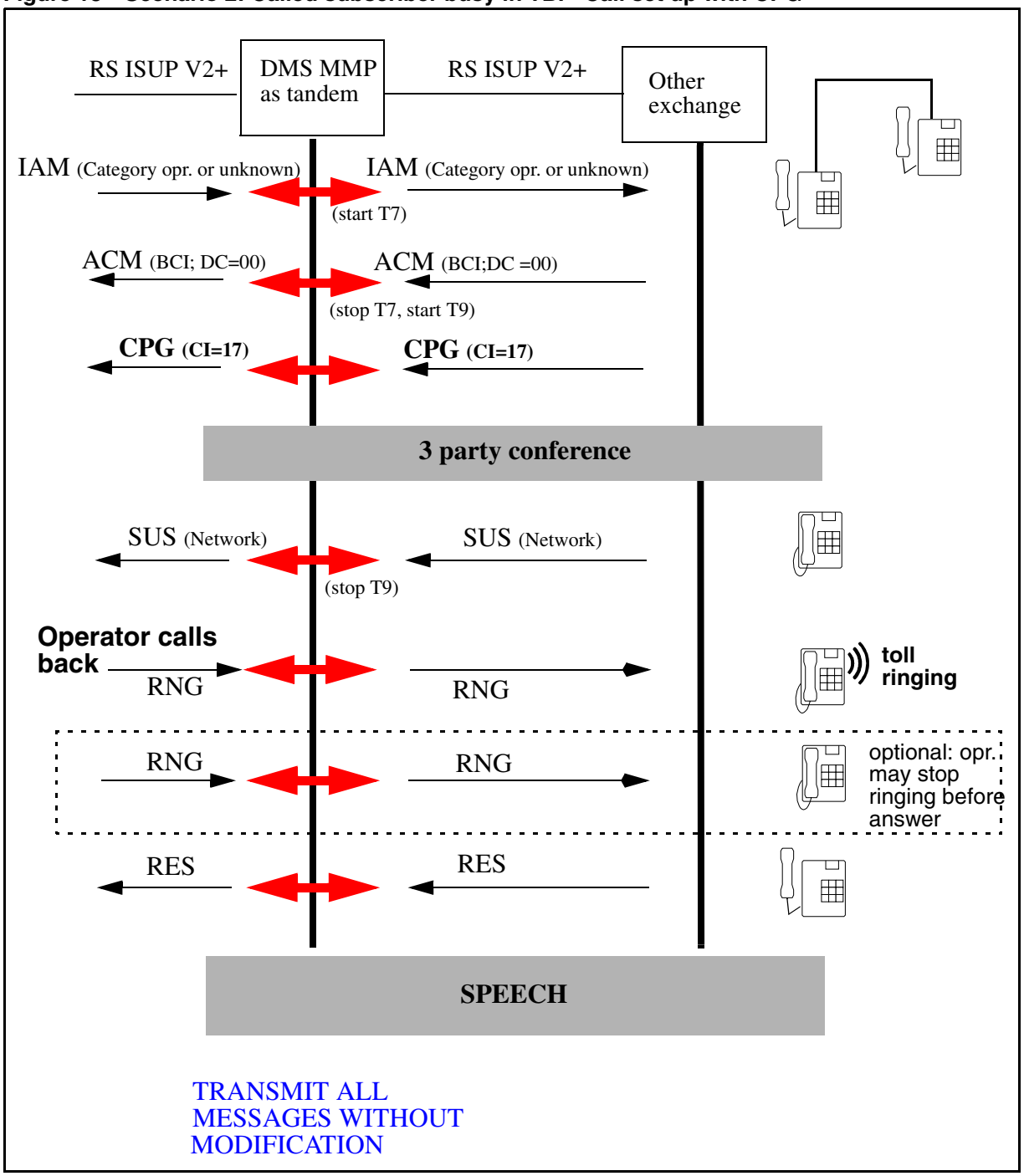
Figure 17 Scenario 1: Called party goes on-hook first



Scenario: 2 Line -> Russian ISUP V2+ -> Russian ISUP V2+ -> Line

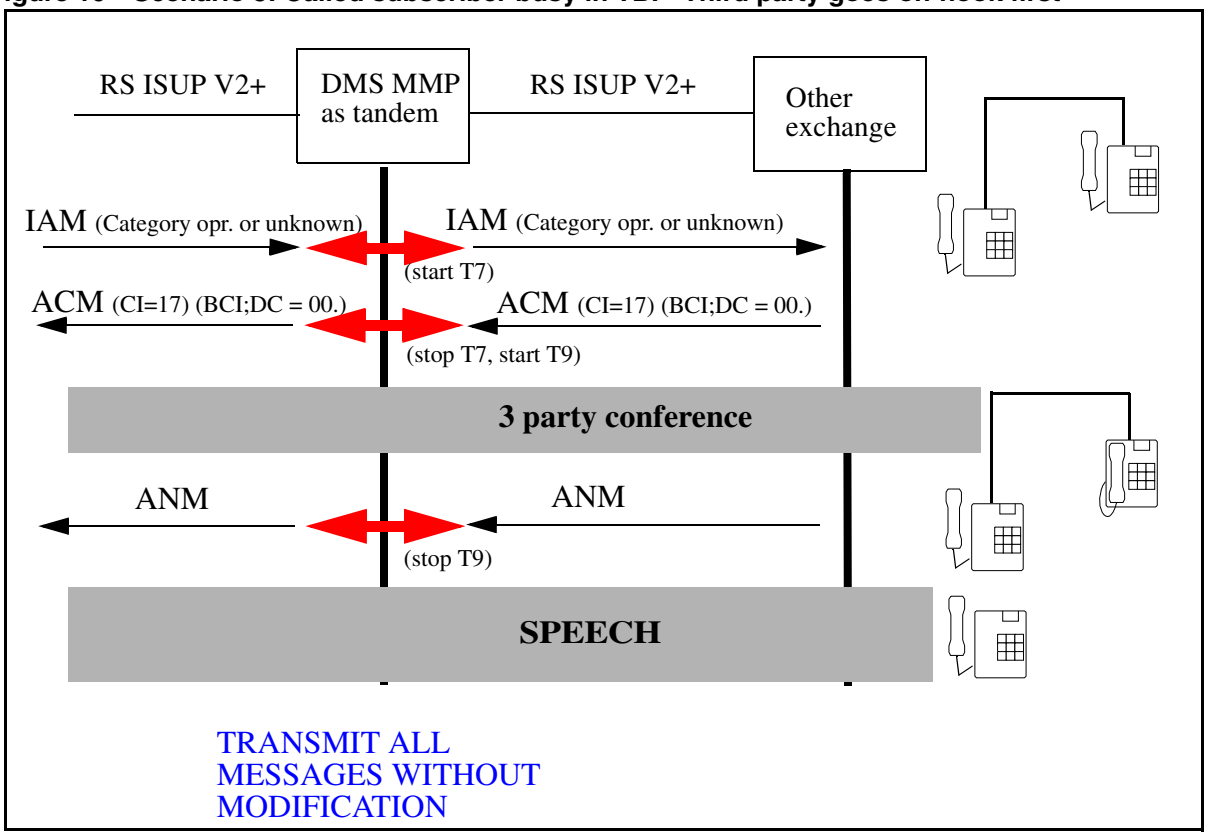
Called Subscriber busy in TBI - call setup with CPG (similar to 1 except the called party is busy)

Figure 18 Scenario 2: Called subscriber busy in TBI - Call set up with CPG



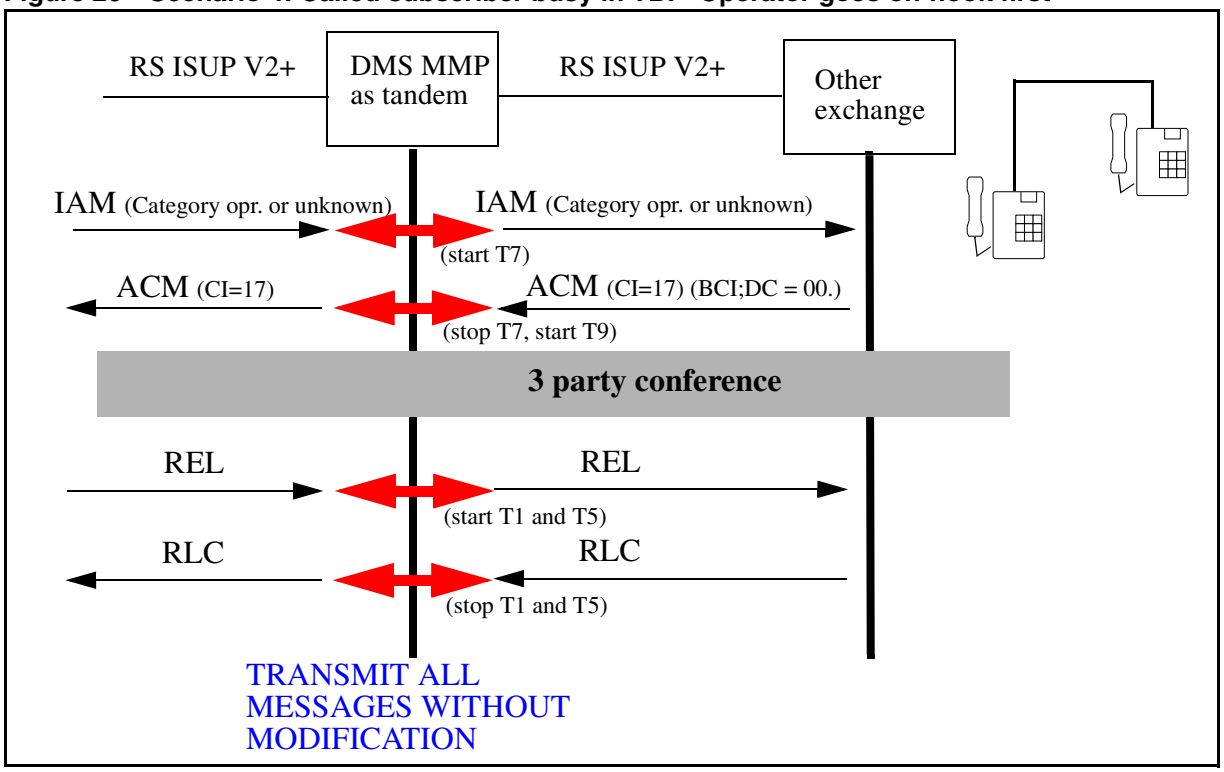
Scenario: 3 Line -> Russian ISUP V2+ -> Russian ISUP V2+ -> Line: Called subscriber busy in TBI - Third party goes on hook (hangs up) first

Figure 19 Scenario 3: Called subscriber busy in TBI - Third party goes on-hook first



Scenario: 4 Line -> Russian ISUP V2+ -> Russian ISUP V2+ -> Line
Up to this part, the scenarios in which the called party accepts the operator call are given. In some scenarios, operator gives up. DMS MMP is also capable of tandeming these scenarios. An example to these scenarios is given Figure 20 in . IAM with Category : Operator or unknown

Figure 20 Scenario 4: Called subscriber busy in TBI - Operator goes on-hook first



74.3.5.1 SWACT Interaction

If warm swact is applied to the peripherals which are connected to Russia ISUP V2+ trunks -involved in the scenarios in Figure 17 (scenario 1 in TBI) and Figure 18 (scenario 2 in TBI) - before ISUP_RES message is received, the call will be dropped.

Note: Operator goes on hook first based on the called party is busy

74.3.5.2 Restriction:

- DMS MMP does not support TBI feature as an originating or terminating exchange. Only on tandem exchanges
- Do not support the feature on warm swact for scenarios 1, 2. But supported on scenario 3.

74.3.6 ISUP Messages CRG and FAC

- CRG: Russia specifications require CRG message to be considered as correct, but ignored. Therefore, it will be recognized as a valid message (i.e. no CFN will be sent), but it will not be processed or originated.

- FAC: FAC message is used for ECT(Explicit Call Transfer) and REV (Reverse Charging) services. ECT is an optional service in Russia specifications and partly supported by DMS MMP.

  Note: This activity supports ISUPR2000.AB01 FAC requirement.

74.3.6.1 Originating Exchange Behavior:

1. CRG: Discards when received CRG at Originating MMP Exchange
2. FAC: No FAC on Originating MMP Exchange.

74.3.6.2 Tandem Exchange Behavior:

1. CRG: DMS MMP transmits CRG message if it is received at tandem exchange over Russia ISUP V2+ trunks.
2. FAC: DMS MMP transmits FAC messages -which are received at tandem node over Russia ISUP V2+ trunks- without changing any parameters, without processing this message, and without sending CFN.

74.3.6.3 Terminating Exchange Behavior:

1. If CRG is received at terminating exchange, message will be discarded without notification.
2. FAC message is not supported at terminating switches. CFN message will be sent if FAC is received from an Russia ISUP V2+ trunk at terminating exchange.

Figure 21 Functional diagram

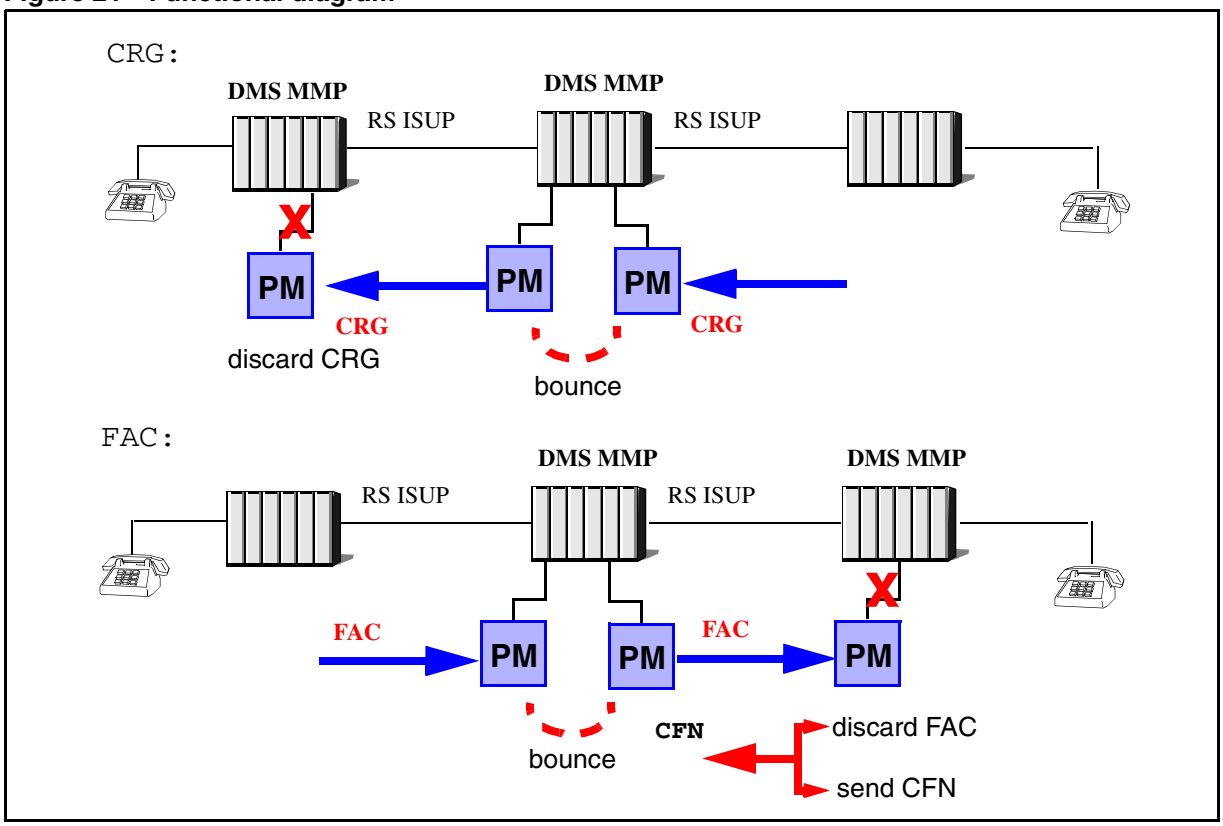
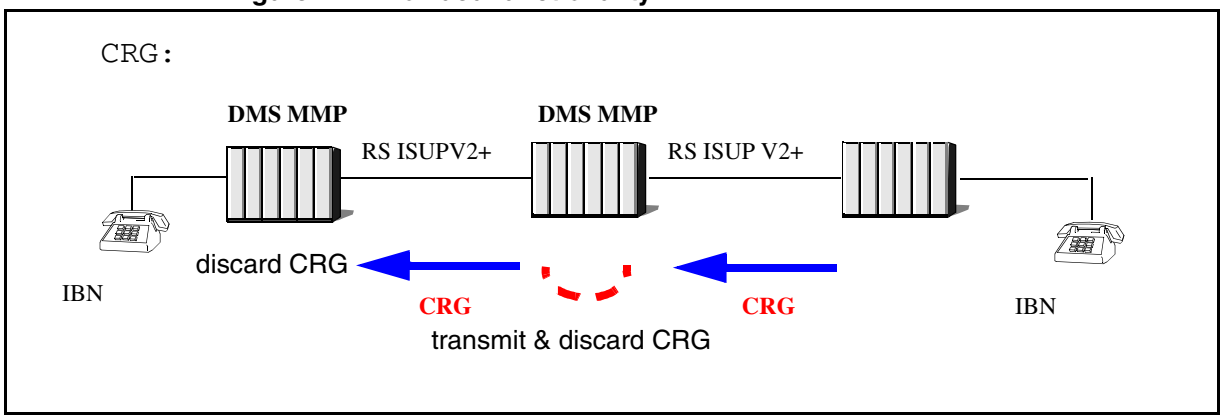


Figure 22 Provided functionality

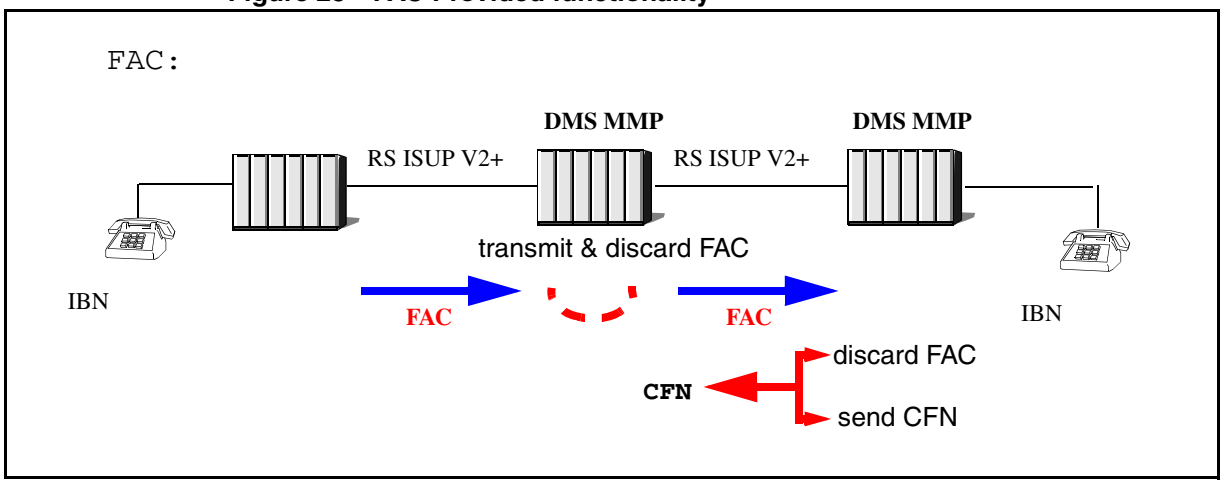


74.3.6.4 Processing CRG message

The behavior of the CRG message is as follows

- If the CRG is a CC message, we send the message to the facility
- If the CRG is a facility message at a tandem, we will bounce the message
- If the CRG is a facility message at an end-office, the message is discarded.

Figure 23 FAC Provided functionality



74.3.7 Russian ISUP Message Parameter Compatibility

Russia specification identify variances in the set of supported optional parameters for ISUP messages. The following table identifies the supported mandatory and optional parameters for each message in SPM STM1.

Table 2 Supported Russia ISUP Messages and Parameters

Mes sage	Mandatory Parms	Optional Parms	Currenly supported by ETSI V2?
ACM	Backward Call Indicator	Access Delivery Information Access Transport Application Transport Call Diversion Information End of Optional Parameters Generic Notification Optional Backward Call Indicators Parameter Compatibility Information Redirection Number Redirection Number Restriction User-To-User Indicators User-To-User information	ETSI V2 supports Cause Indicator and Service Activation Parms. **New formatter required.**
APM		Application transport End of Optional Parameters Message Compatibility Information Parameter Compatibility Information	Same supported set of parms as ETSI V2.

Table 2 Supported Russia ISUP Messages and Parameters

Mes sage	Mandatory Parms	Optional Parms	Currenly supported by ETSI V2?
ANM		Access delivery information Access transport Application transport Backward Call Indicator Call History Information Connect Number End of Optional Parameters Generic Notification Generic Number Optional Backward Call Indicators Parameter Compatibility Information Redirection Number Redirection Number Restriction User-To-User Indicators User-To-User information	ETSI V2 supports Service Activation Parm, but does not support Access transport, BCI, Connect Number or User-To-User information. **New formatter required.**
BLO			Same as ETSI V2
BLA			Same as ETSI V2
CCR			Same as ETSI V2
CCL			**New Message, formatter already being developed**
CFN	Cause Indicators	End of Optional Parms	Same as ETSI V2
CGB	Circuit Group Supervision Message Type Range And Status		Same as ETSI V2
CGBA	Circuit Group Supervision Message Type Range And Status		Same as ETSI V2
CGU	Circuit Group Supervision Message Type Range And Status		Same as ETSI V2
CGUA	Circuit Group Supervision Message Type Range And Status		Same as ETSI V2

Table 2 Supported Russia ISUP Messages and Parameters

Mes sage	Mandatory Parms	Optional Parms	Currenly supported by ETSI V2?
CON	Backward Call Indicator	Access delivery information Access transport Application transport Call History Information Connect Number End of Optional Parameters Generic Notification Generic Number Optional Backward Call Indicators Parameter Compatibility Information Redirection Number Redirection Number Restriction User-To-User Indicators User-To-User information	ETSI V2 supports Service Indicator parm. **New Formatter required.**
COT	Continuity Indicators		Same as ETSI V2
CPG	Event Information	Access delivery information Access transport Application transport Parameter Compatibility Information Backward Call Indicator Call Diversion Information Call History Information End of Optional Parameters Generic Notification Generic Number Optional Backward Call Indicators Redirection Number Redirection Number Restriction User-To-User Indicators User-To-User information	ETSI V2 supports Cause Indicator and Service Activation parms. Also ETSI V2 does not support the Generic Number Parameter. **New Formatter required.**
CRG			Same as ETSI V2.
FAA		End of Optional Parameters Parameter Compatibility Information User-To-User Indicators	Same as ETSI V2
FAC			Same as ETSI V2
FAR	Facility Indicator	End of Optional Parameters Parameter Compatibility Information User-To-User Indicators	Same as ETSI V2
FRJ	Cause Indicators Facility Indicators	End of Optional Parameters User-To-User Indicators	Same as ETSI V2.
GRA			Same as ETSI V2
GRS	Range and Status		Same as ETSI V2

Table 2 Supported Russia ISUP Messages and Parameters

Mes sage	Mandatory Parms	Optional Parms	Currenly supported by ETSI V2?
IAM	Called Party Number Calling Party's Category Forward Call Indicators Nature of Connection Indicators Transmission Medium Requirement **Please refer to 74.3.8 for more details.**	Access transport Application transport Calling Party Number Closed user group interlock code End of Optional Parameters Generic Notification Generic Number Hop Counter Location Number Optional Forward Call Indicators Original Called Number Parameter Compatibility Information Propagation Delay Counter Redirecting Number Redirection Information User Service Information User Teleservice Information User-To-User Indicators User-To-User information **Please refer to 74.3.8 for more details.**	**Already writing new formatter for IAM message to support new CPC values.** Checking of optional parms is not required in the SPM.
IDR		End of Optional Parameters MCID Request Indicator Message Compatibility Information Parameter Compatibility Information	Same as ETSI V2.
INF	Information Indicators	Calling Party Number Calling Party's Category End of Optional Parameters Parameter Compatibility Information	ETSI V2 supports all optional parms except DmsPartyInfo. This messge is processed per leg basis and not on ball basis. **New formatter required.**
INR	Information Request Indicators	End of Optional Parameters Parameter Compatibility Information	ETSI V2 supports all optional parms except DmsPartyInfo. This messge is processed per leg basis and not on ball basis **New formatter required.**

Table 2 Supported Russia ISUP Messages and Parameters

Mes sage	Mandatory Parms	Optional Parms	Currenly supported by ETSI V2?
IRS		Access transport Calling Party Number End of Optional Parameters Generic Number MCID Response Indicator Message Compatibility Information Parameter Compatibility Information	Same as ETSI V2.
REL	Cause Indicaotrs	Access delivery information Access transport End of Optional Parameters Parameter Compatibility Information Redirection Number Restriction User-To-User Indicators User-To-User information ACG (Automatic Congestion Control)	ETSI V2 supports automatic congestion level parameter. **New formatter required.**
RES	Suspend/Resume Indicators	End of Optional Parameters	Same as ETSI V2.
RLC		Cause Indicators End of Optional Parameters	Same as ETSI V2.
RNG			**New Message, formatter already being developed**
RSC			Same as ETSI V2.
SAM			Same as ETSI V2.
SGM		Access transport End of Optional Parameters Generic Notification Generic Number Message Compatibility Information User-To-User information	ETSI V2 supports Generic Digits parameter. **New formatter required**.
SUS	Suspend/Resume Indicators	End of Optional Parameters	Same as ETSI V2.
UBL			Same as ETSI V2.
UBA			Same as ETSI V2.
UPA			Same as ETSI V2.
UPT			Same as ETSI V2.
USR		Access Transport End of Optional Parameters User-To-User Information	ETSI V2 does not support User-To-User information parameter. **New formatter required.**

74.3.7.1 Message Formatter for Optional Parameters

In order to support all of the necessary parms, specific Russia message formatters will have to be created for the following messages:

- ACM
- ANM
- CCL
- CON
- CPG
- IAM
- INF
- INR
- REL
- RNG
- SGM
- USR/UUI

74.3.8 Modification of Mandatory/Optional Parameters in Russia ISUP V2+

Russia specifications require four mandatory parameter fields to be enhanced:

a. Called Party Number-Nature of Address Indicator,

b. Nature of Connection Indicator-Satellite Indicator,

c. Backward Call Indicator - Called Party's Category Indicator and

d. Backward Call Indicator - Echo Control Device Indicator.

Original activity A00000937 addresses these requirements in the core. This activity will ensure that SPM STM1 handles these mandatory and optional paramters correctly when received. For more details, please refer to A00000937.

74.3.8.1 Called Party Number - Nature Of Address Indicator

In Russia network, different contents of IAM has been observed. IAM's observed in Russia network don't cause any problem in DMS MMP. Russia ISUP V2+ meets the market requirements (except NOA and address signals) for IAM.

Table 3, “NOA values for different call types,” on page 1518 shows the call types and the corresponding ‘Nature of Address Indicator’ (NOA) values.

Table 3 NOA values for different call types

Call Types	Nature of Address Indicator
Local Calls	Subscriber Number
National Calls	National (significant) Number
International Calls	International Number

“01-Subscriber Number” is the default value for Called Party Number-NOA.

74.3.8.2 Nature Of Connection Indicators-Satellite Indicator

In Russia specifications, “00-ISUP No Satellite”, “01- ISUP 1 Satellite”, and “02-ISUP 2 Satellite” values for “Nature Of Connection Indicators-Satellite Indicator” are required. These values of “Satellite Indicator” are already supported by the existing ETSI ISUP V2 base variant.

In order to set Satellite Indicator, SAT field of the TRKSGRP table tuple should be set for a trunk group. However, this datafill is not enough to allow 02-ISUP 2 Satellite value at tandem exchanges.

Table SATOVER is used to determine the routes that will allow double satellite hops. In Figure 24, "Datafilling TRKSGRP and SATOVER tables" a sample datafill for SATOVER table is given.

Figure 24 Datafilling TRKSGRP and SATOVER tables

```
TABLE TRKSGRP

- Outgoing RS ISUP V2+ Trunk -
OGRSISUPAB 0 DS1SIG C7UP OG N Y UNEQ NONE Q767 THRH 0 DMS N N RUSSIA
100_WHITE $ 2WN7 CIC

- Incoming RS ISUP V2+ Trunk -
ICRSISUPBA 0 DS1SIG C7UP IC N Y UNEQ NONE Q767 THRH 0 DMS N N RUSSIA
100_WHITE $ 2WN7 CIC

- 2-Way RS ISUP V2+ Trunk -
2WRSISUPBA 0 DS1SIG C7UP 2W N Y UNEQ NONE Q767 THRH 0 DMS N N RUSSIA
100_WHITE $ 2WN7 CIC


TABLE SATOVER

FROM              TO          OVERRIDE
-----------------------------------------------------------
ICRSISUPBA        OGRSISUPBC      Y
```

74.3.8.3 Backward Call Indicator - Called Party's Category Indicator

DMS MMP sends CPC_PAYPHONE within Backward Call Indicator-Called Party's Category field of ACM message, when a call -over Russia ISUP V2+ trunk- terminates to an IBN-COIN line.

74.3.8.4 Backward Call Indicator - Echo Control Device Indicator

DMS MMP sends ECHO_CONTROL_DEVICE_INCLUDED within Backward Call Indicator-Echo Control Device Indicator field of ACM message, if ESUPR field of TRKSGRP table is datafilled as "H" for the incoming Russia ISUP V2+ trunk, at terminating DMS MMP exchange.

74.3.9 New Calling Party Categories (CPC)

New calling party category (CPC) values required by Russia network are given in Table 4, "New CPC values," on page 1519.

Table 4 New CPC values

Category	Meaning
0000 1001	National Operator
0000 1110	Spare
0000 1111	Toll Payphone
0001 0000 - 1101 1111	Spare
1110 0000	Spare. Subscriber category 0
1110 0001	Hotel Subscriber. Subscriber category 2

Table 4 New CPC values

Category	Meaning
1110 0010	Subscriber free of charge. Subscriber category 5
1110 0011	Subscriber with access to special services. Subscriber category 7
1110 0100	Local network subscriber. Subscriber category 3
1110 0101	Local payphone. Subscriber category 9
1110 0110 - 1110 1111	Spare. For national use.
1111 0000	Automatic call , category I- ACCI
1111 0001	Semiautomatic call, categoryI - OCCI
1111 0010	Automatic call , category II- ACCII
1111 0011	Semiautomatic call, categoryII - OCCII
1111 0100	Automatic call , category III- ACCIII
1111 0101	Semiautomatic call, categoryIII - OCCIII
1111 0110	Automatic call , category IV- ACCIV
1111 0111	Semiautomatic call, categoryIV - OCCIV
1111 1000 - 1111 1110	Spare. For national use
1111 1111	Spare

Required Calling Party Category (CPC) values are defined in this activity.

74.3.10 Handling INR and INF Message

Two new message formatters will be required for Russian ISUP V2+ to support INR and INF messages on SPM STM1.

Please refer to the original activity A00000937 for the details on the core configuration/datafill to support INR and INF messages.

74.3.11 Russia Tones and Cadences

The tone parameters (which are calculated according to frequencies, levels and cadences of tones) for each market are kept in the software modules separately and downloaded from the CM to the SPM. The Russia tones has been made as a downloadable tone.Downloadable tones provides one generic tone player application in the DSP RM and downloading the details of each markets toneset from the Core when needed. The Downloadable Tone feature was provided in the SPM by activity A59033579 in SPSH17.

In SPMs the tone parameters which will be downloaded is based on the entry for TONETYPE in table MNCKTPAK.The Russia toneset is selected by setting the TONETYPE field to "**RUSSIA**". To select the TONETYPE the RSRINFO has to be datafilled with INTTONE. The Figure 25 below shows the datafill procedure.

Figure 25 Sample Datafill for RUSSIA tone (CHA)

```
pos SPM 1 1 7 DSP 0 1 WORKING
SPM 1 1 7 DSP 0 1 WORKING (COT 36 ) (DTMF 36 ) (ABBIT 8 )(MF 32 ) $ (SYSB
RPT) (MANB MJ RPT) (ISTB MN RPT) (PROTFAIL CR RPT)
(PATCHFAIL MJ RPT) $ NTLX65AA 01 DSP20CJ

>cha
CPKTYPE: DSP
>
UNITNO: 0
>
DSPGRPID: 1
>
WRKSPR: WORKING
>
RSRTYPE: COT
>
NUM: 36
>
RSRTYPE: DTMF
>
NUM: 36
>
RSRTYPE: ABBIT
>
NUM: 8
>
RSRTYPE: MF
>
NUM: 32

RSRTYPE:
>inttone
NUM:
>255
TONETYPE:
>RUSSIA
```

74.3.12 C7 Timers (Table C7UPTMR)

In Russia specifications, it is required to enlarge ranges of timers T5 and T17 from 320 seconds to 15 minutes(900 secs). Additionally, ranges of timers T13,

T15, T19, T21 and T23 should be enlarged from 640 seconds to 15 minutes. C7 timer values are datafillable in table C7UPTMR based on direction and protocol.

A00000937 activity enhanced the max integer value to 900 secs in core and XPM with PDTC hardware restriction. Please refer to Restriction and Limitation section of the A00000937 FN for PDTC.

In SPMs, the C7 timers will be downloaded with the correct datafilled timers.

74.4 Hardware Requirements or Dependencies

N/A

74.5 Software Requirements or Dependencies

Will be tested on core MMP20 non combo release load lineup. Patch or merge will be requested in SPM for this activity.

74.6 Limitations and restrictions

- As the development is on SPM STM1, any Line related features or services are not required to be supported by this activity
- This feature only defines and transmits Russia specific CPC values. Assigning and processing of these CPC values is not handled by this activity.
- Trunk metering Russia ISUP V2+ is not supported by this activity.
- Enhancements in CCITT timers apply to all CCITT versions/variants. However, enlarged ranges for T5 and T17 timers will be effective only on PDTC's when their both units are equipped with SX05. In other cases (i.e. the PDTC is equipped with MX77 or PM type is different), although it will be allowed to datafill all values between 1-900, highest effective value for T5 and T17 timers will be limited to 320, which is the current maximum for T5 and T17.
- If warm swact is applied to the peripherals which are connected to Russia ISUP V2+ trunks -involved in the TBI scenarios given in section 3.3.5.2 before RES/ANM message is received, the call will be dropped.

74.7 Interactions

74.7.1 Feature Interactions

Generation and reception of CCL message has interactions with call transfer related CEPT services.

- Subscribers are not allowed to FLASH within called controlled calls after the call is answered. CCL message, and called party control applies only

in basic calls. Calls subject to called-party control shall have the following call transfer related services denied:

— Call Hold

— Call Transfer

— Call Waiting

— 3-Way Calling

— 6-Way Calling

- If the originator of a called controlled call is involved in multi-party calls, called-party control will not be activated as given in Figure 11.
- CCL message is not supported in the scenarios where called subscribers - of called controlled calls - involve in complex calls (I3WC, I6WC, ICT, CFX ...etc).
- This activity does not support the interactions between called party control / CCL and CENTREX features.

74.7.2 Billing Interactions

Please refer to the original activity A00000937 for any billing interactions.

74.7.3 Interworking

This activity addresses the ability to support basic calls:

1. Line(IBN) - Russian ISUP - Line(IBN)

2. Line (IBN) - Russia ISUP - Russia ISUP - Line (IBN)

Other Interworking supported are:

3. V5.2-on GPP -> Russian ISUP V2-on SPM -> V5.2-on GPP

4. ISDN BRI Line -> Russian ISUP V2-on SPM -> ISDN BRI Line

5. Line -> ETSI PRI -> Russian ISUP V2-on SPM -> PRI -> Line

6. Operator calls on Busy subscriber (Toll Break In)

Russian ISUP variants will be configured on SPM STM1.

74.8 References

1. AT.59022404 : ISDN BRI Reverse Charging (REV)

2. AT.A00000937 Russian ISUP V2+ - Phase 1

3. ISUPR2000.AB01 in PLS FMDOC

4. ETSI ISUP Compliance Documents:
http://product-planning.europe.nortel.com/product-description/CCS7_links/conformance.html

5. ITU-T Recommendations Q.761-Q764 1993/1997
6. AT.59013592 - Automatic Message Accounting Billing Enhancements for Turkey
7. AT.59033703 - ICR&ICAMA Generation for NCOS on the base of called party code or prefix
8. DMS 100 MMP - AMA Reference Guide
9. A59012154: ETSI ISUP V1/V2 Base support for STM-1 access on the DMS MMP

74.9 Applicable customer facing sections

Fault Management

- Logs ____N/A_
- Alarms ___N/A___

Configuration

- Data Schema ___N/A___
- User Interface ___N/A___
- Element Management ____N/A__
- Security ___N/A__
- Service Order ____N/A__
- Office Parameters ____N/A__

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ____N/A__

74.10 Glossary

Term	Description
3WC	Three Way Call
ACM	Address Complete Message
ANM	Answer Message
BLA	Blocking Acknowledgment message
BLO	Blocking message

CCR	Continuity Check Request message
CI	Cause Indicator
CEPT	
CFN	Confusion message
CGB	Circuit Group Blocking message
CGBA	Circuit Group Blocking Acknowledgment message
CGU	Circuit Group Unblocking message
CGUA	Circuit Group Unblocking Acknowledgment message
CON	Connect message
COT	Continuity message
CPA	Calling Party Address
CPC	Calling Party Category
CPG	Call Progress message
CUG	Closed User Group
CWT	Call Waiting
ECT	Explicit Call Transfer
FOT	Forward-Transfer Message
GRA	Circuit Group Reset Acknowledgment message
GRS	Circuit Group Reset message
IAM	Initial Address Message
REL	Release message
RES	Resume message
REV	Reverse Charging
RLC	Release Complete message
RSC	Reset Circuit message
SAM	Subsequent Address Message
SUS	Suspend message

UBA	Unblocking Acknowledgment message
UBL	Unblocking message
XPM	eXtended Peripheral Module
NOA	Nature of Address Indicator

75: Functional Description (FN): A0006032

75.1 Feature name

Loop Reversal On Answer (LROA), Loop Reversal on Seizure (LRS) and Insert Tone on Coin Phone Termination (NOCOLL) SN07 Support for Cable & Wireless Caribbean

75.2 Description

This feature will allow the use of the following features in ISN07 (International Call Server) with a North American Toneset on the Passport Packet Voice Gateway (PVG) and on the MG9K:

- Loop Reversal On Answer (LROA)
- Loop Reversal on Seizure (LRS)
- Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with trunks on a PVG

75.2.1 Loop Reversal On Answer (LROA)

Loop Reversal On Answer as detailed in AR0502 “Line option for Line Reversal On Answer” will be supported on IBN line types on the MG9K 32 port Global Line Card (GLC-32).

75.2.2 Loop Reversal on Seizure (LRS)

Loop Reversal on Seizure as detailed in A59008303 “Line option for Line Reversal on Seizure” will be supported on IBN line types on the MG9K GLC-32.

75.2.3 Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with PVG trunks

NOCOLL functionality as detailed in A59008313 “Insert Tone on Coin Telephone Termination” will be supported on interworkings with the following PVG trunks types:

- ETSI ISUP
- ANSI ISUP

The pay phone recognition tone will be played on the trunk when terminating to a IBN line with the NOCOLL option. The characteristics of the tone such as frequency, cadence, level, and repetition are defined by the toneset of the PVG.

75.3 Hardware Requirements or Dependencies

75.3.1 Loop Reversal On Answer (LROA)

The MG9K 32 port Global Line Card is required.

75.3.2 Loop Reversal on Seizure (LRS)

The MG9K 32 port Global Line Card is required.

75.3.3 Insert Tone on Coin Phone Termination (NOCOLL) on interworkings with PVG trunks

A VSP3 or VSP3-o card is required on the PVG.

75.4 Software Requirements or Dependencies

None.

75.5 Limitations and restrictions

All limitations and restrictions for the original LROA, LRS, and NOCOLL are still applicable with the exception of the supported hardware configurations as stated in this FN.

LRS and LROA are only supported on the MG9K GLC-32 card for IBN line types.

Playback of the pay phone recognition tone is only supported on the PVG for ANSI ISUP and ETSI ISUP trunk types. Originations from other trunk types on a PVG terminating to IBN lines with the NOCOLL option will not result in the playback of the pay phone recognition tone.

A VSP3 or VSP3-o card is required on the PVG in order for speech to be heard during the playback of the pay phone recognition tone. The use of VSP2 or older card will cause the calling party to only hear the tone playback for the first 13 seconds of the call. During this time, voice from the called party will not be transmitted.

The use of features such as call waiting, call hold, conference calling are not supported on lines with the LROA option. The use of these features may result in the normalization of the polarity reversal.

LRS and LROA are not supported on lines with the CEPT option.

75.6 Interactions

A line with a service which uses flash can also have the NOCOLL option provisioned. If the line flashes while the tone is being applied, the playback of the tone will be halted.

75.7 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

75.8 Glossary

Term	Description
ANSI	American National Standards Institute
ETSI	European Telecommunications Standards Institute
IBN	Integrated Business Network
ISUP	ISDN User Part
LROA	Loop Reversal On Answer
LRS	Loop Reversal on Seizure
NOCOLL	NO COLLect - a servord option associated with the Insert Tone on Coin Phone Termination feature
PVG	Passport Packet Voice Gateway
VSP	Voice Services Processor

Fault Management (FM)

Introduction

This chapter describes impacts to fault management, such as logs and alarms, for the features planned for this release. Only those features with fault-management impacts are listed.

Featid	Title
A00001919.AA09	CEPT Services Password Enhancement
A00001920.AA09	Metering OOS Enhancements
A00002252.AA04	MG9K Lines Preprovisioning
A00002364.AA08	CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20
A00002702.AA15	No Line Origination Without Charging
A00002844.AA09	Excessive Metering Detection (EMD) Support for Metered Trunks
A00003147.AA09	DP Digit Reception Control
A00003696.AA15	G-ISUP Routing Enhancements
A00004565.AA15	Line to Moroccan ISUP V2 interworking

1: Fault Management (FM): A00001919

1.1 Fault management strategy

1.2 Fault management tools and utilities

1.3 CEPT100 Logs

1.3.1 Explanation

Log Title: CEPT100

Name: CEPTPW IS LOCKED REMOTELY

Description: CEPT100 log is generated when CEPT Features' Password (CEPTPW) is locked remotely usage of CEPT features which means subscriber exceeds the maximum wrong PIN entry for CEPTPW feature.

Event type:

1.3.2 Format

The following is the format for log report CEPT 100.

Figure 1 Formats of log reports

```
CEPT100 mmmdd hh:mm:ss ssdd INFO CEPTPW IS LOCKED REMOTELY

BASE DN: <base_dn>

ORIGINATING DN: <orig_dn>

ORIGINATING TRUNK: <orig_cpid>
```

The sample log report is as shown below.

Figure 2 Sample log report (CLI is available)

```
CEPT100 APR28 09:33:57 2909 INFO CEPTPW IS LOCKED REMOTELY

BASE DN: 1027835411

ORIGINATING DN: 1027835475

ORIGINATING TRUNK: CKT       ICISP2BA    0
```

In case of the calling DN unavailability such as, incoming trunk is NTLS01 R1 Trunk, ORIGINATING DN field is printed as empty.

Figure 3 .Sample log report (CLI is not available)

```
CEPT100 APR28 09:33:57 2909 INFO CEPTPW IS LOCKED REMOTELY

BASE DN: 1027835411

ORIGINATING DN:

ORIGINATING TRUNK: CKT      ICNTLS01BA    0
```

If the originating agent is in the same switch that means line to line call (basic call) performed while dialing DISA DN, the ORIGINATING TRUNK field is printed as empty.

Figure 4 .Sample log report (Line to Line call)

```
CEPT100 APR28 09:33:57 2909 INFO CEPTPW IS LOCKED REMOTELY

BASE DN: 1027835411

ORIGINATING DN: 1027835475

ORIGINATING TRUNK:
```

1.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
INFO CEPTPW IS LOCKED REMOTELY	Constant	Indicates a report of CEPT information
BASE DN	Digits (18 digits)	Identifies the SNPA + DN of the base agent.
ORIGINATING DN	Digits (18 digits)	Identifies the SNPA + DN of the originator.

Field	Value	Description
ORIGINATING TRUNK	CPID	Identifies the originator trunk (incoming trunk).

1.3.4 Action

No immediate action is taken.

1.3.5 Associated Operational Measurements or Performance Measurements

CPTRAFAL register in CEPTRA OM group, PWUSG and PWLOCK registers in CEPTPW OM group are pegged. Note that these OMs are pegged for another cases also not only for this scenario.

1.3.6 Additional information

N/A

1.4 CEPT101 Logs

1.4.1 Explanation

Log Title: CEPT101

Name: CEPTRA USAGE ATTEMPT

Description: CEPT101 log is generated when subscriber attempts to use supported CEPT features (ILR, IWUC, CEPTPW, CFD, CFU and CFB) from remote agents via CEPTRA.

Event type:

1.4.2 Format

The following is the format for log report CEPT 101.

Figure 5 Formats of log reports

```
CEPT101 mmmdd hh:mm:ss ssdd INFO CEPTRA USAGE ATTEMPT

BASE DN: <base_dn>

ORIGINATING DN: <orig_dn>

ORIGINATING TRUNK: <orig_cpid>

FEATURE: <requsted_ftr>

ACTION: <ftr_action>
```

Originating DN or Originating Trunk fields could be empty due to unavailable CLI or performing remote access in same switch (line to line call) respectively.

The sample log report is as shown below.

Figure 6 Sample log report (CLI is available)

```
CEPT101 APR28 09:33:57 2909 INFO CEPTRA USAGE ATTEMPT

BASE DN: 1027835411

ORIGINATING DN: 1027835475

ORIGINATING TRUNK: CKT       ICISP2BA    0

FEATURE: ILR

ACTION: INTER
```

In case of the calling DN unavailability such as, incoming trunk is NTLS01 R1 Trunk, ORIGINATING DN field is printed as empty.

Figure 7 .Sample log report (CLI is not available)

```
CEPT101 APR28 09:33:57 2909 INFO CEPTRA USAGE ATTEMPT

BASE DN: 1027835411

ORIGINATING DN:

ORIGINATING TRUNK: CKT      ICNTLS01BA    0

FEATURE: ILR

ACTION: INTER
```

If the originating agent is in the same switch that means line to line call (basic call) performed while dialing DISA DN, the ORIGINATING TRUNK field is printed as empty.

Figure 8 .Sample log report (Line to Line call)

```
CEPT101 APR28 09:33:57 2909 INFO CEPTRA USAGE ATTEMPT

BASE DN: 1027835411

ORIGINATING DN: 1027835475

ORIGINATING TRUNK:

FEATURE: ILR

ACTION: INTER
```

1.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
CEPTRA USAGE ATTEMPT	Constant	Indicates a report of CEPT information
BASE DN	Digits (18 digits)	Identifies the SNPA + DN of the base agent.
ORIGINATING DN	Digits (18 digits)	Identifies the SNPA + DN of the originator.
ORIGINATING TRUNK	CPID	Identifies the originator trunk (incoming trunk).
FEATURE	line_option	Identifies the which CEPT feature is requested.
ACTION	xla_ftr_function (ACT, DEACT, INTER, USAGE, PROG, DELETE)	Indicates the subscriber action on requested CEPT feature.

1.4.4 Action

No immediate action is taken.

1.4.5 Associated Operational Measurements or Performance Measurements

CPTRAATT register in CEPTRA OM group is pegged, and if subscriber is unsuccessful to program one of supported CEPT feature, CPTRAFAL register is pegged; otherwise in case of successful programming CPTRASUC register is pegged. Additionally, requested CEPT feature OM register is pegged according to success of result.Note that these OMs are pegged for another cases also not only for this scenario.

1.4.6 Additional information

N/A

1.5 Related documentation

2: Fault Management (FM): A00001920

2.1 Fault management strategy

N/A

2.2 Fault management tools and utilities

N/A

2.3 Logs

2.3.1 Explanation

Log Title: MTRDEASS DATA LOST

Name: MTR 150

Description: This log is generated when there is no space available in MTRDEASS table for a new entry.

MTRDEASS table is used to keep deassigned meters of subscribers. Adding a new tuple to MTRDEASS table is performed when MOG deletion is done. If there is no space for new entry, MTR 150 log is generated for each deassigned meter of subscriber.

Event type: Information

2.3.2 Format

MTR150 <mmmdd hh:mm:ss ssdd> INFO MTRDEASS DATA LOST

DN: <Directory Number> METER NAME: <Meter Name>

METER COUNT: <Meter Count> WRAP: <Wrap>

NO SPACE IS AVAILABLE IN MTRDEASS TABLE

Example:

MTR150 APR1 12:00:13 1234 INFO MTRDEASS DATA LOST

DN:7835401 METER NAME: LOCAL

METER COUNT: 00000012 WRAP:N

NO FREE SPACE IS AVAILABLE IN MTRDEASS TABLE

2.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
DN	Directory Number	Directory Number of subscriber
Meter Name	character set	Meter names that are defined in table MTRNAMES
Meter Count	Numeric	Meter count of deassigned meter which may be up to 99999999
Wrap	Y/N	Boolean to indicate whether meter counts has exceeded 99999999.

2.3.4 Action

MTR 150 log is an information log. It requires no immediate action.

2.3.5 Associated Operational Measurements or Performance Measurements

N/A

2.3.6 Additional information

N/A

2.4 Related documentation

3: Fault Management (FM): A00002252

3.1 Fault management strategy

ActID 89009298 changes the format of MG9K LENs. Prior to SN06 (CCM19), an MG9K LEN had the following format.

<SITE> <0 to 511> <0 to 9> <subgroup, 0 to 10> <circuit, 0 to 99>

Because of the formula used to calculate terminal ids (TermID) in the core, the MG9K LEN reflects the TermID/terminal number and not the physical location of the MG9K line. For example, the following shows a QLEN on an SN05 MG9K LEN:

```
>QLEN CO10 00 0 01 67
------------------------------------------------------------------------------
LEN:     CO10  00 0 01 67
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     5210621
LINE CLASS CODE:      1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: NPDGP  BNV: NL MNO: N
PM NODE NUMBER     :    103
PM TERMINAL NUMBER :    168
OPTIONS:
DGT
------------------------------------------------------------------------------
```

Note that the terminal number is the LEN slot/circuit + 1.

The new MG9K LEN format reflects the physical location of the line.

<SITE> <frame, 0 to 511> <shelf, 0 to 9> <slot, 2 to 9, 14 to 21> <circuit, 0 to 47>

3.2 Fault management tools and utilities

As stated above ActID 89009298 changes the format of an MG9K LEN. Any OAM&P utility that uses LENs will require the new MG9K LEN format for MG9K lines, and any OAM&P utility that displays LENs will display MG9K LENs in the new format. A sampling of OAM&P that will require or reflect the new MG9K LEN follows. The complete list of changed utilities is essentially everything that uses LENs. Reference the Logs section below for MG9K LEN values and ranges.

- MAPCI: Posting MG9K lines via LEN at the LTP level will require the new format.
- LINE logs in logutil will use the new format.
- SERVORD will require the new format for MG9K lines (SESM).

3.3 Logs

3.3.1 Explanation

All LINE logs generated for MG9K lines will utilize the new LEN format.

3.3.2 Field descriptions

The new MG9K LEN contains the following fields.

Table 1 Field descriptions

Field	Value	Description
<site>	character vector	name of the site from table site
<frame or cf>	0 to 511	frame number in the office
<shelf or rs>	0 to 9	shelf number in the frame
<slot or ss>	2 to 9, 14 to 21	card slot number
<circuit or cc>	0 to 47	circuit on card

3.3.3 Action

Persons responsible for maintenance must realize the MG9K LEN format has changed. The crafts person can now use the log to pinpoint the physical location of the reported MG9K circuit.
None

3.4 Related documentation

None.

4: Fault Management (FM): A00002364

4.1 Fault management strategy

None.

4.2 Fault management tools and utilities

LOGUTIL.

4.3 Logs

4.3.1 Explanation

Log Title: CDR601

Name: CDR LONG LOG

Description: The CDR601 log will be expanded to contain current fields plus new field CLGNUM_IND. The new field only contain values when incoming agent is ANSI ISUP or HK ISUP trunk, otherwise, the new field is blank.The value of the new field indicates which number is captured in CLG_NUM field.

Event type: unchanged.

4.3.2 Format

Please refer to the following example.

The new field is highlighted.

CDR601 JUL26 16:21:50 3100 INFO CDR LONG LOG	
REC_CODE	F0
TYPE_CALL	1
INAP_CALL	0
VPN_CUST	0
EXPANSION_REC	Y
ORIG_DATE	057
ORIG_TIME	58899

DISC_DATE	057
DISC_TIME	58909
CALL_DUR	00000005
ORIG_CLLI	1017
ORIG_MEM	0322
TERM_CLLI	1016
TERM_MEM	0321
CLG_NUM	1234
TNS_VALUE	123456
CUST_COST	
BILL_TYP	255
DIAL_NUM	9701234121
SRV_CODE	05
TNS_SENT	Y
ANSWER	
TRMT_CODE	000
COMPL_CODE	125
CLASS_SERV	00
DATA_CALL	0
PART_NUM	0901
CLI_INDEX	000
DISP_QUAL	001
SATE_IND	0
SEQ_NUM	00038617
NODE_ID	333
DEST_NUM	
BILL_NUM	
T_FCI_NUM	00
CCD	057
CCT	58900
CUST_ID	0000
TTON	NAT

ACCT_EXT	
CPC	0005
OUTP_NUM	5601234121
CLGNUM_IND	**01**

4.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
CLGNUM_IND	00, 01, 10, 11	Indicate which number is captured in CLG_NUM field according to the capture logic.

4.3.4 Action

None.

4.3.5 Associated Operational Measurements or Performance Measurements

None.

4.3.6 Additional information

None.

None.

4.4 Related documentation

None.

5: Fault Management (FM): A00002702

5.1 Fault management strategy

N/A

5.2 Fault management tools and utilities

N/A

5.3 Logs

5.3.1 MTR 158

5.3.1.1 Explanation

Log Title: ILLEGAL CHARGING METHOD

Name: MTR 158

Description: This log is generated when a line origination from IBN, ISDNKSET or P-phone without a valid charging option is on attempted. This log is generated only if the 'No Line Origination Without Charging' feature is activated by setting NCW_CHRG to DISALLOWED.

Event type: Information

5.3.1.2 Format

MTR158 <mmmdd hh:mm:ss ssdd> INFO INVALID CHARGING METHOD

<cpid of origination> <DN of origination>

CALLED DR: <Dialed digits>
CALL RESULT: <Text about the call behavior>

Example:

RSNW4E07 MTR158 JUN12 15:17:50 9600 INFO INVALID CHARGING METHOD

HOST 02 0 00 06 DN 1027835476

CALLED DR 0

CALL RESULT: TRMT- No MOG option

5.3.1.3 Field descriptions

5.3.1.4 Action

Table 1 Field descriptions

Field	Value	Description
CPID of origination	Host number	Identifies the line CP_ID of the originator.
DN of origination	DN number	Identifies the DN number of the originator.
Called DR	Digits	Identifies the dialed digits
Text about the call behavior	Character set	Indicates why a call goes to treatment.

This log indicates a denied call attempt originating from an agent without valid charging option. The agent will be able to originate calls after a valid charging option is assigned to this agent by the operator.

5.3.1.5 Associated Operational Measurements or Performance Measurements

N/A

5.3.1.6 Additional information

Table 2 Possible call result texts in MTR 158 log

No MOG option on a line with CEPT	TRMT- No MOG option
No SMDR or MOG option on a line without CEPT option	TRMT- No MOG or SMDR on line
MOG option on a line without CEPT	TRMT- MOG option on a line without CEPT
SMDR and MOG options both exists on the line	TRMT- MOG & SMDR on line
SMDR activated during translation for a line with MOG option	TRMT-SMDR activation during XLA

5.3.2 MTR 163

5.3.2.1 Explanation

Log Title: ILLEGAL CHARGING METHOD

Name: MTR 163

Description: This log is generated when an origination occurs from an IC PRI trunk without ICMOG datafill in table TRKOPTS. This log is generated only if the active value of NTOW_CHG tuple in table MTRSYSPM is set to DISALLOWED.

Event type: Information

5.3.2.2 Format

MTR163 <mmmdd hh:mm:ss ssdd> INFO INVALID CHARGING METHOD

CKT <Trunk group CLLI > <Member no>
CALL RESULT: NO ICMOG DATAFILL FOR THE TRUNK GROUP

Example:

RSNW4E07CN MTR163 JUN25 03:01:14 2200 INFO INVALID CHARGING METHOD

CKT ICPRICB 0

CALL RESULT: NO ICMOG DATAFILL FOR THE TRUNK GROUP

5.3.2.3 Field descriptions

5.3.2.4 Action

Table 3 Field descriptions

Field	Value	Description
Trunk group CLLI	Trunk CLLI	Identifies the trunk group CLLI of the IC trunk circuit
Member no	Integer	Identifies the member no of the IC trunk circuit
Text about the call behavior	Fixed	Indicates why the call goes to treatment.

This log indicates a denied call attempt originating from an IC trunk group without valid ICMOG datafill in table TRKOPTS. The trunk agent will be able to originate calls after a valid ICMOG datafill is added to table TRKOPTS for the trunk group..

5.3.2.5 Associated Operational Measurements or Performance Measurements

N/A

5.3.2.6 Additional information

N/A

5.4 Alarms

N/A

5.5 Related documentation

N/A

6: Fault Management (FM): A00002844

6.1 Fault management strategy

6.2 Fault management tools and utilities

6.3 Logs

6.3.1 Explanation

Log Title: EMD 101

Name: Excessive Trunk Metering

Description: This log is generated when a subscriber is detected whose meter counts are increased by more than a threshold value in a time period.

Event type: Info

6.3.2 Format

Figure 1 Format of log report EMD 101

```
EMD101 mmmdd hh:mm:ss ssdd INFO EXCESSIVE TRUNK METERING

<clli>

Reason: <rsn>

Previous date: yyyy/mm/dd hh:mm:ss

------------------------------------------------------------

METER NAME  WRP1 COUNT1  WRP2  COUNT2  DELTA

----------  ---- ------  ----  ------  -----

<mtrnm>     <wrp> <cnt>  <wrp>  <cnt>  <dlt>

------------------------------------------------------------

Threshold:<thr>                          Total delta: <tdlt>
```

6.3.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
EXCESSIVE METERING FOR TRUNKS	Constant	Indicates that a trunk agent whose meter counts are increased by more than a threshold value in time period is detected.
CLLI	Symbolic text	Identifies CLLI of trunk
Reason	PERIODIC, BILLING, OOS or WRAP	Indicates the reason for the log generation.
Previous date	Alphanumeric	The copy date for the meter blocks.
METER NAME	Character string	Indicates a valid assigned meter name.
WRP1	YES, NO or ****	Wrap information for the copied meter.
COUNT1	0000 0000 0000 - 9999 9999 9999 or **********	Count information for the current meter.
WRP2	YES, NO or ****	Wrap information for the copied meter.
COUNT2	0000 0000 0000 - 9999 9999 9999 or **********	Count information for the current meter.
DELTA	0 0000 0000 0000 - 1.999.999.999.998 or *********	Difference between the previous count and the current count for that meter.
Total delta	0 0000 0000 0000 - 7.999.999.999.992	Indicates the total of all meter deltas for that subscriber
Threshold	0 0000 0000 0000 - 7.999.999.999.992	Indicates the threshold for the comparison

6.3.4 Action

No immediate action.

6.3.5 Associated Operational Measurements or Performance Measurements

N/A.

6.3.6 Additional information

None.

6.4 Related documentation

None.

7: Fault Management (FM): A00003147

7.1 Fault management strategy

None.

7.2 Fault management tools and utilities

None.

7.3 Logs

7.3.1 Explanation

Log Title: PM181

Name: General Information Log for PM's.

Description: A new reason string is added by this feature. The functionality of the log is unchanged.

Event type: Information only.

7.3.2 Format

Same as before.

7.3.3 Example

RSNW3J07AV PM181 JUL24 08:42:00 0400 INFO PLGC 3 Node: ISTb, Unit0 Act: ISTb, Unit1 Inact: ManB
Could not configure DP Digit Reception Control for unit 1

7.3.4 Field descriptions

Same as before.

7.3.5 Action

Follow existing documentation for the log.

7.4 Related Documentation

None.

8: Fault Management (FM): A00003696

8.1 Fault management strategy

8.2 Fault management tools and utilities

8.3 Logs : ISC600

8.3.1 Explanation

Log Title: ISC600

Name: ISC log Report

Description: Displays the Point Codes and their respective counts for all the calls received on a GISUP trunk, routing to a National variant. It displays up to 480 distinct point Codes with the respective counts. In case the received point codes are more than 480, then these are counted and captured as PC not counted.

Event type: Once in 3 Hours

8.3.2 Format

8.3.2.1 Format1

Below is the format for the ISC log.

```
TCB2_LOG      ISC600 <mmmdd hh:mm:dd>INFO ISC log report
        Originating ISC point Code captured from <from_time> to <to_time>
        ------------------------------------------------------------------
        ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count
        ------------------------------------------------------------------
        <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>
        <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>
        ................
        <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>
        <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>  <pc> <count>

        ------------------------------------------------------------------
        PC not captured : <overflow>
        ------------------------------------------------------------------
```

8.3.2.2 Examples

- Example 1 : No calls on INTL (GISUP)TRK which logs the point Code.

```
TCB2_LOG      ISC600 NOV28 11:55:28 8900 INFO ISC log report
        Originating ISC point Code captured from NOV-28 11:54 to NOV-28 11:55
        ------------------------------------------------------------------
                        No data captured
```

```
        ------------------------------------------------------------------
```

- Example 2 : Few calls received on the INTL (GISUP TRK)

```
TCB2_LOG      ISC600 NOV28 11:55:28 8900 INFO ISC log report
        Originating ISC point Code captured from NOV-28 11:54 to NOV-28 11:55
        ------------------------------------------------------------------
        ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count
        ------------------------------------------------------------------
          100     5     150     1     230     1     250     1   16000     1
        16350     1   16400     1
        ------------------------------------------------------------------
```

- Example 3 : the number of point codes from where the calls are received, exceeds 480.

```
TCB2_LOG      ISC600 NOV28 13:44:44 5472 INFO ISC log report
        Originating ISC point Code captured from NOV-28 13:43 to NOV-28 13:44
        ------------------------------------------------------------------
        ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count   ISCPC Count
        ------------------------------------------------------------------
            1     1       5     1       7     1       8     1      10     1
           22     1      25     1      30     1     100     1     153     1

         ......................

         2001     5    2608     1    3230     1    4250     1    9300     1
        16300     5   16301     1   16302     1   16303     1   16304     1

        ------------------------------------------------------------------
        PC not captured : 10
        ------------------------------------------------------------------
```

8.3.3 Field descriptions

The Fields in the log format are displayed as per format below.

Table 1 Field descriptions

Field	Value	Description
from_time	Date and time	The time when the ISC point Code where captured for the current Log
to_time	Date and time	The time till the ISC point Code were captured for the give log.
pc	0 -16383	Originating ISC point Code received.
count	Integer range	Counter displaying the count of the respective point Code

Table 1 Field descriptions

Field	Value	Description
overflow	Integer range	Counts the number point codes from which the calls were received but are not printed in the log.

8.3.4 Action

Nil

8.3.5 Associated Operational Measurements or Performance Measurements

Nil

8.3.6 Additional information

This data collected form this log will be used for Statistical purpose. The printing of the log is controlled via office parameter CAPTUE_ISC_PC.

8.4 Logs : MCID600

8.4.1 Explanation

Log Title: MCID600

Name: Identification Data

Description: This log is an extension of the MCID logs, introduced for DTAG holding service. It provides information about the Called agent, calling number, called number and the date and time of the call.

Event type: When Holding is activated on the Telco and NANA message is received.

8.4.2 Format

8.4.2.1 Format

Below is the format for the MCID log.

```
AVST1_LOG MCID600 DEC04 <mmmdd hh:mm:dd> INFO IDENTIFICATION DATA
         Calling_Agent  : <originating agent>
         Called_Agent   : <terminating agent>
         Calling_Number : <calling number>
         Called_Number  : <called number>
         Date : <date>
         Time : <time>
```

8.4.2.2 Examples

```
AVST1_LOG MCID600 DEC04 22:23:01 0800 INFO IDENTIFICATION DATA
         Calling_Agent  : CKT     INTGATEISUP 628
```

```
Called_Agent    : CKT     TELKOMIUSP 632
Calling_Number : 033461111
Called_Number  : 033461112
Date : 05.12.2003
Time : 22:23:01
```

8.4.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
Originating Agent	-	CLLI name for the originating agent.
Terminating Agent	-	CLLI name for the terminating agent.
calling_number	digits	Calling party number
called number	digits	Called party number
Date	date	Date on which the call was made
time	time	time on which the call was made

8.4.4 Action

Nil

8.4.5 Associated Operational Measurements or Performance Measurements

Nil

8.4.6 Additional information

This log is currently a temporary place holder for the information to be displayed on the AVST, after receipt of NANA message. It can be further enhanced once the specifications are clear.

8.5 Related documentation

9: Fault Management (FM): A00004565

9.1 Fault management strategy

N/A

9.2 Fault management tools and utilities

N/A

9.3 Logs

9.3.1 MTR161

9.3.1.1 Explanation

Log Title: MTR161

Name: BCKMTR DATAFILL

Description: The metering (MTR) subsystem generates this report if a corresponding MTRTARIF tuple could not be found for a received tariff index within ISUP CRG message.

Event type: Failure

9.3.1.2 Format

MTR161 mmmdd hh:mm:ss ssdd FAIL BCKMTR DATAFILL

LEN <len> DN <dn>

CALLED DR <dn>

NO TARIFF DATAFILL AVAILABLE

FOR THE RECEIVED TARIFF INDEX : <taridx>

LNET = <lnetval> MZONE = <mzoneval>

Example:

XXXX MTR161 DEC12 10:49:18 4900 FAIL BCKMTR DATAFILL

HOST 00 0 00 10 DN 1027835405

CALLED DR 7835406

NO TARIFF DATAFILL AVAILABLE

FOR THE RECEIVED TARIFF INDEX : 3

LNET = LOC MZONE = 0

9.3.1.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
FAIL BCKMTR DATAFILL	Constant	Indicates that backward metering failed because data was missing from the table MTRTARIF
len	Alphanumeric (up to 12 characters)	Gives the line equipment number (LEN) of affected equipment
dn	Numeric(up to 15 digits)	Provides the directory number (DN) associated with the LEN
dn	Numeric(up to 15 digits)	Identifies the contents of the digit register (the called number)
NO TARIFF DATAFILL AVAILABLE FOR THE RECEIVED INDEX	Constant	-
taridx	0 - 255	This field gives the received tariff index within CRG message
lnetval	Symbolic text	This field provides the identifier of the logical network of the call. The entry in the LNETWORK field is in table LNETWORK and specified in translation
mzoneval	0 - 63	This field provides the metering zone value of the call specified in translation

9.3.1.4 Action

This log indicates that the MTRTARIF tuple corresponding to the received tariff index in CRG message is missing. An MTRTARIF tuple using the received index value should be datafilled for charging the call.

9.3.1.5 Associated Operational Measurements or Performance Measurements

N/A

9.3.1.6 Additional information

N/A

9.3.2 MTR162

9.3.2.1 Explanation

Log Title: MTR162

Name: BCKMTR RATE MISMATCH

Description: The Metering (MTR) subsystem generates log report MTR162 for two cases:

- When a mismatch occurs between calculated software meter count and reported hardware metering pulse count for local type backward metering
- When a mismatch occurs between received meter count and reported hardware metering pulse count for distance type backward metering

Event type: Information

9.3.2.2 Format

MTR162 <mmmdd hh:mm:ss ssdd> INFO BCKMTR RATE MISMATCH

<cpid of origination> <DN of origination>

PULSE COUNT MISMATCH - NODE <node no> REPORTED INACCURATE CHARGE

BACKWARD METERING TYPE : <bcktmtr type>

LNETWORK: <LNET value> <tariff index>

<pulse info> PULSE COUNT: <CM meter count>

REPORTED PULSE COUNT: <Pulse count from PM>

Examples:

XXX MTR162 DEC13 19:05:44 5000 INFO BCKMTR RATE MISMATCH

HOST 01 1 15 11 DN 3923652407

PULSE COUNT MISMATCH - NODE 31 REPORTED INACCURATE CHARGE

BACKWARD METERING TYPE :LOCAL

LNETWORK: NATL TARIFF INDEX: 3

CALCULATED PULSE COUNT: 10

REPORTED PULSE COUNT: 16

XXX MTR162 DEC13 19:05:44 5000 INFO BCKMTR RATE MISMATCH

HOST 01 1 15 11 DN 3923652407

PULSE COUNT MISMATCH - NODE 31 REPORTED INACCURATE CHARGE

BACKWARD METERING TYPE : DISTANCE

LNETWORK: NATL

RECEIVED PULSE COUNT: 10

REPORTED PULSE COUNT: 16

9.3.2.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
BCKMTR RATE MISMATCH	Constant	Reports a meter count mismatch between the reported hardware meter pulse and the meter count calculated or accumulated at CM
CPID of origination	Host number	Identifies the line CP_ID of the originator
DN of origination	Numeric(up to 15 digits)	Identifies the DN number of the originator
PULSE COUNT MISMATCH	Constant	
node no	Numeric	PM node number
REPORTED INACCURATE CHARGE	Constant	
REPORTED INACCURATE CHARGE	Constant	

Table 2 Field descriptions

Field	Value	Description
BACKWARD METERING TYPE :	Constant	
bcktmtr type	local/distance	
LNET value	Symbolic text	This field provides the identifier of the logical network of the call. This field is specified in translation.
tariff index	0 to 255	Received tariff index within CRG message for local backward metering.
pulse info	CALCULATED/ RECEIVED	This field is set to 'CALCULATED' for local backward metering and to 'RECEIVED' for distance bacward metering
PULSE COUNT:	Constant	
CM meter count	Numeric	Calculated or accumulated meter count in CM
REPORTED PULSE COUNT:	Constant	
Pulse count from PM	Numeric	Reported pulse count generated for the call

9.3.2.4 Action

For local backward metering, check the metering tables and the static data for differences.

For distance backward metering, no action is necessary. The log is generated only for information.

9.3.2.5 Associated Operational Measurements or Performance Measurements

N/A

9.3.2.6 Additional information

The amount of meter count mismatch which causes MTR162 log generation is determined by the PULMISTH parameter in MTRSYSPM.

For distance metering, meter count mismatch can occur in case the originator line on hooks before all the received pulses are generated.

9.3.3 MTR113

9.3.3.1 Explanation

Log Title: METER DATAFILL

Name: MTR113

Description: The metering (MTR) subsystem generates this report when the system attempts to meter a call and one of the following tables has invalid or missing data:

- universal translations
- metering

Event type: Failure

9.3.3.2 Format

MTR113 mmmdd hh:mm:ss ssdd FAIL METER DATAFILL
LEN <len> DN <dn> CALLED DR <dn>
METERING DATAFILL ERROR
<rsntxt>
LNETWORK = <infotxt>

Example:
MTR113 MAY04 14:11:16 1886 FAIL METER DATAFILL
HOST 05 1 00 20 DN 9096210001
CALLED DR 9096210002
METERING DATAFILL ERROR.
NO MZONE DATAFILLED IN XLA
LNETWORK = LOCAL MZONE 63 0 0

9.3.3.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
LEN	Alphanumeric(up to 12 characters)	Gives the line equipment number (LEN) of affected equipment

Table 3 Field descriptions

Field	Value	Description
DN	Numeric(up to 15 digits)	Provides the directory number (DN) associated with the LEN
CALLED DR	Numeric(up to 15 digits)	Identifies the contents of the digit register (the called number)
rsntxt	Alphanumeric	Provides information on the condition that caused metering to fail
infotxt	Symbolic and numeric	The LNET and MZONE value for the call obtained from translation

9.3.3.4 Action

When this log is generated, the missing table datafill for the call stated in the rsntxt field should be completed in order to meter the call. Either translation or metering table datafills can be missing.

9.3.3.5 Associated Operational Measurements or Performance Measurements

N/A

9.3.3.6 Additional information

Only change for the existing log is a new rsntxt added for backward metering. The new rsntxt is as below:

BACKWARD METERING: NO LNET IN XLA

Figure 1 Example output for the new log text

```
MTR113 MAY04 14:11:16 1886 FAIL METER DATAFILL
HOST 05 1 00 20 DN 9096210001
CALLED DR 9096210002
METERING DATAFILL ERROR
BACKWARD METERING: NO LNET IN XLA
LNETWORK =      MZONE    63          0          0
```

An mtr 113 log with the new rsntxt is generated if no LNET datafill is found for a translation with BCKWMTR option.

9.4 Related documentation

N/A

Configuration Management (CN)

Introduction

This chapter describes impacts to configuration management, such as hardware/software requirements, data schemas, and service orders for the features planned for this release. Only those features with configuration-management impacts are listed.

Featid	Title
A00001914.AA11	CEPT International Line Restriction Enhancements
A00001918.AA13	CEPT Feature Warning with Announcement for Bangladesh
A00001919.AA09	CEPT Services Password Enhancement
A00001920.AA09	Metering OOS Enhancements
A00001921.AA14	CIS Toll Call Ringing
A00001923.AA16	CIS Subscriber Categories
A00001930.AA14	Last and Total Call Meter Inquiry Services
A00001935	Provisioning Support for Centrex-IP Nodes and Lines
A00002053.AA14	AMA Records for Metered Features
A00002101.AA17	ALLOW ITX ONLY SSUTR2
A0002173.AB06	System of Operative-Searching Measures (SOSM) for Digital Multiplex System (DMS) MMP.
A00002252.AA04	MG9K Lines Preprovisioning
A00002291.AA20	Trunk Offering Expansion
A00002293.AA12	Registered Call Line Option
A00002319.AA09	MWI control via ISUP

A00002364.AA08	CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20
A00002365.AA08	CWR Support over Trunks for Brazil Market
A00002377.AA12	10 AFC Keys for BRI Directory Number
A00002639.AA14	CEPT PSTN: Analogue Call Waiting Indication
A00002641.AA20	CEPT PSTN: Analogue Outgoing Call Barring
A00002642.AA14	CEPT PSTN: Analogue Query and 3Party
A00002654.AA24	CEPT AR (Class Callback)
A00002678.AA15	Telefonica IN Enhancements
A00002680.AB09	CEPT / Telefonica Spain Changed Number Indication
A00002702.AA15	No Line Origination Without Charging
A00002713.AA17	Spanish ISUP enhancements for Telefonica
A00002751.AA08	China BRI Supplementary Services using Keypad protocol
A00002754.AA12	China INAP Compliance Enhancement Part 1
A00002755.AA13	China PSTN Line Service Compliance
A00002844.AA09	Excessive Metering Detection (EMD) Support for Metered Trunks
A00002900.AA09	China INAP Compliance Enhancement Part 2
A00002904.AA12	CTI Toggle
A00002916.AA33	CS2K connectivity to XPM remote
A00003051.AA07	CFGD (Call Forward Group Don’t Answer) for BRI Hunt Groups
A00003147.AA09	DP Digit Reception Control
A00003227	SN07, IN support for User to User Service (UUS)
A00003410.AA12	Honduras ETSI ISUP variant
A00003411.AA10	New TONESET for Honduras
A00003467.AA13	Reverse Translations Enhancements via CUSTMOD Option
A00003686.AA11	Re-Routing Based on Release Cause Value
A00003696.AA15	G-ISUP Routing Enhancements

A00004205.AA12	Japan PRI Backward Voice Path Solution
A00004503.AA11	Calling Party Number Serving Country Code(SCC)
A00004563.AA12	Moroccan ISUP v2 on DMS100
A00004565.AA15	Line to Moroccan ISUP V2 interworking
A00004743.AA07	Line originations CLI modification through CALLCNTL in ISN07
A00004750.AA13	Even Bit Inversion(EBI) Support on DTCO2
A00005164.AA06	Russia ISUP V2+ on CS2K
A00005802.AA07	SPM Companding Law Provisioning

1: Configuration (CN): A00001914

1.1 Hardware and Software Requirements

1.2 Initial Configuration

1.3 Office/Subnet parameters (OP/SP) (CM & SESM)

1.4 Upgrade Impact

1.5 Data schema (DS) (CM, MIBS, RDB)

1.5.1 New/modified tables, MIBs, or Database Schema

ISERVOPT, XXCODE AND XXHEAD tables are modified.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED
ACCODE	CHANGED	UNCHANGED

1.5.2 Table/MIB/Remote Database Schema information

1.5.2.1 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

1.5.2.1.1 Functional description

This activity extends the ILRCLS tuple of the table ISERVOPT. A new subfield is added named SDT.

The extended part at ILRCLS tuple:

SDT: This field determines if special dial tone will be given to subscriber on offhook when he has ILR feature active. It can be datafilled as Y or N. Y indicates that SDT will be given and N indicates that ordinary dial tone will be given to subscriber on offhook. The default value for the field is N.

Figure 1 Example Datafill for ILRCLS tuple of ISERVOPT table

```
>table iservopt
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISERVOPT
>pos ilrcls
ILRCLS ILRCLS   Y  Y  N  $
```

1.5.2.1.2 Usage sequence and implications (CM Only)

1.5.2.1.3 There is no requirement to datafill tables in a specific order for ILR tuples.**Size**

1.5.2.1.4 Fields/OIDs

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SDT	NEW		Y, N	Determines weather Special Dial Tone should be applied to costumer on offhook when he has ILR feature active or not.

1.5.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 2 Example of table ISERVOPT datafill

```
>table iservopt
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>y
CR_PSWD:
>n
TUPLE TO BE ADDED:
ILRCLS
                                        ILRCLS Y Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

1.5.2.1.6 Table release history update

None

1.5.2.1.7 Supplementary information

None

1.5.2.1.8 Translation verification other tools

None

1.5.2.2 Name: XXCODE and XXHEAD

These translation tables.

1.5.2.2.1 Functional description

With this activity, a new translation feature function is defined as **TEMPDEACT**. It is used for temporary deactivation of a service.

This feature can be datafilled at all XXCODE and XXHEAD tables.

Not: Table ACCODE is used for CEPT feature service code datafills.

Figure 3 Example Datafill of ACCODE table for TEMPDEACT function.

```
>table accode
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ACCODE
>pos octcept 34 34
OCTCEPT 34 34 FEAT (FTR ILR) (PF 2) (MM 2 15) (FUNC TEMPDEACT) $
```

1.5.2.2.2 Fields/OIDs

Table 4 The following example shows sample datafill for table ACCODE.

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FEAT	Changed	FUNC	TEMPDEACT	Temporary deactivation

1.5.2.2.3 Datafill Example

Figure 4 Example of table ACCODE datafill

```
>table accode
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ACCODE
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
XLANAME:
>octcept
FROMD:
>34
TOD:
>34
XLASEL:
>feat
OSEL:
>pf
PFDIGS:
>2
OSEL:
>mm
MIN:
>2
MAX:
>15
OSEL:
>ftr
FTR:
>ilr
OSEL:
>func
FUNC:
>tempdeact
OSEL:
>$
TUPLE TO BE ADDED:
OCTCEPT          34          34
FEAT (PF 2) (MM 2 15) (FTR ILR) (FUNC TEMPDEACT) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

1.5.2.3 Name: ILRCLASS

International Line Restriction Class

1.5.2.3.1 Functional description

This is the new table defined by activity A00002641. It contains the barring programs for the ILR line option.

1.5.2.3.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

1.5.2.3.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ILRCLASS	0	100	Memory is statically allocated

1.5.2.3.4 Fields

The following table lists fields for ILRCLASS.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Data dictionary type	Entry	Explanation and action
KEY	New	NIL	ILRCLASS_KEY	VECTOR OF UP TO 16 CHAR'S	ILR_CLASS is the name of the barring program. It is used by the ILR line option
RCODE	NEW	NIL	TWO_DIGIT_CODE	VECTOR OF UP TO 2 DIGITS	The RCODE identifies the barring program to the subscriber. It is unique in the table or empty.
IXLAOPT	NEW	NIL	ILRCLASS_IXLA_VECTOR	VECTOR OF UP TO 32 IXLA_CLAS'S	Contains a list of international translation classes to be barred by this program

Field	New or Changed	Subfield or refinement	Data dictionary type	Entry	Explanation and action
DNOPT	NEW	NIL	ILRCLASS_DN_VECTOR	VECTOR OF UP TO 10 VECTORS OF UP TO 15 DIGITS	Contains a list of DNs which are barred additionally to the international translation classes

1.5.2.3.5 Datafill example

The following example shows sample datafill for table ILRCLASS.

Figure 5 Example entry in table ILRCLASS

```
TABLE ILRCLASS
DIDD 02 (CNTL) (ICNTL) (INTL) $(09000) (09001)$
```

1.5.2.3.6 Table release history update

ISN07: Table was created

1.5.2.3.7 Supplementary information

Barring classes in this table can only be deleted if there is no line with ILR in the office referencing this tuple.

If during an ONP from a release before this activity there are no R-codes assigned in the ILRCLS tuple in table ISERVOPT the R-Code in table ILRCLASS is left empty.

1.5.2.3.8 Translation verification other tools

ILRCLASS does not use translation verification tools.

1.6 Service Orders (SO) (CM & SESM)

1.6.1 Service order change details

1.6.2 New commands

1.6.2.1 How service order commands are presented

None

1.6.2.2 How service order options are presented

1.6.2.2.1 Description

ILR line option has been defined with activity A59019295 CEPT International Line Restriction. This ILR line option enables a subscriber to control the origination line by identifying one of the restriction classes that restrict certain dialled numbers.

For detailed information about ILR line option, please refer to the activity A59019295 CEPT International Line Restriction.

Two new restriction classes are added with this activity. These are:

- **DNATL (Deny only NATional):** In this restriction class, only outgoing national calls will be restricted while other call classes are not.
- **DLCL (Deny only LoCaL):** In this restriction class, only outgoing local calls will be restricted while other call classes are not.

1.6.2.2.2 Example

Figure 6 Example of the ILR option in prompt mode

```
SO:
>ado
SONUMBER:    NOW   3  4 11 AM
>
DN_OR_LEN:
>7835482
OPTION:
>ilr
ILRCLASS:
>a
A
 ***  ERROR  ***
|
TYPE OF ILRCLASS IS ILR_CLASS
PLEASE ENTER:
ILRCLASS:
>a
A
 ***  ERROR  ***
|
TYPE OF ILRCLASS IS ILR_CLASS
TYPE    IS  ILR_CLASS  {NIL,DABE,DNI,DAI,DIDD,DNID,DSSV,DABLE,DANID,
                        DNIC,DAIC, DANI,DAT,DOC,DNATL, DLCL}
PLEASE ENTER:
ILRCLASS:
>dlcl
ILRPW:
>nnnn
ILRACTIVE:
>n
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 11 AM 7835482 ( ILR DLCL NNNN N ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 7 Example of the ILR option in no-prompt mode

```
>ado $ 7835482 ilr dnatl  nnnn n $ yy
COMMAND AS ENTERED:
ADO NOW 3 4 11 PM 7835482 ( ILR DNATL  NNNN N ) $
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
```

1.6.2.2.3 Option prompts

Two new restriction classes have been added. Other parameters are not changed.

Table 7 System prompts for the ILR option

Prompt	Valid input	Description	Areas affected by prompts
OPTION	ILR	ILR Line Option	OPTION
ILRCLASS	NIL, DIDD, DAI, DNI, DNID, DABE, DSSV, DANID, DABLE, DNIC, DAIC, DANI, **DNATL, DLCL**	Line Restriction Classes	OPTION
ILRPW	NNNN	Pass Code (including 4 digits)	OPTION
ILRACTIVE	Y, N	Status Flag of ILR Line Option	OPTION

1.6.2.2.4 Line class code compatibility

Table 8 ILR compatibility to LCC

Line class code	Compatible?
IBN	YES

1.6.2.2.5 Assignability

The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

1.6.2.2.6 Option prerequisites

ILR has the following prerequisites:

CEPT line option must be assigned to IBN line before the assignment of ILR line option to this line.

1.6.2.2.7 Notes
None.

1.6.2.2.8 Feature identification
Functionality: ISRV

Feature number: 59019295

1.6.2.2.9 SERVORD+ Exceptions
None.

1.7 Software optionality control (SOC)
N/A.

1.8 Element Management
N/A.

1.9 Command interface changes
N/A.

1.10 Security
N/A.

1.11 Configuration Walkthrough
N/A.

2: Configuration (CN): A00001918

2.1 Hardware and Software Requirements

2.2 Initial Configuration

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

2.4 Upgrade Impact

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name:ISERVOPT

This table is used to configure switch wide information for service related feature.

2.5.2.1.1 Functional description

This activity introduces a new tuple named as CEPT_ANN in ISERVOPT table and a new field SPECIAL_DIAL_TONE for the existing tuple CEPT_CFX.

Fields of the **CEPT_ANN** tuple ;

ANN_STATE: This field can be datafilled with one of the following;

- **DIAL_TONE** : For providing dial tone until the announcement returns to the beginning
- **SPECIAL_DIAL_TONE** : For providing special dial tone until the announcement returns to the beginning
- **IMMEDIATELY** : For providing the announcement immediately

CEPTANNS : This field consists of the following options

- **CFU :** For providing CFU warning announcement,
- **CFB :** For providing CFB warning announcement,
- **CFD :** For providing CFD warning announcement,
- **CDND :** For providing CDND warning announcement,
- **CDTA :** For providing CDTA warning announcement,
- **CDTO :** For providing CDTO warning announcement,
- **IWUC :** For providing WAKEUP warning announcement,

New field for the existing **CEPT_CFX** tuple ;

SPECIAL_DIAL_TONE : This field can be datafilled with one of the following;

- **Y** : The subscriber gets special dial tone when he goes off hook.
- **N** : The subscriber gets dial tone when he goes off hook.

2.5.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

2.5.2.1.4 Fields/OIDs

The following table lists fields for table ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	NEW		CEPT_ANN	This is the key in ISERVOPT
OPTION	NEW		CEPT_ANN	This is the option name
ANN_STATE	NEW			This field consists of one of the below options

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIAL_TONE SPECIAL_DIAL_TONE IMMEDIATELY	NEW NEW NEW			Announcement state options
CEPTANNS	NEW			This field consists of the below options
CFU CFB CFD CDND CDTA CDTO IWUC	NEW NEW NEW NEW NEW NEW NEW			CEPT Announcement options
SOPTSKEY	OLD		CEPT_CFX	This is the key in ISERVOPT
OPTION	OLD		CEPT_CFX	This is the option name
SPECIAL_DIAL_TONE	NEW			Boolean; Datafilled as **Y** or **N**

2.5.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 Example of table ISERVOPT datafill

```
>table iservopt
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_ann
OPTION:
>cept_ann
ANN_STATE:
>IMMEDIATELY
CEPTANNS:
>CFU
CEPTANNS:
>CFB
CEPTANNS:
>CFD
CEPTANNS:
>CDND
CEPTANNS:
>CDTA
CEPTANNS:
>CDTO
CEPTANNS:
>IWUC
TUPLE TO BE ADDED:
CEPT_ANN CEPT_ANN IMMEDIATELY (CFU) (CFB) (CFD) (CDND) (CDTA) (CDTO)
(IWUC) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Figure 2 Example of table ISERVOPT datafill

```
>lis
SOPTSKEY SOPTSVAR
-----------------
CEPT_ANN CEPT_ANN IMMEDIATELY (CFU) (CFB) (CFD) (CDND) (CDTA) (CDTO)
(IWUC) $
```

Figure 3 Example CEPT_CFX tuple of table ISERVOPT datafill

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>cept_cfx
OPTION:
>cept_cfx
OPTIONAL_HASH:
>y
FROM_RANGE:
>1
TO_RANGE:
>18
PRG_OVERRIDE:
>y
ACTIVATE_WITHOUT_PRG:
>y
ISUP_RESTRICTION:
>n
CDND_BSY_TRTMT_SUPP:
>n
MULTIPLE_CFX_ACTIVE:
>n
CFRA_ANNC:
>n
SPECIAL_DIAL_TONE:
>y
CFD_CFB_INDICATION:
>y
TUPLE TO BE ADDED:
CEPT_CFX CEPT_CFX Y 1 18 Y Y N N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Figure 4 Example CEPT_CFX tuple of table ISERVOPT datafill

```
>lis
SOPTSKEY SOPTSVAR
-----------------
CEPT_CFX CEPT_CFX Y 1 18 Y Y N N N N Y Y
```

2.5.2.1.6 Table release history update

This feature adds a new tuple named as **CEPT_ANN** in **ISERVOPT** table. The fields of this new tuple is used for providing the CEPT warning announcement when the subscriber goes off hook.

ANN_STATE field indicates the status of the announcement to be given and can be datafilled with one of **DIAL_TONE, SPECIAL_DIAL_TONE** or **IMMEDIATELY.**

CEPTANNS field is datafilled with the feature options which have warning announcements. These options are;

CFU, CFB, CFD, CDND, CDTA, **CDTO** and **IWUC**

Also a new field **SPECIAL_DIAL_TONE** is implemented for the existing tuple **CEPT_CFX**. This field is datafilled as **Y** or **N**. According to this datafill the user hears special dial tone or only normal dial tone when he goes off hook.

2.5.2.1.7 Supplementary information

2.5.2.1.8 Translation verification other tools

2.6 Service Orders (SO) (CM & SESM)

2.7 Software optionality control (SOC)

2.8 Element Management

2.9 Command interface changes

2.10 Security

2.11 Configuration Walkthrough

3: Configuration (CN): A00001919

3.1 Hardware and Software Requirements

3.2 Initial Configuration

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

3.4 Upgrade Impact

3.5 Data schema (DS) (CM, MIBS, RDB)

3.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

3.5.2 Table/MIB/Remote Database Schema information

3.5.2.1 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

3.5.2.1.1 Functional description

This activity introduces a new tuple named as CEPTPW in ISERVOPT table.

Fields of the **CEPTPW** tuple:

MAX_PIN_RETRY: indicates that how many times that subscriber can enter wrong pin sequentally while doing password related issues.

DEFAULT_PIN: indicates that the initial pin when administrator assigns this feature (CEPTPW) to the subscriber.

PIN_VALIDATION {BOOLEAN}: indicates that changing of unique password of which all digits are same as each other such as ‘2222 or 3333’ is disallowed or allowed. If it is set as ‘Y’, PIN validity is on and such PIN

programming is not allowed and subsciber will get NACK tone or related announcement; otherwise, tones are applied instead of announcements.

ANNOUNCE: indicates the announcements are used instead of tones (SDT, SIT) while subscriber actions to control password related CEPT features. Announcements will be applied to the subscriber if it is set as 'Y'; otherwise tones are used instead of announcements.

ANNOUNCE_STATE {SILENCE, AUD_ RNG}: indicates that the subscriber hears only silence or audible ringing until the announcement retuns to the beginning, then he listens related announcement. **This field is visible only if ANNOUNCE field is set as 'Y'; otherwise it is unvisible because there is no need to define announcement state since tones are used instead of them.**

CEPT_ANNCS {CEPT_ANNC_VECTOR}: indicates the used announcements in CEPTRA and CEPTPW features and the corresponding announcement trunk which is connected for the entered announcement name.

- The entered CLLIs should be an announcement trunk CLLI, otherwise an error message is occured "**DATAFILL FOR** *ENTERED_CLLI* **MISSING IN TABLE ANNS**" where ENTERED_CLLI is the provisioned CLLI.
- The announcement name should not be entered more than once, otherwise an error message is occured "**ANNOUNCEMENT TYPE (***announcement_ID***) IS DUPLICATED**", where announcement_ID (CHGPIN, LOCKED, VLDPIN, DNPIN, SCODE) is provisioned more than once.
- In case of non-existance of the announcement trunks in table ANNMEMS, there is a warning message "**Warning: DATAFILL FOR** *ENTERED_CLLI* **MISSING IN TABLE ANNMEMS**.", where ENTERED_CLLI is the provisioned CLLI.
- This feature supports only STANDART announcements, so in case of CUSTOM announcement provisioning, there occurs an error message "**ANNC CLLI** *ENTERED_CLLI* **MUST BE A STANDARD ANNOUNCEMENT**", where ENTERED_CLLI is the provisioned CLLI of which announcement type is CUSTOM.

3.5.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

3.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

3.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	NEW		CEPTPW	This is the key in ISERVOPT
OPTION	NEW		CEPTPW	This is the option name
MAX_PIN_RETRY	NEW		0 TO 9	If ‘0’ is entered, there is no limit for wrong pin entry.
DEFAULT_PIN	NEW		0000 TO 9999	Default PIN of CEPTPW
PIN_VALIDATION	NEW		Y, N	to control programming of a unique password of which digits are same as each other
ANNOUNCE	NEW		Y, N	for selecting announcements or tones are used
ANNC_STATE	NEW		SILENCE, AUD_ RNG	for selecting what subscriber hears (audible_ring or silence) while announcement returns to beginning.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

CEPT_ANNC	NEW		{
			{
			CHGPIN,
			LOCKED,
			VLDPIN,
			DNPIN,
			SCODE
			},
			CLLI
			}
				Related announcements
				
				The announcements used by the CEPTRA & CEPTPW and corresponding announce CLLI can be entered for each ANNAME field. To terminate $ should be entered for this field.

3.5.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT

Figure 1 Example of ISERVOPT table datafill (ANNOUNCE is 'Y')

```
>table iservopt
>add
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT PIN:
>1111
PIN_VALIDATION:
>y
ANNOUNCE
>y
ANNC_STATE:
>SILENCE
CEPT_ANNCS:
>dnpin ceptann_dnpin
CEPT_ANNCS:
>chgpin ceptann_chgpin
CEPT_ANNCS:
>vldpin ceptann_vldpin
CEPT_ANNCS:
>$
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1234 Y Y AUD_RNG (DNPIN CEPTANN_DNPIN)
(CHGPIN CEPTANN_CHGPIN) (VLDPIN CEPTANN_VLDPIN) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

ANNC_CLLIs should be provisioned with the real announcement trunk CLLIs which are provisioned in TABLE ANNS.

Figure 2 The View of CEPTPW Tuple in ISERVOPT Table (ANNOUNCE is 'Y')

```
>table iservopt

SOPTSKEY                                                SOPTSVAR
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
CEPTPW  CEPTPW 3 1111 Y Y SILENCE (DNPIN CEPTANN_DNPIN) (CHGPIN CEPTANN_CHGPIN)
(VLDPIN CEPTANN_VLDPIN)$
```

Figure 3 Example of ISERVOPT table datafill (ANNOUNCE is 'N')

```
>table iservopt
>add
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT PIN:
>1111
PIN_VALIDATION:
 >y
ANNOUNCE
 >n
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1111 Y N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Figure 4 The View of CEPTPW Tuple in ISERVOPT Table (ANNOUNCE is 'N')

```
>table iservopt

SOPTSKEY                                          SOPTSVAR
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
CEPTPW  CEPTPW                                   3 1111 Y N$
```

There is no restriction to remove this tuple, however since CEPTPW feature is working according the values in this tuple, CEPTPW can not activated/ programmed even if it is already on agent in case of this tuple removal.

Because of this reason, during CEPTPW tuple deletion there is a warning message displayed to warn the operator as:

"**WARNING: CEPTPW can be on any agent or default CEPT feature. WARNING: CEPTPW does not work without this tuple.**"

3.5.2.1.6 Table release history update

3.5.2.1.7 Supplementary information

3.5.2.1.8 Translation verification other tools.

3.6 Service Orders (SO) (CM & SESM)

3.6.1 Service order change details

3.6.1.1 LCC and options

CEPTPW line option is created with this activity and can be assigned to each IBN and ETSI ISDN BRI line via service order session.

3.6.1.1.1 Incompatible options

AUL is incompatible with CEPTPW option

Table 4 Meridian digital centrex feature assignment requirements

Feature	500 2500	IBN	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
					SET	SUBSET	KEY	DN	DEDKEY	LAMP	CODE	DISPLAY
CEPTPW	N	Y	N	Y				X				

This feature must be assigned to any key on which DN is defined.

3.6.2 New commands

3.6.2.1 How service order commands are presented

None

3.6.2.2 How service order options are presented

3.6.2.2.1 Description

CEPTPW option is introduced with this activity. CEPTPW option provides password enhancement for CEPT features by introducing a unique password for the subscriber. This password is valid for the features which are ILR (International Line Restriction) and OCB (Outgoing Call Barring).

Subscriber can use this unique password to control these features, and this password can be activated, changed and interrogated by subscriber. This unique password is used for existing password controlled features ILR, OCB and new feature CEPT Features Remote Access which is also introduced with this activity.

3.6.2.2.2 Example

CEPTPW could be assigned both IBN and ETSI ISDN BRI lines.

The administrator is authorized to assign, deassign, activate or deactivate CEPTPW to IBN and ETSI ISDN BRI lines via service order.

If CEPTPW line option is to be assigned to a subscriber not having CEPT option for IBN lines, a message "**Can not add CEPTPW option if line does not have CEPT option, firstly add CEPT line option**" is printed on screen.

The administrator should enter the status of the CEPTPW while performing servord actions.

The administrator can apply the following operations via Service Order:

Assignment: STATUS field should be entered as 'DEACTIVE'. This means subscriber should activate password by using password changing sequence.

'LOCKED' or 'ACTIVE' as STATUS can not be entered by administrator during assignment via Service Order. An error message ' **STATUS should be datafilled as DEACTIVE**'.

An example of CEPTPW assignment is shown in figure 5 and figure 6for IBN lines, figure 7 and 8 for BRI lines.

Deassignment: The CEPTPW option is deassigned form a line by using DEO (Delete Option) command via Service Order.

An example of CEPTPW deassignment is shown in figure 9 and figure 10 for IBN lines, figure 11 and 12 for BRI lines.

Administrator Activation: The administrator can activate the CEPTPW if and only if CEPTPW is in "LOCKED" state which means subscriber is prohibited to control password related CEPT features due to maximum wrong

pin entry. Otherwise, CEPTPW is not in 'LOCKED' state, an error message '**CEPTPW should be in LOCKED state**' is printed.

This action is performed when subscriber remembers the old PIN and wants to continue using this PIN as CEPT password.

An example of CEPTPW activation is shown in figure 13 and figure 14 for IBN lines, figure 15 and figure 16 for BRI lines.

Administrator Deactivation: The administrator may deactivate the CEPTPW on a subscriber line by using the CHF (Change Feature) command, this action can be performed if and only if CEPTPW is already in "ACTIVE" or "LOCKED" states. "LOCKED" state means subscriber is prohibited to control password related CEPT features due to maximum wrong pin entry. Otherwise, CEPTPW is not in "ACTIVE" or 'LOCKED' state, an error message '**CEPTPW should be in LOCKED or ACTIVE state**' is printed.

This action is performed when subscriber does not remember the old PIN and wants to use default password as CEPT password. However, subscriber should have activate the CEPTPW after this function because it is now in DEACTIVE state.

An example of CEPTPW activation is shown in figure 17 and figure 18 for IBN lines, figure 19 and figure 20 for BRI lines.

Figure 5 Example of the CEPTPW assignment to IBN line in prompt mode

```
>servord
SO:
>ado
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
---------------------------------------------------------------------------------------
>qdn 7835487
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DN:       7835487
NAME: UNASSIGNED
TYPE: SINGLE PARTY
LINESNPA: 111   SIG: DT    LNATTIDX:    1
LINE EQUIPMENT NUMBER:     HOST  00 0 00 04
LINE CLASS CODE:      STD
LINE TREATMENT GROUP:     0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    45
PM TERMINAL NUMBER :    5
OPTIONS
DGT  CEPT  CEPTPW  DEACTIVE
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 6 Example of the CEPTPW assignment to IBN line in no-prompt mode

```
>SERVORD
SO:
> ADO $ 7835487 CEPTPW DEACTIVE $
```

Figure 7 Example of the CEPTPW assignment to BRI line in prompt mode

```
>servord
SO:
>ado
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
>1
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
>qdn 7831012
------------------------------------------------------------------------------
DN:    7831012
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN1      2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC
CEPTPW DEACTIVE

------------------------------------------------------------------------------
```

Figure 8 Example of the CEPTPW assignment to BRI line in no-prompt mode

```
>SERVORD
SO:
> ADO $ 7831012 1 CEPTPW DEACTIVE $
```

Figure 9 Example of the CEPTPW deassignment from IBN line in prompt mode

```
>servord
SO:
>deo
SONUMBER:    NOW  0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 0 2 15 AM  7835487 (CEPTPW) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY?  (Y OR N)
>y
```

Figure 10 Example of the CEPTPW deassignment from IBN line in no-prompt mode

```
>SERVORD
SO:
> DEO $ 7831012 CEPTPW $
```

Figure 11 Example of the CEPTPW deassignment from BRI line in prompt mode

```
>servord
SO:
>deo
SONUMBER:    NOW  0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY
>1
OPTION:
>ceptpw
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 0 2 15 AM  7835487 (CEPTPW) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY?  (Y OR N)
>y
```

Figure 12 Example of the CEPTPW deassignment from BRI line in no-prompt mode

```
>SERVORD
SO:
> DEO $ 7831012 1 CEPTPW $
```

Figure 13 Example of the CEPTPW activation to IBN line in prompt mode

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>ACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW ACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
```

Figure 14 Example of the CEPTPW activation to IBN line in no-prompt mode

```
>SERVORD
SO:
> CHF $ 7835487 CEPTPW ACTIVE $
```

Figure 15 Example of the CEPTPW activation to BRI line in prompt mode

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
> 1
OPTION:
>ceptpw
STATUS:
>ACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW ACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
```

Figure 16 Example of the CEPTPW activation to BRI line in no-prompt mode

```
>SERVORD
SO:
> CHF $ 7831012 1 CEPTPW ACTIVE$
```

Figure 17 Example of the CEPTPW deactivation to IBN line in prompt mode

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7835487
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7835487 (CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
```

Figure 18 Example of the CEPTPW deactivation to IBN line in no-prompt mode

```
>SERVORD
SO:
> CHF $ 7835487 CEPTPW DEACTIVE $
```

Figure 19 Example of the CEPTPW deactivation to BRI line in prompt mode

```
>servord
SO:
>chf
SONUMBER:    NOW   0  2 15 AM
>
DN_OR_LEN:
>7831012
OPTKEY:
> 1
OPTION:
>ceptpw
STATUS:
>DEACTIVE
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 0 2 15 AM 7831012 ( 1 CEPTPW DEACTIVE) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y  OR  N)
>y
```

Figure 20 Example of the CEPTPW deactivation to BRI line in no-prompt mode

```
>SERVORD
SO:
> CHF $ 7831012 1 CEPTPW DEACTIVE $
```

3.6.2.2.3 Option prompts

The system prompts for CEPTPW are shown in order of their appearance.

Table 5 System prompts for CEPTPW option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	CEPTPW	CEPTPW line option	OPTION
STATUS	DEACTIVE, ACTIVE, LOCKED	state of the CEPTPW feature	OPTION

3.6.2.2.4 Line class code compatibility

Table 6 CEPTPW compatibility to LCC

Line class code	Compatible?
IBN	Yes
BRI	Yes

3.6.2.2.5 Assignability

The following functionalities apply to this option to ETSI ISDN BRI:

- set functionality: No
- subset functionality: No
- DN functionality: Yes
- key functionality: No

3.6.2.2.6 Option prerequisites

CEPTPW has the following prerequisites:

CEPT line option must be assigned to IBN line before the assignment of CEPTPW line option to this line.

3.6.2.2.7 Notes

None

3.6.2.2.8 Feature identification

Functionality: None

Feature number: A00001919

3.6.2.2.9 SERVORD+ Exceptions

3.7 Software optionality control (SOC)

3.8 Element Management

3.9 Security

3.10 Configuration Walkthrough

4: Configuration (CN): A00001920

4.1 Hardware and Software Requirements

N/A

4.2 Initial Configuration

N/A

4.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

4.4 Upgrade Impact

None

4.5 Data schema (DS) (CM, MIBS, RDB)

4.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MTRDEASS	NEW	NEW

4.5.2 Table/MIB/Remote Database Schema information

4.5.2.1 Name: MTRDEASS

Deassigned meters table.

4.5.2.1.1 Functional description

MTRDEASS table is used to keep deassigned meters of subscriber to be able to restore them when a MOG reprovisioning is done.

A new tuple is added to this table when a MOG deletion is performed and tuple is deleted when agent is assigned with same MOG option.

4.5.2.1.2 Usage sequence and implications (CM Only)

User has no chance to datafill MTRDEASS table. Entries are added into this table internally. But in order to be able add a tuple into MTRDEASS table internally, world metering tables are needed to be available in office.

4.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MTRDEASS	0	65536	Memory is allocated automatically for each new tuple.

4.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for MTRDEASS table.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DEAKEY	New	None	Up to 18 digits	Directory Number of subscriber
METER1	New	None	00000000 - 99999999	Meter Counts of deassigned meter
WRAP1	New	None	Y/N/-	Indicates whether counts are wrapped or not.
METER2	New	None	00000000 - 99999999	Meter Counts of deassigned meter
WRAP2	New	None	Y/N/-	Indicates whether counts are wrapped or not.
METER3	New	None	00000000 - 99999999	Meter Counts of deassigned meter
WRAP3	New	None	Y/N/-	Indicates whether counts are wrapped or not.
METER4	New	None	00000000 - 99999999	Meter Counts of deassigned meter
WRAP4	New	None	Y/N/-	Indicates whether counts are wrapped or not.
OUTDATE	New	None	YYYY/MM/DD HH:MM:SS	Date of deassigning meters

4.5.2.1.5 Datafill example

The following example shows sample datafill for table MTRDEASS.

```
TABLE MTRDEASS
TOP

DEAKEY      METER1 WRAP1 METER2 WRAP2 METER3 WRAP3 METER4 WRAP4 OUTDATE
-------------------------------------------------------------------------------------------------------------------------------
1027835401  00000012    N   00000015    N   00000020    N   --------    -   2003/03/31 16:03:56

BOTTOM
```

4.5.2.1.6 Table release history update

MTRDEASS table is introduced in ISN07. Maximum table size of 65536 tuples for deassigned meters.

4.5.2.1.7 Supplementary information

- Tuples of MTRDEASS table can not be changed or deleted.
- New tuples can not be added manually.
- When maximum number of tuples is reached, MTR150 log is generated.

4.5.2.1.8 Translation verification other tools

MTRDEASS table does not use translation verification tools.

4.6 Service Orders (SO) (CM & SESM)

N/A

4.7 Software optionality control (SOC)

There are two new SOC options that are introduced with this feature; *METR_Deassigned_Support* and *METR_Prevent_Sent_OOS*.

METR_Deassigned_Support is defined under METR SOC group. Functionality of feature is controlled with this SOC option. It is a state SOC, whose states can be ON or IDLE. When state of *METR_Deassigned_Support* is ON, feature becomes functional.

Table 4 METR_Deassigned_Support SOC

SOC option name:	METRxxxx
SOC option title:	METR_Deassigned_Support
SOC option control type:	state
New SOC option?	Yes
SOC option order code	METRxxxx

Table 4 METR_Deassigned_Support SOC

Option defined in DRU:	WT
Affected products:	ISN07

The second SOC, *METR_Prevent_Sent_OOS*, is defined under METR SOC group and it is used to decide sending recycled meters to OOS or not. For Bangladesh, recycled meters should not be sent to OOS. So when this SOC is ON, sending recycled meters to OOS is prevented.

Table 5 METR_Prevent_Sent_OOS SOC

SOC option name:	METRxxxx
SOC option title:	METR_Prevent_Sent_OOS
SOC option control type:	state
New SOC option?	Yes
SOC option order code	METRxxxx
Option defined in DRU:	WT
Affected products:	ISN07

There is a dependency between these two SOC options. *METR_Deassigned_Support* can not be made IDLE when *METR_Prevent_Sent_OOS* is ON. Furthermore, *METR_Prevent_Sent_OOS* can be made ON only when *METR_Deassigned_Support* is ON.

4.8 Element Management

N/A

4.9 Command interface changes

4.9.1 Directory: <directory name/MAP level>

4.9.2 Command: DEASSCLR

Clear Deassigned Meters

4.9.2.1 Command type: NON-MENU

4.9.2.2 Command target: BRISC, XACORE

4.9.2.3 Command availability: NONRES

4.9.2.4 Command description

This command is used to clear all content of MTRDEASS table.

4.9.2.5 Command syntax

There is no parameter for DEASSCLR command.

Table 6 DEASSCLR command parameters and variables

Command	Parameters and variables
DEASSCLR	N/A

4.9.2.6 Qualifications and warnings

A warning message is displayed to inform user about loss of deassigned meter data.

4.9.2.7 Responses

After displaying warning message, user is asked to confirm his/her request since executing command results with loss of deassigned meter data.

4.9.2.7.1 Confirmation Message

Y: content of MTRDEASS table is cleared

N: user gives up clearing the content of MTRDEASS table.

Table 7 MAP outputs with associated meanings and actions

Command: DEASSCLR
WARNING: All deassigned meters data will be lost. Do you wish to continue? Please confirm (“Yes”, “Y’, “No”, “N”). **Meaning:** This response warns user that all tuples in MTRDEASS table are cleared and this result with loosing meter counts of deassigned meters. **System or user actions:** User should select Yes/Y to continue or No/N to give up.

4.9.2.8 Example

Table 8 Usage examples for DEASSCLR command

Description of task:	
Description of task	Clear all content of MTRDEASS table

Table 8 Usage examples for DEASSCLR command

Command:	>DEASSCLR
MAP response:	>WARNING: All deassigned meters data will be lost. Do you wish to continue? Please confirm (“Yes”, “Y”, “No”, “N”). >Y >Table MTRDEASS is cleared...

4.10 Security

N/A

4.11 Configuration Walkthrough

N/A

5: Configuration (CN): A00001921

5.1 Data schema (DS) (CM, MIBS, RDB)

5.1.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	CHANGED	UNCHANGED
ISERVOPT	CHANGED	UNCHANGED

5.1.2 Table/MIB/Remote Database Schema information

5.1.2.1 Name: TRKOPTS

Trunk options

5.1.2.1.1 Functional description

Table TRKOPTS is used to give trunk group specific options to trunk groups. LDA trunk group option gives ability of toll call ringing to the terminating exchange office.

If CLI is not available then the toll call recognition is done depending on the value of ALERT_NO_CLID of the new tuple LDA in table ISERVOPT.

If it's value is Y, then distinctive alerting is provided to the terminating line.

If it's value is N, feature processing will continue to check table TRKOPTS for an alerting indication. Incoming trunk CLLI with LDA option is searched in the table TRKOPTS for toll call determination. If found incoming trunk CLLI with LDA option in table TRKOPTS is ETSI ISUP V2+,the value of CHECK_NOA field is seen. If this field is datafilled as Y, local terminating exchange checks the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message and applies toll call ringing patterns to terminating line if NOA is equal to:

- National Number
- International Number

If this CHECK_NOA field is datafilled as N, toll call ringing pattern is applied to the terminating line.

5.1.2.1.2 Usage sequence and implications (CM Only)

The current datafill sequence will be changed to datafill LDA option to the trunk group. TRKGRP and TRKSGRP datafill of this trunk group must be done before LDA option is datafilled to the table TRKOPTS.

5.1.2.1.3 Size

Unchanged.

5.1.2.1.4 Fields/OIDs

The following table lists fields/OIDs for table TRKOPTS

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Changed	CLLI TRKOPTS_OPTION	CLLI name of any incoming or 2-way trunks. LDA	Trunk group name datafilled in table CLLI and LDA trunk group option.
OPTINFO	Changed	OPTION CHECK_NOA	LDA BOOLEAN	LDA trunk group option and CHECK_NOA field with boolean entry.

5.1.2.1.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

Figure 1 Example of datafilling of the LDA tuple in TRKOPTS table

```
> table trkopts
>add
SOPTSKEY:
>icrsisupba    lda
OPTION:
>lda
CHECK_NOA:
>y
```

Figure 2 The View of LDATuples in TRKOPTS Table

```
>table trkopts

 OPTKEY                                                    OPTINFO
-------------------------------------------------------------------------
 ICRSISUPBA      LDA                                  LDA        Y
```

5.1.2.1.6 Table release history update

ISN07 ACT.A00001921 “CIS Toll Call Ringing”

5.1.2.1.7 Supplementary information

A new field “CHECK_NOA” is added to the existing tuple related with “LDA” feature in table TRKOPTS.

CHECK_NOA : If CLLI is a ETSI ISUP V2+ trunk group, this field is checked to apply toll ringing to the terminating line. If this field is Y, local terminating exchange checks the Nature of Address (NOA) indicator of called party number parameter in received ISUP_IAM message and applies toll call ringing patterns to terminating line if NOA is equal to:

- National Number
- International Number

If this CHECK_NOA field is datafilled as N, toll call ringing pattern is applied to the terminating line.

The default value of CHECK_NOA field will be N.

LDA option can be given to only incoming trunks. If the administrator tries to give this option to outgoing trunks, the following error is displayed.

“ LDA option can only be assigned to incoming and 2W trunks”

To datafill LDA option in TRKOPTS, table TRKSGRP must be datafilled for the CLLI before. If this condition is not satisfied, the following error is generated.

“ Trunk not datafilled in Table TRKSGRP.

Datafill Table TRKSGRP with the CLLI first.”

5.1.2.1.8 Translation verification other tools

N/A.

5.1.2.2 Name: ISERVOPT

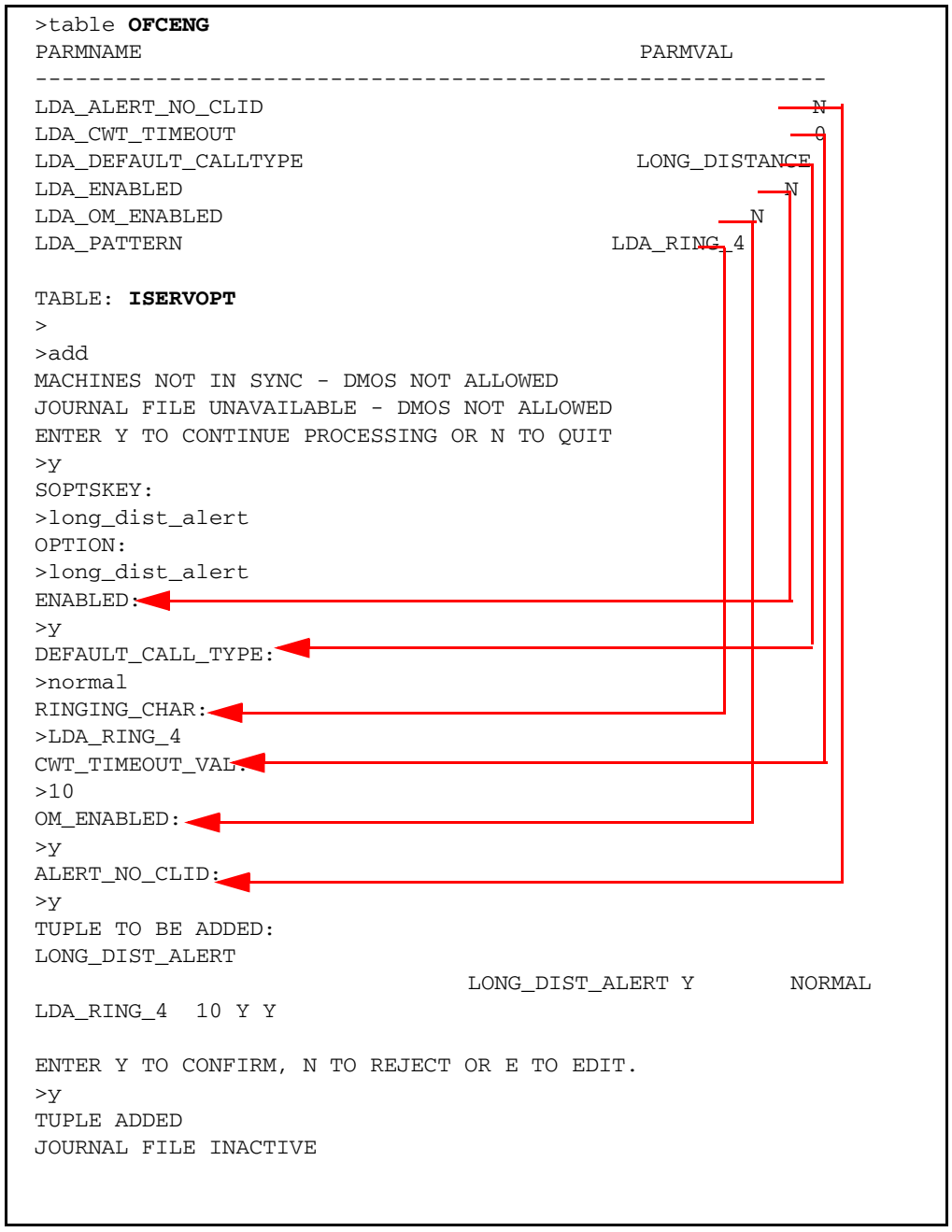
This table is used to configure switch wide information for service related feature.

5.1.2.2.1 Functional description

This activity introduces a new tuple named as LONG_DIST_ALERT in ISERVOPT table.

Existing office parameters LDA_ENABLED, LDA_DEFAULT_CALLTYPE, LDA_OM_ENABLED, LDA_ALERT_NO_CLID, LDA_CWT_TIMEOUT, LDA_PATTERN in table OFCENG are moved to the new tuple "LONG_DIST_ALERT" in table ISERVOPT.

Table 3 Remove from table OFCENG to table ISERVOPT



```
>table OFCENG
PARMNAME                                          PARMVAL
-----------------------------------------------------------
LDA_ALERT_NO_CLID                                       N
LDA_CWT_TIMEOUT                                         0
LDA_DEFAULT_CALLTYPE                       LONG_DISTANCE
LDA_ENABLED                                             N
LDA_OM_ENABLED                                      N
LDA_PATTERN                                LDA_RING_4

TABLE: ISERVOPT
>
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>long_dist_alert
OPTION:
>long_dist_alert
ENABLED:
>y
DEFAULT_CALL_TYPE:
>normal
RINGING_CHAR:
>LDA_RING_4
CWT_TIMEOUT_VAL:
>10
OM_ENABLED:
>y
ALERT_NO_CLID:
>y
TUPLE TO BE ADDED:
LONG_DIST_ALERT
                                  LONG_DIST_ALERT Y       NORMAL
LDA_RING_4  10 Y Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

5.1.2.2.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order for LONG_DIST_ALERT tuples.

5.1.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

5.1.2.2.4 Fields/OIDs

The following table lists fields/OIDs for table ISERVOPT

Table 5 Field descriptions for LDA tuple in ISERVOPT table

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	NEW		LONG_DIST_ALERT	This is the key in ISERVOPT
OPTION	NEW		LONG_DIST_ALERT	This is the option name
ENABLED	NEW		Y,N	Long distance alert(LDA) enabled field.The field that are supported by the market can be entered.
DEFAULT_CALL_TYPE	NEW		NORMAL,LONG_DISTANCE	LDA default call type field.The field that are supported by the market can be entered.
RINGING_CHAR	NEW		LDA_RING_1, LDA_RING_2, LDA_RING_3, LDA_RING_4, LDA_RING_5, LDA_RING_6, LDA_RING_7, LDA_RING_8	LDA pattern field.The field that are supported by the market can be entered.
CWT_TIMEOUT_VAL	NEW		0 TO 316	LDA cwt timeout value field.The field that are supported by the market can be entered.
OM_ENABLED	NEW		Y,N	LDA om enabled field.The field that are supported by the market can be entered.
ALERT_NO_CLID	NEW		Y,N	LDA alert no CLID field.The field that are supported by the market can be entered.

5.1.2.2.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 3 Example of datafilling of the LONG_DIST_ALERT tuple in ISERVOPT table

```
> table iservopt
>add
SOPTSKEY:
>long_dist_alert
OPTION:
> long_dist_alert
ENABLED:
>y
DEFAULT_CALL_TYPE:
>LONG_DISTANCE
RINGING_CHAR:
> LDA_RING_4
CWT_TIME_OUT_VAL:
>10
OM_ENABLED:
>y
ALERT_NO_CLID:
>y
```

Figure 4 The View of LONG_DIST_ALERT Tuples in ISERVOPT Table

```
>table iservopt

SOPTSKEY                                                SOPTSVAR
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
LONG_DIST_ALERT   LONG_DIST_ALERT   Y   LONG_DISTANCE
                                        LDA_RING_4  10    Y     Y
```

5.1.2.2.6 Table release history update

ISN07 ACT.A00001921 “CIS Toll Call Ringing”

5.1.2.2.7 Supplementary information

A new tuple with a symbol “LONG_DIST_ALERT” is added to the table ISERVOPT to provide CIS market requirement related with “Toll Call Ringing” feature. The sub fields of this new tuple will be “ENABLED”, “DEFAULT_CALL_TYPE”, “RINGING_CHAR”, “CWT_TIME_OUT_VAL”, “OM_ENABLED” and “ALERT_NO_CLID”.

ENABLED : This is moved from table OFCENG-LDA_ENABLED parameter to table ISERVOPT under new ENABLED field of new tuple. This field is used to activate or deactivate LDA functionality office-wide. If it is set

to N, LDA functionality is available to none of the lines in the switch. Its default value will be N.

DEFAULT_CALL_TYPE : This is moved from table OFCENG-LDA_DEFAULT_CALL_TYPE parameter to table ISERVOPT under new DEFAULT_CALL_TYPE field of new tuple. This field is used to determine the call type if it is not able to identify the type of the call by screening through the table LDASCRN. It takes the value of NORMAL or LONG_DISTANCE. Its default value will be LONG_DISTANCE.

RINGING_CHAR : This is moved from table OFCENG-LDA_PATTERN parameter to table ISERVOPT under new RINGING_CHAR field of new tuple. This field is used to determine which toll ringing pattern is applied to the terminating line.

CWT_TIME_OUT_VAL : This is moved from table OFCENG-LDA_CWT_TIMEOUT parameter to table ISERVOPT under new CWT_TIME_OUT_VAL field of new tuple. This field gives the operating company the ability to force a toll call that is call waited for more than a specified duration to be routed to the NTRS treatment. The parameter allows the operating company to specify the length of this duration. Its default value will be 0.

OM_ENABLED : This is moved from table OFCENG-LDA_OM_ENABLED parameter to table ISERVOPT under new OM_ENABLED field of new tuple.This field turns OM pegging ON or OFF. Its default value will be N.

ALERT_NO_CLID : This is moved from table OFCENG-LDA_ALERT_NO_CLID parameter to table ISERVOPT under new ALERT_NO_CLID field of new tuple.This field allows the operating company to specify whether distinctive alerting should be provided to the terminating line when the CLID is not delivered along with the incoming call. If ALERT_NO_CLID is set to ‘N’, the feature will not provide distinctive alerting by default, and will continue feature processing by checking table TRKOPTS for an alerting indication. Its default value will be N.

5.1.2.2.8 Translation verification other tools

N/A.

6: Configuration (CN): A00001923

6.1 Hardware and Software Requirements

N/A

6.2 Initial Configuration

N/A

6.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

6.4 Upgrade Impact

6.4.1 Dump and Restore

N/A

6.4.2 Element Management Upgrade

N/A

6.5 Data schema (DS) (CM, MIBS, RDB)

6.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED
CISCPCPR	NEW	UNCHANGED
CUSTSTN	CHANGED	UNCHANGED
CPCOPMAP	CHANGED	UNCHANGED

6.5.2 Table/MIB/Remote Database Schema information

6.5.2.1 Name: ISERVOPT

A new tuple to table ISERVOPT will be added: zonetoll_scrn. An example datafill is as: zonetoll_scrn zonetoll_scrn Y Y.

6.5.2.1.1 Functional description

It is used to activate zone toll screening for the office in CIS network. Hence, zone toll office is also defined. It is accessed with the Table Control operations. Tuple can be added, deleted or changed.

Zone toll screening active field determines whether office is a zone toll office or not.

Line screening active field determines whether office makes screening for lines connected to itself or not.

When this tuple does not exist, it is accepted to have values NO (not a zone toll office).

6.5.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

6.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	UNCHANGED	UNCHANGED	UNCHANGED

6.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ZONETOLL SCREENING	NEW	NO	zonetoll_scrn	filled as zonetoll_scrn
ZONETOLL SCREENING	NEW	NO	zonetoll_scrn	filled as zonetoll_scrn
ZONETOLL SCREENING ACTIVE	NEW	NO	YES_NO	zone toll screening is activated or deactivated for incoming Russian ISUP V2+ trunk call Y (Yes), N (No)

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LINE SCREENING ACTIVE	NEW	NO	YES_NO	line screening is activated or deactivated for call whose originator is connected to office Y (Yes), N (No)

6.5.2.1.5 Datafill example

The following examples show sample datafill for table ISERVOPT.

Figure 1 Adding ZONETOLL_SCRN parameter to table ISERVOPTContinued

```
CI:
> TABLE ISERVOPT
TABLE: ISERVOPT
>ADD ZONETOLL_SCRN ZONETOLL_SCRN Y Y
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
        ZONETOLL_SCRN
                                        ZONETOLL_SCRN Y Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
>LIS
            SOPTSKEY
                                            SOPTSVAR
--------------------------------------------------------------------------------
        ZONETOLL_SCRN
                                        ZONETOLL_SCRN Y Y
                    STEPWISE PARAMETER ADDITION
>ADD
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ZONETOLL_SCRN
OPTION:
>ZONETOLL_SCRN
ZONETOLL_SCRN:
>Y
ZONETOLL_LINE_SCRN:
>Y
```

```
TUPLE TO BE ADDED:
        ZONETOLL_SCRN
                                        ZONETOLL_SCRN Y Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
```

from Figure 1

Figure 2 Changing ZONETOLL_SCRN parameter in ISERVOPT

```
>CHA
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
OPTION: ZONETOLL_SCRN
>
ZONETOLL_SCRN: Y
>N
ZONETOLL_LINE_SCRN: Y
>N
TUPLE TO BE CHANGED:
        ZONETOLL_SCRN
                                        ZONETOLL_SCRN N N

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
```

Figure 3 Deleting ZONETOLL_SCRN parameter from ISERVOPT

```
>DEL
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE DELETED:
        ZONETOLL_SCRN
                                        ZONETOLL_SCRN N N


ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE DELETED
```

6.5.2.1.6 Table release history update

NONE

6.5.2.1.7 Supplementary information

NONE

6.5.2.1.8 Translation verification other tools

NONE

6.5.2.2 Name: CISCPCPR

A new table CISCPCPR (Commonwealth of Independent States Calling Party Category PRivileges) is defined. Table is not initialized to default values. This table is only used at CIS network.

6.5.2.2.1 Functional description

Table is used to define network and service access privileges in terms of CPC value and call translation class. It is accessed with the Table Control operations. Add, delete and changing a tuple is possible.

When a tuple for a CPC type does not exist, no restrictions are applied to calls having that CPC type.

When a tuple for a CPC type exists, call translation classes it has are allowed to for calls.

6.5.2.2.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

6.5.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CISCPCPR	0	17	-

6.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for CISCPCPR.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
cpc	NEW	NO	CPC_name_type	INDEX FIELD CPC values in Please refer to "Table 6 CPC name and Call translation class entry values for table CISCPCPR" on page 1627.are valid inputs
class	NEW	NO	ixla_class	INDEX FIELD Call translation class values in Table 6 are valid inputs
privilege	NEW	NO	Yes_No	privilege information It is YES, when CPC and translation class have privilege.

Table 6 CPC name and Call translation class entry values for table CISCPCPR

CPC_name_type	Call translation class
UNKNOWN	UNKW
ORD	IAGRP
PRIOR	ATT
MAINT	DATT
SPM	LCL
OPER	SPEC
TRAN	EMRG
ITDN	NATL
FOC	CNTL
METER	ICNTL
LOCL	INTL
VIS	OPRA
CNDB	IOPRA
HOTEL	RURAL
AU_ORD	COLL
AU_PRIO	CELL
RSRVD	

6.5.2.2.5 Datafill example

The following example shows sample datafill for table CISCPCPR.

Call translation class values entered are evaluated as YES in privilege field of CISCPCPR table (calls allowed). Call translation class values which are not entered are evaluated to have NO privilege in table (calls not allowed).

Figure 4 Adding parameter to table CISCPCPRAdding and changing

```
CI:
>TABLE CISCPCPR
EMPTY TABLE
TABLE: CISCPCPR
>ADD
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
CPC_NAME:
>ORD
XLACLASS:
>LCL
XLACLASS:
>INTL
XLACLASS:
>NATL
XLACLASS:
>$
TUPLE TO BE ADDED:
   ORD
                              (  LCL ) ( INTL ) ( NATL )$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
```

SINGLE COMMAND LINE ADDITION

>ADD RSRVD LCL CELL $

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>Y

TUPLE TO BE ADDED:

RSRVD

(LCL) (CELL)$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>Y

TUPLE ADDED

>CHA

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>Y

XLACLASS: LCL

>

XLACLASS: CELL

>NATL

XLACLASS:

>INTL

XLACLASS:

>$

TUPLE TO BE CHANGED:

RSRVD

(LCL) (NATL) (INTL)$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>Y

TUPLE CHANGED

parameter in table CISCPCPR

Figure 5 Deleting parameter from table CISCPCPR

```
>DEL
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE DELETED:
  RSRVD
                                ( LCL ) ( NATL ) ( INTL )$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE DELETED
```

6.5.2.2.6 Table release history update

NONE

6.5.2.2.7 Supplementary information

NONE

6.5.2.2.8 Translation verification other tools

NONE

6.5.2.3 Name: CUSTSTN

A new field to table CUSTSTN is added: CPC. Tuple can be added, deleted or changed. An example datafill is as: CUST783 CPC CPC **ORD.**

6.5.2.3.1 Functional description

It is used to assign CPC value to customer groups. It is accessed with the Table Control operations.

6.5.2.3.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

6.5.2.3.3 Size

Table 7 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CUSTSTN	UNCHANGED	UNCHANGED	UNCHANGED

6.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs for CUSTSTN.

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CUSTNAME	Changed	NO	Customer_group	INDEX FIELD Customer group which will be assigned CPC is entered in this field.
OPTNAME	Changed	NO	CPC	Customer group Option Name is entered as CPC
OPTION	Changed	NO	CPC	Option is entered as CPC.
CPC	NEW	NO	CPC_name_type	CPC name which will be assigned to customer group is entered in this field.

Table 9 Entry values for CPC_name_type for table CUSTSTN

CPC_name_type	
UNKNOWN	FOC
ORD	METER
PRIOR	VIS
MAINT	LOCAL
SPM	CNDB
OPER	HOTEL
TRAN	AU_ORD
ITDN	AU_PRIO
	RSRVD

6.5.2.3.5 Datafill example

The following example shows sample datafills for table CUSTSTN.

Figure 6 CPC option addition to customer group in table CUSTSTNChanging

CI:

>**TABLE CUSTSTN**

TABLE: CUSTSTN

>**ADD CUST783A CPC CPC ORD $ Y Y**

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>**Y**

TUPLE TO BE ADDED:

CUST783A CPC CPC ORD

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>**Y**

TUPLE ADDED

STEPWISE ADDITION

>**ADD**

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>**Y**

CUSTNAME:

>**CUST783A**

OPTNAME:

>**CPC**

OPTION:

>**CPC**

CPC_NAME:

>**ORD**

TUPLE TO BE ADDED:

CUST783A CPC CPC ORD

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>**Y**

TUPLE ADDED

```
>CHA
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
OPTION: CPC
>
CPC_NAME: ORD
>RSRVD
TUPLE TO BE CHANGED:
    CUST783A       CPC                          CPC   RSRVD
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
```

CPC option of a customer group in table CUSTSTN

Figure 7 Deleting CPC option of a customer group in table CUSTSTN

```
>DEL
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE DELETED:
    CUST783A       CPC                          CPC   RSRVD
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE DELETED
```

6.5.2.3.6 Table release history update

NONE

6.5.2.3.7 Supplementary information

NONE

6.5.2.3.8 Translation verification other tools

NONE

6.5.2.4 Name: CPCOPMAP

CPCOPMAP is a table of CPC line options feature (A59032371.AA07).

6.5.2.4.1 Functional description

Table CPCOPMAP translates CPC values to ISUP CPC and R2 categories (CP activity). Table datafill can be changed with change (CHA) table control command.

In this feature, a new CPC value (RSRVD) is added to range of CPC values. And this value is also used in CPCOPMAP table. However, table CPCOPMAP is not used in CIS network.

Default values loaded at IPL for RSRVD are shown in datafill example section below.

6.5.2.4.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

6.5.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CPCOPMAP	UNCHANGED	UNCHANGED	UNCHANGED

6.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for CPCOPMAP.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CPCMKEY	NEW	NO	CPC_name_type	INDEX FIELD CPC name is entered.
ISUPCPC	NEW	NO	ISUP CPC name	ISUP CPC value corresponding to CPC name is entered here (Please refer to “Table 12 Entry values for ISUP CPC name and CP Activity” on page 1636.).

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MFCACT	NEW	NO	CP ACTIVITY	CP activity value corresponding to CPC name is entered here (Please refer to “Table 12 Entry values for ISUP CPC name and CP Activity” on page 1636.).

Table 12 Entry values for ISUP CPC name and CP Activity

ISUP CPC name	
Default ISUP CPC name	**CP Activity**
ISUP_CPC_UNKNOWN	REGULAR
ISUP_CPC_SUBSCRIBER_1	PRIORITY
ISUP_CPC_PRIORITY	MTE_EQ
ISUP_CPC_TEST_CALL	LOCAL_COIN
ISUP_CPC_PAYPHONE	OPER
ISUP_CPC_OP_NATIONAL	DATA
ISUP_CPC_DATA_CALL	VIS_CALL
ISUP_CPC_VOICE_INFOSERVICE	CLI_RESTRICTED

6.5.2.4.5 Datafill example

The following example shows sample datafill for table CPCOPMAP.

Figure 8 Changing a tuple in table CPCOPMAP

```
CI:
>TABLE CPCOPMAP
TABLE: CPCOPMAP
>LIS ALL
TOP
 CPCCAT              ISUPCPC          MFCACT
--------------------------------------------------
UNKNOWN       ISUP_CPC_UNKNOWN          REGULAR
   ORD   ISUP_CPC_SUBSCRIBER_1          REGULAR
  PRIOR       ISUP_CPC_PRIORITY          PRIORITY
  MAINT      ISUP_CPC_TEST_CALL           MTC_EQ
   SPM       ISUP_CPC_PAYPHONE         LOCAL_COIN
   OPER    ISUP_CPC_OP_NATIONAL             OPER
   TRAN      ISUP_CPC_DATA_CALL             DATA
   ITDN   ISUP_CPC_SUBSCRIBER_1          REGULAR
    FOC   ISUP_CPC_SUBSCRIBER_1          REGULAR
  METER   ISUP_CPC_SUBSCRIBER_1        LOCAL_COIN
   LOCL   ISUP_CPC_SUBSCRIBER_1          REGULAR
    VIS   ISUP_CPC_SUBSCRIBER_1          VIS_CALL
   CNDB   ISUP_CPC_SUBSCRIBER_1     CLI_RESTRICTED
  HOTEL   ISUP_CPC_SUBSCRIBER_1          REGULAR
 AU_ORD   ISUP_CPC_SUBSCRIBER_1          REGULAR
AU_PRIO   ISUP_CPC_SUBSCRIBER_1          REGULAR
 RSRVD   ISUP_CPC_SUBSCRIBER_1          REGULAR
BOTTOM
>POS RSRVD
 RSRVD   ISUP_CPC_SUBSCRIBER_1          REGULAR
>CHA ISUPCPC ISUP_CPC_UNKNOWN MFCACT DATA
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
```

Figure 9 Continued from Figure 11

```
>Y
TUPLE TO BE CHANGED:
 RSRVD      ISUP_CPC_UNKNOWN          REGULAR
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
```

6.5.2.4.6 Table release history update

NONE

6.5.2.4.7 Supplementary information

NONE

6.5.2.4.8 Translation verification other tools

NONE

6.6 Service Orders (SO) (CM & SESM)

6.6.1 Service order change details

6.6.1.1 LCC and options

This feature introduces new value **RSRVD** for CPC line option field.

6.6.2 New commands

This feature introduces a new value for existing service order option CPC.

6.6.2.1 How service order commands are presented

N/A

6.6.2.2 How service order options are presented

6.6.2.2.1 Description

CPC option can be assigned as line option via SERVORD commands.

6.6.2.2.2 Example

Figure 10 Example of the CPC option in prompt mode

```
> ADO
SONUMBER:    NOW   1  3 11 PM
>
DN_OR_LEN
>3450001
OPTION:
>CPC
CPC_VALUE:
>RSRVD
>$
```

Figure 11 Example of the CPC option in no-prompt mode

```
> ADO $ 3450001 CPC ORD $ yy
```

6.6.2.2.3 Option prompts

Table 13 System prompts for CPC option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	CPC	CPC line option	

Table 13 System prompts for CPC option

Prompt	Valid input	Description	Areas affected by prompt
CPC_VALUE	UNKNOWN	unknown subscriber	
	ORD	ordinary subscriber	
	PRIOR	subscriber with priority	
	MAIN	test call	
	SPM	pay phone	
	OPER	national operator	
	TRAN	data call	
	ITDN	subscriber with special services	
	FOC	free change subscriber	
	METER	local pay phone	
	LOCAL	local network subscriber	
	VIS	voice information services subscriber	
	CNDB	subscriber owner of CNDB	
	HOTEL	hotel subscriber	
	AUORD	automatic subscriber without priority	
	AUPRIO	automatic subscriber with priority	
	RSRVD	**Reserved (CIS Subs. Cat. 0) (new)**	

6.6.2.2.4 Line class code compatibilit

Table 14 CPC compatibility to LCC

Line class code	Compatible?
IBN	YES
BRI	YES

6.6.2.2.5 Assignability

The following functionalities apply to this option:

- set functionality: NO

- subset functionality: NO
- DN functionality: YES
- key functionality: NO

6.6.2.2.6 Option prerequisites

CPC has no prerequisites.

6.6.2.2.7 Notes

N/A

6.6.2.2.8 Feature identification

Functionality: WT20

Feature number:A00001923

6.6.2.2.9 SERVORD+ Exceptions

N/A

6.7 Software optionality control (SOC)

N/A

6.8 Element Management

N/A

6.9 Command interface changes

N/A

6.10 Security

N/A

6.11 Configuration Walkthrough

N/A

7: Configuration (CN): A00001930

7.1 Hardware and Software Requirements

This feature uses the Enhanced Digital Recorded Announcement Machine (EDRAM) to provide the announcement for CMI service. The CMI simple phrases are loaded into EDRAM as voice files.

7.2 Initial Configuration

N/A

7.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

7.4 Upgrade Impact

N/A

7.5 Data schema (DS) (CM)

7.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CUSTSTN	CHANGED	UNCHANGED
IBNXLA	CHANGED	UNCHANGED

7.5.2 Table Information

7.5.2.1 Table Name: CUSTSTN

Customer Station Table

7.5.2.1.1 Functional description

The function of the table is unchanged.

7.5.2.1.2 Datafill sequence and implications

Current datafill order is unchanged.

7.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CUSTSTN	Same	Same	Current limits are maintained

7.5.2.1.4 Table Fields

The following table lists fields of the CMI option of table CUSTSTN.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTNAME	Changed	None	CMI	The new CUSTSTN option, CMI, is datafileld here.
OPTION	Changed	CMI_OPTION	{CMI LCMI} {CMI TCMI}	LCMI and TCMI options datafilled here

7.5.2.1.5 Datafill example

The following example shows sample datafill for table CUSTSTN for the CMI Customer Group Option.

Figure 1 Assigning CMI Options to a Customer Group

```
>table CUSTSTN
>add CUST111 CMI CMI (TCMI) (LCMI) $
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE ADDED:
        CUST111         CMI CMI (TCMI) (LCMI) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
>lis
CUSTNAME       OPTNAME OPTION
-----------------------------------------------
CUST111        CMI CMI (TCMI) (LCMI) $
```

Figure 2 Deassigning LCMI Option from a Customer Group

```
>table CUSTSTN
>lis CUST111 CMI
CUSTNAME      OPTNAME OPTION
-----------------------------------------------
CUST111       CMI CMI (TCMI) (LCMI) $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
OPTION: CMI
>
CMIOPT: TCMI
>
CMIOPT: LCMI
>$
TUPLE TO BE CHANGED:
        CUST111        CMI CMI (TCMI) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
JOURNAL FILE INACTIVE
>lis
CUSTNAME      OPTNAME OPTION
-----------------------------------------------
CUST111       CMI CMI (TCMI) $
```

Figure 3 Deassigning CMI Option completely from a Customer Group

```
>table CUSTSTN
>lis CUST111 CMI
CUSTNAME      OPTNAME OPTION
-----------------------------------------------
CUST111       CMI CMI (TCMI) (LCMI) $

>del
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE DELETED:
        CUST111        CMI CMI (TCMI) (LCMI)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE DELETED
JOURNAL FILE INACTIVE
WARNING:  CURRENTLY NOT POSITIONED
```

7.5.2.1.6 Table release history update

A new customer group option, CMI, is added to be datafilled in table CUSTSTN.

7.5.2.1.7 Supplementary information

N/A

7.5.2.1.8 Translation verification other tools

CUSTSTN table does not use translation verification tools.

7.5.2.2 Table Name: IBNXLA

IBN Translation

7.5.2.2.1 Functional description

The function of the table is unchanged.

7.5.2.2.2 Datafill sequence and implications

Current datafill order is unchanged.

7.5.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNXLA	Same	Same	Current limits are maintained

7.5.2.2.4 Table Fields

The following table lists fields for IBNXLA table.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FEATURE	Changed	None	TCMI LCMI	Total Call Meter Inquiry Feature Last Cal Meter Inquiry Feature

7.5.2.2.5 Datafill example

The following example shows sample datafill for table IBNXLA.

Figure 4 Sample IBNXLA datafill for LCMI and TCMI services

```
TABLE: IBNXLA
KEY RESULT
----------
NETXLA 117 FEAT N N LCMI
NETXLA 118 FEAT N N TCMI
```

7.5.2.2.6 Table release history update

Two new features, LCMI and TCMI, are added to be datafilled in table IBNXLA.

7.5.2.2.7 Supplementary information

N/A

7.5.2.2.8 Translation verification other tools

Traver Example

```
>traver l 7835410 118 b
TABLE IBNLINES
HOST 00 0 10 09 0 DT STN IBN 7835410 CUST783 0 0 102 (TCMI)
(LCMI) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
Originator is not an EIN agent, therefore EIN info is not
processed.
Originator is not an EIN agent, therefore EIN info is not
processed.
TABLE NCOS
CUST783 0 0 0 $ ( XLAS NETXLA STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT,
AND DIGCOL
CUST783 NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME NETXLA
NETXLA 118 FEAT N N LCMI

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature CMI        not supported by TRAVER


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

7.6 Service Orders (SO) (CM & SESM)

7.6.1 Service order change details

7.6.1.1 LCC and options

Two new line options, LCMI and TCMI, are introduced by this feature. LCMI and TCMI line options are not DN based.

7.6.1.1.1 LCMI and TCMI Line Options

Two new line options TCMI and LCMI are introduced. CMI line options are boolean options, which means it has no subfields. For ETSI BRI lines, they are compatible with point to point and point to multi point mode.

CMI line options can be assigned/deassigned to subscriber via SERVORD software. When TCMI/LCMI line options are assigned to a line, datafill will be added into one of tables IBNLINES (for IBN lines) or KSETLINE (for ETSI BRI lines) depending on the line type.

- **Administrator Assignment**

CMI line options can be assigned to IBN lines and ETSI BRI lines through SERVORD software via ADO (Add Option) and NEW commands. TCMI and LCMI line options can be assigned to IBN and ETSI BRI subscribers only. In order to assign TCMI or LCMI option to a line, line should have a MOG or FPS option. Please note that FPS option is supported for IBN lines only.

```
ado $ <DN> TCMI $

ado $ <DN> LCMI $
```

If line has none of MOG or FPS options, new CMI otion can not be assigned to the subscriber. In this case system will reply with one of the following error messages.

```
"Cannot add LCMI since line does not have MOG or FPS option"

"Cannot add TCMI since line does not have MOG or FPS option"
```

If MOG and CMI options are intended to be assigned at the same time, MOG option should be given first so that the feature metering of administrative assignment is done correctly. Please refer to section 2.2.5 Feature Metering for more information on feature metering.

- **Administrator Deassignment**

The administrator may deassign CMI option by using the DEO (Delete Option) and OUT commands through SERVORD software.

```
deo $ <DN> TCMI $

deo $ <DN> LCMI $
```

- **Deassignment of MOG Option**

If both MOG and CMI options are intended to be deassigned from a line at the same time, CMI option must be deassigned first, so that feature metering of administrator deassignment is done correctly. Please refer to section 2.2.5 Feature Metering for more information on feature metering.

```
deo $ <DN> LCMI MOG $
```

```
deo $ <DN> TCMI MOG $
```

MOG option deletion is prohibited if line has TCMI and/or LCMI option. The following error message is generated:

```
"Error: Cannot delete MOG since TCMI requires MOG option."

"Error: Cannot delete MOG since LCMI requires MOG option."
```

- **Deassignment of FPS Option**

FPS option deletion is prohibited if line has LCMI and/or TCMI line options. The following error message is generated FPS option is attempted to be deassigned from a line which has LCMI/TCMI line option.

```
"Error: Cannot delete FPS since TCMI requires FPS option."

"Error: Cannot delete FPS since LCMI requires FPS option."
```

- **Example**

Figure 5 Assigning LCMI and TCMI Options to an IBN line

```
>qdn 7835411
-------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
DGT MOG MOG_2
-------------------------------------------------
>SERVORD
SO:
>ado $ 7835411
OPTION:
>TCMI
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 5 25 AM 7835411 ( TCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 6 Assigning LCMI and TCMI Options to an IBN line (Cont)

```
>qdn 7835411
-------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
TCMI DGT MOG MOG_2
-------------------------------------------------
>ado $ 7835411
OPTION:
>LCMI
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 5 25 AM 7835411 ( LCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>qdn 7835411
-------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
TCMI LCMI DGT MOG MOG_2
-------------------------------------------------
```

Figure 7 Deassigning TCMI Option From an IBN Line

```
>qdn 7835411
-------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
TCMI LCMI DGT MOG MOG_2
-------------------------------------------------
>deo $ 7835411
OPTION:
>TCMI
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 5 25 AM 7835411 ( TCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>Y
```

Figure 8 Deassigning TCMI Option from an IBN Line (Cont)

```
>qdn 7835411
------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
LCMI DGT MOG MOG_2
------------------------------------------------
```

Figure 9 Assigning LCMI Option to an ISDN Line

```
>qdn 7831018
------------------------------------------------
DN:     7831018
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN4       2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC
MOG MOG_2 MLPP NIL_DOMAIN FLASH N $

------------------------------------------------
>ado $ 7831018 1 LCMI $
COMMAND AS ENTERED:
ADO NOW 3 6 2 AM 7831018 ( 1 LCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 10 Assigning LCMI Option to an ISDN Line

```
>qdn 7831018
------------------------------------------------
DN:     7831018
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG:  N/A    LNATTIDX: N/A
LTID: ISDN4       2
LTCLASS:  BRAFS
LINE CLASS CODE:   ISDNKSET
KEY:  1
CUSTGRP:       CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
OPTIONS:
SFC LCMI
MOG MOG_2 MLPP NIL_DOMAIN FLASH N $

------------------------------------------------
```

Figure 11 Deassigning MOG Option from a line

```
>qdn 7835411
------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
LCMI DGT MOG MOG_2
------------------------------------------------
```

Figure 12 Deassigning MOG Option from a line (Cont)

```
>SERVORD
SO:
>deo $ 7835411 MOG $
COMMAND AS ENTERED:
DEO NOW 3 5 27 PM 7835411 ( MOG ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
Error: Cannot delete MOG since LCMI requires MOG
Option
MOG DID NOT PASS CHECKING
***  ERROR - INCONSISTENT DATA  ***
COMMAND AS ENTERED:
DEO NOW 3 5 27 PM 7835411 ( MOG ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>N
>deo $ 7835411 LCMI $
COMMAND AS ENTERED:
DEO NOW 3 5 25 AM 7835411 ( LCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>deo $ 7835411 MOG $
COMMAND AS ENTERED:
DEO NOW 3 5 27 PM 7835410 ( MOG ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 13 Deassigning MOG Option from a line (Cont)

```
>qdn 7835411
-------------------------------------------------
DN:     7835411
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
DGT
-------------------------------------------------
```

Figure 14 Deassigning LCMI and MOG Option from a line at the same time

```
>qdn 7835410
-------------------------------------------------
DN:     7835410
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
LCMI DGT MOG MOG_2
-------------------------------------------------
>SERVORD
SO:
>deo $ 7835410 LCMI MOG $
COMMAND AS ENTERED:
DEO NOW 3 5 27 PM 7835411 ( LCMI ) ( MOG ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>qdn 7835410
-------------------------------------------------
DN:     7835410
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 10 10
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    331
OPTIONS:
DGT
-------------------------------------------------
```

Figure 15 Assining LCMI Line Option to an IBN Line with FPS Option

```
>qdn 7835401
-------------------------------------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    4
OPTIONS:
DGT FPS MOG_2 FPS1 176
-------------------------------------------------
>SERVORD
SO:
>ado $ 7835401 LCMI $
COMMAND AS ENTERED:
ADO NOW 3 5 25 AM 7835401 ( LCMI ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL  FILE  IS  INACTIVE,  SERVICE  ORDERS  NOT
ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
>qdn 7835401
-------------------------------------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    4
OPTIONS:
DGT LCMI FPS MOG_2 FPS1 176

-------------------------------------------------
```

Figure 16 Deassigning FPS Option from a line

```
>qdn 7835401
------------------------------------------------
DN:     7835401
TYPE: SINGLE PARTY LINE
SNPA: 102   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 00 03
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        CUST783     SUBGRP: 0  NCOS: 0
CARDCODE:  6X93AA    GND: N  PADGRP: STDLN  BNV: NL
MNO: N
PM NODE NUMBER     :    43
PM TERMINAL NUMBER :    4
OPTIONS:
DGT LCMI FPS MOG_2 FPS1 176

------------------------------------------------
>servord
SO:
>deo $ 7835401 fps
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 6 5 AM 7835401 ( FPS ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
Error: Cannot delete FPS since LCMI requires FPS
Option
***  ERROR - INCONSISTENT DATA  ***
```

7.6.1.1.2 Line class code compatibility

LCMI and TCMI Line options are compatible with IBN and ISDNKSET LCCs.

7.6.1.1.3 Option prerequisites

LCMI and TCMI line options require MOG or FPS option on the subscriber.

7.6.1.1.4 Interaction with EST command

LCMI and TCMI line options cannot be added via EST (Establih hunt group) command, since addition of MOG and FPS by EST is not allowed and LCMI and TCMI line options require MOG or FPS previously assigned (Sec. 13.6.1.1.3).

7.6.1.1.5 Interaction with SWAP and CLN Commands

Last call and last feature meter counts of FPS and MOG agents are preserved during SWAP and CLN operations. In other words, last call and last feature meter counts of old len will be moved to new len during SWAP and CLN.

Behavior of SWAP and CLN commands were not like this before this activity, since idea of keeping last call and last feature meter counts was being introduced by this activity. But please note that this enhancement does not change the general behavior of CLN and SWAP commands when SVBI0033 SOC in IDLE, or appiled to agents that does not have MOG or FPS assigned when SVBI0033 SOC is ON.

The following example shows the behavior of CMI service when SWAP command is applied to FPS agent (Behavior of MOG agent is the same). Please note that CMI SOC is ON.

Figure 17 SWAP Example (FPS Subscriber)

```
Before SWAP
FPS:
>qfps all
WARNING: Query of all FPS counters may take a significant
amount of time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835401  MOG_ID: MOG_1             FPS1   160
Last Call Credit    : 10
Last Feature Credit : 3

DN:      1027835402  MOG_ID: MOG_2             FPS2   203
Last Call Credit    : 12
Last Feature Credit : 5

============================================================
TOTAL: 2 FPS subscriber(s) found
>
>swap $ 7835401 7835402 $ loop y y
>
After SWAP
>qfps all
WARNING: Query of all FPS counters may take a significant
amount of time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835402  MOG_ID: MOG_2             FPS2   203
Last Call Credit    : 12
Last Feature Credit : 5

DN:      1027835401  MOG_ID: MOG_1             FPS1   160
Last Call Credit    : 10
Last Feature Credit : 3

============================================================
TOTAL: 2 FPS subscriber(s) found
```

7.6.2 New commands

N/A

7.7 Software optionality control (SOC)

A new state SOC, SVBI0033 SOC, is introduced by this feature.

7.7.1 SVBI0033 SOC

In order to control the officewide functionality of the TCMI and LCMI services, one state SOC is designed, which is given the name SVBI0033 SOC. SVBI0033 SOC has two states: SOC_ON and SOC_IDLE. In the SOC_ON

state, SVBI0033 SOC is fully functional. In the IDLE state, the LCMI and TCMI features can be provisioned, but the usage of the service is not enabled.

Table 6 SVBI0033 SOC

SOC Group	SVBI
SOC Option Name	SVBI0033
SOC Option Title	Call Meter Inquiry
SOC Option Control Type	State
New SOC Option?	Yes
Option defined in DRU	WT20
Affected Products	DMS100 - MMP

Default state of SOC is IDLE.

Activation/Deactivation of SOC is done by password control. The password is unique for each office.

However, datafilling tables (i.e IBNXLA, IBNLINES, CUSTSTN, etc.) does not depend on the state of the SOC. This means that datafills could be done even if SVBI0033 SOC is not ON. But note that CMI services can not be activated if SVBI0033 SOC is not ON.

For all MOG and FPS subscribers, last call and last feature meter counts are initialized when state of SVBI0033 SOC is changed to IDLE.

State of SVBI0033 SOC can not be changed from ON to IDLE while one of DUMP, METERING RESTORE, or METERING LINE RECOVERY processes. One of following error messages are displayed:

“DUMP is in progress“

“METER LINE RECOVERY process is in progress“

“METER RESTORE is in progress“

and change state is aborted.

7.8 Element Management

N/A

7.9 Command interface changes

7.9.1 Directory: <directory name/MAP level>

N/A

7.9.2 Command: MTRCOUNT

MTRCOUNT command, which displays the software meter counts of the subscriber having MOG, is enhanced in order to display the last call meter count, last feature meter count, and the total of all meter counts assigned to the subscriber when SVBI0033 SOC is ON.

When MTRCOUNT command is used with TRUNK/LMG (Line Meter Group) option, when SVBI0033 SOC is ON, TOTAL of assigned meter counts of trunk/lmg is displayed.

But general structure and operation of the command remains the same.

7.9.2.1 Command type: NON-MENU

7.9.2.2 Command target:

BRISC, XACORE.

7.9.2.3 Command availability:

RES

7.9.3 Example

Figure 18 Map Display for MTRCOUNT LINE command

```
>mtrcount LINE 7835406
************************************************************

DN     : 1027835406
DATE   : 03/07/18
MTR NAME: FEATURE           MTR COUNT:  00000000 WRAP: N
MTR NAME: LOCAL             MTR COUNT:  00000000 WRAP: N
MTR NAME: TOLL              MTR COUNT:  00000000 WRAP: N

          TOTAL             MTR COUNT: 000000000
          LAST CALL         MTR COUNT:  00000000
          LAST FEATURE      MTR COUNT:  00000000
************************************************************
```

Figure 19 Map Display for MTRCOUNT TRUNK command

```
>mtrcount trunk 2WBDISP2AB
 ************************************************************

 TRUNK GROUP: 2WBDISP2AB
 DATE   : 04/03/05

 INCOMING CALLS
 --------------
 MTR NAME: METER1           MTR COUNT:  000000000000 WRAP:Y
 MTR NAME: METER2           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER3           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER4           MTR COUNT:  999999999999 WRAP:Y

           TOTAL            MTR COUNT: 6999999999997

 OUTGOING CALLS
 --------------
 MTR NAME: METER1           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER2           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER3           MTR COUNT:  999999999999 WRAP:Y
 MTR NAME: METER4           MTR COUNT:  999999999999 WRAP:Y

           TOTAL            MTR COUNT: 7999999999996

************************************************************
```

Figure 20 Map Display for MTRCOUNT LMG command

```
>mtrcount lmg 533
************************************************************

LOGICAL METERING GROUP: 533
DATE   : 04/03/05

INCOMING CALLS
--------------
MTR NAME: TLOCAL           MTR COUNT:  999999999999 WRAP:N
MTR NAME: TTOLL            MTR COUNT:  000000000134 WRAP:Y

          TOTAL            MTR COUNT: 2000000000133

OUTGOING CALLS
--------------
MTR NAME: TLOCAL           MTR COUNT:  000000000145 WRAP:N
MTR NAME: TTOLL            MTR COUNT:  000000000125 WRAP:Y

          TOTAL            MTR COUNT: 1000000000270
************************************************************
```

7.9.4 Command: QFPS

QFPS FPS CI command, which displays the FPS credit of the subscriber having FPS, is enhanced in order to display the last call meter count, last

feature meter count, and the total of all meter counts assigned to the subscriber when SVBI0033 SOC is ON. QFPS command with ZERO, UNUSEDFOR, DN and ALL options are enhanced by this activity. Map display is as follows:

7.9.4.1 Command type: NON-MENU

7.9.4.2 Command target:
BRISC, XACORE.

7.9.4.3 Command availability:
RES

7.9.5 Example

Figure 21 Map Display for QFPS command

```
>qfps all
WARNING: Query of all FPS counters may take a significant amount of
time
Please confirm ("YES", "Y", "NO", or "N"):
>y
DN:      1027835401  MOG_ID: MOG_2             FPS1   154
Last Call Meter Count         : 0
Last Call Feature Meter Count : 0
================================================================
TOTAL: 1 FPS subscriber(s) found
>
>qfps dn 7835401
----------------------------------------------------------------
DN: 7835401     MOG_ID: MOG_2             FPS1   154

Last Call Meter Count         : 0
Last Call Feature Meter Count : 0
>
```

7.10 Security
N/A

7.11 Configuration Walkthrough
N/A

8: Configuration (CN): A00001935

8.1 Hardware and Software Requirements

Not applicable.

8.2 Initial Configuration

Not applicable.

8.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable. This feature leverages a previously defined gateway profile for CICM gateways.

8.4 Upgrade Impact

8.4.1 Dump and Restore

Not applicable.

8.4.2 Element Management Upgrade

Not applicable.

Upgrade of CICM data to SN07 is not supported. SN06.1 and SN06.2 data must be removed and then re-added in SN07 in order to leverage any flow through capabilities delivered by this feature. Both new and old format CICM data will be allowed to co-exist in SN07, however the SN06 format CICM will be managed generically (same as in SN06).

8.5 Data schema (DS) (CM, MIBS, RDB)

8.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LGRPINV	CHANGED	UNCHANGED
LNINV	CHANGED	UNCHANGED

8.5.2 Table/MIB/Remote Database Schema information

8.5.2.1 Name: LGRPINV

Logical Group Inventory

8.5.2.1.1 Functional description
In SN06, the field GRPTYPE of the table LGRPINV is set to “C” for non-MG9K logical groups and to “S” for MG9K logical groups. In SN07, the unused value “M” will be used in this field to indicate that the logical group is assigned to a CICM gateway.

8.5.2.1.2 Usage sequence and implications (CM Only)
The table LGRPINV is provisioned by the SESM. No manual datafill or change is allowed. Manual changes to this table will cause data corruption.

8.5.2.1.3 Size
Not applicable.

8.5.2.1.4 Fields/OIDs
Not applicable. This feature will use an already defined and supported field.

8.5.2.1.5 Datafill example
The following example shows sample datafill for table LGRPINV.

Preprovisioned MG(e.g MG9K) : SLOA 00 0 GWC 3 S $

Preprovisioned CICM gateways : CICM 00 0 GWC 3 M $

Non preprovisioned MG(e.g. Cable MG) : LG 01 0 GWC 3 C $

8.5.2.1.6 Table release history update
Not applicable.

8.5.2.1.7 Supplementary information
Not applicable.

8.5.2.1.8 Translation verification other tools
Not applicable.

8.5.2.2 Name: LNINV
Line Inventory

8.5.2.2.1 Functional description
In SN07, the field SUBGROUP and CIRCUIT fields of the table LNINV are refined based on their associated LGRPINV GRPTYPE field.

The SUBGROUP/SLOT and CIRCUIT fields are defined as follows:

```
(GRPTYPE C) LINE SUBGROUP {0 TO 10}

(GRPTYPE M) LINE SUBGROUP {0 TO 10}

(GRPTYPE S) SLOT          {2-9, 14-21}
```

```
(GRPTYPE C) CIRCUIT   {0 TO 99}

(GRPTYPE M) CIRCUIT   {0 TO 99} FOR SUBGROUP {0 TO 10}

(GRPTYPE S) CIRCUIT   {0 TO 47}
```

8.5.2.2.2 Usage sequence and implications (CM Only)

Entries will be automatically configured by SESM at CICM gateway provisioning time.

8.5.2.2.3 Size

Not applicable.

8.5.2.2.4 Fields

The following table lists fields for LNINV.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SUBGROUP	Changed	M	{0 to 10}	
CIRCUIT	Changed	M	{0 to 99}	

8.5.2.2.5 Datafill example

The following example shows sample datafill for table LNINV.

Preprovisioned MG(e.g MG9K) line:

SLOA 00 0 21 31 RDTLSG PKLNL HASU N NL N NIL

Preprovisioned CICM gateway line:

International - HOST 00 0 10 22 **GWLEBS** NPDGP HASU N NL N NIL

North America - HOST 00 0 10 22 **RDTEBS** NPDGP HASU N NL N NIL

Non preprovisioned MG(e.g. Cable MG) line:

LG 01 0 00 00 RDTLSG PKLNL WORKING N NL N NIL

8.5.2.2.6 Table release history update

Not applicable.

8.5.2.2.7 Supplementary information

Not applicable.

8.5.2.2.8 Translation verification other tools

Not applicable.

8.5.2.3 Gateway and Termination Name Mapping to Logical Group and Line Equipment Number (LEN)

8.5.2.3.1 Functional description

The definitions of the various portions of the logical group, LEN, GW and termination names are defined to provide a visual correlation between their respective values.

8.5.2.3.2 GW

<GWNAME>-<NNN>, e.g. "CICM-142"
where:

<GWNAME> = String
CICM Identifier (configurable)

<NNN> = 000-511
The CICM gateway identifier.

8.5.2.3.3 Logical Group

<SITE> <NNN> <G>, e.g. "HOST 142 0", “CICM 142 0”, etc.
where:

<SITE> = SITE name chosen at gateway provisioning time. Matching gateway name to SITE name is not an enforced rule, however it is suggested that a “CICM” SITE name be defined in the XACore and that all CICM gateway provisioning utilize the “CICM” SITE name. “HOST” is used in this example simply to show the flexibility of the provisioning system (any SITE name may be chosen at CICM gateway provisioning time). Actual utilization of the “HOST” SITE name is NOT recommended as it may collide with legacy LCM definitions in the XACore.

<NNN> defined as in GW name.

<G> = 0-2
The group number. Each gateway will span 3 logical groups.

8.5.2.3.4 Termination/Endpoint

tp/<G>/<TTtt>, eg. "tp/0/1013"
where:

<G> defined as in the logical group.

<TT> = 00-10
<tt> = 00-99, except where <TT> = 10 in which case <tt> = 00-22.

8.5.2.3.5 LEN Format

<SITE> <NNN> <G> <TT> <tt>, eg “CICM 142 0 10 13"
where:

<SITE>, <NNN>, <G>, <TT>, and <tt>, defined as in gateway and logical group.

8.5.2.3.6 Logical Group and LEN to GW and Termination Correlation for a CICM Processor Pair

- One CICM "GW" mapped to Three logical groups in the XACore.
- 3069 CICM terminations mapped to the three logical group's LENs in the XACore.
- 3 terminal numbers are reserved in the XACore (one for each logical group) for maintenance/messaging.

Table 3 LEN to GW, Termination and Terminal Number Mapping

LEN	GW	Termination	Terminal Number
CICM 142 0 00 00	CICM-142	tp/0/0000	1 **
CICM 142 0 00 01	CICM-142	tp/0/0001	2
:	:	:	:
CICM 142 0 10 22	CICM-142	tp/0/1022	1023
CICM 142 1 00 00	CICM-142	tp/1/0000	1 **
CICM 142 1 00 01	CICM-142	tp/1/0001	2
:	:	:	:
CICM 142 1 10 22	CICM-142	tp/1/1022	1023
CICM 142 2 00 00	CICM-142	tp/2/0000	1 **
CICM 142 2 00 01	CICM-142	tp/2/0001	2
:	:	:	:
CICM 142 2 10 22	CICM-142	tp/2/1022	1023

** Terminal number 0 is reserved in the XACore for the maintenance/ messaging terminal on the node. The formula currently used by the XACore to convert non-MG9K LEN to terminal number is as follows:

terminal number = ((100 * TT) + tt + 1)

8.6 Service Orders (SO) (CM & SESM)

8.6.1 Service order change details

No new service orders are introduced by this feature. CICM client specific SERVORD+ commands (NEW, EST, OUT, etc.) may contain USERID and PASSWD option flags which will be stripped from the command by SESM before being processed by the CM.

8.6.1.1 How service order options are presented

8.6.1.1.1 Description

The USERID and PASSWD options are used to specify CICM client information in the various SERVORD+ commands which create or modify lines. These options may be provisioning using any valid key number on the CICM client, however they are not key specific options (they affect the entire set).

8.6.1.1.2 Example

Figure 1 Example of the USERID option in no-prompt mode for SERVORD+

```
NEW $ 6137210992 M5216 PRADEFAULT 0 0 1 N LATA1 9 CICM 142 0 10 13 1 7 USERID 12345(
```

8.6.1.1.3 Line class code compatibility

USERID to LCC compatibility

Table 4 <abbreviated option name> compatibility to LCC

Line class code	Compatible?
M5216	Yes
All others	No (but not functionally enforced)

8.6.1.1.4 SERVORD+ Exceptions

No SERVORD+ command exclusions although some servord commands will not be integrated with CICM provisioning. The non-integrated commands will still function normally from a SERVORD+ and XACore perspective.

8.7 Software optionality control (SOC)

Not applicable.

8.8 Element Management

8.8.1 New/modified GUIs

The CS2000 Management Tools GUI is modified by this feature. Specifically the Associate Media Gateway dialog box will be altered.

The profile name “CICM” which was added in SN06 to the list of profiles that appears in the Gateway profile name drop down list, will be unmodified in SN07. The Reserved terminations for this profile will be 3069.

CICM gateways provisioned prior to SN07, will have their profile names changed to an obsolete value (eg. “OBSOLETE_CICM”) to allow them to continue to function within the various provisioning systems as they did in SN06.

8.9 Command interface changes

Not applicable.

8.10 Security

Not delivered under this feature.

8.11 Configuration Walkthrough

The general order of provisioning is as follows:

- Provision table SITE in XACore. SITE values for CICM should be retricted from use for other logical group types..
- Provision table PADDATA in XACore (PKLNL and PKNIL entries).
- Provision CICM gateway in SESM (autocreates LGRPINV and LNINV entries).
- Configure CICM gateway at the CICM-EM (some data is retrieved from SESM via OSSGate)
- Execute SERVORD+ commands via OSSGate (service is assigned to LENs in LNINV).
- USERNAME and PASSWD data is configured (via OSSGate SERVORD+) on the CICM client to enable service.

9: Configuration (CN): A00002053

9.1 Hardware and Software Requirements

None.

9.2 Initial Configuration

For the software initialization, the datafills given in the section 2.2.4 of the FN document are required for this feature.

9.3 Office/Subnet parameters (OP/SP) (CM & SESM)

9.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCVAR	FTR_RECORD_FOR_ICR_OPT	NEW	CM

9.3.2 Parameter information

9.3.2.1 FTR_RECORD_FOR_ICR_OPT

Feature Record for ICR Option

9.3.2.1.1 Functional description

The parameter FTR_RECORD_FOR_ICR_OPT is newly created by this activity to make the FTR record generation optional for metered actions of ICR feature option. When the subscriber having ICR option is charged for the ICR operations (assignment / deassignment / usage), the FTR record is generated only if the FTR_RECORD_FOR_ICR_OPT is Y in table OFCVAR.

9.3.2.1.2 Provisioning rules

The parameter FTR_RECORD_FOR_ICR_OPT is set to Y to generate FTR record for the charged ICR operations of subscribers (as shown in Figure 1). But, beside of this parameter setting, all required datafill should exist for the generation of the FTR record. Please refer to the Section 2.2.4 in the FN document for the FTR record provisioning.

Figure 1 The new OFCVAR parameter

```
> Table OFCVAR

PARMNAME PARMVAL
-----------------------------
FTR_RECORD_FOR_ICR_OPT      Y
```

When the parameter FTR_RECORD_FOR_ICR_OPT is changed from “N” to “Y”, the following message is displayed;

“WARNING: FTR record generation for ICR feature is activated”

Opposite when FTR_RECORD_FOR_ICR_OPT is changed from “Y” to “N” the following message is displayed;

“WARNING: FTR record generation for ICR feature is deactivated”

9.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
TRUE (Y)	FALSE (N)	FALSE (N)

9.3.2.1.4 Activation
Change activation is immediate. No additional action is necessary.

9.3.2.1.5 Dependencies
None.

9.3.2.1.6 Verification
After changing this parameter, it is enough to check it by ‘pos’ command in the table OFCVAR.

9.3.2.1.7 Memory requirements
No memory impact.

9.3.2.1.8 Parameter release history update
A new parameter addition.

10: Configuration (CN): A00002101

10.1 Hardware and Software Requirements

This feature is supported only on SX05 DTCO/DTCO2 processor.

10.2 Initial Configuration

N/A

10.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

10.4 Upgrade Impact

N/A

10.5 Data schema (DS) (CM, MIBS, RDB)

10.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TABLE TRKOPTS	CHANGED	UNCHANGED

10.5.2 Table/MIB/Remote Database Schema information

10.5.2.1 Name: TRKOPTS

Trunk Options Table

10.5.2.1.1 Functional description

Table TRKOPTS is used to assign a trunk option which is supported for a certain trunk type.

10.5.2.1.2 Usage sequence and implications (CM Only)

No change due to this feature.

10.5.2.1.3 Size

No change due to this feature.

10.5.2.1.4 Fields/OIDs

Below you can find the field information related to the new option, TELETAXE_ITX_SIG, in the table TRKOPTS.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Changed	Multiple with CLLI and OPTION	CLLI and TELETAXE_ITX_SIG	TELETAXE_ITX_SIG is datafilled with CLLI to which assigned this option at OPTKEY field.
OPTINFO	Changed	OPTION	TELETAXE_ITX_SIG	TELETAXE_ITX_SIG is datafilled at OPTION field after entry of the OPTKEY field.

10.5.2.1.5 Datafill example

The following example shows sample datafill for table TRKOPTS.

TABLE: TRKOPTS

TOP

OPTKEY OPTINFO

2WFTUPAB TELETAXE_ITX_SIG TELETAXE_ITX_SIG

10.5.2.1.6 New Error Messages

Below you can find the error messages generated during making datafill verification related to the option TELETAXE_ITX_SIG.

Figure 1

"TELETAXE option not supported for the ISUP variant assigned to this trunk group in table TRKSGRP.
Error reported by option TELETAXE_ITX_SIG with VPROC operation defined in module FTUPDEF."

Generated when the operator tries to assign TELETAXE_ITX_SIG option to an ETSI ISUP trunk of which variant is other than France.

Figure 2

**"TELETAXE option not supported for the signalling data selector assigned to this trunk group in table TRKSGRP.
Error reported by option TELETAXE_ITX_SIG with VPROC operation defined in module FTUPDEF."**

Generated when the operator tries to assign TELETAXE_ITX_SIG option to a CAS trunk.

Figure 3

**"TELETAXE option is supported only on IBN incoming and two-way trunk types.
Error reported by option TELETAXE_ITX_SIG with VPROC operation defined in module FTUPDEF."**

Generated when the operator tries to assign TELETAXE_ITX_SIG option to an OG SSUTR2 trunk or a PRI trunk.

Figure 4

"OPTIONS are not the same in key and optinfo fields”

Generated when the operator tries to assign an option other than TELETAXE_ITX_SIG to a trunk datafilled with TELETAXE_ITX_SIG at OPTKEY field of the table TRKOPTS.

Figure 5

"TELETAXE_NOSIG option previously assigned to this trunk."

Generated when the operator tries to assign TELETAXE_ITX_SIG option to an IC/2W SSUTR2 trunk to which previosly TELETAXE_NOSIG assigned.

Figure 6

"TELETAXE_ITX_SIG option previously assigned to this trunk."

Generated when the operator tries to assign TELETAXE_NOSIG option to an IC/2W SSUTR2 trunk to which previosly TELETAXE_ITX_SIG assigned.

Figure 7

"SSUTR2_TAX_GEN option previously assigned to this trunk."

Generated when the operator tries to assign TELETAXE_ITX_SIG option to an IC/2W SSUTR2 trunk to which previosly SSUTR2_TAX_GEN assigned.

Figure 8

"TELETAXE_ITX_SIG option previously assigned to this trunk."

Generated when the operator tries to assign SSUTR2_TAX_GEN option to an IC/2W SSUTR2 trunk to which previosly TELETAXE_ITX_SIG assigned.

Figure 9

"WARNING - the peripheral must be equipped with an SX05 processor for this parameter to be functional"'

Generated when the operator tries to assign TELETAXE_ITX_SIG option to an IC/2W SSUTR2 trunk which is datafilled on peripheral is not equipped with an SX05 processor.

10.5.2.1.7 Table release history update

N/A.

10.5.2.1.8 Supplementary information

None.

10.5.2.1.9 Translation verification other tools

N/A.

10.6 Service Orders (SO) (CM & SESM)

N/A.

10.7 Software optionality control (SOC)

No changes due to this feature. Existing SOC options for backward charging functionality are used.

10.8 Element Management

N/A.

10.9 Command interface changes

N/A.

10.10 Security

N/A.

10.11 Configuration Walkthrough

N/A.

11: Configuration (CN): A00002173

11.1 Hardware and Software Requirements

Software requirements in order to work with this activity are as follows:

- SOC SOSM0001 must be activated.
- Tables MPCLINK, TRKGRP, SOSMMPC, SOSMTRK and SOSMPARM must have been datafilled before receiving START SOSM command from CP.

Hardware Requirements are as follows:

- SOSM system uses conference ports from a common pool in the DMS MMP. If all ports are used by SOSM, normal 3-way or 6-way calls will be denied. Similarly, if all ports are used by 3-way or 6-way calls, SOSM monitored calls will be unable to obtain an MCL connection.
- For X25 Messaging Interface, MPC cards must have been installed in DMS office (IOC (NT1x89) or IOM).
- Maximum 224 SPC trunks are needed for transmission of call content.

11.2 Initial Configuration

- Turn on SOC SOSM0001.
- Install MPC cards to the DMS MMP office.
- Datafill SPC trunks and SPC lines.
- If X25 messages will be sent over trunk, make the hardware connection of MPC links to the SPC trunks over modems and datafill the table SPCCON based on hardware connection that is used for SOSM.
- Datafill table SOSMMPC.
- Datafill table SOSMTRK appropriately.
- Modify parameters in SOSMPARM table if required.

11.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None

11.4 Upgrade Impact

11.4.1 Dump and Restore

When a software upgrade is taking place via a One Night Process (ONP), all static SOSM data (data in tables SOSMTRK, SOSMMPC, MPCLINK, MPC, SOSMPARM and TRKGRP) is transferred to the new software load

automatically. Dynamic tables are not transferred. After SWACT, appropriate message is sent to CP and SOSM is stopped.

11.4.2 Element Management Upgrade

NA.

11.5 Data schema (DS) (CM, MIBS, RDB)

11.5.1 New tables Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SOSMMPC	NEW	NEW
SOSMTRK	NEW	NEW
SOSMPARM	NEW	NEW

11.5.2 Table Schema information

11.5.2.1 Name: SOSMMPC

System of Operative Searching Measures (SOSM) MPC table

11.5.2.1.1 Functional description

This table provides the mechanism to allocate MPC cards for the DMS-Control Point X.25 Interface of SOSM feature. For each pair of channels, a tuple is added to this table.

11.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Table MPC

Table MPCLINK

Table SOSMMPC

11.5.2.1.3 Size

11.5.2.1.4 Fields

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SOSMMPC	0	8	This table is dynamically sized at tuple add time.Memory is automatically allocated for 8 SOSMMPC entry.

Table 3 Table SOSMMPC field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Key (SOSMLINK)	New	None	0 to 7	The name of the key field is SOSMLINK. None default value. This field is used to index the table by the SOSM X.25 application. Up to eight pairs of channels may be datafilled
DATACH1	New	None	MPCNO (0 to 255) LNKNO (0 to 3)	None default value. Specifies the MPC card and Link number to be used for DMS to CP Data Channel 1 (CP Command Interface)
DATACH2	New	None	MPCNO (0 to 255) LNKNO (0 to 3)	None default value. Specifies the MPC card and Link number to be used for DMS to CP Data Channel 2 (Call Information Channel)

11.5.2.1.5 Datafill example

The following example shows sample datafill for table SOSMMPC. Accessable only via SOSMCONF CI increment with a valid password

Table 4 Table SOSMMPC example datafill

RNBDLINK	CHNL1	CHNL2
0	3 2	3 3
1	4 2	4 3

SOSMMPC table entries can be edited only if the following criteria are met:

- SOSM0001 is ON,
- SOSMCONF CI increment is accessed with a valid password, and
- SOSM system is inactive (not activated by a CP command).

11.5.2.1.6 Table release history update
This table is added to the system by activity A00002173 in ISN07 context.

11.5.2.1.7 Supplementary information
NA.

11.5.2.1.8 Translation verification other tools
SOSMMPC does not use translation verification tools.

11.5.2.2 Name: SOSMTRK
System of Operative Searching Measures (SOSM) Trunk table

11.5.2.2.1 Functional description
This table is used by the SOSM system for mapping generic trunk groups into dedicated SOSM trunks. Each entry identifies a trunk group to be used for the PCM-30 group of MCLs.

11.5.2.2.2 Usage sequence and implications (CM Only)
Tables must be datafilled in the following sequence :

Table CLLI

Table TRKGRP

Table TRKSGRP

Table TRKMEM

Table SOSMTRK

11.5.2.2.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SOSMTRK	0	8	Memory is statistically allocated for 8 SOSMMPC entry. This table consumes 16 bytes in protected memory.

11.5.2.2.4 Fields

Table 6 Table SOSMTRK field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Key : SOSMGRP	New	None	0 to 7	This field identifies the PCM-30 group number.
CLLI	New	None	Common Language Name (CLLI)	This field identifies the trunk group to be used by SOSM. The CLLI entered here must correspond to a valid trunk datafilled in tables CLLI, TRKGRP, TRKSGRP and TRKMEM.

11.5.2.2.5 Datafill Example

The following example shows sample datafill for table SOSMTRK. SOSMTRK table is accessable only via SOSMCONF CI increment with a valid password.

Table 7 Table SOSMTRK example datafill

SOSMGRP	CLLI
0	SOSMGRP0
1	SOSMGRP1

SOSMTRK table entries can be edited only if the following criteria are met:

- SOSM0001 is ON,
- SOSMCONF CI increment is accessed with a valid password, and
- SOSM system is inactive (not activated by a CP command).

11.5.2.2.6 Table release history update
This table is added to the system by activity A00002172 in ISN07 context.

11.5.2.2.7 Supplementary information
NA.

11.5.2.2.8 Translation verification other tools
The following example shows the output from FINDREF when it is used to verify SOSMTRK.

11.5.2.3 Name: SOSMPARM
System of Operative Searching Measures (SOSM) Parameters

11.5.2.3.1 Functional description
Table SOSMPARM is used by SOSM system for saving SOSM specific parameters.

11.5.2.3.2 Usage sequence and implications (CM Only)
SOSMPARM is not referenced by any other tables.

SOSMPARM does not use any other tables.

11.5.2.3.3 Size
Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SOSMPARM	3	3	This table currently contains three tuples, and its memory is allocated statistically.

11.5.2.3.4 Fields

Table 9 Table SOSMPARM field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PARMNAME (Key)	New	None	TOLL_EXIT_CODE INTRAZONAL_CODE or INTERNTNL_CODE	This is the name of the SOSM specific parameter.
PARMVAL	New	PARMSEL	TOLL, INTRAZONAL, INTERNTNL	This subfield is the selector which determines the refinement used for the corresponding SOSM parameter. TOLL is valid only for TOLL_EXIT_CODE. INTRAZONAL is valid only for INTRAZONAL_CODE INTERNTNL is valid only for INTERNTNL_CODE parameters.
		PARMSEL : TOLL EXIT_CODE	Digit {0 to 9}	Toll exit code consists of a single digit between 0-9.
		PARMSEL : INTRAZONAL EXIT_CODE	Digit {0 to 9}	Zonal exit code consists of a single digit between 0-9.
		PARMSEL : INTERNTNL EXIT_CODE	2 digits of each {0 to 9}	International exit code consists of two digits, each between 0-9.

11.5.2.3.5 Datafill example

The following table shows default datafill for table SOSMPARM. This table is accessible only via SOSMCONF CI increment with a valid password.

Table 10 Default SOSMPARM tuples

PARMNAME	PARMVAL	
	PARMSEL	EXIT_CODE
TOLL_EXIT_CODE	TOLL	8 (1 digit is allowed for this parameter)
INTRAZONAL_CODE	INTRAZONAL	2 (1 digit is allowed for this parameter)
INTERNTNL_CODE	INTERNTNL	10 (1-2 digit(s) are allowed for this parameter)

Data in SOSMPARM table can not be deleted. Furthermore, addition of new tuples with table editing commands is prevented by SOSM software.

It is not permitted to change PARMSEL for the default parameters (TOLL_EXIT_CODE, INTRAZONAL_CODE and INTERNTNL_CODE) by table editing commands.

SOSMPARM table entries can be edited only if the following criteria are met:

- SOSM0001 is ON,
- SOSMCONF CI increment is accessed with a valid password, and
- SOSM system is inactive (not activated by a CP command).

11.5.2.3.6 Table release history update

This table is added to the system by activity A00002172 in ISN07 context.

11.5.2.3.7 Supplementary information

NA.

11.5.2.3.8 Translation verification other tools

NA.

11.6 Service Orders (SO) (CM & SESM)

NA.

11.7 Software optionality control (SOC)

Table 11 SOC

SOC option name:	SOSM - System of Operative-Searching Measures
SOC option title:	System of Operative-Searching Measures
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	SOSM0001
Option defined in DRU:	WT
Affected products:	MMP

Software Optionality Control is provided for SOSM feature. SOC order code is SOSM0001.

While SOSM0001 is OFF:

- Any message received from CP are ignored. (DMS MMP neither executes the command nor sends response to the control point at this state.)
- Access to SOSM configuration CI level is not permitted even if the valid password is entered.
- SOSM configuration tables SOSMMPC, SOSMTRK and SOSMPARM can be reached only within SOSMCONF CI level. Since access to SOSMCONF CI level is not permitted at this state, access to SOSM configuration tables is not possible while SOSM0001 is OFF.

Activation of SOSM0001:

- It is not allowed to turn SOSM0001 to ON state, while there is any other active NBD flavor (DNBD, etc...) on the switch.

While SOSM0001 is ON:

- Activation of any other Network Broadcast Delivery (NBD) application is not allowed after turning SOSM0001 to ON state.
- Access to SOSM configuration tables via SOSMCONF CI level is possible.
- Commands received from CP are processed as described in the previous sections.

Deactivation of SOSM0001:

- Turning SOSM0001 OFF deactivates all SOSM applications on the exchange. SOSM is stopped, and all dynamic data within MCL and monitoring order databases are cleared.
- SOSM system password is reset with the initial password.
- Data in SOSMMPC, SOSMTRK and SOSMPARM tables remains unchanged. However, access to these tables are prevented as indicated above.

11.8 Element Management

None.

11.9 Command Interface changes

11.9.1 Directory: SOSMCONF

System of Operative Searching Measures (SOSM) Configuration

11.9.1.1 Directory description

Access to SOSM configuration tables, namely, SOSMMPC, SOSMTRK and SOSMPARM is restricted. The only way to reach these tables is with this new CI level called SOSMCONF (SOSM Configuration).

11.9.1.2 Accessing directory: CI

11.9.1.2.1 Command Interface**Access to directory or MAP level and return to CI**

To access SOSMCONF from CI level, enter SOSMCONF.

While accessing to SOSMCONF, the user is asked for the access password. Appropriate access password should be provided when it is requested..

To return to the CI environment, enter quit.

12: Configuration (CN): A00002252

12.1 Hardware and Software Requirements

Act ID 89009298 functionality is resident in the CCM19 and CNA19 software layers in the core. While this functionality may be resident, it is dormant unless features 89008782 and 89008025 are present. These features reside in MG9K EM and SESM respectively. Feature 89008025 specifically provisions MG9K lines with the new LEN format.

Initial Configuration This specific feature does not require changes to initial configuration.

12.2 Office/Subnet parameters (OP/SP) (CM & SESM)

The functionality of office parm RDT_SUCC_AUTOCREATE_LNINV is altered with this feature for MG9K lines. For MG9K lines the value of ACTIVE is ignored, and no autoprovisioning of table LNINV is allowed. DEFAULT_MNO is used for MG9K lines.

12.3 Upgrade Impact

This feature does not directly impact a system upgrade. However, upgrading a Succession MG9K GW network from SN05 to SN06 does require special handling. Essentially, existing MG9K LENs and terminal ids will be migrated to use the new LEN format. All of this will be driven by MG9K EM and will be completely transparent for a core SN05 to SN06 upgrade. Please refer to 89008025 documentation for more info.

12.3.1 Dump and Restore

This feature does not impact dump and restore on upgrades.

12.3.2 Element Management Upgrade

This feature does not impact EMs.

12.4 Data schema (DS) (CM, MIBS, RDB)

12.4.1 New/modified tables, MIBs, or Database Schema

The previously unused field GRPTYPE in Table LGRPINV is used in this feature to denote a specific type of LGRP. The values for GRPTYPE are S, M, and C. This feature disables SERVORD autoprovisioning for GRPTYPE S for groups on shelves 0 to 3; refer to the FN section for more info. Currently,

GRPTYPE S will denote a set of LGRPs that for now will only include MG9K LGRPs.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LGRPINV	CHANGED	UNCHANGED
PADDATA	CHANGED	UNCHANGED

Table PADDATA will have two new pad groups which will be used by gateway lines. Pad group PKLNL will be used by gateways lines with LGRP GRPTYPE set to S. PKNIL will be used by gateway lines with LGRP GRPTYPE set to C.

12.4.2 Table/MIB/Remote Database Schema information

12.4.2.1 Name: LGRPINV

Logical Group Inventory Table

12.4.2.1.1 Functional description

Table LGRPINV contains logical group information for gateway lines.

12.4.2.1.2 Usage sequence and implications (CM Only)

SESM will provision table LGRPINV for LGRPs with GRPTYPE S.

12.4.2.1.3 Size

Table size is not changed via this feature.

12.4.2.1.4 Fields

The following table details the GRPTYPE field in table LGRPINV.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GRPTYPE	Changed	None	S C M	S denotes a specific set of LGRPs that includes MG9K LGRPs. C denotes all other LGRPs M is currently not used.

12.4.2.1.5 Datafill example

The following example shows sample datafill for table LGRPINV.

```
    GRPNO       SRVRNAME GRPTYPE                    LGRPOPTS
------------------------------------------------------------------------
CO10  00 0        GWC   1              S                        $
```

12.4.2.1.6 Table release history update
A GRPTYPE value of S denotes a specific set of LGRPs that include MG9K LGRPs. A GRPTYPE value of C is used for all other gateway LGRPs. GRPTYPE M is currently not used.

12.4.2.1.7 Supplementary information
None.

12.4.2.1.8 Translation verification other tools
Table LGRPINV is not displayed for TRAVER.

12.4.2.2 Name: PADDATA
Pad Data Table

12.4.2.2.1 Functional description
Table PADDATA contains attenuation and boost settings for different device interactions. Pads are applied to devices in order to balance volume levels.

12.4.2.2.2 Usage sequence and implications (CM Only)
Pad groups PKLNL and PKNIL will be defined and will appear in table PADDATA in the nodatafill base load.

12.4.2.2.3 Size
Pad value settings will be created for the two new pad groups. New table size will be within the allocated size.

12.4.2.2.4 Fields
Fields will not change with these changes.

12.4.2.2.5 Datafill example
The following example would apply a 3db attenuation to a line with pad group PKLNL and a 3db gain to a line with pad group STDLN whenever the lines are connected:

```
PKTLN   STDLN   3L   3G
```

12.4.2.2.6 Table release history update
Pad group PKLNL is to be used only by gateway lines that have LGRP GRPTYPE set to S. Pad group PKNIL is to be used only by gateway lines that have LGRP GRPTYPE set to C. Gateway lines will automatically have the appropriate pad group assigned when they are provisioned.

12.4.2.2.7 Supplementary information
None.

12.4.2.2.8 Translation verification other tools
Table PADDATA is not used in TRAVER.

12.5 Service Orders (SO) (CM & SESM)

12.5.1 Service order change details
Act ID 89009298 disables SERVORD autoprovisioning for gateway lines that have an LGRP type of S (table LGRPINV field GRPTYPE) that reside on shelves 0 to 3. Autoprovisioning provisions or deletes datafill to table LNINV for specific SERVORD+ commands received from SESM. SESM will preprovision table LNINV at the time of node provisioning; reference documentation for Act ID 89008025. This functionality supercedes the setting of office parm RDT_SUCC_AUTOCREATE_LNINV which is applicable to ther types of line gateways. Previously, office parm RDT_SO_AUTOCREATE_LNINV was used for setting autoprovisioning for gateway lines (SN05). RDT_SUCC_AUTOCREATE_LNINV was introduced in SN06 specifically for gateway line autoprovisioning. Neither office parm is applicable for MG9K gateway lines.

Pad group PKLNL will be assigned to gateway lines that have LGRP GRPTYPE set to S via SERVORD. Pad group PKNIL will be assigned to gateway lines that have LGRP GRPTYPE set to C via SERVORD. Attempts to change the pad group via SESM or SERVORD will not be successful. The appropriate gateway pad group will be assigned. However, the pad group can be changed in table LNINV via table control if need be.

12.6 Software optionality control (SOC)
This feature has no effect on SOC.

12.7 Element Management
This feature has no effect on EM. However, Act ID 89008782 does.

12.8 Command interface changes
Act ID 89009298 changes the format for gateway LENs that have GRPTYPE set to S in table LGRPINV. Please refer to the FN for detailed information on the change. Consequently, any CI command that requires a LEN for input must use the new format for a gateway line with GRPTYPE set to S in table LGRPINV. Likewise, any gateway LEN with GRPTYPE set to S in table LGRPINV display via a CI command (or MAPCI) will be displayed in the new format.

12.9 Security
None.

12.10 Configuration Walkthrough

Please reference Act ID 89008782 documentation.

13: Configuration (CN): A00002291

13.1 Hardware and Software Requirements

There is no special Hardware/Software Requirements.

13.2 Initial Configuration

N/A

13.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

13.4 Upgrade Impact - N/A

13.5 Data schema (DS) (CM, MIBS, RDB)

13.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	CHANGED	UNCHANGED

13.5.2 Table/MIB/Remote Database Schema information

13.5.2.1 Table Name: TRKOPTS.

13.5.2.1.1 Functional description

The new trunk option TKO_FDCP should be assigned to incoming FDCP trunk in the table TRKOPTS. It will allow TKO feature **for specific incoming directions**.

13.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

13.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	0		

13.5.2.1.4 Fields/OIDs

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTINFO	Changed	refinement	TKO_FDCP	The new trunk option ***TKO_FDCP*** should be assigned to incoming FDCP trunk in the table TRKOPTS. It will allow TKO feature **for specific incoming directions**.

13.5.2.1.5 Datafill example

Figure 1 New trunk option TKO_FDCP in table TRKOPTS.

```
TABLE: TRKOPTS.
>
        OPTKEY        OPTINFO
-------------------------
R2IC TKO_FDCP      TKO_FDCP
```

Figure 2 New trunk option TKO_FDCP in table TRKOPTS.

```
TABLE: TRKOPTS.
ran 2
TYPE IS TRKOPTS_OPTINFO_VAR_AREA MULTIPLE WITH
        OPTION                   TRKOPTS_OPTION REFINEMENTS:
        {SLOWREL}                TRKOPTS_OPTINFO_BOOL_AREA
        {FLEXCLI}                MULTIPLE WITH

         ........
         ........
         ........

        {BWRLSIND}               TRKOPTS_OPTINFO_BOOL_AREA
        {FWRLSIND}               TRKOPTS_OPTINFO_BOOL_AREA
        {RINGBACK}               TRKOPTS_OPTINFO_BOOL_AREA
        {TKO_FDCP}                 TRKOPTS_OPTINFO_BOOL_AREA
```

13.5.2.1.6 Table release history update

13.5.2.1.7 Supplementary information

None.

13.5.2.1.8 Translation verification other tools

Table TRKOPTS does not use translation verification tools.

13.6 Service Orders (SO) (CM & SESM)

N/A

13.7 Software optionality control (SOC)

N/A

13.8 Element Management

N/A

13.9 Command interface changes

N/A

13.10 Security

N/A

13.11 Configuration Walkthrough

N/A

14: Configuration (CN): A00002293

14.1 Hardware and Software Requirements

MMP20

14.2 Initial Configuration

14.2.1 RGC Datafill for Activation / Deactivation

The following datafill in the table **IBNXLA** is needed:

— for RGC activation by dialing *66 on IBN lines

FXRES 66 FEAT N N RGC

— for RGC deactivation by dialing #66 on IBN lines

OCTRES 66 FEAT N N RGCDE

— for RGC activation by dialing *66 on ISDN lines

FXISDN 66 FEAT N N RGC

— for RGC deactivation by dialing #66 on ISDN lines

OCTISDN 66 FEAT N N RGCDE

14.2.2 Translation verification tools

The following examples show the output from TRAVER when it is used to verify table IBNXLA:

Figure 1 RGC feature activation (*66) on IBN line

```
>traver l 3651800 B66 b
TABLE IBNLINES
URM 00 0 14 08 0 DT STN IBN 3360007 RESGRP 0 10 303 (MTR) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP EINGRP
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
RESGRP 10 0 0 CL1FR ( XLAS CMAIN10 NXLA NDGT) (PUB_NET_ACC $ (LINEATTR 10
303_NPRT_10 NIL_RATE)$)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA FXRES 0 POTS
TABLE DIGCOL
POTS specified: POTS digit collection
NCOS FEAT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME FXRES
FXRES 66 FEAT N N RGC

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature RGC        not supported by TRAVER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 2 RGC feature deactivation (#66) on ISDN line

```
>traver 1 3650205 C66 b
TABLE KSETLINE
ISDN1 205 1 DN N 3650205 ISDNGRP 0 0 454 (SFC) $ BRI UNDEF N $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE NCOS
ISDNGRP 0 0 0 ISDN ( XLAS PRISDN0 NXLA POTS) (PUB_NET_ACC $ (LINEATTR 3
454_NPRT_3 NLCA_NILLA_0)$)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
ISDNGRP NXLA ISDNXLA FXISDN 0 POTS
TABLE DIGCOL
POTS specified: POTS digit collection
NCOS OCT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME OCTISDN
OCTISDN 66 FEAT N N RGCDE
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature RGCDE        not supported by TRAVER


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

14.3 Data schema (DS) (CM, MIBS, RDB)

14.3.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

14.3.2 Table/MIB/Remote Database Schema information

14.3.2.1 Name: ISERVOPT

International Service Option

14.3.2.1.1 Functional description

Operating company personnel uses table ISERVOPT to configure switch information for service-related features. This table groups multiple related pieces of data in single entry.

Each service that uses this table provides a subfield related to that service. Each subfield asks for information in a format relevant to the service. This table accepts an entry if operating company personnel enter a service that is in the load.

14.3.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

14.3.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	100	Static memory allocation

14.3.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT:.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	New		RGC	
SOPTSVAR	Changed	OPTION	RGC	Registered Call
	New	AUTO_DEACT _TIMEOUT	5 to 30 minutes	AUTO_DEACT_TIME OUT determines the maximum timeout between RGC activation and automatic feature deactivation. The default value is **10**

14.3.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

SOPTSKEY SOPTSVAR

RGC RGC 10

Note: *This datafill indicates that DMS supports RGC feature and that RGC feature can be automatically deactivated in 10 minutes.*

14.3.2.1.6 Table release history update

The following information was added:

— entry RGC added to field SOPTSKEY

— entry of selector RGC with subfield AUTO_DEACT_TIMEOUT added to field SOPTSVAR

14.3.2.1.7 Supplementary information

NONE.

14.3.2.1.8 Translation verification other tools

ISERVOPT does not use translation verification tools.

14.4 Service Orders (SO) (CM & SESM)

14.4.1 Service order change details

14.4.1.1 LCC and options

- New line option RGC is applied to the following line class code (LCC): IBN and ISDNKSET and is added to table LCCOPT.

Figure 3 Example of RGC tuples in table LCCOPT

```
 IBN  (ACB) (AR) ..... (VMI) (WML) (WUCR) (RGC) $

ISDNKSET (AFC) (AUL) (CFB)..... (VMI) (WML) (WUCR) (RGC) $
```

- LIST options NOT compatible with new RGC option is added to OPTOPT table:

Figure 4 Example of RGC tuple in table OPTOPT

```
RGC (ACB) (AR) (AUL) (DLH) (DNH) (GIC) (MAN) (MLH) (MPB) (WML)$
```

14.4.2 Servord commands for RGC line option

14.4.2.1 How service order options are presented

14.4.2.1.1 Description

A new RGC (Registered Call) line option is added.

RGC option enables the subscriber on the assigned line automatic redialing to the last valid call (that passed translation and routing in the switch).

For ISDN set, the RGC option is assigned on a per-key.

14.4.2.1.2 Option prompts

Table 4 System prompts for RGC option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	RGC	Specifies the option to assign to the line	
TIMEOUT	{1 TO 20} seconds	Specifies the timeout in seconds between off-hook and starting dialing after feature activation	

14.4.2.1.3 Example of service order prompt

Figure 5 Example of the RGC option in prompt mode for IBN line

```
>ADO
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>3651801
OPTION:
>RGC
TIMEOUT:
>5
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 3 25 AM 3651801 ( RGC 5 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT

>CHF
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>3651801
OPTION:
>RGC
TIMEOUT:
>14
OPTION:
>$
COMMAND AS ENTERED:
CHF NOW 3 3 25 AM 3651801 ( RGC 14 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT

>DEO
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>HOST  02 0 18 01
OPTION:
>RGC
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 3 25 AM HOST 02 0 18 01 ( RGC ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

Figure 6 Example of the RGC option in no-prompt mode for IBN line

```
>ADO $ 3651801 RGC 5 $ yy
COMMAND AS ENTERED:
ADO NOW 3 3 25 AM 3651801 ( RGC 5 ) $

>CHF $ 3651801 RGC 14 $ yy
COMMAND AS ENTERED:
CHF NOW 3 3 25 AM 3651801 ( RGC 14 ) $

>DEO $ HOST  02 0 18 01 RGC $ yy
COMMAND AS ENTERED:
DEO NOW 3 3 25 AM HOST 02 0 18 01 ( RGC ) $
```

Figure 7 Example of the RGC option in prompt mode for BRI line

```
>ADO
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>3650200
OPTKEY:
>1
OPTION:
>RGC
TIMEOUT:
>5
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 3 25 AM 3650200 ( 1 RGC 5 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

```
>CHF
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>ISDN1 200
OPTKEY:
>1
OPTION:
>RGC
TIMEOUT:
>17
OPTKEY:
>$
COMMAND AS ENTERED:
CHF NOW 3 3 25 AM ISDN1 200 ( 1 RGC 17 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT

>DEO
SONUMBER:    NOW   3  3 25 AM
>
DN_OR_LEN:
>ISDN1 200
OPTKEY:
>1
OPTION:
>RGC
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 3 3 25 AM ISDN1 200 ( 1 RGC ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

Figure 8 Example of the RGC option in no-prompt mode for BRI line

```
>ADO $ ISDN1 200 1 RGC 5 $ yy
COMMAND AS ENTERED:
ADO NOW 3 3 25 AM ISDN1 200 ( 1 RGC 5 ) $

>CHF $ 3650200  1 RGC 17 $ yy
COMMAND AS ENTERED:
CHF NOW 3 3 25 AM 3650200 ( 1 RGC 17 ) $
```

```
>DEO $ ISDN1 200 1 RGC $ YY
COMMAND AS ENTERED:
DEO NOW 3 3 25 PM ISDN1 200 ( 1 RGC ) $
```

14.4.2.1.4 Example of QDN/QLT commands

Figure 9 Example of the RGC option in QDN prompt

```
>qdn 3360007
--------------------------------------------------------------------------
DN:     3360007
TYPE: SINGLE PARTY LINE
SNPA: 303   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     URM   00 0 14 08
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:        RESGRP     SUBGRP: 0  NCOS: 10
CARDCODE:  6K18AA    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    56
PM TERMINAL NUMBER :    457
OPTIONS:
MTR DGT RGC N 5
```

where N — field pointed to RGC feature state (Y-active, N-deactive)
5 — timeout between off-hook and starting dialing

Figure 10 Example of the RGC option in QLT prompt

```
>qlt ISDN1 200
------------------------------------------------------------------------------
LTID:  ISDN1     200
SNPA: 454
DIRECTORY NUMBER:     3650200
LT GROUP NO: 1
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:      ETSI  ISSUE: 0
LEN: HOST  02 0 02 00    TEI: UNATEI
CUSTGRP:        ISDNGRP  SUBGRP: 0  NCOS: 0  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 24
OPTIONS:
SFC HOLD
RGC N 5

  KEY      DN
  ---      --
   1       DN        4543650200
   4       DN        4543651200

  KEY     FEATURE
  ---     -------
   1      RGC N  5
```

14.4.2.1.5 RGC option appearance in tables IBNFEAT/KSETFEAT

Figure 11 Example of displaying RGC option in table IBNFEAT

```
>TABLE IBNFEAT

LEN DNNO DF FEATURE DATA
------------------------
HOST 02 0 18 01 0 RGC RGC N 3651804 5
```

Figure 12 Example of displaying RGC option in table KSETFEAT

```
>TABLE KSETFEAT

FEATKEY FEATURE KVAR
--------------------
ISDN1 200 1 RGC RGC N 3651804 5
```

Note: ***N*** *— field pointed to RGC feature state (Y-active, N-deactive)*
3651804 *— last dialed number that was stored after activation was done.*
5 *— timeout between off-hook and starting dialing*

14.4.2.1.6 Notes

The following notes apply to RGC option:

Field ACTIVE in tables IBNFEAT and KSETFEAT can not be changed via Servord and is updated after feature activation/deactivation is done ONLY.

14.5 Configuration Walkthrough

Following are the provisioning steps for the RGC performance:

- Datafill RGC tuple in table ISERVOPT (“14.3.2.1.5 Datafill example”).
- Datafill table IBNXLA for feature/activation (“14.2.1 RGC Datafill for Activation / Deactivation”)

- Servord:
  - — Add RGC option to the line (“14.4.2 Servord commands for RGC line option”)

Next steps are needed to establish RGC successful call:

- Perform successful call from the RGC line to line/trunk
- Off hook a phone and dial the RGC activation code (*66)
- Verify that the confirmation tone is heard
- On hook the phone
- Off hook, wait for timeout defined in table IBNFEAT / KSETFEAT to establish call to the last dialed destination number

15: Configuration (CN): A00002319

15.1 Hardware and Software Requirements

- MMP20.
- PDTC (with the ETSI ISUP Hardware configuration) or Shrink CPM are required.

15.2 Initial Configuration

The following initial definitions should be supported:

15.2.1 Datafill for IBN and BRI subscribers.

Figure 1 Datafill for IBN subscriber without LAMP.

```
SERVORD:
ADO $ 3220070 CFD N 15043220070 A CFB N 15043220070 A MWT STD N N N$ YY

QDN 3220070
DN:     3220070
TYPE: SINGLE PARTY LINE
SNPA: 071   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 03 10
LINE CLASS CODE:      IBN
IBN TYPE: STATION
CUSTGRP:          RESGRP     SUBGRP: 0  NCOS: 8
CARDCODE:  6K17AC    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    23
PM TERMINAL NUMBER :    107
OPTIONS:
DGT CFD N 15043220070 A CFB N 15043220070 A MWT STD N N N
```

Note: To support MWI functionality for busy or does not answer line, Call Forward Busy Line(CFB) or Call Forward Don’t Answer(CFD) features should be defined correspondingly in addition to MWT line option.

Figure 2 Datafill for IBN subscriber with LAMP.

```
SERVORD:
ADO $ 3220070 CFD N 15043220070 A CFB N 15043220070 A MWT CMWI Y N N N$ YY

QDN 3220070
DN:     3220070
TYPE: SINGLE PARTY LINE
SNPA: 071   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     HOST  00 0 03 10
LINE CLASS CODE:      IBN
IBN TYPE: STATION
CUSTGRP:          RESGRP     SUBGRP: 0  NCOS: 8
CARDCODE:  6K17AC    GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER     :    23
PM TERMINAL NUMBER :    107
OPTIONS:
DGT CFD N 15043220070 A CFB N 15043220070 A MWT CMWI Y N N N
```

Figure 3 Datafill for BRI subscriber

```
SERVORD:
>ADO $ ISDN1 381 1 VMI N N $ Y Y
>ADO $ ISDN1 381 1 CFD N 15063381010 $ 1 CFB N 15263381010 $ $ Y Y

QLT ISDN1 381
LTID:  ISDN1     381
SNPA: 306
DIRECTORY NUMBER:     3381010
LT GROUP NO: 1
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  03 0 16 12    TEI: UNATEI
CUSTGRP:         ISDNGRP  SUBGRP: 0  NCOS: 72  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 32
OPTIONS:
AFC
CFB N 15263381010 A $ CFD N 15063381010 A $ COT NOAMA $ VMI N N SFC PROVHLC
VBINFO CMDATA COLP HOLD PROVCGS VBINFO CMDATA PROVCDS VBINFO CMDATA PROVLLC
VBINFO CMDATA

   KEY       DN
   ---       --
     1       DN          3063381010
     4       DN          3063381011
     7       DN          3063381012
    10       DN          3063381013
    14       DN          3083791099

   KEY     FEATURE
   ---     -------
     1       HOLD
     1        CFB N                    15263381010         A $
     1        CFD N                    15063381010         A $
     1        COT NOAMA $
     1        VMI N N
     2        AFC
     5        AFC
     8        AFC
```

Note: To support MWI functionality for busy or does not answer line, Call Forward Busy Line(CFB) or Call Forward Don't Answer(CFD) features should be defined correspondingly in addition to VMI line option.

Figure 4 Datafill for BRI subscriber with secondary DN

```
SERVORD:
>ADO $ ISDN 500 1 CFK $ 1 CFD P $ 1 CFB P $ 1 VMI N N 4 VMI N N $ YY

QLT ISDN 500
LTID:  ISDN      500
SNPA: 700
DIRECTORY NUMBER:     5003500
LT GROUP NO: 0
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  00 0 05 00    TEI: UNATEI
CUSTGRP:         ISDNGRP  SUBGRP: 0  NCOS: 30  RING: N
LINE CLASS CODE: ISDNKSET
MAXKEYS: 64
OPTIONS:
AFC
CFK $ I $ CFB P $ I $ CFD P $ I $ VMI N N SFC

   KEY       DN
   ---       --
     1       DN          7005003500
     4       DN          7005003510

   KEY     FEATURE
   ---     -------
     1        CFK                              $ I $
     1        CFB P                              $          I $
     1        CFD P                              $          I $
     4        CFK                              $ I $
     4        CFB P                              $          I $
     4        CFD P                              $          I $
     1        VMI N N
     2        AFC
     3        AFC
     4        VMI N N
     5        AFC
     6        AFC
```

15.2.2 Table Control

Figure 5 Datafill example for setting SDT on / turning LAMP on.

```
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F

TABLE: PXCODE
ISDN 5553 5553 DMOD ( INSRT 100) ( DEL 3) ( XLT PX MWICR)$

TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F

TABLE: PXCODE
MWICR 1003 1003 RTE MM 10 10 DEST 1003 CLASS NATL
MWICR 1006 1006 RTE MM 10 10 DEST 125 CLASS NATL

TABLE: PXRTE
MWICR   1003 CND  VMI   T   OFRT   88
MWICR   125 S         TRISUP1

TABLE: OFRT
88 TRMT CONF

TABLE: TMTMAP
Q767 CONF ALLBC  ISUP  NOLOCAL  NORMCLR  LOCLNET N
```

Figure 6 Datafill example for setting SDT off / turning LAMP off.

```
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F

TABLE: PXCODE
ISDN 7773 7773 DMOD ( INSRT 101) ( DEL 3) ( XLT PX MWICR)$

TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F

TABLE: PXCODE
MWICR 1013 1013 RTE MM 10 10 DEST 1003 CLASS NATL
MWICR 1016 1016 RTE MM 10 10 DEST 125 CLASS NATL

TABLE: PXRTE
 MWICR   1003 CND  VMI   T   OFRT   88
 MWICR   125 S         TRISUP1

TABLE: OFRT
88 TRMT CONF

TABLE: TMTMAP
Q767 CONF ALLBC  ISUP  NOLOCAL  NORMCLR  LOCLNET N
```

Figure 7 Additional datafill for MWI feature.

```
TABLE FEATOPTS
VMI VMI
MWT MWT N $
TABLE LCCOPT
IBN      (MWT)
ISDNKSET     (VMI)
TABLE DNREVXLA
CLD2FLXD  0338  0338   DEFAULT 1 306

The following tuple should be defimed only for subscribers with LAMP:
TABLE RESOFC
CMWI Y SUBSCR CMWI SINGLE 5 $
```

15.3 Upgrade Impact

15.3.1 Dump and Restore

No DUMP and Restore reformat algorithm is required for this feature.

15.3.2 Element Management Upgrade

N/A

15.4 Data schema (DS) (CM, MIBS, RDB)

15.4.1 New/modified tables, MIBs, or Database Schema

The PXRTE table will be modified. The CNDSEL of the CND route selector will be enhanced with VMI CND route condition.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
PXRTE	CHANGED	UNCHANGED

15.4.2 Table/MIB/Remote Database Schema information

15.4.2.1 Name: PXRTE

Prefix code Route.

15.4.2.1.1 Functional description

Table PXRTE is a member of the universal translation tables. The universal translation tables are organized to translate the incoming digit string in

segments. Table PXRTE translates the prefix code digit segment, together with tables PXHEAD and PXCODE.

15.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

15.4.2.1.3 Size

The table size is not changed.

Memory is allocated dynamically. When the first tuple for a given XLANAME is added, table size is allocated to accommodate the given route reference. As tuples are added, the table increases to accommodate the largest route reference index.

15.4.2.1.4 Fields/OIDs

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CNDSEL	Changed	refinement	VMI	The CND_RTE_CONDITION type is extended with VMI value.

15.4.2.1.5 Datafill example

Figure 8 The PXRTE datafill example.

```
XLANAME RTEREF RTELIST
-----------------------------------------
ISDN 100 (CND VMI T OFRT 88) $
```

Where RTELIST includes the following selectors and subfields:

RTESEL - the type is route_selector {S, N, T, **CND**, RT, SO, NOT, DCRT, NODE, SG}

CNDSEL - the type is cnd_rte_condition {ALWAYS, RND, SNPA, EA, TOD, NARS, COSMAP, NRR, SITE, CALLCHR, **VMI**}

RTETYPE - the type is cnd_rte_type {ST,T,SK}

TABNAME - the type is rter_id {OFRT, OFR2, OFR3, OFR4, IRTE, RRTE, IBNRTE, IBNRT2, IBNRT3, IBNRT4, TOPS}

INDEX - type is extended_route_ref_index {0 TO 1023}

15.4.2.1.6 Supplementary information

None.

15.4.2.1.7 Translation verification other tools

- The following examples shows the output from TRAVER when it is used to verify the PXRTE table (**CND VMI tuple is defined).**

Figure 9 Example of STD activation.

```
>traver tr ORISUP2 5553650006 b
TABLE TRKGRP
ORISUP2 IBNT2 0 LCO NCRT TRKPSTN 0 LIDL 0 N ANSDISC 0 N N N N N N N 0 0 N 0 0 0
    0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP EINGRP
TABLE NCOS
TRKPSTN 0 0 0 TRK ( XLAS PRTRK0 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PRTRK0
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK0
    (NET N N 0 N POTS N N GEN (LATTR 1000 454_NPRT_0 NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
POTS specified: POTS digit collection
TABLE LINEATTR
1000 NLCC NONE NT 1000 0 NILSFC 7 PX ISDN NIL 00 454_NPRT_0 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
454_NPRT_0 NSCR 454 NPRT NONE N $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    5553650006
TABLE PXCODE
ISDN 5553 5553 DMOD ( INSRT 100) ( DEL 3) ( XLT PX MWICR)$
TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    1003650006
TABLE PXCODE
MWICR 1003 1003 RTE ( MM 10 10) ( DEST 101) ( CLASS NATL)$
TABLE: PXRTE
KEY:    MWICR  101
 . CND VMI T OFRT 100
 .  . TABLE OFRT
 .  .  100 TRMT CONF
TABLE TMTCNTL
TITRKGRP ( 0)
 . SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 60)
 . SUBTABLE TREAT
 . CONF N S BST5
 .  . EXIT TABLE OFRT
EXIT TABLE PXRTE
TABLE TRIGGRP
EINGRP INFOANAL
 . GENTRIG (CDPN EINDIG)$ NIL
```

Figure 10 Example of STD deactivation.

```
>traver tr ORISUP2 777 3650006 b
TABLE TRKGRP
ORISUP2 IBNT2 0 LCO NCRT TRKPSTN 0 LIDL 0 N ANSDISC 0 N N N N N N N 0 0 N 0 0 0
    0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP EINGRP
TABLE NCOS
TRKPSTN 0 0 0 TRK ( XLAS PRTRK0 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PRTRK0
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK0
    (NET N N 0 N POTS N N GEN (LATTR 1000 454_NPRT_0 NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
POTS specified: POTS digit collection
TABLE LINEATTR
1000 NLCC NONE NT 1000 0 NILSFC 7 PX ISDN NIL 00 454_NPRT_0 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
454_NPRT_0 NSCR 454 NPRT NONE N $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    7773650006
TABLE PXCODE
ISDN 7773 7773 DMOD ( INSRT 101) ( DEL 3) ( XLT PX MWICR)$
TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    1013650006
TABLE PXCODE
MWICR 1013 1013 RTE ( MM 10 10) ( DEST 101) ( CLASS NATL)$
TABLE: PXRTE
KEY:    MWICR  101
 . CND VMI T OFRT 100
 .  . TABLE OFRT
 .  .  100 TRMT CONF
TABLE TMTCNTL
TITRKGRP ( 0)
 . SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 60)
 . SUBTABLE TREAT
 . CONF N S BST5
 .  . EXIT TABLE OFRT
EXIT TABLE PXRTE
TABLE TRIGGRP
EINGRP INFOANAL
 . GENTRIG (CDPN EINDIG)$ NIL
```

- The following examples shows the output from TRAVER when it is used to verify the PXRTE table (**CND VMI tuple is not defined).**

Figure 11 Example of STD activation.

```
>traver tr ORISUP2 5553650006 b
TABLE TRKGRP
ORISUP2 IBNT2 0 LCO NCRT TRKPSTN 0 LIDL 0 N ANSDISC 0 N N N N N N N 0 0 N 0 0 0
    0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP EINGRP
TABLE NCOS
TRKPSTN 0 0 0 TRK ( XLAS PRTRK0 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PRTRK0
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK0
    (NET N N 0 N POTS N N GEN (LATTR 1000 454_NPRT_0 NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
POTS specified: POTS digit collection
TABLE LINEATTR
1000 NLCC NONE NT 1000 0 NILSFC 7 PX ISDN NIL 00 454_NPRT_0 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
454_NPRT_0 NSCR 454 NPRT NONE N $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    5553650006
TABLE PXCODE
ISDN 5553 5553 DMOD ( INSRT 100) ( DEL 3) ( XLT PX MWICR)$
TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    1003650006
TABLE PXCODE
MWICR 1003 1003 RTE ( MM 10 10) ( DEST 125) ( CLASS NATL)$
TABLE: PXRTE
KEY:    MWICR   125
 . S TRISUP1
EXIT TABLE PXRTE
TABLE TRIGGRP
EINGRP INFOANAL
 . GENTRIG ( CDPN EINDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES
1 TRISUP1               1006012001         ST
TREATMENT ROUTES.  TREATMENT IS: GNCT
1 BST6
```

Figure 12 Example of STD deactivation.

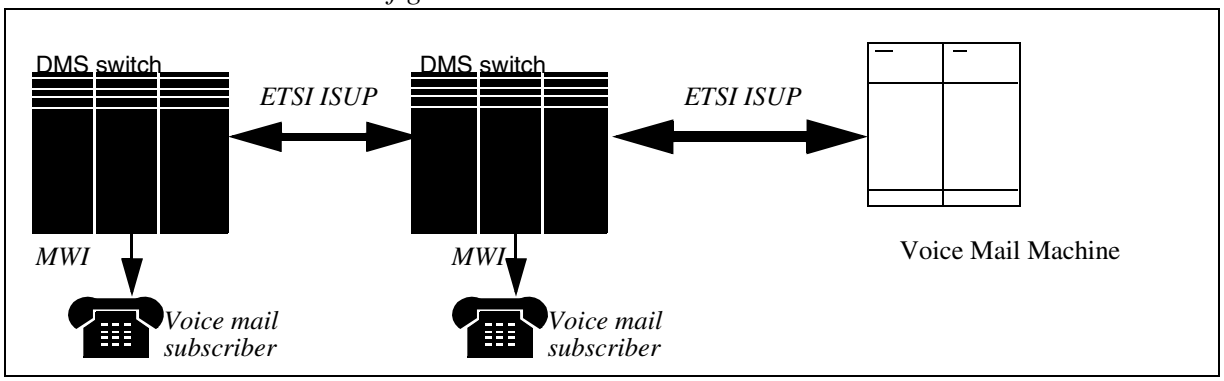
```
>traver tr ORISUP2 7773650006 b
TABLE TRKGRP
ORISUP2 IBNT2 0 LCO NCRT TRKPSTN 0 LIDL 0 N ANSDISC 0 N N N N N N N 0 0 N 0 0 0
    0 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP EINGRP
TABLE NCOS
TRKPSTN 0 0 0 TRK ( XLAS PRTRK0 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP:  no subscribed trigger.
TABLE IBNXLA: XLANAME PRTRK0
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK0
    (NET N N 0 N POTS N N GEN (LATTR 1000 454_NPRT_0 NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
POTS specified: POTS digit collection
TABLE LINEATTR
1000 NLCC NONE NT 1000 0 NILSFC 7 PX ISDN NIL 00 454_NPRT_0 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
454_NPRT_0 NSCR 454 NPRT NONE N $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
ISDN SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    7773650006
TABLE PXCODE
ISDN 7773 7773 DMOD ( INSRT 101) ( DEL 3) ( XLT PX MWICR)$
TABLE PXHEAD
MWICR SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    1013650006
TABLE PXCODE
MWICR 1013 1013 RTE ( MM 10 10) ( DEST 125) ( CLASS NATL)$
TABLE: PXRTE
KEY:     MWICR  125
 . S TRISUP1
EXIT TABLE PXRTE
TABLE TRIGGRP
EINGRP INFOANAL
 . GENTRIG ( CDPN EINDIG)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

 DIGIT TRANSLATION ROUTES
 1 TRISUP1              1016012001         ST
 TREATMENT ROUTES.  TREATMENT IS: GNCT
1 BST6
 +++ TRAVER: SUCCESSFUL CALL TRACE +++
```

15.5 Configuration Walkthrough

There are the provisioning steps for the “MWI control via ISUP” performance:

1. The following network configuration must be supported:

Network configuration.



2. Use Service Order tool to define the MWT line option for IBN Voice Mail subscribers (Figure 1, "Datafill for IBN subscriber without LAMP.", Figure 2, "Datafill for IBN subscriber with LAMP.").

3. Use Service Order tool to define the VMI line option for BRI Voice Mail subscribers (Figure 3, "Datafill for BRI subscriber").

4. Use Service Order tool to define the appropriate Call Forward line option for subscribers that have MWT or VMI line option.

5. Datafill tables (Figure 5, "Datafill example for setting SDT on / turning LAMP on.", Figure 6, "Datafill example for setting SDT off / turning LAMP off.", Figure 7, "Additional datafill for MWI feature.").

6. Perform a successful call to a VM subscriber. Leave a voice message.

7. Off hook the subscriber.

8. Verify that SDT is heard/Lamp is turned on.

9. Clear the voice message.

10. On hook the subscriber.

11. Off hook the subscriber.

12. Verify that SDT is not heard/Lamp is turned off.

16: Configuration (CN): A00002364

16.1 Hardware and Software Requirements

None.

16.2 Initial Configuration

None.

16.3 Office/Subnet parameters (OP/SP) (CM & SESM)

16.3.1 New/modified office/subnet parameters

None.

16.3.2 Parameter information

None.

16.4 Upgrade Impact

16.4.1 Dump and Restore

None.

16.4.2 Element Management Upgrade

None.

16.5 Data schema (DS) (CM, MIBS, RDB)

16.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CLICNTL	CHANGED	UNCHANGED

16.5.2 Table/MIB/Remote Database Schema information

16.5.2.1 Name: CLICNTL

16.5.2.1.1 Functional description

A new BILLING_OPTION named OCN is introduced by this feature to capture OCN in CDR. The new option is only created as a BILLING_OPTION, so it can be only added to the CLICTKEY which direction is incoming.

16.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

16.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CLICNTL	unchanged	unchanged	unchanged

16.5.2.1.4 Fields/OIDs

The following table lists fields changed by this feature for CLICNTL.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BILLING_OPTIONS	changed	None	{RDN,CLI, SCRN_NUM..... **OCN**	OCN is added by this feature to provide the capability to capture OCN in CDR

16.5.2.1.5 Datafill example

Figure 1 Datafill example for new option OCN

```
TABLE: CLICNTL

CLICTKEY DIRECTN
---------------
NONE IC $ (RDN) (CLI) $ Y

CLI_ONLY IC (CLI) $ (CLI) $ Y

RDN_ONLY IC (RDN) $ (RDN) $ Y

CLI_THEN_RDN IC (CLI) (RDN) $ (SCRN_NUM) $ Y

RDN_THEN_CLI IC (RDN) (CLI) $ (SCRN_NUM) $ Y

RDN_OCN_CLI IC $ (RDN) (OCN) (CLI) $ Y
```

16.5.2.1.6 Table release history update

Entry OCN is added to field BILLING_OPTIONS

16.5.2.1.7 Supplementary information

The entry OCN can not be added to a CLICTKEY which direction is ongoing, otherwise, an error will occur and related error message is displayed.

16.5.2.1.8 Translation verification other tools

None.

16.6 Service Orders (SO) (CM & SESM)

None.

16.7 Software optionality control (SOC)

None.

16.8 Element Management

None.

16.9 Command interface changes

None.

16.10 Security

None.

16.11 Configuration Walkthrough

None.

17: Configuration (CN): A00002365

17.1 Data schema (DS) (CM, MIBS, RDB)

17.1.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	changed	unchanged
TRKOPTS	changed	unchanged

17.1.2 Table information

17.1.2.1 Name: ISERVOPT

International Service Option

17.1.2.1.1 Functional description

N/A

17.1.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

There is no requirement to datafill tables in a specific order.

17.1.2.1.3 Size

N/A

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
N/A	N/A	N/A	N/A

17.1.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	Changed	-	CWR_ON_TRUNK	The new option CWR_ON_TRUNK is added to table ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSVAR	New	Option	CWR_ON_TRUNK	The option CWR_ON_TRUNK contains trunk types ETSI_ISUP, IBN7 and R2 that can be enabled or disabled for CWR over trunk.
SOPTSVAR	New	ETSI_ISUP	Y, N	The subfield ETSI_ISUP can be set to Y or N. Y enables and N disables CWR on trunk.
SOPTSVAR	New	IBN7	Y, N	The subfield IBN7 can be set to Y or N. Y enables and N disables CWR on trunk.
SOPTSVAR	New	R2	Y, N	The subfield R2 can be set to Y or N. Y enables and N disables CWR on trunk.

The following Figure 1 shows the list of table ISERVOPT including the new option CWR_ON_TRUNK.

Figure 1 List of CWR_ON_TRUNK in Table ISERVOPT

```
>table iservopt
TABLE: ISERVOPT
>ran
 1 SOPTSKEY        SERVOPTS_KEY
 2 SOPTSVAR        SERVOPTS_VAR_AREA
LOGICAL TUPLE TYPE: SERVOPTS_LOG_TUPLE
>ran 1
 1 SOPTSKEY        SERVOPTS_KEY
TYPE IS SERVOPTS_KEY MULTIPLE WITH
      SOPTNAME    SERVOPTSKEY
>ran 2
 2 SOPTSVAR        SERVOPTS_VAR_AREA
TYPE IS SERVOPTS_VAR_AREA            MULTIPLE WITH
      OPTION                  SERVOPTSKEY REFINEMENTS:
...
      {CWR_ON_TRUNK}              MULTIPLE WITH
         ETSI_ISUP {N,Y}
         IBN7 {N,Y}
         R2 {N,Y}
...
```

17.1.2.1.5 Datafill example

The following example in Figure 2 shows sample datafill for table ISERVOPT.

Figure 2 Example for Adding and Activating CWR_ON_TRUNK

```
>table iservopt
>pos cwr_on_trunk
TUPLE NOT FOUND
>add cwr_on_trunk
>y
OPTION:
>cwr_on_trunk
ETSI_ISUP:
>y
IBN7:
>n
R2:
>y
TUPLE TO BE ADDED:
        CWR_ON_TRUNK
                                CWR_ON_TRUNK Y N Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>pos cwr_on_trunk
        CWR_ON_TRUNK
                                CWR_ON_TRUNK Y N Y
>
```

17.1.2.1.6 Table release history update

Option CWR_ON_TRUNK added to field SOPTSVAR.

Option contains the subfields ETSI_ISUP, ISUP and R2.

Entries for the subfields are Y or N.

17.1.2.1.7 Supplementary information

N/A

17.1.2.1.8 Translation verification other tools

N/A

17.1.3 Table information

17.1.3.1 Name: TRKOPTS

Trunk Options

17.1.3.1.1 Functional description
N/A

17.1.3.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

17.1.3.1.3 Size
N/A

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
N/A	N/A	N/A	N/A

17.1.3.1.4 Fields/OIDs
The following table lists fields/OIDs for TRKOPTS.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTINFO	Changed	-	CWR_OFF	CWR_OFF option is assigned to a trunk group if CWR over trunk needs to be deactivated
OPTINFO	New	-	CWR_OFF	CWR_OFF option is assigned to a trunk group if CWR over trunk needs to be deactivated

17.1.3.1.5 Datafill example
The following example in Figure 3 shows sample datafill for table TRKOPTS.

Figure 3 Deactivate CWR for Specific Trunk Group

```
>table trkopts
>add rua501isupv2lp cwr_off
>y
OPTION:
>cwr_off
TUPLE TO BE ADDED:
 RUA501ISUPV2LP        CWR_OFF
                                          CWR_OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>pos rua501isupv2lp cwr_off
 RUA501ISUPV2LP        CWR_OFF
                                            CWR_OFF
>
```

17.1.3.1.6 Table release history update

Option CWR_OFF added to field OPTINFO.

17.1.3.1.7 Supplementary information

N/A

17.1.3.1.8 Translation verification other tools

N/A

18: Configuration (CN): A00002377

18.1 Hardware and Software Requirements

N/A

18.2 Initial Configuration

N/A

18.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

18.4 Upgrade Impact

N/A

18.5 Data schema (DS) (CM, MIBS, RDB)

N/A

18.6 Service Orders (SO) (CM & SESM)

This activity does not add a new service order (SO), it just increases the upper limit of the provisionable number of AFC Keys.

The old code allowed provisioning up to 4 AFC Keys on one DN. This activity increases the provisioning number of AFC Keys to 10 per DN for the DMS ETSI BRI implementation.

The master DN, known as SFC (Single Functional Call) key is able to have up to 10 AFC Keys associated with it. This can be specified through servord by using the AFC line option. If the AFC line option is added to a DN on a BRI set, the user is prompted for NUMCALLS indicating the number of call references permitted to be associated with that DN.

18.6.1 Service order change details

Increasing the upper limit of the provisionable number of AFC Keys just affects the DMS ETSI BRI variant. Other DRUs (such as NA) and other BRI variants (such as VN4 and AUSTEL) is not affected from the SO change.

18.6.2 New commands

N/A

18.6.3 Examples

The followings are assumed:

```
>qlt isdn2 1
-----------------------------------------------------
```

```
LTID:  ISDN2       1
SNPA: 102
DIRECTORY NUMBER:     7831004
LT GROUP NO: 2
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  25 0 00 04    TEI: UNATEI
CUSTGRP:        CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 5
OPTIONS:
SFC

   KEY       DN
   ---       --
     1       DN          1027831004


KEY     FEATURE
---     -------
      NONE
```

18.6.3.1 Before The Activity: Attempt to give 4 AFC (upper limit) to the SFC DN (for the ETSI and the NON-ETSI BRI variants)

```
>servord
SO:
>ADO
SONUMBER:     NOW   3  7 14 AM
>
DN_OR_LEN:
>ISDN2 1
OPTKEY:
>1
OPTION:
>AFC
NUMCALLS:
>4
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 7 14 AM ISDN2 1 ( 1 AFC 4 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

```
>Y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>Y
additional functional calls now exist on keys 2 TO 5



>qlt isdn2 1
-------------------------------------------------------
LTID:  ISDN2       1
SNPA: 102
DIRECTORY NUMBER:     7831004
LT GROUP NO: 2
LTCLASS:  BRAFS    DEFAULT LOGICAL TERMINAL: Y
EKTS: N   CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE   VBD   CMD
CS: Y PS: N
ELN: N
VERSION:       ETSI  ISSUE: 0
LEN: HOST  25 0 00 04    TEI: UNATEI
CUSTGRP:        CUST783A  SUBGRP: 0  NCOS: 2  RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 5
OPTIONS:
AFC
SFC

   KEY       DN
   ---       --
     1       DN          1027831004

   KEY     FEATURE
   ---     -------
     2        AFC
     3        AFC
     4        AFC
     5        AFC
-------------------------------------------------------
```

18.6.3.2 Before The Activity: Attempt to give 5 AFC (exceeds the upper limit) to the SFC DN (for ETSI and the NON-ETSI BRI variants)

```
>servord
SO:
```

```
>ADO
SONUMBER:     NOW   3  7 14 AM
>
DN_OR_LEN:
>ISDN2 1
OPTKEY:
>1
OPTION:
>AFC
NUMCALLS:
>5
5
 ***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
PLEASE ENTER:
NUMCALLS:
>5
5
 ***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
TYPE IS AFC_CALLS_ON_SFC_DN {1 TO 4}
PLEASE ENTER:
NUMCALLS:
>
```

18.6.3.3 After The Activity: Attempt to give 10 AFC (upper limit for the ETSI BRI) to the SFC DN (for the ETSI BRI)

```
>servord
SO:
>ADO
SONUMBER:     NOW   3  7 14 AM
>
DN_OR_LEN:
>ISDN2 1
OPTKEY:
>1
OPTION:
>AFC
NUMCALLS:
>10
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 7 14 AM ISDN2 1 ( 1 AFC 10 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
```

```
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>Y
additional functional calls now exist on keys 2 TO 11
```

18.6.3.4 After The Activity: Attempt to give 11 AFC (exceeds the upper limit) to the SFC DN (for the ETSI BRI)

```
>servord
SO:
>ADO
SONUMBER:     NOW   3  7 14 AM
>
DN_OR_LEN:
>ISDN2 1
OPTKEY:
>1
OPTION:
>AFC
NUMCALLS:
>11
11
 ***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
PLEASE ENTER:
NUMCALLS:
>11
11
 ***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
TYPE IS AFC_CALLS_ON_SFC_DN {1 TO 10}
PLEASE ENTER:
NUMCALLS:
>
```

18.6.3.5 After The Activity: Attempt to give 10 AFC (exceeds the upper limit) to the SFC DN (for the NON-ETSI BRI variants)

```
>servord
SO:
>ADO
SONUMBER:     NOW   3  7 14 AM
>
DN_OR_LEN:
>ISDN2 1
OPTKEY:
>1
```

```
OPTION:
>AFC
NUMCALLS:
>10
10
***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
PLEASE ENTER:
NUMCALLS:
>10
10
 ***  ERROR  ***
|
TYPE OF NUMCALLS IS AFC_CALLS_ON_SFC_DN
TYPE IS AFC_CALLS_ON_SFC_DN {1 TO 4}
PLEASE ENTER:
NUMCALLS:
>
```

18.7 Software optionality control (SOC)

N/A

18.8 Element Management

N/A

18.9 Command interface changes

N/A

19: Configuration (CN): A00002639

19.1 Hardware and Software Requirements

Standard CS2K Configuration.

19.2 Initial Configuration

Not applicable.

19.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

19.4 Upgrade Impact

Not applicable.

19.5 Data schema (DS) (CM, MIBS, RDB)

19.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

19.5.2 Table/MIB/Remote Database Schema information

19.5.2.1 Name: ISERVOPT

19.5.2.1.1 Functional description

A new tuple ICWT is introduced by this activity in table ISERVOPT. This tuple specifies whether CWT announcements to be applied to the Call Waiting Party. If the booleans ICWT_ANN_ACTIVE and ICWT_TMO_ANN_ACTIVE are set to 'Y', the "Caller Call Waiting" and "Called Party Ignores Waiting Call" announcements are applied to the Call Waiting Party. ICWT_TIMEOUT_TREATMENT sub field controls ffter 30 secs timer expiry (and after the Called Party Ignores Waiting Call announcment, if being applied), a treatment (busy, answer, no_service_circuit timeout etc.) is applied to the Call Waiting Line. The treatment is defined by datafill

For the functional details, please refer to the FN section of this activity.

19.5.2.1.2 Usage sequence and implications (CM Only)

Not applicable.

19.5.2.1.3 Size
Unchanged.

19.5.2.1.4 Fields/OIDs
The following table lists fields/OIDs for ISERVOPT.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	Changed	-	ICWT	New entry ICWT defined.
SOPTSVAR	Changed	option	ICWT	New entry ICWT defined.
SOPTSVAR	New	icwt_ann_active	{Y, N}	icwt_ann_active: Whether “Caller Call Waiting” announcement should be applied ore not.
SOPTSVAR	New	icwt_tmo_ann_active	{Y, N}	icwt_tmo_ann_active: Whether “Called Party Ignores Waiting Call” announcement should be applied ore not.
SOPTSVAR	New	icwt_timeout_treatment	one of the *extended_treatment*	icwt_timeout_treatment:After 30 secs timer expiry a treatment (busy, answer, no_service_circuit timeout etc.) is applied to the Call Waiting Line

19.5.2.1.5 Datafill example
The following examples shows sample datafill for table ISERVOPT.

- If CWT announcements to the Waiting Party should be turned ON:
  ICWT ICWT Y Y UNDT
- If CWT announcements to the Waiting Party should be turned OFF:
  ICWT ICWT N N UNDT
- To set a timeout treatment to BUSY ICWT_TIMEOUT_TREATMENT field should be changed:
  ICWT ICWT N N BUSY

19.5.2.1.6 Table release history update
The following information was added:

Entry ICWT added to field SOPTSKEY and SOPTSVAR/OPTION.

New fields ICWT_ANN_ACTIVE, ICWT_TMO_ANN_ACTIVE and ICWT_TIMEOUT_TREATMENT are added to entry ICWT in field SOPTSKEY and SOPTSVAR/OPTION.

19.5.2.1.7 Supplementary information

None.

19.5.2.1.8 Translation verification other tools

ISERVOPT does not use translation verification tools.

19.6 Service Orders (SO) (CM & SESM)

Not applicable.

19.7 Software optionality control (SOC)

Not applicable

19.8 Element Management

Not applicable.

19.9 Command interface changes

Not applicable.

19.10 Security

Not applicable.

19.11 Configuration Walkthrough

In order to have CWT announcements to be applied to the Waiting Party, the following configuration is required:

- The Called Party has ICWT line option datafilled and activated,
- The CWT announcements datafilled and brought in service, and
- The ISERVOPT option ICWT is datafilled and its booleans ICWT_ANN_ACTIVE and ICWT_TMO_ANN_ACTIVE are activated.
- In order to change timeout treatment, the initial value should be selected via ICWT_TIMEOUT_TREATMENT field in ICWT tuple.

19.11.1 Datafilling ICWT Line Option

The following figure shows the steps for adding the ICWT line option to the Called Party:

Figure 1 Steps for adding ICWT line option to the Called Party

```
>servord
SO:
>ado $ 8888587771001
OPTION:
>CEPT
OPTION:
>ICWT
ICWT_ACTIVE:
>y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 6 7 PM 8888587771001 ( CEPT ) ( ICWT Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

19.11.2 Datafilling CWT Announcements

The “Call Waiting” and “Called User Ignores Waiting Call” announcements are datafilled using the existing CS2K announcement capabilities. Please, note that the CLLIs used for “Call Waiting” and “Called User Ignores Waiting Call” announcements are **hardcoded** to **ICWTANN** and **ICWTTMOANN**, respectively.

The following figure shows the steps for datafilling the CWT announcements:

Figure 2 Example for datafilling CWT Announcements

```
table clli
ove; ver off;
add ICWTANN 70 10 ICWT_ANNOUNCEMENT y y
add ICWTTMOANN 71 10 ICWT_ANNOUNCEMENT y y
quit

table anns
ove; ver off;
add ICWTANN NETWK 5 10 1 STND N 5
add ICWTTMOANN NETWK 5 10 1 STND N 5
quit

table annmems
ove; ver off;
add ICWTANN 0 UAS AUD 0 AUD 0
add ICWTTMOANN 0 UAS AUD 0 AUD 0
quit

table annphlst
ove; ver off;
add ICWTANN 0 AUD_546 $
add ICWTTMOANN 0 AUD_547 $
quit
```

The following figure shows the steps for bringing the CWT announcement trunks inservice:

Figure 3 Steps for bringing the CWT announcement trunks Inservice

```
mapci;mtc;trks;ttp

post g ICWTANN
bsy; rts

post g ICWTTMOANN
bsy; rts

quit all
```

19.11.3 Datafilling ISERVOPT Options

The following figure shows the steps for adding the ISERVOPT option ICWT and activating its booleans ICWT_ANN_ACTIVE and ICWT_TMO_ANN_ACTIVE:

Figure 4 Example for adding ICWT and activating its booleans

```
>table iservopt
>add icwt
>y
OPTION:
>icwt
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
> BUSY (one of the EXTENDED_TREATMENT)
TUPLE TO BE ADDED:
ICWT   ICWT    Y    Y BUSY

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

20: Configuration (CN): A00002641

20.1 Hardware and Software Requirements

All software upgraded to the SN07 line up.

20.2 Initial Configuration

All software upgraded to the SN07 line up.

20.3 Upgrade Impact

20.3.1 Dump and Restore

No impact. Handled automatically

20.3.2 Element Management Upgrade

N/A

20.4 Data schema (DS) (CM, MIBS, RDB)

20.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ILRCLASS	NEW	NEW
ISERVOPT	CHANGED	UNCHANGED

20.4.2 Table Schema information

20.4.2.1 Name: ILRCLASS

International Line Restriction Class

20.4.2.1.1 Functional description

Table ILRCLASS contains the barring programs for the ILR line option

20.4.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

20.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ILRCLASS	0	100	Memory is statically allocated

20.4.2.1.4 Fields

The following table lists fields for ILRCLASS.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Data dictionary type	Entry	Explanation and action
KEY	New	NIL	ILRCLASS _KEY	VECTOR OF UP TO 16 CHAR'S	ILR_CLASS is the name of the barring program. It is used by the ILR line option
RCODE	NEW	NIL	TWO_DIGI T_CODE	VECTOR OF UP TO 2 DIGITS	The RCODE identifies the barring program to the subscriber. It is unique in the table or empty.
IXLAOPT	NEW	NIL	ILRCLASS _IXLA_VE CTOR	VECTOR OF UP TO 32 IXLA_CLA S'S	Contains a list of international translation classes to be barred by this program
DNOPT	NEW	NIL	ILRCLASS _DN_VECT OR	VECTOR OF UP TO 10 VECTOR S OF UP TO 15 DIGITS	Contains a list of DNs which are barred additionally to the international translation classes

20.4.2.1.5 Datafill example

The following example shows sample datafill for table ILRCLASS.

Figure 1 Example entry in table ILRCLASS

```
TABLE ILRCLASS
DIDD 02 (CNTL) (ICNTL) (INTL) $(09000) (09001)$
```

20.4.2.1.6 Table release history update

ISN07: Table was created

20.4.2.1.7 Supplementary information

Barring classes in this table can only be deleted if there is no line with ILR in the office referencing this tuple.

If during an ONP from a release before this activity there are no R-codes assigned in the ILRCLS tuple in table ISERVOPT the R-Code in table ILRCLASS is left empty.

20.4.2.1.8 Translation verification other tools

ILRCLASS does not use translation verification tools.

20.4.3 Table/MIB/Remote Database Schema information

20.4.3.1 Name: ISERVOPT

International Service Option

20.4.3.1.1 Functional description

unchanged

20.4.3.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

20.4.3.1.3 Size

unchanged

20.4.3.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

SOPTSKEY = ILRCLS

If the entry in field SOPTSKEY is ILRCLASS, datafill field SOPTSVAR as shown in the field description table

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSVAR	Changed	ILRCLS	OPTIONS	The options field is deleted. The information contained in this field is now available in table ILRCLASS

20.4.3.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 2 Example entry in table ISERVOPT

```
TABLE ISERVOPT
ILRCLS ILRCLS Y Y
```

20.4.3.1.6 Table release history update

ISN07: removed OPTIONS field in ILRCLS selector

20.4.3.1.7 Supplementary information

None

20.4.3.1.8 Translation verification other tools

ISERVOPT does not use translation verification tools.

21: Configuration (CN): A00002642

21.1 Hardware and Software Requirements

All software upgraded to the SN07 line up.

21.2 Initial Configuration

All components of the CS2k initialized

21.3 Upgrade Impact

21.3.1 Dump and Restore

no impact. New fields are initialized automatically

21.3.2 Element Management Upgrade

no impact

21.4 Data schema (DS) (CM, MIBS, RDB)

21.4.1 New/modified tables

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

21.4.2 Table information

21.4.2.1 Name: ISERVOPT

International Service Option

21.4.2.1.1 Functional description

unchanged.

21.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

21.4.2.1.3 Size

unchanged

21.4.2.1.4 Fields

The following table lists fields for ISERVOPT.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSVAR	Changed	ICONF		
		WARNING_TONE	{Y,N}	Set to 'Y' to apply warning tone during I3WC conferences
		PREVENT_WML_DURING_ENQUIERY	{Y,N}	Set to 'Y' to prevent WML to be active during enquiry mode
		PREVENT_HELD_TONE	{Y,N}	Set to 'Y' to prevent held tone to be applied for the party on hold

21.4.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 ICONF tuple in ISERVOPT

```
>add iconf
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
OPTION:
>iconf
ALLOW_ICT_IN_I3WC:
>y
CLF_FLASH_IGNORE:
>y
WARNING_TONE:
>Y
PREVENT_WML_DURING_ENQUIRY
>Y
PREVENT_HELD_TONE
>Y
TUPLE TO BE ADDED:
                   ICONF
                                                          ICONF Y Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

21.4.2.1.6 Table release history update

ISN07: refined ICONF to include WARNING_TONE, PREVENT_WML_DURING_ENQUIERY and PREVENT_HELD_TONE

21.4.2.1.7 Supplementary information

NONE

21.4.2.1.8 Translation verification other tools

Not applicable

21.5 Software optionality control (SOC)

Not applicable

22: Configuration (CN): A00002654

22.1 Hardware and Software Requirements

n/a

22.2 Initial Configuration

n/a

22.3 Office/Subnet parameters (OP/SP) (CM & SESM)

n/a

22.4 Upgrade Impact

22.4.1 Dump and Restore

NAOCFEAT is a new table.

22.4.2 Element Management Upgrade

n/a

22.5 Data schema (DS)

22.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NAOCFEAT	NEW	NEW
IBNFEAT	CHANGED	UNCHANGED
CUSTSTN	CHANGED	UNCHANGED
xxCODE[a]	CHANGED	UNCHANGED

a. This change applies to any XLA CODE table.

22.5.2 Table/MIB/Remote Database Schema information

22.5.2.1 Name: NAOCFEAT

Network Advice of Charge Feature Charging Table

22.5.2.1.1 Functional description

Table NAOCFEAT contains Network Advice of Charge charging information for features when one or more of the following feature actions occur:

Feature Action	Description
Administration Assignment	Operating company personnel add a feature to a line.
Administration Deassignment	Operating company personnel remove a feature from a line.
Administration Activation	Operating company personnel change the state of a feature from inactive to active.
Administration Deactivation	Operating company personnel change the state of a feature from active to inactive.
Administration Programming	Operating company personnel change feature data.
Subscriber Activation	A subscriber causes the state of a feature to change from inactive to active.
Subscriber Deactivation	A subscriber causes the state of a feature to change from active to inactive.
Subscriber Programming	A subscriber causes a change to feature data.
Subscriber Usage	A subscriber uses a feature.
Subscriber Interrogation	A subscriber queries a feature, to determine whether it is active, and/or to display the data programmed for the feature.

Table NAOCFEAT has a two-part key, containing

- a Carrier or Reseller Name (from tables CARNAME or RESNAME)
- an MMP line option name or an enquiry action

Current enquiry actions are:

- Register Recall (RR) - a subscriber flashes and switches between the parties involved in the call
- Register recall Target Number (RTN) - a subscriber flashes and dials a number for another subscriber

Associated with each key are an assigned feature code and a list of chargeable feature actions and their assigned charge.

Note: The presence of datafill in table NAOCFEAT for line options and/or enquiry actions does not necessarily mean that these features are being charged or should be charged. Table NAOCFEAT, like table MTRFEAT for World Metering, provides the flexibility for the telco to supply datafill for each

subscriber feature with one or more chargeable activities, even though Network Advice of Charge is not currently active for the feature. The user must refer to the individual service documents to verify whether a particular feature is chargeable.

22.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- CARNAME
- RESNAME
- NAOCFEAT

22.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NAOCFEAT	0	32766	Memory is automatically allocated as the tuples are datafilled.

22.5.2.1.4 Fields/OIDs

The following table lists the new fields for table NAOCFEAT

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Key	New		see subfields	This field contains two subfields: CARRSNAM and FEATNAME
	New	CARRSNAM	8 character vector	Carrier or Reseller name. Enter a carrier or carrier reseller name as it was entered in either table CARNAME or table RESNAME..

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

	New	FEATNAME	<line option>, RR, RTN	Feature Name.
				
				Enter a line option (as listed in the SERVORD Reference Manual) or an enquiry action.
				
				Enquiry actions are:
				`RR - Register Recall`
				`RTN - Register recall Target Number`

FEATCODE	New		00-99	Feature Code. Enter a two-digit number to be used to identify the feature in a charge record.
ACTIONS	New		see subfields	This field is a vector of up to 10 entries where each entry consists of two subfields, FEATACTN and CHARGE.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	New	FEATACTN	ASSIGN, DEASSIGN, ADMACT, ADMDEACT, ADMPROG, , SUBACT, SUBDEACT, SUBPROG, USAGE, INTERROG, $	Feature Action. ASSIGN - Administration Assignment DEASSIGN - Administration Deassignment ADMACT - Administration Activation ADMDEACT - Administration Deactivation ADMPROG - Administration Programming SUBACT - Subscriber Activation SUBDEACT - Subscriber Deactivation SUBPROG Subscriber Programming USAGE - Subscriber Usage INTERROG - Subscriber Interrogation
	New	CHARGE	0-255	Feature Action Charge. Enter the charge value to be charged for the action.

22.5.2.1.5 Datafill example

The following example shows sample datafill for table NAOCFEAT:

```
KEY     FEATCODE
                                                                ACTIONS
-------------------------------------------------------------------------------
```

CAR01 ACRJ 01
(ASSIGN 4) (DEASSIGN 3) (USAGE 5)$

22.5.2.1.6 Table release history update
Added to WT20 by feature A00002654.

22.5.2.1.7 Supplementary information
None.

22.5.2.1.8 Translation verification other tools
NAOCFEAT does not use translation verification tools.

22.5.2.2 Name: IBNFEAT
IBN Features Table

22.5.2.2.1 Functional description
IBNFEAT displays data associated with various IBN features.

22.5.2.2.2 Usage sequence and implications (CM Only)
Current datafill order unchanged.

22.5.2.2.3 Size
The size of the table is not changed.

22.5.2.2.4 Fields/OIDs
This activity allows AR and ACRJ to appear in the FEATURES list of the SEC (Security Code option) as shown below:

TYPE FEATURES_LIST_TYPE STRING RANGE

'DCPK' 0

'AR' 1

'ACRJ' 2

END STRING RANGE

(0, 4, 0, 4)

Table 4 Table field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
DATA	changed	FEATURES	DCPK, AR, ACRJ	Enter DCPK, AR, and/or ACRJ. These are the line options associated with feature SEC.

22.5.2.2.5 Datafill example

The following example shows sample datafill for table IBNFEAT.

```
HOST 00 1 10 05 0 SEC SEC (AR) $ 0000
```

22.5.2.2.6 Table release history update

The SEC feature option is modified to include the AR and ACRJ options in its Features List.

22.5.2.2.7 Supplementary information

None

22.5.2.2.8 Translation verification other tools

None

22.5.2.3 Name: ACCODE

Access Code Table

22.5.2.3.1 Functional description

Access Code Table, and other code tables, work in conjunction with the universal translations head tables (for example, table ACHEAD) to provide the digit path through universal translations.

The access code table translates the access code digit segment of the incoming digit string. The access code is used for access to another networks, an attendant, or a feature.

22.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

22.5.2.3.3 Size

The size of the table is not changed.

22.5.2.3.4 Fields/OIDs

The feature option selector (i.e., FTR) of the XLA feature selector (i.e., FEAT) of the XLA CODE table will be modified to add the additional features AR and ACRJ.

Table 5 Table field descriptions

Field XLASEL	New or Changed	Subfield OSEL	Entry	Explanation and action
FEAT	changed	FTR	<XLA_FEATURE_NAME> {ILR, ICWT, SC, SCR, CCBS, WML, CFU, CFF, CFBF, CFBP, CFDF, CFDP, CDND, CDTA, CDTO, IWUC, VMWI, CNDB, SUPP, CND, VALIDATE, PATH_REPLACEMENT, CALLCHAR, TLC, CLCTDIGS, CALLBACK, REV, FRB, FOC, FDT, NTC, **AR**, **ACRJ** }	Feature name. If the entry in subfield OSEL is FTR, enter an international line feature name. New feature names for AR and ACRJ have been added.

22.5.2.3.5 Datafill example

The following example shows sample datafill for table ACCODE.

```
starcept 921 921 FEAT (FTR AR) (PF 3) (MM 3 15) (FUNC ACT) $

starcept 934 934 FEAT (FTR ACRJ) (PF 3) (MM 3 15) (FUNC ACT) $
```

22.5.2.3.6 Table release history update

The feature option selector (i.e., FTR) of the XLA feature selector (i.e., FEAT) of the XLA CODE table will be modified to add the additional features AR and ACRJ.

22.5.2.3.7 Supplementary information

None.

22.5.2.3.8 Translation verification other tools

The example in Figure 1, "Example Traver for AR activation" shows the output from **traver** when it is used to verify Table ACCODE.

Figure 1 Example Traver for AR activation

```
>traver l 8406101 b921 b
TABLE IBNLINES
LG 00 0 00 00 0 DT STN IBN 8406101 IPGRP1 0 0 141 (CEPT) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
IPGRP1 0 0 0 0 ( XLAS IPGRP1XL STARCEPT IPGRP1DG)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
IPGRP1 NXLA IPGRP1XL POTSXLA 0 IPGRP1DG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME STARCEPT
STARCEPT C NET N N 0 N NDGT N N GEN (LATTR 2 IPGRP1XP IPGRP1RA)$ $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
2 IBN NONE NT 0 0 NILSFC 0 PX STARCEPT NIL 00 IPGRP1XP IPGRP1RA $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
IPGRP1XP NSCR 141 NPRT NONE N $ $
TABLE RATEAREA
IPGRP1RA NLCA NIL NILLATA $
TABLE PXHEAD
STARCEPT DFLT CONT ( XLT OFC STARCEPT)$ NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE OFCHEAD
STARCEPT DFLT CONT ( XLT AC STARCEPT)$ NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE OFCCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE ACHEAD
STARCEPT SDFLT NODFOP NOCON C
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                              921
TABLE ACCODE
STARCEPT 921 921 FEAT ( FTR AR) ( PF 3) ( MM 3 15) (FUNC ACT)$

+++ TRAVER: SUCCESSFUL CALL TRACE +++

CALL ROUTES TO FEATURE PROCESSING ENVIRONMENT


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

22.6 Service Orders (SO) (CM & SESM)

22.6.1 Service order change details

This feature will expand the existing SEC (Security Code) option to accept two more additional values (AR and ACRJ) when it is prompted for its feature list. The feature list contains a list of features for which the Security Code PIN applies.

As well, this feature will expand the provisioning for AR (for CEPT lines **only**) by adding an additional sub-option to define the initial status of the AR feature.

22.6.1.1 LCC and options

The LCC compatibility of SEC is not being changed by this activity.

Table 6 Meridian digital centrex feature assignment requirements

Feature	500 2500	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
				SET	SUBSET	KEY	DN	DEDKEY	LAMP	CODE	DISPLAY

22.6.2 New commands

NA- No new Servord commands are being introduced by this activity.

22.6.2.1 How SEC service order options are presented

22.6.2.1.1 Description

With this activity, the FEATURES prompt of the SEC option will allow two new values, AR and ACRJ. Previously, only DCPK was a valid option.

22.6.2.1.2 Example

Figure 2 Example of Servord sequence in prompt mode

```
SO:
>ado
SONUMBER:      NOW    3   6 16 PM
>
DN_OR_LEN:
>0 1 10 5
OPTION:
>sec
FEATURES:
>ar  (or acrj) <---------- The new features to which the SEC PIN applies
FEATURES:
>$
SEC_CODE:
>0000
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 6 16 PM HOST 00 1 10 05 ( SEC ( AR) $ 0000 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Figure 3 Example of Servord sequence in no-prompt mode

SO:
ado $ 0 0 18 5 sec **acrj** $ 0000 $ y y

22.6.2.1.3 Option prompts

The new SEC FEATURES values are shown in **bold** below.

Table 7 Change to SEC FEATURES sub-option prompt

Prompt	Valid input	Description
FEATURES	DCPK, **AR**, **ACRJ**	The FEATURES field indicate the line features using the SEC PIN.

22.6.2.1.4 Line class code compatibility

The LCC compatibility of SEC is not being changed by this activity.

22.6.2.1.5 Assignability

The SEC option is assignable to a line.

22.6.2.1.6 Option prerequisites

For the SEC PIN to apply to AR and ACRJ, the CEPT option needs to be present on the line. The SEC PIN will not apply to non-CEPT AR and ACRJ.

22.6.2.1.7 Notes

None.

22.6.2.1.8 Feature identification

Feature number: A00002654 (CEPT AR), A00002655 (CEPT ACRJ)

22.6.2.1.9 SERVORD+ Exceptions

None.

22.6.2.2 How CEPT AR service order options are presented

22.6.2.2.1 Description

With this activity, the CEPT **AR** option will require two sub-options in addition to the feature option name, they are:

- **billing_option**

  This sub-option is **not** a new sub-option with respect to AR.

- **cnd_status**

  This sub-option pertains to CEPT AR only. This defines the initial state of the CEPT AR option, i.e., active or inactive.

  Note: This feature state can be toggled via the feature access codes as defined in the FN section of this design document. As well, the current CEPT AR feature state can be viewed via the QDN or QLEN commands.

22.6.2.2.2 Example

Figure 4 Example of Servord sequence in prompt mode - CEPT AR

```
>ado
SONUMBER:      NOW    4 10 18 PM
>
DN_OR_LEN:
>6320401
OPTION:
>ar
BILLING_OPTION: NOAMA
>noama
CND_STATUS:  <---------- new for CEPT AR only!!
>inact
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 4 10 18 PM 6320401 ( AR NOAMA INACT ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Figure 5 Example of Servord sequence in no-prompt mode - CEPT AR

```
SO:
ado $ 6320401 ar noama inact $ y y
```

22.6.2.2.3 Option prompts

The new CEPT AR sub-option prompts are shown below.

Table 8 CEPT AR sub-option prompts

Prompt	Valid input	Description
BILLING_OPTION	NOAMA AMA (not allowed for CEPT AR) <CLASS_AMA_STATUS>	Indicates whether an AMA billing record should or should not be created. If the line is provisioned with the CEPT option then input of AMA will be rejected by SERVORD.

Table 8 CEPT AR sub-option prompts

Prompt	Valid input	Description
CND_STATUS	INACT ACT UNIVI (not allowed for CEPT AR) UNIVA (not allowed for CEPT AR) <CLASS_ACTIVITY_STATUS>	This defines the initial state of the CEPT AR option, i.e., inactive or active. If the line is provisioned with the CEPT option then input of UNIVI or UNIVA will be rejected by SERVORD. If the line is **not** provisioned with the CEPT option then input of INACT will be rejected by SERVORD.

22.6.2.2.4 Line class code compatibility

The LCC compatibility of CEPT AR is not being changed by this activity.

22.6.2.2.5 Assignability

The CEPT AR option is assignable to a line.

22.6.2.2.6 Option prerequisites

The prompt for the CEPT AR **cnd_status** will only appear if the customer group, that the line is a member of, has the CEPT option assigned (in Table CUSTSTN).

It is **highly recommended** that the line also be provisioned with the CEPT option prior to adding the CEPT AR option (although this is not enforced by SERVORD).

22.6.2.2.7 Notes

None.

22.6.2.2.8 Feature identification

Feature number: A00002654 (CEPT AR)

22.6.2.2.9 SERVORD+ Exceptions

None.

22.7 Software optionality control (SOC)

n/a

22.8 Element Management

n/a

22.9 Command interface changes

n/a

22.10 Security

n/a

22.11 Configuration Walkthrough

n/a

23: Configuration (CN): A00002678

23.1 Hardware and Software Requirements

No non-standard hardware or software requirements.

23.2 Initial Configuration

Not applicable.

23.3 Office/Subnet parameters (OP/SP) (CM & SESM)

23.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	WTIN_TDP4_ACTIVE	NEW	CM
OFCENG	INAP_ASF_FILTERING_TIMEOUT_DUR	NEW	CM
OFCENG	INAP_VARIANT	Changed	CM

23.3.2 Parameter information

23.3.2.1 WTIN_TDP4_ACTIVE

Intelligent Networks Trigger Detection Point 4 Active

23.3.2.1.1 Functional description

TDP4 Query on Release (QoR) Triggering is being introduced by this activity. TDP4 occurs when a release indication is received from the network or internally within the switch. The feature partially implements TDP4, it only allows IN to be trigger on receipt of an ISUP REL message (from ETSI ISUP).The criteria for triggering TDP-4 is based on the cause value received in the ISUP message. The release cause value required to trigger TDP-4 is specified in a new criteria type CAUSE in table TRIGGRP.

Checking for a matching CAUSE criteria introduces a real-time hit for during release message processing. To reduce this a new office parm, WTIN_TDP4_ACTIVE has been introduced. If TDP-4 triggering is required in the office this office parm can be set to TRUE. If the office parm is set to FALSE TDP-4 triggering will be disabled regardless of datafil in table TRIGGRP.

23.3.2.1.2 Provisioning rules

The value should be set to TRUE if TDP-4 triggering is required in this office, and FALSE if it is not required.

23.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
FALSE	TRUE	FALSE

23.3.2.1.4 Activation

Any changes are activated immediately

23.3.2.1.5 Dependencies

None

23.3.2.1.6 Consequences

If TDP-4 triggering is not required and this office parm is set to TRUE, there will be an unnecessary real time hit for all calls, during backward release.

23.3.2.1.7 Verification

Make a call which will trigger at TDP-4, if the office is parm is set to TRUE to call will result in the trigger being generated, if set to FALSE the trigger will not occur.

23.3.2.1.8 Memory requirements

No memory impact.

23.3.2.1.9 Parameter release history update

Created WTIN_TDP4_ACTIVE office parameter in table OFCENG.

23.3.2.2 INAP_ASF_FILTERING_TIMEOUT_DUR

Intelligent Network Application Part ActivateService Filtering Timeout Duration

23.3.2.2.1 Functional description

This activity provides the ability to specify a network default ASF duration. If the SSP receives an ASF operation with a duration of -2, this indicates the value is network specific and the network default duration should be used.

A new office parm has been created called INAP_ASF_FILTERING_TIMEOUT_DUR in table OFCENG to specify the network specific ASF duration.

23.3.2.2.2 Provisioning rules
This office parm is only applicable to networks which require a network specific ASF duration. The value of this office parm should match the network specific ASF duration or if not required should be entered as 0

23.3.2.2.3 Range information
The range accepted by this office parm is -1 - 86,400 seconds. A value of -1 represents an infinite duration

Table 3 Range Information

Minimum	Maximum	Default
-1	86,400	0

23.3.2.2.4 Activation
Any changes are activated immediately but will only affect new ASF operations and not any that may currently be processing.

23.3.2.2.5 Dependencies
None

23.3.2.2.6 Consequences
If there is a network specific ASF duration and the value of this parameter does not match it, an incorrect duration will be used if the network specific duration is requested by the SCP. If there isn't a network specific ASF duration, and this office parm is not datafilled as 0, should an ASF operation be received with a duration of -2, it will not be treated as an error and instead the value of the office parm will be used for the duration of the ASF operation.

23.3.2.2.7 Verification
Send an ASF operation to the SSP with a duration of -2 and use the ASF MAP CI tool to display the ASF entries and check the duration parameter is set as expected.

23.3.2.2.8 Memory requirements
No memory impact.

23.3.2.2.9 Parameter release history update
Created INAP_ASF_FILTERING_TIMEOUT_DUR office parameter in table OFCENG

23.3.2.3 INAP_VARIANT
Intelligent Network Application Part Variant

23.3.2.3.1 Functional description
Unchanged

23.3.2.3.2 Provisioning rules
For the Spanish National Market this office parm should be set to TELEFONICA

23.3.2.3.3 Range information
A new value of TELEFONICA has been added for the Spanish national market

23.3.2.3.4 Activation
Unchanged

23.3.2.3.5 Dependencies
None

23.3.2.3.6 Consequences
If this office parameter is not set correctly INAP operations may be encoded/ decoded incorrectly

23.3.2.3.7 Verification
Unchanged

23.3.2.3.8 Memory requirements
Unchanged

23.3.2.3.9 Parameter release history update
Added a new variant TELEFONICA

23.4 Upgrade Impact

23.5 Data schema (DS) (CM)

23.5.1 New/modified tables

Table 4 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRIGGRP	CHANGED	UNCHANGED
SERVINFO	CHANGED	UNCHANGED

23.5.2 Table information

23.5.2.1 Name: TRIGGRP
Trigger Group

23.5.2.1.1 Functional description
Unchanged

23.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

CPCCHAR

TRIGGRP

23.5.2.1.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRIGGRP	Unchanged	Unchanged	Unchanged

23.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for TRIGGRP.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CRITERIA	Changed	Subfield	{..., **CAUSE**, **CPC**,...}	
CPC	New		Alphanumeric 1- 8 characters	Index to table CPCCHAR

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CAUSE	New		Alphanumeric (one of CSE_0, UNALLOC, NRTOTN, NRTODEST, SSINFTN, MISDTRPR, CSE_6, CSE_7, CSE_8, CSE_9, CSE_10, CSE_11, CSE_12, CSE_13, CSE_14, CSE_15, NORMCLR, USERBUSY, NOUSRESP, NOANSWER, CSE_20, CALLREJ, NUMCHANG, CSE_23, CSE_24, XLAFAIL, CSE_26, DOOSRVC, ADDINCOM, FACREJ, CSE_30, NORMUNSP, CSE_32, CSE_33, NOCIRCAV, CSE_35, CSE_36, CSE_37, NTWKOOO, CSE_39, CSE_40, TEMPFAIL, SWEQCONG, UINFDISC, CHANUNAV, PREEMPT, NPMPTCKT, RESUNAV, CSE_48, CSE_49, CSE_50, CSE_51, OTGCBARD, CSE_53, CSE_54, INCBCUG, CSE_56, BCNAUTH, BCNAVAIL, CSE_59, CSE_60, CSE_61, CSE_62, SONAVAIL, CSE_64, BCNIMPL, CHNLNIMP, CSE_67, CSE_68, FACNIMP, RESBCINF, CSE_71, CSE_72, CSE_73, CSE_74, CSE_75, CSE_76, CSE_77, CSE_78, SONIMPL, CSE_80, INVCRVAL, CSE_82, CSE_83, CSE_84, CSE_85, CSE_86, USERNCUG, INCOMDST, CSE_89, CSE_90, CSE_91, CSE_92, CSE_93, CSE_94, INVMSG, CSE_96, MSGNIMPL, CSE_98, PARMNIMP, INVPARMC, CSE_101, CSE_102, PNIPASS, CSE_104, CSE_105, CSE_106, CSE_107, CSE_108, CSE_109, CSE_110, PROTERR, CSE_112, CSE_113, CSE_114, CSE_115, CSE_116, CSE_117, CSE_118, CSE_119, CSE_120, CSE_121, CSE_122, CSE_123, CSE_124, CSE_125, CSE_126, INTWUNSP)	Release cause value to trigger on at TDP-4

23.5.2.1.5 Datafill example

The following example shows sample datafill for table TRIGGRP.

Figure 1 Example datafill TRIGGRP

```
 KEY
                                                                        TRIGDATA
-------------------------------------------------------------------------------
-
         ETSIGRP NETBUSY
(GENTRIG ( CAUSE CSE_126) $ MDCKEY1)$

         ETSIGRP  INFOCOL
(GENTRIG (CPC UNKNOWN) $ MDCKEY1)$
```

23.5.2.1.6 Table release history update

Added new CRITERIA types of CPC and CAUSE

23.5.2.1.7 Supplementary information

A CRITERIA of CAUSE can only be entered for the TERMATT trigger. CPC can only be entered for INFOCOL, INFOANAL and TERMATT triggers.

23.5.2.1.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify TRIGGRP.

Figure 2 Example TRAVER using CPC triggering at TDP-2

```
 >traver tr pubm411eiswbe 01628430000 b
TABLE TRKGRP
PUBM411EISWBE IBNT2 0 NPDGP NCRT PUBLIC162MEL 0 MIDL 0 N ANSDISC 0 Y N N N N N
    0 0 N 0 1 0 1 N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
PUBLIC162MEL 0 0 0 DFLT ( CPCRTE )$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
PUBLIC162MEL NXLA PUBMXLA PUBMFET 0 PUBMDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE TRIGGRP
ETSIGRP INFOCOL
 . GENTRIG (CPC UNKNOWN)$ MDCKEY1
Please enter a CPCCHAR protocol name or N
to specify CPC Routing not required
Protocol Name:
>etsiisup
ENTER CPC VALUE FOR ETSIISUP
CPC VALUE:
>0
TABLE CPCCHAR
 . Matched on UNKNOWN
Trigger INAPV8 GENTRIG is applicable to office.
 .  . TABLE TRIGINFO
 .  . MDCKEY1 EVENT TCAP INAPV8 SS7 EINJAZZ DFLT (SERVKEY 4441)
(SERVINFO_INDEX4441)
 .  .     $
 .  .  . TABLE SERVINFO
 .  .  . 4441
 .  .  .     (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) $)
 .  .  .     (BILL_INFO (FCI_OPT FREEFORM ) $)
 .  .  .     (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
 .  .  .     (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
 .  .  . EINJAZZ CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EINJAZZ 4441 4441 PCSSN (K1197RS1 EIN 50) $ SSN
INAP Info Collected TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++


INAP Info Collected TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

23.5.2.2 Name: SERVINFO

Intelligent Network Service Information Table

23.5.2.2.1 Functional description

Unchanged

23.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

23.5.2.2.3 Size

Table 7 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	Unchanged	Unchanged	Unchanged

23.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FCI_OPT	Changed	refinement	{..., **TELFONICA**,...}	
TELFONICA	New		FORMAT_IDENTIFIER	Specifies that Telefonica FCI handling should be used
FORMAT_IDENTIFIER	New	Subfield	numeric (in the range 127 to 255)	Denotes a vendor-specificFCIBCC format or IN service
INITDP_PARMS	Changed	refinement	{..., **CAUSE**, ...}	
CAUSE	New		none	Specifies that the release CAUSE value should be included in the InitDP.

23.5.2.2.5 Datafill example

The following example shows sample datafill for table SERVINFO.

Figure 3 Example datafill SERVINFO

```
SERVIDX                                                              OPTION
-------------------------------------------------------------------------------

4441    (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) (CAUSE)$)
           (BILL_INFO (FCI_OPT TELEFONICA 127) $)
           (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
           (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
```

23.5.2.2.6 Table release history update

Added new FCI_OPT option TELEFONICA and INITDP_PARMS option CAUSE.

23.5.2.2.7 Supplementary information

None

23.5.2.2.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify SERVINFO.

Figure 4 Example TRAVER using CPC triggering at TDP-2

```
>traver tr pubm411eiswbe 06001234 b
TABLE TRKGRP
PUBM411EISWBE IBNT2 0 NPDGP NCRT PUBLIC162MEL 0 MIDL 0 N ANSDISC 0 Y N N N N N N
    0 0 N 0 1 0 1 N N N N N N N N N N NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
PUBLIC162MEL 0 0 0 DFLT $
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
PUBLIC162MEL NXLA PUBMXLA PUBMFET 0 PUBMDIG
TABLE DIGCOL
PUBMDIG 0 COL L 7
TABLE TRIGGRP
ETSIGRP INFOCOL
 . GENTRIG ( FTC K11FTC)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME PUBMXLA
PUBMXLA 0600 NET N N 0 N NDGT N N DOD N 310 162_NPRT_201 NLCA_NILLA_200 NONE $
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
310 IBN NONE NT 0 0 NILSFC 0 PX PUBM0PX NIL 00 162_NPRT_201 NLCA_NILLA_200 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
162_NPRT_201 NSCR 162 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_200 NLCA NIL NILLATA $
TABLE PXHEAD
PUBM0PX DFLT CONT ( XLT PX PUBMPX)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        06001234
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE PXHEAD
PUBMPX SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        06001234
TABLE PXCODE
PUBMPX 0600 0600 CONT ( MM 5 8) ( XLT FA PUBMPSTN)$
TABLE FAHEAD
PUBMPSTN DFLT RTE( MM 8 11)( DEST 1)( CLASS NATL)$DFOP( MM 8 11)( CLASS NATL)$ CON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        06001234
TABLE FACODE
PUBMPSTN 06001 06001 RTE ( MM 3 30) ( DEST 301) ( CLASS NATL)$
TABLE: FARTE
KEY: PUBMPSTN  301
 . S K1197EISWBE
 . S K1197BTWBE
EXIT TABLE FARTE
TABLE TRIGGRP
ETSIGRP INFOANAL
 . GENTRIG ( CDPN K1197GRP)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
 .  . TABLE TRIGDIG
 .  . K1197GRP GENTRIG 06001 GENTRIG EVENT TCAP INAPV8 SS7 EINJAZZ CALLED
 .  .     (SERVKEY 1111) (SERVINFO_INDEX 1111) $
 .  .  . TABLE SERVINFO
 .  .  . 1111
 .  .  .     (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) (CAUSE) $)
 .  .  .     (BILL_INFO (FCI_OPT TELEFONICA) $)
 .  .  .     (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
 .  .  . EINJAZZ CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EINJAZZ 06001234 06001234 PCSSN (K1197RS1 EIN 0) $ SSN
INAP Info Analyzed TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

23.6 Configuration Walkthrough

Please refer to the FN for ACT.00002678 for details on configuring this functionality.

24: Configuration (CN): A00002680

24.1 Hardware and Software Requirements

24.2 Initial Configuration

24.3 Office/Subnet parameters (OP/SP) (CM & SESM)

24.4 Upgrade Impact

24.5 Data schema (DS) (CM, MIBS, RDB)

This activity does not introduce new tables, however, it does make use of three existing tables that were previously introduced via activity BV1522. These tables are PAUSPATT, ISCASSGN, and AISDBS. Investigation reveals no reference to these tables in the existing NTP documentation. These tables need to be added to the NTP documentation based on the description given in BV1522.

24.6 Service Orders (SO) (CM & SESM)

24.7 Software optionality control (SOC)

24.8 Element Management

24.9 Command interface changes

24.10 Security

24.11 Configuration Walkthrough

25: Configuration (CN): A00002702

25.1 Data schema (DS) (CM, MIBS, RDB)

25.1.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MTRSYSPM	CHANGED	UNCHANGED
MTRSYSPM	CHANGED	UNCHANGED

25.1.2 Table/MIB/Remote Database Schema information

25.1.2.1 Name: MTRSYSPM

25.1.2.1.1 Functional description

NCW_MOG field of the table is renamed to NCW_CHG.

25.1.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

25.1.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MTRSYSPM	10	10	One tuple is added to this table. That means 1 bit memory is allocated from the memory conception.

25.1.2.1.4 Fields/OIDs

The following table lists fields/OIDs for MTRSYSPM.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NCW_CHG	Changed	-	Allowed or Disallowed	Field name is renamed from NCW_MOG

25.1.2.1.5 Datafill example

Figure 1 Datafill example of table MTRSYSPM (function is inactive)

```
TOP
MTRPARM MTRDATA
---------------
MFP MFP SUCCEED
MAXPULSE MAXPULSE 2
MTRBCKUP MTRBCKUP 0 0 2
MTRAUDIT MTRAUDIT 0 0 2
PULMISTH PULMISTH 1
CRTCOUNT CRTCOUNT 500
EMD EMD NO 4 15 1 20000
NCW_CHG NCW_CHG ALLOWED
.....................
BOTTOM
```

Figure 2 Datafill example of table MTRSYSPM (function is active

```
TOP
MTRPARM MTRDATA
---------------
MFP MFP SUCCEED
MAXPULSE MAXPULSE 2
MTRBCKUP MTRBCKUP 0 0 2
MTRAUDIT MTRAUDIT 0 0 2
PULMISTH PULMISTH 1
CRTCOUNT CRTCOUNT 500
EMD EMD NO 4 15 1 20000
NCW_CHG NCW_CHG DISALLOWED
...................
BOTTOM
```

25.1.2.1.6 Table release history update

NCW_MOG field is renamed to NCW_CHG

25.1.2.1.7 Supplementary information

None

25.1.2.1.8 Translation verification other tools

MTRSYSPM does not use translation verification tools.

25.1.2.2 Name: MTRSYSPM

25.1.2.2.1 Functional description

A new tuple NTOW_CHG is added to this table in order to datafill the NO_TRK_ORIG_WITHOUT_CHG field. This field is used to activate or deactivate the IC PRI trunks call origination restriction described in FN Section 2.2.6.

25.1.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

25.1.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MTRSYSPM	12	12	One tuple is added to this table. That means 1 bit memory is allocated from the memory conception.

25.1.2.2.4 Fields/OIDs

The following table lists fields/OIDs for MTRSYSPM.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NO_TRK_ORIG_ WITHOUT_CHG	New	-	Allowed or Disallowed	**Allowed:** IC ETSI PRI Calls are not affected from the NTOW_CHG function. **Disallowed:** IC ETSI PRI Calls are not allowed if IC trunk has no ICMOG datafill.

25.1.2.2.5 Datafill example

Figure 3 Datafill example of table MTRSYSPM (function is inactive)

```
TOP
MTRPARM MTRDATA
---------------
MFP MFP SUCCEED
MAXPULSE MAXPULSE 2
MTRBCKUP MTRBCKUP 0 0 2
MTRAUDIT MTRAUDIT 0 0 2
PULMISTH PULMISTH 1
CRTCOUNT CRTCOUNT 500
EMD EMD NO 4 15 1 20000
NCW_CHG NCW_CHG ALLOWED
REST_PSW REST_PSW DEACTIVATED
NTOW_CHG NTOW_CHG ALLOWED

.....................
BOTTOM
```

Figure 4 Datafill example of table MTRSYSPM (function is active

```
TOP
MTRPARM MTRDATA
---------------
MFP MFP SUCCEED
MAXPULSE MAXPULSE 2
MTRBCKUP MTRBCKUP 0 0 2
MTRAUDIT MTRAUDIT 0 0 2
PULMISTH PULMISTH 1
CRTCOUNT CRTCOUNT 500
EMD EMD NO 4 15 1 20000
NCW_CHG NCW_CHG DISALLOWED
REST_PSW REST_PSW DEACTIVATED
NTOW_CHG NTOW_CHG DISALLOWED
...................
BOTTOM
```

25.1.2.2.6 Table release history update

- New field NO_TRK_ORIG_WITHOUT_CHG and new tuple NTOW_CHG is added.
- The tuple size of the table is increased to 12.

25.1.2.2.7 Supplementary information

A reload restart is required to activate the functionality bound to NTOW_CHG tuple, so the operator is warned with a message when this tuple is changed.

Figure 5 Example of activating the function.

```
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
MTRSEL: NTOW_CHG
>NTOW_CHG
NO_TRK_ORIG_WITHOUT_CHG: ALLOWED
>DISALLOWED
TUPLE TO BE CHANGED
NTOW_CHG NTOW_CHG DISALLOWED
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
*** WARNING: ALL ETSI PRI TRUNK ORIGINATED CALLS
WILL BE AFFECTED

NOTE:
A RELOAD RESTART is necessary to activate new value. When
NTOW_CHG is DISALLOWED, calls which are originated by
ETSI PRI trunks having no ICMOG datafill, will NOT be allowed.
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

When NTOW_CHG value is changed from ALLOWED to DISALLOWED, if user attempts to list the tuples in MTRSYSPM table, user is informed about the mismatch between the active used value and the value in table.

Figure 6 Mismatch Warning Message in DISALLOWED case

```
WARNING: NTOW_CHG - DISALLOWED value is not active yet
A RELOAD restart is required to activate
```

Figure 7 Example to deactivating the function

```
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
MTRSEL: NTOW_CHG
>NTOW_CHG
NO_TRK_ORIG_WITHOUT_CHG: ALLOWED
>ALLOWED
TUPLE TO BE CHANGED
NTOW_CHG NTOW_CHG ALLOWED
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
*** WARNING: ALL LINE ORIGINATED CALL WILL BE AFFECTED

NOTE:
A RELOAD RESTART is necessary to activate new value. When
NTOW_CHG is DISALLOWED, calls which are originated by
ETSI PRI trunks having no ICMOG datafill, will NOT be allowed.
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

In this case, when NTOW_CHG value is changed from DISALLOWED to ALLOWED, mismatch warning message occurs as following;

Figure 8 Mismatch Warning Message in ALLOWED case

```
WARNING: NTOW_CHG - ALLOWED value is not active yet
A RELOAD restart is required to activate
```

Since changed value in table will be active after a reload restart, mismatch message will be displayed each time the tuple is listed until the restart reload is performed.

Also, this mismatch warning message occurs in every attempt to enter MTRSYSPM table.

25.1.2.2.8 Translation verification other tools

MTRSYSPM does not use translation verification tools.

26: Configuration (CN): A00002713

26.1 Hardware and Software Requirements

N/A

26.2 Initial Configuration

N/A

26.3 Office parameters (OP)

26.3.1 New/modified office parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	ORIGNETID	NEW	CM

26.3.2 Parameter information

26.3.2.1 ORIGNETID

Originating Network Identification

26.3.2.1.1 Functional description

This is Parameter will be datafilled with a numeric value.This parameter determines the originating network identification number.This value is in the range (0 to 65535). This parameter will be the default value and is used for calls from line agents.

For Interconnect trunks, this value will be different and will be datafilled in the table TRKOPTS against the corresponding spanish ISUP V2 trunk.

26.3.2.1.2 Provisioning rules

26.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	65535	0

26.3.2.1.4 Activation
Immediate.

26.3.2.1.5 Dependencies
None.

26.3.2.1.6 Consequences

26.3.2.1.7 None.Verification
The following figure shows the verification for setting the parameter to the possible datafills.

Table 3 %% Changing the parameter value to 34532

```
CI> TABLE OFCVAR;FORMAT PACK
>pos ORIGNEID
>ORIGNEID 12345
>cha
>y
PARMVAL: 34532
Y
TUPLE TO BE CHANGED:
ORIGNEID 34532
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

26.3.2.1.8 Memory requirements
No memory impact.

26.3.2.1.9 Parameter release history update
N/A

26.4 Upgrade Impact
N/A

26.5 Data schema (DS) (CM, MIBS, RDB)
N/A

26.6 Service Orders (SO) (CM & SESM)

26.7 Software optionality control (SOC)

N/A

26.8 Element Management

N/A

26.9 Command interface changes

N/A

26.10 Security

N/A

26.11 Configuration Walkthrough

N/A

27: Configuration (CN): A00002751

27.1 Hardware and Software Requirements

27.2 Initial Configuration

27.3 Office/Subnet parameters (OP/SP) (CM & SESM)

27.4 Upgrade Impact

27.5 Data schema (DS) (CM, MIBS, RDB)

27.5.1 Table name: IBNXLA

This table is used to translate digits dialled by subscribers.

27.5.1.1 Functional description

This activity introduces new entries for IBN_LOG_FEATURE that are COLRA for COLR activation, COLRD for COLR deactivation, CWACT for CW activation, CWDEACT for CW deactivation

27.5.1.2 Datafill sequence and implications

There is no requirement to datafill this tuple in a specific order.

27.5.1.3 Table size

Table 1 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNXLA	Unchanged	Unchanged	Unchanged

27.5.1.4 Table fields

The following table lists fields for table IBNXLA.

Table 2 Table field descriptions

Field	New or Changed, Unchnaged	Subfield or refinement	Entry	Explanation and action
KEY	Unchanged			

Table 2 Table field descriptions

Field	New or Changed, Unchnaged	Subfield or refinement	Entry	Explanation and action
RESULT	Changed	FEAT	In addition to Current entries, COLRA, COLRD, CWACT, CWDEACT.	Feature filed of FEAT refinement includes COLRA, COLRD, CWACT, and CWDEACT entries.

27.5.1.5 Datafill example

The following examples shows sample datafill for table IBNXLA:

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
KEY:
>featxla 34
TRSEL:
 >feat
ACR:
>n
SMDR:
 >n
FEATURE:
>colra
TUPLE TO BE ADDED:
   FEATXLA 34   FEAT   N  N   COLRA
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
KEY:
>defeatxla 34
TRSEL:
 >feat
ACR:
>n
SMDR:
 >n
FEATURE:
>colrd
TUPLE TO BE ADDED:
    DEFEATXLA 34    FEAT   N  N   COLRD
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y


>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
KEY:
>featxla 74
TRSEL:
 >feat
ACR:
>n
SMDR:
 >n
FEATURE:
>cwact
TUPLE TO BE ADDED:
    FEATXLA   74    FEAT   N  N   CWACT
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
KEY:
>defeatxla 74
TRSEL:
 >feat
ACR:
>n
SMDR:
 >n
FEATURE:
>cwdeact
TUPLE TO BE ADDED:
    DEFEATXLA 74   FEAT   N  N   CWDEACT
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

The tuples can be seen in table IBNXLA as follows:

```
TABLE IBNXLA
-------------------------
FEATXLA 34 FEAT N N COLRA
DEFEATXLA 34 FEAT N N COLRD
FEATXLA 74 FEAT N N CWACT
DEFEATXLA 74 FEAT N N CWDEACT
```

27.5.1.6 Table release history update

None.

27.5.1.7 Supplementary information

None.

27.5.1.8 Translation verification tools

None.

27.6 Service Orders (SO) (CM & SESM)

27.6.1 Service order change details

27.6.1.1 LCC and options

27.6.2 New commands

27.6.2.1 How service order commands are presented

27.6.2.2 How service order options are presented

27.6.2.2.1 Description

A new line option CWACT is introduced to provide Call Waiting Activation/ Deactivation(CWACT) function. The function allows the subscriber to activate and deactivate call waiting via feature access codes (i.e. *74, #74).

The function is provided by assigning CWACT line option to subscriber by means of SERVORD command. It works with CW service. The CWACT can only be assigned to a BRI DN that already has CW (Call Waiting), therefore the removal of CW from the DN with CWACT will not be allowed.

27.6.2.2.2 Example

Figure 1 Example of the assignment example of CWACT option

```
>SERVORD
SO:
>ado
SONUMBER MAY 95 6 46 PM
>[Enter]
DN_OR_LEN
>ISDN 400
OPTKEY
>1
OPTION:
>CWACT
CW_ACTIVE:
>Y
OPTKEY
>$
COMMAND AS ENTERED:
ADO MAY 95 6 46 PM ISDN 400(1 CWACT Y) $
Enter Y to confirm, N to reject or E to edit
>Y
```

Figure 2 Example of the CWACT option in no-prompt mode

```
> servord
SO:
> ado $ 6020400 1 CWACT Y $
```

27.6.2.2.3 Option prompts

Table 3 System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	CWACT	The name of the new option	N/A
CW_ACTIVE	Y or N	Indicate if the CW service can be active.	N/A

27.6.2.2.4 Line class code compatibility

Table 4 CWACT compatibility to LCC

Line class code	Compatible?
ISDNKSET	YES

27.6.2.2.5 Assignability

The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

27.6.2.2.6 Option prerequisites

To assign the option to a BRI DN, the CW option must exist on this DN.

27.6.2.2.7 Notes

To delete CW option, CWACT option must be deleted firstly.

27.6.2.2.8 Feature identification

Feature number: A00002751

27.6.2.2.9 SERVORD+ Exceptions

27.7 Software optionality control (SOC)

27.8 Element Management

27.9 Command interface changes

27.10 Security

27.11 Configuration Walkthrough

28: Configuration (CN): A00002754

28.1 Hardware and Software Requirements

N/A.

28.2 Initial Configuration

N/A.

28.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

28.4 Upgrade Impact

N/A.

28.5 Data schema (DS) (CM, MIBS, RDB)

28.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
OFCENG	Changed	Changed
SERVINFO	Changed	Unchanged

28.5.2 Table/MIB/Remote Database Schema information

28.5.2.1 Name: OFCENG

28.5.2.1.1 Functional description

The range of INAP_TSSF_WFI_TIMER is changed from ‘1-10’ to ‘1-60’, and the datafillable value is changed from ‘1-10’ to ‘1-10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60’.

Usage example: suppose the following datafill is supplied. The SSP will use

Table 2 Datafill Example:

```
TABLE: OFCENG
PARMNAME PARMVAL
----------------
INAP_TSSF_WFI_TIMER 15
```

value 15 as the default timer in the WFI state.

28.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

28.5.2.1.3 Size

Table 3 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFCENG	no change	no change	N/A

28.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for OFCENG.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INAP_TSSF_WFI_TIMER	Changed	refinement	OFFICE_PARM_VALUE	value range and datafillable value changed

28.5.2.1.5 Datafill example

Table 5 Datafill Example:

```
TABLE: OFCENG
PARMNAME PARMVAL
----------------
INAP_TSSF_WFI_TIMER 15
```

28.5.2.1.6 Table release history update

The range of INAP_TSSF_WFI_TIMER is changed from ‘1-10’ to ‘1-60’, and the datafillable value is changed from ‘1-10’ to ‘1-10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60’.

28.5.2.1.7 Supplementary information
N/A.

28.5.2.1.8 Translation verification other tools
N/A.

28.5.2.2 Name: SERVINFO

28.5.2.2.1 Functional description
A new selection: CIRP is introduced into CS1R option to indicate that: If CIRP is datafilled in the CS1R option of table SERVINFO, the outgoing CIRP will use the CS-1R format, the legID will not be included:

Table 6 Table SERVINFO

```
SERVIDX                                                                  OPTION
-------------------------------------------------------------------------------
200    (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) $)
           (TCAP_INFO ( INAP_OPT (AUTO_CONTINUE) $)(TCAP_VERSION CCITT_V1)$)
           (CS1R ( CIRP) $)$
```

28.5.2.2.2 Usage sequence and implications (CM Only)
Current datafill order unchanged.

28.5.2.2.3 Size

Table 7 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	no change	no change	N/A

28.5.2.2.4 Fields/OIDs
The following table lists fields/OIDs for SERVINFO.

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CS1R	Changed	refinement	enumerated value	Add new selection: CIRP

28.5.2.2.5 Datafill example

Table 9 Table SERVINFO

```
SERVIDX                                                                    OPTION
-------------------------------------------------------------------------------
200    (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) $)
           (TCAP_INFO ( INAP_OPT (AUTO_CONTINUE) $)(TCAP_VERSION CCITT_V1)$)
           (CS1R ( CIRP) $)$
```

28.5.2.2.6 Table release history update

A new selection: CIRP is introduced into CS1R option to indicate that: If CIRP is datafilled in the CS1R option of table SERVINFO, the outgoing CIRP will use the CS-1R format, the legID will not be included.

28.5.2.2.7 Supplementary information

N/A.

28.5.2.2.8 Translation verification other tools

N/A.

28.6 Service Orders (SO) (CM & SESM)

N/A.

28.7 Software optionality control (SOC)

N/A.

28.8 Element Management

N/A.

28.9 Command interface changes

N/A.

28.10 Security

N/A.

28.11 Configuration Walkthrough

N/A.

29: Configuration (CN): A00002755

29.1 Hardware and Software Requirements

29.2 Initial Configuration

29.3 Office/Subnet parameters (OP/SP) (CM & SESM)

29.4 Upgrade Impact

29.5 Data schema (DS) (CM, MIBS, RDB)

29.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

29.5.2 Table/MIB/Remote Database Schema information

29.5.2.1 Name: ISERVOPT

International Services options

29.5.2.1.1 Functional description - Tuple CEPTONCNETREX

A new field MARKET into the tuple CEPTONCENTREX in table ISERVOPT. The field MARKET is used to identify in which market the line services are working. Now, two value are available for this field. One is DEFAULT and another is CHINA. For the chinese office, this field must be set to CHINA.

In order to allow all CEPT line services mentioned above on the IBN line without CEPT option, the corresponding service options must be present in tuple CEPTONCENTREX in table ISERVOPT. Table 2 below shows the available options in tuple CEPTONCENTREX, and the associated CEPT line services:

***Note**: The CEPTONCENTREX options with **bold** font are introduced by this activity.*

Table 2 CEPTONCENTREX Options and CEPT Line Services

CEPTONCENTREX OPTION	Associated CEPT Line Service
SC	SCL, SCS
WML	WML
ILR	ILR
CDIV	CDND, CFU, CFB, CFD, CFF, CDTA, CDTO, CFRA
ICT	ICT
ICWT	ICWT
IWUC	IWUC
ICWT	ICWT
CCBS	CCBS
I3WC	I3WC
I6WC	I6WC
CEPTPW	CEPTPW
CEPTRA	CEPTRA

29.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

29.5.2.1.3 Size

Current table size unchanged.

29.5.2.1.4 Fields/OIDs

The following table lists fields for table ISERVOPT;

Table 3 Table field descriptions for tuple CEPTONCENTREX

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MARKET	New		DEFAULT, CHINA	Indicate in which market the line service is used.
OPTIONS	Changed		{SC, WML, ILR, CDIV, ICT, ICWT, CCBS, I3WC, IWUC, I6WC, CE PTPW, CEPTRA}	Indicate if the corresponding CEPT line services are allowed to work on IBN line without CE PT line option or not.

29.5.2.1.5 Datafill example

Refer to the following datafill example of tuple CEPTONCENTREX:

Figure 1 Datafill example of tuple CEPTONCENTREX

```
TABLE ISERVOPT
==============
CEPTONCENTREX CEPTONCENTREX CHINA (SC) (WML) (ILR) (IWUC) (CDIV)
(ICT) (ICWT) (CCBS) (I3WC) (I6WC) (CEPTPW) (CEPTRA) $
```

29.5.2.1.6 Table release history update

A new field MARKET and new CEPT line service options are introduced into the tuple CEPTONCENTREX by this activity.

29.5.2.1.7 Supplementary information

N/A.

29.5.2.1.8 Translation verification other tools

N/A.

29.5.2.1.9 Functional description - Tuple ILRCLS

A new field SHOW_CHG_PSWD is introduce into the tuple ILRCLS in table ISERVOPT. If this field is set to Y, the ILR password allows to be displayed and changed.

29.5.2.1.10 Usage sequence and implications (CM Only)

Current datafill order unchanged.

29.5.2.1.11 Size

Current table size unchanged.

29.5.2.1.12 Fields/OIDs

The following table lists fields for table ISERVOPT;

Table 4 Table field descriptions for tuple CEPTONCENTREX

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SHOW_CHG_ PSWD	New		{Y, N}	Indicate if the ILR password can be shown and changed.

29.5.2.1.13 Datafill example

Refer to following datafill example of tuple ILRCLS:

Figure 2 Datafill example of tuple ILRCLS

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ILRCLS
OPTION:
>ILRCLS
ILR_PROG:
>N
SDT:
>N
CR_PSWD: N
>Y
SHOW_CHG_PSWD: N
>Y
TUPLE TO BE ADDED:
ILRCLS ILRCLS N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

29.5.2.1.14 Table release history update

A new field SHOW_CHG_PSWD is introduced into the tuple ILRCLS by this activity.

29.5.2.1.15 Supplementary information

N/A.

29.5.2.1.16 Translation verification other tools

N/A.

29.5.2.1.17 Functional description - Tuple IWUC

A new field ABORT_IF_IN_USE is introduced into the tuple IWUC in table ISERVOPT. If this field is set to Y, the wakeup request is aborted automatically when the line is in use at the scheduled time, and the IWUC102 log with the reason ‘LINE IN USER’ will be generated to indicate the abortion of the wakeup request.

29.5.2.1.18 Usage sequence and implications (CM Only)

Current datafill order unchanged.

29.5.2.1.19 Size

Current table size unchanged.

29.5.2.1.20 Fields/OIDs

The following table lists fields for table ISERVOPT;

Table 5 Table field descriptions for tuple CEPTONCENTREX

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ABORT_IF_IN _USE	New		{Y, N}	Indicate if the wakeup request is aborted or not when the line is in use at the scheduled time.

29.5.2.1.21 Datafill example

Refer to following datafill example of tuple IWUC:

Figure 3 Datafill example of tuple IWUC

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>IWUC
OPTION:
>IWUC
MIN_AHEAD_TIME:
>1
REPEAT_NEXT_DAYS: N
>
ABORT_IF_IN_USE: N
>Y
REPEAT_PER_REQUEST:
>1
NUMBER_OF_REQUEST:
>ONE
OVERWRITE: N
>Y
TUPLE TO BE ADDED:
IWUC IWUC 1 N Y 1 ONE Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

29.5.2.1.22 Table release history update

A new field ABORT_IF_IN_USE is introduced into the tuple ILRCLS by this activity.

29.5.2.1.23 Supplementary information

N/A.

29.5.2.1.24 Translation verification other tools

N/A.

29.5.2.1.25 Functional description - Tuple ICWT

A new field ICWT_IGNORE_WAITING_TMO is introduced into tuple ICWT in table ISERVOPT. The operator can specify a value from 10 to 45 seconds for the timer “Called Party Ignores Waiting Call” of ICWT service.

By default, if the tuple ICWT is not datafilled in table ISERVOPT, the time-out of timer “Called Party Ignores Waiting Call” is 30 seconds.

29.5.2.1.26 Usage sequence and implications (CM Only)

Current datafill order unchanged.

29.5.2.1.27 Size

Current table size unchanged.

29.5.2.1.28 Fields/OIDs

The following table lists fields for table ISERVOPT;

Table 6 Table field descriptions for tuple CEPTONCENTREX

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ICWT_IGNORE _WAITING_TMO	New		{10 TO 45}	This field specifies the time-out of the timer “Called Party Ignores Waiting Call” for ICWT service.

29.5.2.1.29 Datafill example

Refer to following datafill example of tuple ICWT:

Figure 4 Datafill example of tuple ICWT

```
TABLE ISERVOPT
==============
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>icwt
OPTION:
>icwt
ICWT_IGNORE_WAITING_TMO:
>15
ICWT_ANN_ACTIVE: N
>N
ICWT_TMO_ANN_ACTIVE: N
>N
ICWT_TIMEOUT_TREATMENT:
>NOSC
TUPLE TO BE ADDED:
ICWT ICWT 15 N N NOSC
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

29.5.2.1.30 Table release history update

A new field ICWT_IGNORE_WAITING_TMO is introduced into the tuple ICWT by this activity.

29.5.2.1.31 Supplementary information

N/A.

29.5.2.1.32 Translation verification other tools

N/A.

29.5.2.1.33 Functional description - Tuple CEPTPW

A new field COLLECT_DNPIN_IN_DIFF_STAGES and two announcement IDs COLLECT_DN_ONLY and COLLECT_PIN_ONLY are introduced into tuple CEPTPW.

If the field COLLECT_DNPIN_IN_DIFF_STAGES is set to Y in tuple CEPTPW, a new DN and PIN dialing sequence is adopted by CEPTRA, that is, the subscriber should input DN firstly, and receive announcement, then input PIN.

When the subscriber dials the DISA DN in order to use CEPTRA service, if the field COLLECT_DNPIN_IN_DIFF_STAGES and ANNOUNCE are set to Y in tuple CEPTPW and the announcements are provisioned correctly, the subscriber will hear the announcement associated by announcement ID COLLECT_DN_ONLY to prompt to input DN, after the subscriber inputs the

valid DN, he/she will hear the announcement associated by announcement ID COLLECT_PIN_ONLY to prompt to input password.

29.5.2.1.34 Usage sequence and implications (CM Only)

Current datafill order unchanged.

29.5.2.1.35 Size

Current table size unchanged.

29.5.2.1.36 Fields/OIDs

The following table lists fields for table ISERVOPT;

Table 7 Table field descriptions for tuple CEPTONCENTREX

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
COLLE CT_DNPIN_IN_ DIFF_STAGES	New		{N,Y}	This field indicates if the new DN and PIN dialing sequence is adopted for CEPTRA service. If this field is set to Y, the subscriber should input DN firstly, and receive announcement, then input PIN. If the field is set to N, the subscriber should input DN and PIN as “DN*PIN” at once dialing.
CEPTANNID	Changed		{DNPIN,CHGPI N,SCODE ,VLDPIN,LOCK, **COLLE CT_DN_ONLY, COLLE CT_PIN_ONLY**}	New announcement IDs for the new DN and PIN dialing sequence.

29.5.2.1.37 Datafill example

Refer to following datafill example of tuple CEPTPW:

Figure 5 Datafill example of tuple CEPTPW

```
TABLE ISERVOPT
==============
>abort
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>3333
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>y
ANNOUNCE:
>y
ANNC_STATE:
>SILENCE
CEPT_ANNCS:
>chgpin ceptpw_chgpin
CEPT_ANNCS:
>vldpin ceptpw_vldpin
CEPT_ANNCS:
>collect_dn_only ceptra_coll_dn
CEPT_ANNCS:
>collect_pin_only ceptra_coll_pin
CEPT_ANNCS:
>$
TUPLE TO BE ADDED:
CEPTPW CEPTPW 3 1234 Y Y AUD_RNG (CHGPIN CEPTPW_CHGPIN)
(VLDPIN CEPTPW_VLDPIN) (COLLECT_DN_ONLY CEPTRA_COLL_DN)
(COLLECT_PIN_ONLY CEPTRA_COLL_PIN)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

29.5.2.1.38 Table release history update

A new field COLLECT_DNPIN_IN_DIFF_STAGES and two announcement IDs COLLECT_DN_ONLY and COLLECT_PIN_ONLY are introduced into tuple CEPTPW by this activity.

29.5.2.1.39 Supplementary information

N/A.

29.5.2.1.40 Translation verification other tools

N/A.

29.6 Service Orders (SO) (CM & SESM)

29.7 Software optionality control (SOC)

29.8 Element Management

29.9 Command interface changes

29.10 Security

29.11 Configuration Walkthrough

30: Configuration (CN): A00002844

30.1 Hardware and Software Requirements

N/A.

30.2 Initial Configuration

N/A.

30.3 Data schema (DS) (CM, MIBS, RDB)

30.3.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MTRSYSPM	CHANGED	CHANGED

30.3.2 Table/MIB/Remote Database Schema information

30.3.2.1 Name: MTRSYSPM

Metering System Parameters

30.3.2.1.1 Functional description

A new parameter “trunk_threshold” is added into EMD tuple in MTRSYSPM table.

Also, existing “threshold” field of EMD tuple is renamed as “line_threshold”.

30.3.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

30.3.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MTRSYSPM	11	11	EMD tuple is changed. A new parameter has been added, so there is not a fundamental change on memory consumption.

30.3.2.1.4 Fields/OIDs

The following table lists changed fields/OIDs for MTRSYSPM.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
EMD	Changed	TRUNK THRESHOLD	0 to 2,100,000,000	It identifies maximum delta value between current and previous trunk meter counts.

30.3.2.1.5 Datafill example

The following example shows sample datafill for table MTRSYSPM.

Table 4 Datafill example of EMD tuple in table MTRSYSPM

Field name	Default Value
ACTIVATION	NO
HOUR	4
MINUTE	15
PERIOD	1
LINE_THRESHOLD	20.000
TRUNK_THRESHOLD	200.000

There are some properties related to table MTRSYSPM as follows:

- New tuples cannot be added manually.
- Tuples can not be deleted.
- MTRSEL selector value must be identical to key value.
- Only changing is allowed.

30.3.2.1.6 Table release history update

Definition of EMD tuple has been made in MMP15. With this activity in SN07, parameters of EMD tuples is changed to include threshold value for trunks.

30.3.2.1.7 Supplementary information

None.

30.3.2.1.8 Translation verification other tools

MTRSYSPM does not use translation verification tools.

31: Configuration (CN): A00002900

31.1 Hardware and Software Requirements

N/A.

31.2 Initial Configuration

N/A.

31.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

31.4 Upgrade Impact

N/A.

31.5 Data schema (DS) (CM, MIBS, RDB)

31.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	Unchanged

31.5.2 Table/MIB/Remote Database Schema information

31.5.2.1 Name: SERVINFO

31.5.2.1.1 Functional description

Option INITDP_PARMS of table SERVINFO is extended to add two new fields **IP_AVA** and **IPSSP_CAP** to indicate whether parameters IPAvailable and IPSSPCapabilities will be carried in IDP. These two fields should be datafilled at the same time.

Meanwhile, option SRF_INFO is extended to add new filed **IP_INFO** to provide detailed information of the IP capability within SSP.

If IP_AVA and IPSSP_CAP are datafilled and IP_INFO is not datafilled, parameters iPAvailable and iPSSPCapabilities are set to default value according to China INAP, the default value of iPAvailable is ‘01’H (which indicates that the IP is available), the default value of iPSSPCapabilities is ‘#0C00’ (which indicates that DTMF digit collection and tone & announcement is supported). If IP_INFO is datafilled, then iPAvailable and iPSSPCapabilities are set according to this datafill. That means IP_INFO will take effect only if IP_AVA and IPSSP_CAP are datafilled, otherwise, the information of this datafill will not be carried in IDP.

IP_INFO contains two subfields: **IP_AVA** and **IP_SSP_CAPABILITIES**, which are for parameter IPAvailable and IPSSPCapabilities respectively.

31.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

31.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	no change	no change	N/A

31.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INITDP_PARMS	Changed	refinement	Boolean Value	Add new selections: IP_AVA and IPSSP_CAP.
SRF_INFO	Changed	refinement	Boolean Value	Add new sub-option: IP_INFO
IP_INFO	New	Subfield	Boolean Value	Add new sub-options: IP_AVA and IP_SSP_CAPABILITIES
IP_AVA	New	Subfield	Boolean Value	Indicate whether the IP is available.
IP_SSP_CAPABILITIES	New	Subfiled	Boolean	Provide the detailed information of IP capabilities. (See table 4 for details)

According to China INAP, there are 14 kinds of IP capabilities which are indicated by parameter iPSSPCapabilities. These capabilities can be datafilled in IP_SSP_CAPABILITIES as shown in table 4:

Table 4 IP Capabilities defined in China INAP

IPSSPCapabilites parameter	Value	Meaning	IPSSP_CAPABILITIES selections
1st byte, bit 0	0/1	Not support/Support IPRoutingAddress	IPRA
1st byte, bit 1	0/1	Not support/Support VoiceBack	VOICE_BACK
1st byte, bit 2	0/1	Not support/Support VoiceInformation, recognize through voice, speech.	VOICE_INFO_SPEECH
1st byte, bit 3	0/1	Not support/Support VoiceInformation, recognize through voice, voice.	VOICE_INFO_VOICE
1st byte, bit 4	0/1	Not support /SupportText to Voice conversion.	TEXT_TO_VOICE
1st byte, bit 5	0/1	Not support/Support fax.	FAX
1st byte, bit 6	0/1	Not support/Support recorder.	RECORDER
1st byte, bit 7	0/1	Not support/Support script.	SCRIPT
2nd byte, bit 0	0/1	Not support/Support manual operator.	MAN_OPERATOR
2nd byte, bit 1	0/1	Not support/Support conference.	CONFERENCE
2nd byte, bit 2	0/1	Not support/Support tone & announcement.	TONE_ANNC
2nd byte, bit 3	0/1	Not support/Support DTMF digit collection.	DTMF_DIGCOL
2nd byte, bit 4	0/1	Not support/Support sending DTMF signal.	SEND_DTMF_SIG
2nd byte, bit 5	0/1	Not support/Support sending FSK signal.	SEND_FSK_SIG
2nd byte, bit 6,7	To be defined.		
3rd, 4th bytes	To be defined.		

31.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVINFO:

Example of datafill:
TABLE SERVINFO
200 (INITDP_PARMS (SERVKEY) (CDPA)(**IP_AVA**) (**IPSSP_CAP**) $)
(SRF_INFO (EARLY_ANS ANS_ON_ANNS)
(**IP_INFO Y** (**IPRA**) (**VOICE_INFO_SPEECH**)
(**TONE_ANNC**)(**DTMF_DIGCOL**)$)$)$

31.5.2.1.6 Table release history update

New sub-option IP_AVA, IPSSP_CAP are added to option INITDP_PARMS. New sub-option IP_INFO is added to SRF_INFO and new option IP_INFO has 2 sub-options: IP_AVA and IP_SSP_CAPABILITIES.

31.5.2.1.7 Supplementary information

N/A.

31.5.2.1.8 Translation verification other tools

N/A.

31.6 Service Orders (SO) (CM & SESM)

N/A.

31.7 Software optionality control (SOC)

N/A.

31.8 Element Management

N/A.

31.9 Command interface changes

N/A.

31.10 Security

N/A.

31.11 Configuration Walkthrough

N/A.

32: Configuration (CN): A00002904

32.1 Hardware and Software Requirements

There is no specific hardware requirement for this feature. The basic ICM software package as well as basic call with 3WC is needed to use this feature.

32.2 Initial Configuration

The subscription to this feature has to be done according to the DS section below.

32.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

32.4 Upgrade Impact

32.4.1 Dump and Restore

No new table are being added for this feature.

32.4.2 Element Management Upgrade

N/A

32.5 Data schema (DS) (CM, MIBS, RDB)

32.5.1 New/modified tables, MIBs, or Database Schema

The following table describes changed table information.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SCAISSRV	Changed	unchanged

32.5.2 Table/MIB/Remote Database Schema information

32.5.2.1 Name: SCAISSRV>

Switch Computer Application Interface Subservices table

32.5.2.1.1 Functional description

N/A

32.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

32.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SCAISSRV	0	511	Protected

32.5.2.1.4 Fields

The following table lists fields for table SCAISSRV.

The default tuples TPCC16$ and SCAI3WC15$ will be added to the table SCAISSRV. The new function TOGGCALL will be added under each of these categories. The default tuples must be present in the table for subscription to the new functions.

The default tuple SCAICC10$ will be added to the table SCAISSRV. The function CALLHELD and CALLUNHELD will contain the new parameter HDUHDLEG. The default tuples must be present in the table to receive the additional parameter that indicates which leg of the call was held/unheld.

TPCC16$

TPCC (CONSULTEV Y) (CONFEVNT Y) (TRANSFEREV Y) (CNTRLREL Y)(NCTRLREL Y) (HOLDCALL) (UNHOLDCALL) (CALLUNHELD Y **Y**(ANSWCALL)(RELSCALL Y) (ADDPTY Y Y Y Y) (CONFPTY Y) (DROPPTY Y Y) (TRANPTY Y)(MAKECALL Y Y) (CALLHELD Y **Y**) **(TOGGCALL)**$

SCAI3WC15$

SCAI3WC (CONSULTEV Y) (CONFEVNT Y) (TRANSFEREV Y) (CNTRLREL Y) (NCTRLREL Y) (ADDPTY Y Y Y) (CONFPTY Y) (DROPPTY Y Y) (TRANPTY Y) **(TOGGCALL) $**

SCAICC10$

SCAICC (HOLDCALL) (UNHOLDCALL) (CALLUNHELD Y **Y**) (ANSWCALL) (RELSCALL Y) (CALLHELD Y **Y)** $

32.5.2.1.5 Datafill example

The following example shows sample datafill for table SCAISSRV:

```
TABLE: SCAISSRV
```

```
>add TOGGTUP1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
CATEGORY:
>TPCC
FUNCTION:
>TOGGCALL
FUNCTION:
>$
TUPLE TO BE ADDED:
TOGGTUP21 TPCC (TOGGCALL) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y

>add TOGGTUP2
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
> y
CATEGORY:
>SCAI3WC
FUNCTION:
>TOGGCALL
FUNCTION:
>$
TUPLE TO BE ADDED:
TOGGTUP2 SCAI3WC (TOGGCALL) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

```
>add HELDTUP1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
> y
CATEGORY:
>SCAICC
FUNCTION:
>CALLHELD
NCALLID: Y
HDUHDLEG: Y
FUNCTION:
> CALLUNHELD
NCALLID: Y
HDUHDLEG: Y
FUNCTION:
>$
TUPLE TO BE ADDED:
HELDTUP1 SCAICC (CALLHELD Y Y) (CALLUNHELD YY)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

32.5.2.2 Table release history update

The field that is added under categories TPCC and SCAI3WC of table SCAISSRV is **TOGGCALL.**

The new parameter added under catergory SCAICC of table SCAISSRV function CALLHELD and CALLUNHELD is **HDUHDLEG**.

32.5.2.3 Supplementary information

NA

32.5.2.4 Translation verification tools

SCAISSRV does not use translation verification tools.

32.6 Service Orders (SO) (CM & SESM)

N/A

32.7 Software optionality control (SOC)

Order code ICM00079, CTI Toggle Transfer optionalized the functionality of the dv_Toggle_Call message. When ICM00079 SOC is in the IDLE state, the invoke of the above message will be rejected by the DMS.

SOC-ON_TO-IDLE warning messages

The following warning message is displayed when the CTI Toggle Transfer SOC ICM00079 is toggled from ON to IDLE state. The warning message indicates that state transition disables the associated dv_Toggle_Call functionality.

SERVICE AFFECTING: This transition will disable the dv_Toggle_Call functionality for all current and future subscribers.

The table below summarizes the SOC option ICM00079 for CTI Toggle Transfer

Table 3 SOC

SOC option name:	ICM
SOC option title:	Toggle Transfer
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	ICM00079
Option defined in DRU:	CCM
Affected products:	LEC00020, LET00020, LLT00020, SN07, ISN07

33: Configuration (CN): A00002907

33.1 Hardware and Software Requirements

ISN07 software load on CS2K DMS.

33.2 Initial Configuration

Not applicable.

33.3 Office/Subnet parameters (OP/SP) (CM & SESM)

33.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	INAP_VARIANT	CHANGED	CM

33.3.2 Parameter information

33.3.2.1 INAP_VARIANT

Intelligent Network Application Protocol Variant.

33.3.2.1.1 Functional description

The value of the INAP_VARIANT office parameter determines whether INAP variant specific requirements are considered when handling INAP operations.

33.3.2.1.2 Provisioning rules

The value should be set to TINAP, if T-INAP support is required.

33.3.2.1.3 Range information

Table 2 Range Information

Valid Values	Maximum	Default
DFLTINAP, CHINESE, TINAP		DFLTINAP

33.3.2.1.4 Activation

Any changes are activated immediately.

33.3.2.1.5 Dependencies

None.

33.3.2.1.6 Consequences

When setting INAP_VARIANT to TINAP, Deutsche Telekom (DTAG) specific INAP extensions are activated.

33.3.2.1.7 Verification

Enable T-INAP support and verify, whether Deutsche Telekom specific INAP extensions are activated.

The following functionality is supported with the INAP_VARIANT office parameter set to TINAP:

- When ActivityTest operation fails, send an U-ABORT with activityTestFailed error code to the SCP.
- Encode userUser parameter in the ERB operation for DP9.
- Decode the DTAG private parameters in the Connect operation.

33.3.2.1.8 Memory requirements

No memory impact.

33.3.2.1.9 Parameter release history update

New TINAP option is implemented for the INAP_VARIANT office parameter.

33.4 Upgrade Impact

33.4.1 Dump and Restore

No impact.

33.4.2 Element Management Upgrade

No impact.

33.5 Data schema (DS) (CM, MIBS, RDB)

33.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	UNCHANGED

33.5.2 Table/MIB/Remote Database Schema information

33.5.2.1 Name: SERVINFO

Intelligent Network Service Information Table.

33.5.2.1.1 Functional description
Unchanged.

33.5.2.1.2 Usage sequence and implications (CM Only)
Current datafill order unchanged.

33.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	unchanged	unchanged	unchanged

33.5.2.1.4 Fields/OIDs
The following table lists fields/OIDs for SERVINFO.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INITDP_PARMS	Changed	refinement	{..., **ACPN, HLC**,...}	Parameters included when building an InitDP operation.
ACLI	New			Additional Calling Line Identity.
HLC	New			High Layer Compatibility.
INITDP_EXTENSIONS	Changed	refinement	{..., **SF_ENC, GAP_INT, NCPC, IN_CONT**, ...}	Additional Parameters included when building an InitDP operation.
SF_ENC	New			SF Encountered.
GAP_INT	New			GAP Interval.
NCPC	New			National Calling Partys Category.
IN_CONT	New			IN Container.

33.5.2.1.5 Datafill example
The following example shows sample datafill for table SERVINFO.

Figure 1 Example datafill SERVINFO

```
SERVIDX                                                              OPTION
-------------------------------------------------------------------------------

1234    ( INITDP_PARMS ( CDPA) ( ACLI) ( HLC) $)
        ( INITDP_EXTENSIONS ( SF_ENC) ( GAP_INT) ( NCPC) ( IN_CONT) $)
            (CS1R (CONTINUE) (CWA) $)$
```

33.5.2.1.6 Table release history update

Extended existing INITDP_PARMS parameter attribute list.
Extended existing INITDP_EXTENSIONS parameter attribute list.

33.5.2.1.7 Supplementary information

None

33.5.2.1.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify SERVINFO.

Figure 2 Example TRAVER using TINAP extensions

```
>traver tr step29isupv2 800333123456 b
TABLE TRKGRP
STEP29ISUPV2 IBNT2 0 NPDGP NCRT STEPDEFAULT 0 ASEQ 0 7848810029 ANSDISC 0 N N N
    N N N N 0 0 N 0 0 0 0 N N N N N N N N N NATL (BCNAME 3_1KHZ) $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
STEPDEFAULT 0 0 0 STTRK $
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
STEPDEFAULT NXLA STEPDEF NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME STEPDEF
TUPLE NOT FOUND
Default from table XLANAME:
STEPDEF
    (NET N N 0 N NDGT N N DOD N 59 NPRT_2 NLCA_NILLA_1 NONE $) $ F
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
59 NLCC NONE NT 1 1 NILSFC 0 PX STEPINTL NIL 00 NPRT_51 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
STEPINTL DFLT RTE ( DEST 10)$ DFOP $ CON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 800333123456
TABLE PXCODE
STEPINTL 080 080 CONT ( CLASS INTL) ( XLT FA STEPXLFA)$
TABLE FAHEAD
STEPXLFA DFLT RTE ( DEST 100)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                    800333123456
TABLE FACODE
STEPXLFA 800 800 RTE ( MM 5 18) ( DEST 1)$
TABLE: FARTE
KEY: STEPXLFA    1
 . S STEP01PRIN
EXIT TABLE FARTE
TABLE TRIGGRP
DFLTGRP INFOANAL
 . GENTRIG ( CDPN TDP3INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
 .  . TABLE TRIGDIG
 .  . TDP3INST GENTRIG 800333 GENTRIG EVENT TCAP INAPV8 SS7 EINJAZZ CALLED
 .  .     (SERVINFO_INDEX 1) $
 .  .  . TABLE SERVINFO
 .  .  . 1
 .  .  .     (INITDP_PARMS ( CDPA) (CLI) (ACLI) (HLC) $)
              (INITDP_EXTENSIONS (SF_ENC) (GAP_INT) (NCPC) (IN_CONT) $)
              (CS1R (CONTINUE) (CWA) $)$
 .  .  . TABLE C7GTTYPE
 .  .  . EINJAZZ CCITT7 0 NATL E164 $
 .  .  . TABLE C7GTT
 .  .  . EINJAZZ 800333123456 800333123456 PCSSN (K1297CCITT_RS0 K1297 0) $ SSN
INAP Info Analyzed TDP:  trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++
```

34: Configuration (CN): A00002916

34.1 Hardware and Software Requirements

34.2 Initial Configuration

34.3 Office/Subnet parameters (OP/SP) (CM & SESM)

34.4 Upgrade Impact

34.5 Data schema (DS) (CM, MIBS, RDB)

34.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
RCO2MAP	New	New

34.5.2 Table/MIB/Remote Database Schema information

34.5.2.1 Name: RCO2MAP

RCO2 Mapping Table

34.5.2.1.1 Functional description

The new Table RCO2MAP has been created to map the RCO2 C-side links to PRI terminals. Datafilling a RCO2 hosted off a GWC in table RCCINV auto-datafills a NIL tuple in table RCO2MAP. This tuple can then be modified by the craftsperson by datafilling the PRI trunks. This results in static data download to the GWC, of the mapping information of the RCO2 c-side links to PRI trunks.

34.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- SERVRINV
- CLLI
- SITE
- RCCINV

- TRKSGRP
- TRKMEM
- RCO2MAP

34.5.2.1.3 <Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RCO2MAP	0	255	

34.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

<conditional information>

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RMGNAME	New	S_PMT RCCNO	4 CHARS 0 TO 255	This is the key for the table and is autodatafilled in table RCO2MAP when table RCCINV is datafilled.
HOSTGWC	New	XPMTYPE XPMNO	GWC 0 TO 255	C-Side PM-This field must be datafilled with the RCO2's c-side PM as datafilled in Table RCCINV. The XPMTYPE must be GWC.
GWCPRITB	New	TAB COUNT	0 TO max_clli 0 TO 20	PRI CLLI datafill. Refer Figure 34.5.2.1.5, "Datafill example"for details.

34.5.2.1.5 Datafill example

The following example shows sample datafill for table <abbreviated name of table>

Datafilling an RCO2 hosted off a GWC in table RCCINV results in table RCO2MAP being datafilled with a nil tuple as follows :

Figure 1 Table RCO2MAP- sample tuple auto-datafilled

```
TABLE RCO2MAP

RCCNAME CSPM GWCPRITAB
-------------------------------------------------------------------------
RM02 RCO2 0 GWC 205 NIL 0
```

This tuple can then be modified by the craftsperson by datafilling the PRI trunk. The PRI CLLI datafilled in RCO2MAP will be a PRI variant that supports NFAS (Non-Facility Associated Signalling) functionality, on which one D-channel supports B-channels from a number of PRI trunks. A sample tuple in table RCO2MAP is as per following figure.

Figure 2 Table RCO2MAP- PRI NFAS Variant

```
TABLE RCO2MAP
RCCNAME CSPM GWCPRITAB
-------------------------------------------------------------------------
RM02 RCO2 0 GWC 205 (PRICLLITST1 1) (PRICLLITST2 1) (PRICLLITST1 31)
```

The first and second PRI starting terminal number will correspond to the D-channel for RCO2 unit 0 and unit 1 respectively. Hence, the first and second starting CLLI must be unique. Also, for these CLLI's Table TRKSGRP must be datafilled with the D-channel information. The subsequent PRI starting terminal numbers correspond to the messaging links. For each of these messaging links table TRKMEM must have the next consecutive 31 time slots datafilled.

The above sample tuple has 3 PRI trunk starting CLLI's - (PRICLLITST1 1) (PRICLLITST2 1) and (PRICLLITST1 31). Each PRI trunk starting terminal number corresponds to an E1 on the RCO2's c-side. Hence, it is imperative that the number of PRI trunk starting terminal numbers keyed in by the user in table RCO2MAP, must be equal to the number of RCO2 c-side links provisioned in the CSLNKTAB field in table RCCINV.

34.5.2.1.6 Table release history update

34.5.2.1.7 Supplementary information

Restrictions/Warnings:

- A Tuple in table RCO2MAP is deleted when the corresponding tuple in table RCCINV is deleted.
- Tuples in table TRKMEM that are referenced in table RCO2MAP cannot be deleted. First delete the tuple in table RCCINV, this will auto-delete the tuples in table RCO2MAP, then delete the table TRKMEM datafill.

34.5.2.1.8 Translation verification other tools

The following example shows the output from <ToolName> when it is used to verify <abbreviated name of table>.

RCO2MAP does not used translation verification tools.

<abbreviated name of table> does not use translation verification tools.

34.5.2.2 Name: RCCINV

Remote Cluster Controller Inventory

34.5.2.2.1 Functional description

Changes are implemented in table RCCINV to enable provisioning of a CSPM type of GWC for a RCO2. Datafilling a RCO2 subtending a GWC in table RCCINV will result in an auto-datafill of a NIL tuple in table RCO2MAP.Deleting a RCO2 subtending a GWC in table RCCINV will delete the corresponding tuple in table RCO2MAP.

34.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- SERVRINV
- CLLI
- SITE
- RCCINV

34.5.2.2.3 <Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RCCINV	0	255	

The Table RCCINV size is unchanged.

34.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

<conditional information>

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RCCNAME		SITENM	alphanumeric	Site name. Enter the site name assigned to the remote location.
		PMTYPE	RCO2	Peripheral Module type.
		RCCNO	0-255	Remote cluster controller number. Enter the PM number
ADNUM			0 to 4095	Administration number.
FRTYPE			CRSC,MCRM,MCRMS,RCE, RCEI	Frame type. Enter the frame type on which the PM equipment is mounted.
FRNO			0 to 511	Frame number. Enter the number of the frame on which the PM is mounted.
SHPOS			0 to 77	Shelf position.Enter the position of the llower of the two shelves on the frame unit.
FLOOR			0 to 99	Floor. Enter the number of the floor on which the PM frame is located.
ROW			A to Z and AA to ZZ	Row. Enter the row in which the PM equipment frame is located.
FRPOS			0 to 99	Frame position. Enter the bay position of the PM equipment frame.
EQPEC			MX85AA	Equipment product engineering code.Enter MX85AA for the RCO2.
LOAD			alphanumeric (vector of upto eight characters)	Load. Enter the name given to the issue of PM software. Table PMLOADS must be datafilled first with the load used.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
EXECTAB		TRMTYPE EXEC	KEYSET, POTS, RMM_TERM KSETEX, POTSEX, RSMEX	Terminal type. Enter the type of PM terminals used Executive programs. Enter the set of executive programs required for the PM specified in field TRMTYPE. Enter KSETEX if TRMTYPE is KEYSET. Enter POTSEX if TRMTYPE is POTS. Enter RSMEX if TRMTYPE is RMM_TERM.
CSPM	Changed	XPMTYPE	GWC	Peripheral module type. Enter the type of PM to which the RCO2 C-side is attached
		XPMNO	(0 to 255)	Peripheral module number. Enter the number of the PM to which the RCC C-side is attached.
CSLNKTAB				C-side link table. This field is a vector of up to 16 entries.Enter the RCO2's C-side links that are connected to the PVG.
ESA			N	ESA is not supported in a RCO2.
INTRASW			N	Intraswitching is not supported in a RCO2.
ADDLMSGL			N	Additional message link. Additional message links are not supported.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTCARD				Optional card. This field is a vector of up to 10 entries.
TONESET				Tone set. Enter the tone set appropriate for RCO2.
PROCPEC				Processor equipment product engineering code.
E2LOAD			alphanumeric (vector of upto eight characters)	EEPROM load name. Enter the erasable electronic programming read only memory (EEPROM) load name.
EXTINFO		EXTSHELF	Y/N	Extension shelf.Enter Y if the CPM has an extension shelf and continue datafill for the subfields. Otherwise, enter N.
		EXTFRTYP	CEXT,MCRMS, RCEI	Extension frame type. Enter the type of frame in which the extension shelf is located.
		EXTFRNO	0 to 511	Extension frame number. Enter the frame number of the frame type in which the extension shelf is placed.
		EXTSHPOS	0 to 77	Extension shelf position. Enter the shelf position in inches above the floor.
		EXTFLOOR	0 to 99	Extension shelf floor location. Enter the floor on which the extension shelf is located.
		EXTROW	A to Z (except I and O)	Extension shelf row location. Enter the row in which the extension shelf is located.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
		EXTFRPOS	0 to 99	Extension shelf frame position. Enter the extension shelf position within the frame.
OPTATTR			METER	Assign/Remove the METER option to enable/disable AOC for RCO2s.

34.5.2.2.5 Datafill example

The following example shows sample datafill for table RCCINV that provisions a RCO2 subtending a GWC.

Figure 3 Table RCCINV- Sample Datafill

```
RCCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD
 EXECTAB CSPM CSLNKTAB ESA INTRASW ADDLMSGL OPTCARD TONESET
 PROCPEC E2LOAD EXTINFO OPTATTR
----------------------------------------------------------------------
RM02 RCO2 0 1 CRSC 0 6 1 C 4 MX85AA WRI17AY
(RMM_TERM RSMEX) (ESALINES ESAEX) $
GWC 205 (1) (2) (3) $Y Y N (UTR6 )(RAM6X69 ) (ISP 16) $ UK100
AX74AA AX74AA UPFWNU01 Y CEXT 1 6 1 C 5 MX86AA L$
```

34.5.2.2.6 Table release history update

The following information was added :

In CSPM subfield XPMTYPE - added GWC.

CSLNKTAB field for a RCO2 subtending GWC indicates the C-side links on the RCO2.

34.5.2.2.7 Supplementary information

Restrictions/Warnings:

- Datafilling a RCO2 subtending a GWC in table RCCINV, autodatafills a NIL tuple in table RCO2MAP.
- Deleting a RCO2 subtending a GWC in table RCCINV, deletes the corresponding tuple in table RCO2MAP.

- GWC Tuples in table SERVRINV, that are datafilled in table RCCINV cannot be deleted. First delete the tuple in table RCCINV and then delete the GWC from table SERVRINV.

34.5.2.2.8 Translation verification other tools

The following example shows the output from <ToolName> when it is used to verify <abbreviated name of table>.

RCCINV does not used translation verification tools.

<abbreviated name of table> does not use translation verification tools.

34.6 Service Orders (SO) (CM & SESM)

34.7 Software optionality control (SOC)

34.8 Element Management

34.9 Command interface changes

34.10 Security

34.11 Configuration Walkthrough

35: Configuration (CN): A00003051

35.1 Hardware and Software Requirements

N/A

35.2 Initial Configuration

N/A

35.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

35.4 Upgrade Impact

N/A

35.5 Data schema (DS) (CM, MIBS, RDB)

N/A

35.6 Service Orders (SO) (CM & SESM)

35.6.1 Service order change details

35.6.1.1 LCC and options

This feature enhances the line option CFGD. This option assigns CFGD to lines with a line class code (LCC) of ISDNKSET.

35.6.2 New commands

This feature introduces a new LCC value for existing service order option CFGD.

35.6.2.1 How service order commands are presented

N/A

35.6.2.2 How service order options are presented

35.6.2.2.1 Description

CFGD option can be assigned as line option via the following SERVORD commands:

- ADO (add option)
- DEO (delete option)
- CHF (change feature information for current feature)
- EST (establish a hunt or call pickup group)

35.6.2.2.2 Example

Figure 1 Example of the CFGD option in prompt mode

```
>EST
SONUMBER:    NOW   3  8 21 PM
>
GROUPTYPE:
>DNH
PILOT_DN:
>7831005
LCC:
>ISDNKSET
GROUP:
>CUST783A
SUBGRP:
>0
NCOS:
>2
SNPA:
>102
KEY:
>1
RINGING:
>Y
LTG:    0
>
PILOT_LEN:
>ISDN3 1
DN_LEN:
>7831007
LEN:
>0 0 2 3
KEY:
>1
DN_LEN:
>$
OPTION:
>CFGD
INTERNAL:
>N
CFGDN:
>7831016
SPECTIME:
>Y
TIMEOUT:
>12
CFGTYPE:
>CFGDI
OPTION:
>$
GROUPSIZE:
>4
```

Figure 2 Example of the CFGD option in no-prompt mode

```
>EST $ DNH 7831005 ISDNKSET CUST783A 0 2 102 1 Y 0 ISDN3 1 +
7831007 0 0 2 3 1 $ CFGD N 7831016 Y 12 CFGDI $ 4
```

35.6.2.2.3 Option prompts

Table 1 System prompts for CFGD option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	CFGD	Specifies the option to assign. Enter CFGD.	
INTERNAL	Y, N	Specifies the forwarding destination. Enter Y to forward calls to the next hunt group member. Enter N to forward calls to a specified DN.	
CFGDN	Up to 24 digits	Specifies the forward-to DN. Enter a maximum of 24 digits. Note: This prompt appears if you enter N at the INTERNAL prompt.	
SPECTIME	Y, N	Specifies... Enter Y if you enter a time-out value. Enter N if you use the time-out value in Table CUSTSTN.	
TIMEOUT	12 to 325	Specifies the time-out value in seconds. Enter a value from 12 to 325. Note: This prompt appears if you enter Y at the SPECTIME prompt.	
CFGTYPE	N, CFGDI, CFGDE	Enter N if restrictions do not apply. Forward all incoming calls. Enter CFGDI for restrict intragroup. Do not forward calls from the hunt groups customer group. Enter CFGDE for restrict extragroup. Do not forward calls from outside the hunt groups customer group.	

35.6.2.2.4 Line class code compatibility

Table 2 CFGD compatibility to LCC

Line class code	Compatible?
ISDNKSET	Yes

35.6.2.2.5 Assignability

The following functionalities apply to this option:

- set functionality: No
- subset functionality: No
- DN functionality: Yes
- key functionality: No

35.6.2.2.6 Option prerequisites

N/A

35.6.2.2.7 Notes

N/A

35.6.2.2.8 Feature identification

Functionality: WT20

Feature number: A00003051

35.6.2.2.9 SERVORD+ Exceptions

N/A

35.7 Software optionality control (SOC)

N/A

35.8 Element Management

N/A

35.9 Command interface changes

N/A

35.10 Security

N/A

35.11 Configuration Walkthrough

N/A

36: Configuration (CN): A00003147

36.1 Hardware and Software Requirements

Not applicable.

36.2 Initial Configuration

Not applicable.

36.3 Office/Subnet parameters (OP/SP) (CM & SESM)

36.3.1 New/modified office/subnet parameters

Table 1 New of modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	DISABLE_DP_RECEPTION_ON_DGT	NEW	CM

36.3.2 Parameter information

36.3.2.1 DISABLE_DP_RECEPTION_ON_DGT

Disable DP Reception on lines assigned DGT option

36.3.2.1.1 Functional description

A new parameter named DISABLE_DP_RECEPTION_ON_DGT in table OFCENG is used to control(enable/disable) DP digit reception for lines assigned DGT option.

DP Digit Reception Disabled (DISABLE_DP_RECEPTION_ON_DGT=Y)
With this selection, DP Digit Reception is disabled officewide for lines assigned DGT option. This eliminates the generation of fake calls and unwanted billing records by line faults.

DP Digit Reception Enabled (DISABLE_DP_RECEPTION_ON_DGT=N)
With this selection, DP digit functionality remains unchanged.

36.3.2.1.2 Provisioning rules

If generation of fake calls and unwanted billing records occur on lines assigned DGT option by line faults, DISABLE_DP_RECEPTION_ON_DGT should be set to Y.

Otherwise, set DISABLE_DP_RECEPTION_ON_DGT to N.

36.3.2.1.3 Range information

Not applicable. The parameter can be set to Y or N, and will default to a value of N.

36.3.2.1.4 Activation

Changes to DISABLE_DP_RECEPTION_ON_DGT are immediately effective.

36.3.2.1.5 Dependencies

None.

36.3.2.1.6 Consequences

The following summary describes the effects of the DP digit control office parameter.

If DISABLE_DP_RECEPTION_ON_DGT is Y:

- DP digit reception is disabled on lines assigned DGT option.
- DP digit reception is unchanged on lines assigned DP option.
- Dial pulse phones on lines with DGT option are not supported.
- Generation of phantom calls on lines assigned DGT option is prevented.

If DISABLE_DP_RECEPTION_ON_DGT is N:

- DP digit functionality is unchanged.

36.3.2.1.7 Verification

Not applicable.

36.3.2.1.8 Memory requirements

No memory impact.

36.3.2.1.9 Parameter release history update

DISABLE_DP_RECEPTION_ON_DGT is added to table OFCENG in SN07 to control DP digit reception on lines assigned DGT option.

36.4 Upgrade Impact

Not applicable.

36.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

36.6 Service Orders (SO) (CM & SESM)

Not applicable.

36.7 Software optionality control (SOC)

Not applicable.

36.8 Element Management

Not applicable.

36.9 Command interface changes

Not applicable.

36.10 Security

Not applicable.

36.11 Configuration Walkthrough

Not applicable.

37: Configuration (CN): A00003227

37.1 Hardware and Software Requirements

N/A

37.2 Initial Configuration

N/A

37.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

37.4 Upgrade Impact

N/A

37.5 Data schema (DS) (CM, MIBS, RDB)

37.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	Unchanged

37.5.2 Table/MIB/Remote Database Schema information

37.5.2.1 Name: SERVINFO

37.5.2.1.1 Functional Description

Option INITDP_PARMS of table SERVINFO is extended to add a new field **UUI** to indicate whether parameter UUI data contained in an incoming ETSI ISUP V2 is carried in InitDP.

37.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

37.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVINFO	no change	no change	N/A

37.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INITDP_PARMS	Changed	Refinement	Boolean Value	Add new selection: UUI

37.5.2.1.5 Datafill example

Example of datafill;

>TABLE SERVINFO

200 (INITDP_PARMS (SERVKEY) (CDPA)**(UUI)** $)

37.5.2.1.6 Supplementary information

N/A

37.5.2.1.7 Translation verification other tools

The following example shows the outgoing IAM message and output from EINTRACE when it is used to verify TABLE SERVINFO.

```
>display 1

 C7TU MESSAGE       SIO           DPC              OPC        SLS
num type length  ni pr  si   XXXX XXXX XXXX   XXXX XXXX XXXX
 1  IAM    170    1  2 ISUP  --- default routing label ---
   Message bytes:
    0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
   -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
   A4 00 FD 04 FD 01 65 25 D0 04 12 67 00 01 00 60 00 0A 00 02
   07 05 83 90 50 55 0F 0A 07 03 13 01 72 38 45 68 03 04 1E 02
   84 83 20 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7E B9 00 00 00
   00 00 00 00 A1 00 00 FC 4F 00 00 00 00 82 A1 00 00 00 00 20
   20 20 20 A1 00 00 1C 85 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 1D 03 80 90 A3 00
>EINTRACE
```

```
>open
14:25:49 TCAP MESSAGE             Tid :  26  36
Agent  : CKT        2WISUPBA    0
================================================
62 81 F8 48 04 00 00 4F 00 6C 81 EF A1 81 EC 02
01 00 02 01 00 30 81 E3 80 01 63 81 04 03 9C 50
55 82 04 83 90 55 05 83 07 03 13 01 72 38 45 68
85 01 0A 87 01 00 AB 08 30 06 80 01 00 81 01 00
8C 02 00 08 AF 1B 30 19 02 01 0E 0A 01 00 A1 14
04 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 AF 81 84 30 81 81 02 01 11 0A 01 00 A1 79 04
77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7E
B9 00 00 00 00 00 00 00 A1 00 00 FC 4F 00 00 00
00 82 A1 00 00 00 00 20 20 20 20 A1 00 00 1C 85
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 9A 02 60 00 BB 03 81 01
00 9C 01 03 9D 02 00 08 9E 01 00
================================================
Type of Package : 62 = BEGIN
  Originating TRID : 00 00 00 4F
  Component Type : A1 = INVOKE
    Invoke ID : 00
    Operation : 00 = INITIAL DP
      Service Key : 63 = 99
      Dialled Digits
        Odd/Even Indicator : 0 = EVEN
        Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER
        INN Indicator : 1 = ROUTING TO INTERNAL NETWORK NUMBER NOT ALLOWED
        Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
        Digits : 50 55 = 0555
      Called Party Number
        Odd/Even Indicator : 1 = ODD
        Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER
        INN Indicator : 1 = ROUTING TO INTERNAL NETWORK NUMBER NOT ALLOWED
        Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
```

```
        Digits : 55 05 = 555
      Calling Party Number
        Odd/Even Indicator : 0 = EVEN
        Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER
        NI Indicator : 0 = COMPLETE
        Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
        Presentation Restriction : 00 = PRESENTATION ALLOWED
        Screening Indicator : 03 = NETWORK PROVIDED
        Digits : 01 72 38 45 68 = 1027835486
      Calling Partys Category : 0A = ORDINARY CALLING SUBSCRIBER
      CG Encountered : 00 = noCGencountered
      Misc Call Info
        Message Type : 00 = REQUEST
        dpAssignment : 00 = individualLine
      Original Called Party ID
        Odd/Even Indicator : 0 = EVEN
        Nature Of Address : 00 = SPARE
        Numbering Plan Indicator : 00 = UNKNOWN
        Presentation Restriction : 02 = ADDRESS NOT AVAILABLE
        Digits :
      Extensions
        Extension Field
          Type : 0E = CLI NAME
          Criticality : 00 = IGNORE
          Value
            CLI Name : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 = ``
      Extensions
        Extension Field
          Type : 14 = UUI
          Criticality : 00 = IGNORE
          Value
           UUI : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
        End to end method Indicator : 00 = no end to end method available
        Interworking Indicator : 0 = no_interworking_encountered
        End to end information : 0 = no_end_to_end_available
        ISDN user part Indicator : 1 = ISDN_user_part_used_all_the_way
        ISDN user part preference Indicator : 01 =
ISDN_user_part_not_required_used_all_the_way
        ISDN access Indicator : 0 = originating_access_non-ISDN
        SCCP method Indicator : 00 = no_indication
      Bearer Capability
        Transmission Medium Requirement : 00 = SPEECH
      Event Type BCSM : 03 = ANALYZED INFORMATION
      Redirecting Party ID
        Odd/Even Indicator : 0 = EVEN
        Nature Of Address : 00 = SPARE
        Numbering Plan Indicator : 00 = UNKNOWN
        Presentation Restriction : 02 = ADDRESS NOT AVAILABLE
        Digits :
      Redirection Information
        Redirecting Indicator : 00 = NO REDIRECTION
        Original Redirection Reasons : 00 = UNKNOWN/NOT AVAILABLE
```

37.6 Service Orders (SO) (CM & SESM)

N/A

37.7 Software optionality control (SOC)

N/A

37.8 Element Management

N/A

37.9 Command interface changes

N/A

37.10 Security

N/A

37.11 Configuration Walkthrough

N/A

38: Configuration (CN): A00003410

38.1 Hardware and Software Requirements

There is no special Hardware/Software Requirements.

38.2 Initial Configuration

N/A.

38.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

38.4 Upgrade Impact - N/A

38.4.1 Dump and Restore

38.4.2 Element Management Upgrade

38.5 Data schema (DS) (CM, MIBS, RDB)

38.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKSGRP	CHANGED	UNCHANGED

38.5.2 Table/MIB/Remote Database Schema information

38.5.2.1 Table Name: TRKSGRP.

38.5.2.1.1 Functional description

DMS100 switches are all based on ETSI V2 White book specification. Each market which its requirements are different from the base, can implement it by using the ability to declare its own VARIANT. Each market can use the VARIANT that already has been declared by the ISUP Platform.

For example: The Honduras national variant is identified by datafilling of the VARIANT field as ‘HONDURAS’ in table TRKSGRP for the Honduras ETSI ISUP trunks.

The VERSION field in table TRKSGRP is datafilled when the PROTOCOL field in table TRKSGRP indicates Q767 (ETSI ISUP). The 100_WHITE is available whenever the PROTOCOL is datafilled as Q767. The datafilled Version 100_WHITE together with the Variants define whether ETSI ISUP V2 or another market of ETSI ISUP V2 is used for that particular trunk group.

38.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

38.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKSGRP	0		

38.5.2.1.4 Fields/OIDs

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VARIANT	Changed	subfield	HONDURAS	See 13.5.2.1.1

38.5.2.1.5 Datafill example

HONDURAS variant in Table TRKSGRP

```
                SGRPKEY  CARDCODE
SGRPVAR
                                                                                SGRPVAR
-------------------------------------------------------------------------------------------------------------
  HONDURAS_ISUP 0        DS1SIG
       C7UP
2W N N UNEQ NONE Q767 THRL 0  DMSNODE  N Y HONDURAS 100_WHITE $ ETSI
CIC
                              ↓                                  ↓      ↓
                        External Protocol                     Variant  Version
```

38.5.2.1.6 Table release history update

38.5.2.1.7 Supplementary information
None.

38.5.2.1.8 Translation verification other tools
Table TRKSGRP does not use translation verification tools.

38.6 Service Orders (SO) (CM & SESM)
N/A.

38.7 Software optionality control (SOC)
N/A.

38.8 Element Management
N/A.

38.9 Command interface changes
N/A.

38.10 Security
N/A.

38.11 Configuration Walkthrough
N/A.

39: Configuration (CN): A00003411

39.1 Hardware and Software Requirements

The NTMX76AB card must be equipped on GPP line peripherals with SX05 processor.
The NTMX76CA card must be equipped on DTCO2 trunk peripherals SX05 processor.
The QPO20xx or QCI20xx load files should be supported for SX05 processor.

39.2 Initial Configuration

GPP should be loaded with QPO20xx load file.

DTCO2 should be loaded with QCI20xx load file.

NTMX76AB tone cards must be equipped on GPP peripherals.

NTMX76CA tone cards must be equipped on DTCO2 peripherals.

The LTCINV table should be datafilled with the new 'HONTONES' toneset.

The GPP/DTCO2 static data should be downloaded

39.3 Office/Subnet parameters (OP/SP) (CM & SESM)

FEATURE_TONE_SET office parameter.

39.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	FEATURE_TONE_SET	CHANGED	CM

39.3.2 Parameter information

39.3.2.1 <abbreviated parameter name>

<Feature Tone Set>

39.3.2.1.1 Functional description

The FEATURE_TONE_SET office parameter is responsible for providing market specific feature treatment definitions instead of default hardcoded definitions.

This office parameter will be expanded so as to include the new HONTONES toneset that is required for the Honduras market.

39.3.2.1.2 Provisioning rules

For the Honduras market the FEATURE_TONE_SET office parameter must be set to HONTONES value.

39.3.2.1.3 Activation

For activation of the office parameter the Restart Reload must be performed.

39.3.2.1.4 Dependencies

None

39.3.2.1.5 Consequences

If this office parameter is not set to HONTONES, the CWT tone will not be connected during CWT feature usage for Honduras market.

39.3.2.1.6 Memory requirements

No memory impact.

39.4 Upgrade Impact

N/A

39.5 Data schema (DS) (CM, MIBS, RDB)

39.5.1 New/modified tables, MIBs, or Database Schema

The LTCINV table will be modified. The TONESET field will be enhanced with HONTONES tones set.

Table 2 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	CHANGED	UNCHANGED

39.5.2 Table/MIB/Remote Database Schema information

39.5.2.1 Name: LTCINV.

Line and Trunk Controller Inventory.

39.5.2.1.1 Fields/OIDs

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TONESET	Changed	refinement	HONTONES	The TONE_SET_TYPE type is extended with HONTONES value.

39.5.2.1.2 Datafill example

Figure 1 The LTCINV datafill example.

```
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB
CSLNKTAB OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
-----------------------------------------------------------------------
PLGC 0 2 IDTE 0 51 0 D 3 6X02UC TLG17TAC (POTS POTSEX) (KEYSET KSETEX)
(RMM_TERM RSMEX) $ (0 8) (0 9) (1 24) (1 25) (0 10) (0 11) (0 12) (0 13)
(0 14) (0 15) (1 26) (1 27) (1 28) (1 29) (1 30) (1 31) $ (UTR15 ) (UTR17 )
(MSG6X69 ) (CMR13 CMR10A) (NT6X44EA ) $ HONTONES MX77AA MX77AA 0 UPFWNU01
(METER ) $ 6X40AC N
```

39.5.2.1.3 Supplementary information

NONE

39.5.2.1.4 Translation verification other tools

N/A

39.6 Service Orders (SO) (CM & SESM)

N/A

39.7 Software optionality control (SOC)

N/A

39.8 Element Management

N/A

39.9 Command interface changes

N/A

39.10 Security

N/A

39.11 Configuration Walkthrough

- Verify that the TL6K69LB tone card exists on the peripheral.
- Verify that this card is datafilled in the LTCINV tuple.
- Verify that the ‘HONTONES’ toneset is defined for the peripheral with the TL6K69LB tone card.
- Load Static Data to the peripheral

40: Configuration (CN): A00003467

40.1 Hardware and Software Requirements

40.2 Initial Configuration

40.3 Office/Subnet parameters (OP/SP) (CM & SESM)

40.4 Upgrade Impact

40.5 Data schema (DS) (CM, MIBS, RDB)

40.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ACCODE	CHANGED	UNCHANGED
FTCODE	CHANGED	UNCHANGED
NSCCODE	CHANGED	UNCHANGED
CTCODE	CHANGED	UNCHANGED
FACODE	CHANGED	UNCHANGED
OFCCODE	CHANGED	UNCHANGED
PXCODE	CHANGED	UNCHANGED
CT2CODE	CHANGED	UNCHANGED
FA2CODE	CHANGED	UNCHANGED
OFC2CODE	CHANGED	UNCHANGED
PX2CODE	CHANGED	UNCHANGED
AMCODE	CHANGED	UNCHANGED
ACHEAD	CHANGED	UNCHANGED
FTHEAD	CHANGED	UNCHANGED

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NSCHEAD	CHANGED	UNCHANGED
CTHEAD	CHANGED	UNCHANGED
FAHEAD	CHANGED	UNCHANGED
OFCHEAD	CHANGED	UNCHANGED
PXHEAD	CHANGED	UNCHANGED

40.5.2 Table/MIB/Remote Database Schema information

All of these effected tables are members of the universal translation tables. The modification on ACCODE is applied to all of these tables.

40.5.2.1 Name: ACCODE

Access Code Table

40.5.2.1.1 Functional description

This is an existing table**.**

40.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

40.5.2.1.3 Size

Table size unchanged.

40.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ACCODE.

XLASEL = FEATINFO

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XLADATA		XLASEL	FEATINFO	
		FTR	VALIDATE	

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	Changed	VALDATOP	CUSTMOD	Enter CUSTMOD, followed by a space, to alter the internal network class of service (NCOS) and customer group to new value for a given directory number (DN) based on the CUSTINFO attribute in table DNSCRN. The source of the DN used as an index into table DNSCRN is determined by the VALIDATE datafill. Datafill refinement CUSTSCRN, **followed by a space.** **Datafill refinement REV_XLA (Reverse_Translations_Trigger)**
	New	REV_XLA	Y or N	Reverse_Translations_Trigger Enter Y to start the reverse translation immediately just after processing the featinfo selector and datafill refinement DELDIGS. Otherwise enter N to deactivate REV_XLA functionality
	New	DELDIGS	0 to 18	Delete Prefix Digits If the entry in refinement REV_XLA is Y, datafill refinement DELDIGS. Enter the number of prefix digits to delete

40.5.2.1.5 Datafill example

The following example shows sample datafill for table ACCODE.

Figure 1 MAP display example for the CUSTMOD option

```
TABLE: ACCODE
>LIS 2
 XLANAME        FROMD           TOD
                                                                    XLADATA
------------------------------------------------------------------------
  NETXLA          987           987
FEATINFO VALIDATE
(SUBSCRN ( GENERAL Y Y Y Y) $) (CUSTMOD Y Y 0) $ 0 0 24 PX PTTXLA

  NETXLA          988           988
FEATINFO VALIDATE
(SUBSCRN ( GENERAL Y Y Y Y) $) (CUSTMOD Y N) $ 0 0 24 PX PTTXLA

>
```

40.5.2.1.6 Table release history update

Refinement REV_XLA (and REV_XLA's refinement DELDIGS) is added to option CUSTMOD.

40.5.2.1.7 Supplementary information

NONE

40.5.2.1.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify ACCODE.

Figure 2 traver example for the CUSTMOD option

```
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                  8887835470
TABLE PXCODE
PTTXLA 888 888 FEATINFO VALIDATE ( SUBSCRN ( GENERAL Y Y Y Y)$) ( CUSTMOD
Y Y 0) $ 0 0 24 PX VALIDATE
PLEASE ENTER CLI DIGITS:
>7835476
TABLE DNSCRN
```

40.6 Service Orders (SO) (CM & SESM)

40.7 Software optionality control (SOC)

Table 3 SOC

SOC option name:	XLAS Rev Trans Custmod
SOC option title:	Yes
SOC option control type:	state
New SOC option?	Yes
SOC option order code	XLAS0054
Option defined in DRU:	WT
Affected products:	ISN07

This feature is patched backed to SW000004. The patch ID is NAP43. NAP43 is a password activateble patch. For an ONP from (ISN04 - ISN06) to (ISN07 and beyond), the state of the SOC option XLAS0054 will automatically be set to 'ON', if NAP43 was activated before the ONP, and also all of the functionalities of this feature will be ON after the ONP, too. But for this ONP, a password for SOC option is still required to change the RTU field of the SOC option XLAS0054 in loads SW000007 and beyond. "SOC states and RTU values of the SOC optionXLAS0054 after ONPs" is described in table 14.

Table 41 SOC states and RTU values of the SOC option XLAS0054 after ONPs

ONP	State of SOC option after ONP		RTU of SOC option after ONP	
	IF State of SOC option in ISN07 (nodatafill load) before ONP is IDLE	**IF State of SOC option in ISN07 (nodatafill load) before ONP is ON**	**IF RTU of SOC option in ISN07 (nodatafill load) before ONP is N**	**IF RTU of SOC option in ISN07 (nodatafill load) before ONP is Y**
ISN04 (ISN04 or ISN06) to ISN07 (ISN07 or beyond) NAP43 is active on ISN04 (or ISN06)	ON	ON	N	Y

Table 41 SOC states and RTU values of the SOC option XLAS0054 after ONPs

ONP	State of SOC option after ONP		RTU of SOC option after ONP	
	IF State of SOC option in ISN07 (nodatafill load) before ONP is IDLE	IF State of SOC option in ISN07 (nodatafill load) before ONP is ON	IF RTU of SOC option in ISN07 (nodatafill load) before ONP is N	IF RTU of SOC option in ISN07 (nodatafill load) before ONP is Y
ISN04 (ISN04 or ISN06) to ISN07 (ISN07 or beyond) NAP43 is not active on ISN04 (or ISN06)	IDLE	ON	N	Y

41.1 Element Management

41.2 Command interface changes

41.3 Security

41.4 Configuration Walkthrough

42: Configuration (CN): A00003686

42.1 Hardware and Software Requirements

42.2 Initial Configuration

N/A

42.3 Office/Subnet parameters (OP/SP) (CM & SESM)

42.4 Upgrade Impact

42.5 Data schema (DS) (CM, MIBS, RDB)

42.6 Service Orders (SO) (CM & SESM)

42.7 Software optionality control (SOC)

There is one new SOC option that is introduced with this feature,XLAS Reroute Rel Cause.

XLAS Reroute Rel Cause is defined under XLAS SOC group.Functionality of feature is controlled with this SOC option.It is a state SOC, whose can be ON or IDLE.When state of XLAS Reroute Rel Cause is ON, feature becomes functional.

Table 1 XLAS Reroute Rel Cause SOC

SOC option name:	XLASxxxx
SOC option title:	XLAS Reroute Rel Cause
SOC option control type:	state
New SOC option?	Yes
SOC option order code	XLASxxxx
Option defined in DRU:	WT
Affected products:	ISN07

This feature is patched backed to ISN04. The patch ID is NAP45. NAP45 is an password activateble patch. For an ONP from ISN04 to ISN07 and beyond, the

state of the SOC option XLAS0053 will automatically be set to ‘ON’. And all of the functionalities of this feature will be ON. But after the ONP, a password for SOC option is still required to change the RTU field of the SOC option XLAS0053 in loads ISN07 and beyond.

42.8 Element Management

N/A

42.9 Command interface changes

N/A

42.10 Security

N/A

42.11 Configuration Walkthrough

N/A

43: Configuration (CN): A00003696

43.1 Hardware and Software Requirements

Not Applicable to the activity A00003696

43.2 Initial Configuration

Not Applicable to the activity A00003696

43.3 Office/Subnet parameters (OP/SP) (CM & SESM)

43.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	CAPTURE_ISC _PC	NEW	CM

43.3.2 Parameter information

43.3.2.1 Name: CAPTURE_ISC_PC

Capturing International Switching Center Point Code

43.3.2.1.1 Functional description

This parameter will enable/disable the printing of LOG that captures ISC Point Code information. This parameter is of type boolean{N,Y}. The implentation of this parameter is being done in ISN07 (SNWCSH07).

43.3.2.1.2 Provisioning rules

This parameter enables the LOG output when set to TRUE and disables when the value is set to FALSE.

43.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
Boolean{N,Y}	n/a	N

43.3.2.1.4 Activation

Any changes are activated immediately.

43.3.2.1.5 Dependencies
None

43.3.2.1.6 Consequences
None

43.3.2.1.7 Verification
No verification required for this parameter.

43.3.2.1.8 Memory requirements
No memory impact.

43.3.2.1.9 Parameter release history update
Created office parameter CAPTURE_ISC_PC in the table OFCENG.

43.4 Upgrade Impact

Not Applicable to the activity A00003696

43.5 Data schema (DS) (CM, MIBS, RDB)

43.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
KKSCRN	NEW	OLD

43.5.2 Table/MIB/Remote Database Schema information

43.5.2.1 Name: KKSCRN
KundenKennung Screening

43.5.2.1.1 Functional description
A mechanism to facilitate KK, IPI and TMR based screening and routing has to be provided as a part of this activity. To organize the data required to fulfill the above requirement, a new table KKSCRN has been created.

Access to this table from call processing and TRAVER starts with table TRKOPTS which then moves to CALLCNTL. After this, all other tables would be accessed depending on the particular datafill in CALLCNTL.

A screening index is datafilled against the trunk group (TRKOPTS) and the same screening index is also datafilled in the table (KKSCRN) which will be screened first.

The KK for the call is used along with this screen index to look up the entry in table KKSCRN. This entry can specify a customer group to use for translations (if no other BC or IPI specific routing is required), or a new screen index and the next screening table (IPISCRN)

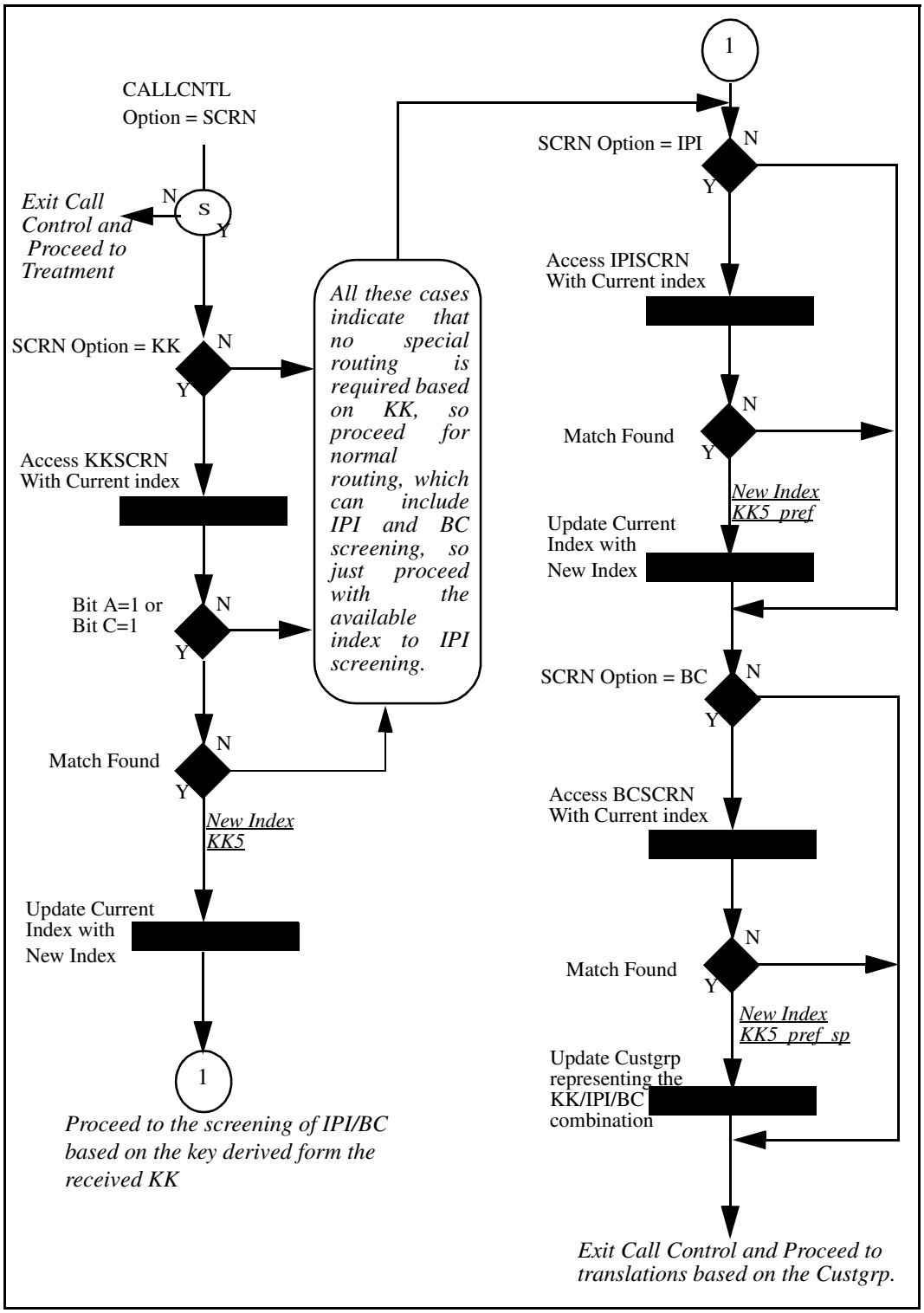
The IPI for the call is used along with the current screen index to look up the entry in table IPISCRN. This entry can specify a customer group to use for translations (if no other IPI specific routing is required), or a new screen index and the next screening table (BCSCRN).

The BC for the call is used along with the current screen index to loop up the entry in BCSCRN. This entry specifies the customer group to use for translations.

The end result is that the customer group for the call can be specified uniquely for each KK/IPI/BC combination.

The special routing will be invoked based Bit A and Bit C of national parameter NP.UKK. if either Bit A = 1 or Bit C = 1 is set in the message, else it proceeds for Normal routing.

Figure 1 Flow Diagram for KK screening



43.5.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

TABLE TRKOPTS

TABLE CALLCNTL

TABLE CDPNSCRN

SUBTABLE CDPNDATA

TABLE KKSCRN

TABLE IPISCRN

TABLE BCSCRN

43.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
KKSCRN	0	8191	Memory is automatically allocated for 16 DPC devices.

43.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for KKSCRN.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KKKEY	NEW	SCRNKEY	Any valid index in table CALLCNTL	KundenKennung Key. Subfield KundenKennung Screening Key has to be datafilled first in table TRKOPTS and then table CALLCNTL before datafilling into this table
	NEW	KK	0-16383	KundenKennung.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NEWSCKEY	NEW		Any valid index in table CALLCNTL	New Screening Index. This index has must exist in table CALLCNTL. This filed is of type THIRTY_TWO_CHAR_VECTOR
CCOPTION	NEW		Call Control Option	Call Control Option. This filed is of type THIRTY_TWO_CHAR_VECTOR

43.5.2.1.5 Datafill example

The following example shows sample datafill for table KKSCRN.

```
TABLE TRKOPTS
STEP27ISUPV2 CCNTLIDX CCNTLIDX INDEX

TABLE CALLCNTL
INDEX (SCRN (UKKCDPN) (KK) (IPI) (BC) $)$

TABLE CDPNSCRN
INDEX (1)
.................SUBTABLE CDPNDATA
                003336 003336 NO_KEY (TREAT PDIL) $

TABLE KKSCRN
INDEX 5 KK5 $

TABLE IPISCRN
KK5 PREFERRED KK5_PREFERRED $

TABLE BCSCRN
KK5_PREFERRED        SPEECH        KK5_PREFERRED        (CUSTGRP
KK5_PREFERRED_SPEECH_CUSTGRP1) $
```

43.5.2.1.6 Table release history update

Created table KKSCRN as a part of this activity.

43.5.2.1.7 Supplementary information

43.5.2.1.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify KKSCRN.

Figure 2 Example Traver for UKKCDPN,KK screen

```
>traver tr step27isupv2 0033391234 b
TABLE TRKGRP
STEP27ISUPV2 IBNT2 0 NPDGP NCRT STEPDEFAULT 0 ASEQ 0 7848810022
ANSDISC 0 N N N
    N N N N 0 0 N 0 0 0 0 N N N N N N N N N NATL (BCNAME 3_1KHZ) $
TABLE TRKOPTS
STEP27ISUPV2 CCNTLIDX CCNTLIDX ENTRY
TABLE CALLCNTL
ENTRY
    (SCRN (UKKCDPN) ( KK ) (IPI ) (BC ) $)$
PLEASE ENTER VALUE FOR NPUKK:
>PRESENT
PLEASE ENTER VALUE FOR ENTER BIT E:
>BIT_E_1
PLEASE ENTER VALUE FOR SPECIALROUTING INDICATOR
>1
PLEASE ENTER VALUE FOR KUNDENKENNUNG:
>5
 .  . TABLE KKSCRN
 .  . ENTRY 5 KK5 $
PLEASE ENTER VALUE FOR ISDN PREFERENCE INDICATOR:
>preferred
 .  . TABLE IPISCRN
 .  . KK5 PREFERRED KK5_PREFERRED $
PLEASE ENTER VALUE FOR BEARER CAPABILITY:
>speech
 .  . TABLE BCSCRN
 .  . KK5_PREFERRED  SPEECH   KK5_PREFERRED_SPEECH  (CUSTGRP
RUADEFAULT) $
 . TABLE CALLCNTL
 . TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP DFLTGRP
INAP Origination Attempt TDP:  no subscribed trigger.
TABLE NCOS
RUADEFAULT 0 0 0 RUTRK $
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND
DIGCOL
RUADEFAULT NXLA RUADEF NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE TRIGGRP
DFLTGRP INFOCOL
 . GENTRIG ( SPC TDP2INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Collected TDP:  trigger criteria not met.
TABLE IBNXLA: XLANAME RUADEF
TUPLE NOT FOUND
Default from table XLANAME:
RUADEF
    (NET N N 0 N NDGT N N DOD N 69 NPRT_2 NLCA_NILLA_1 NONE $) $ F
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
69 NLCC NONE NT 1 1 NILSFC 0 PX RUAINTL NIL 00 NPRT_10 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
NPRT_2 NSCR 755 NPRT NONE N $ $
```

Figure 3 Example Traver for UKKCDPN,KK screen (continued)

```
NPRT_2 NSCR 755 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
RUAINTL SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
0033481111
TABLE PXCODE
RUAINTL 00 00 CONT ( PF 2) ( CLASS INTL) ( CONSUME 2) ( XLT CT
RUAXLCT)$
TABLE CTHEAD
RUAXLCT DFLT RTE ( DEST 100)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
33481111
TABLE CTCODE
RUAXLCT 334 334 RTE ( PF 3) ( MM 4 18) ( DEST 14) ( LNET INTERNAT)
( MZONE 3)$
TABLE: CTRTE
KEY:  RUAXLCT   14
 . S RUA14ISUPV2LP
EXIT TABLE CTRTE
TABLE TRIGGRP
DFLTGRP INFOANAL
 . GENTRIG ( CDPN TDP3INST)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
INAP Route Select Failure TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++
DIGIT TRANSLATION ROUTES

1 RUA14ISUPV2LP 0033491111                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

43.6 Service Orders (SO) (CM & SESM)

Not Applicable to the activity A00003696

43.7 Software optionality control (SOC)

Not Applicable to the activity A00003696

43.8 Element Management

Not Applicable to the activity A00003696

43.9 Command interface changes

Not Applicable to the activity A00003696

43.10 Security

Not Applicable to the activity A00003696

43.11 Configuration Walkthrough

Not Applicable to the activity A00003696

44: Configuration (CN): A00004205

44.1 Hardware and Software Requirements

All the necessary hardwares and datafills should be available to make calls over the following interworkings:

Table 1 Supported Interworkings

From: \ To:	Japan PRIv1	Japan PRIv2	JI-ISUP	ANSI7+(Q764)
Japan PRIv1	YES	YES	YES	YES
Japan PRIv2	YES	YES	YES	YES

44.2 Initial Configuration

N/A

44.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

44.4 Upgrade Impact

N/A

44.5 Data schema (DS) (CM, MIBS, RDB)

44.5.1 New/modified tables, MIBs, or Database Schema

Table 2 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	CHANGED	UNCHANGED

44.5.2 Table/MIB/Remote Database Schema information

44.5.2.1 Name: ISERVOPT

44.5.2.1.1 Functional description

The new tuple JAPANPRI will be introduced by this activity in table ISERVOPT. This tuple holds entries for every Japan PRI related enhancement which is intended to be switched on and off by datafill. At the moment table ISERVOPT will allow an entry for opening backward voice path on the Japan PRI PBXs by sending a second PI#8 in the PROGRESS/ALERT messages.

Value Yes ‘Y’ implies that this service should be supported, value No ‘N’ or absence of JAPANPRI tuple in the iservopt table means the service is not supported.

44.5.2.1.2 Usage sequence and implications (CM Only)
There is no requirement to datafill tables in a specific order.

44.5.2.1.3 Size
Unchanged.

44.5.2.1.4 Fields/OIDs
The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	Changed	-	JAPANPRI	New entry JAPANPRI defined.
SOPTSVAR	Changed	option	JAPANPRI	New entry JAPANPRI defined.
SOPTSVAR	New	allow_backward_voice_path	{Y, N}	Whether second PI#8 should be added or not to the PROGRESS/ ALERT messages.

44.5.2.1.5 Datafill example
The following examples shows sample datafill for table ISERVOPT.

- Addition of the second PI#8 should be turned on:
  JAPANPRI JAPANPRI Y
- Addition of the second PI#8 should be turned off:
  JAPANPRI JAPANPRI N

44.5.2.1.6 Table release history update
The following information was added:

New entry JAPANPRI added to fields SOPTSKEY and SOPTSVAR.

New option ALLOW_BACKWARD_VOICE_PATH added to the JAPANPRI.

44.5.2.1.7 Supplementary information
None.

44.5.2.1.8 Translation verification other tools
ISERVOPT does not use translation verification tools.

44.6 Service Orders (SO) (CM & SESM)

N/A

44.7 Software optionality control (SOC)

N/A

44.8 Element Management

N/A

44.9 Command interface changes

N/A

44.10 Security

N/A

44.11 Configuration Walkthrough

N/A

45: Configuration (CN): A00004503

45.1 Hardware and Software Requirements

N/A.

45.2 Initial Configuration

N/A

45.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

45.4 Upgrade Impact

45.4.1 Dump and Restore

If the boolean field CGSCCDEA exists in the prior releases, it is transferred unchanged; if it does not exist, it is moved in ONPs by ‘N’ as default.

45.4.2 Element Management Upgrade

45.5 Data schema (DS) (CM, MIBS, RDB)

45.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKGRP	CHANGED	CHANGED

45.5.2 Table/MIB/Remote Database Schema information

45.5.2.1 Name: TRKGRP

Trunk group table

45.5.2.1.1 Functional description

TRKGRP table is used to store agent basis information about trunks to be able to define and change variable options about trunks including group type, trunk direction, class of service,....etc.

A new field is added to this table to provide a new control mechanism in order to activate/deactivate terminating SCC processing for CGPN.

45.5.2.1.2 Usage sequence and implications (CM Only)

In order to be able to add a new tuple into table TRKGRP, current datafill order is unchanged.

45.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKGRP	0	912	

45.5.2.1.4 Fields/OIDs

The following table lists new field added into TRKGRP table.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CGSCCDEA	NEW	None	Y/N	Terminating CGPN SCC processing deactivation/ activation

45.5.2.1.5 Datafill example

The following example shows sample datafill for table TRKGRP:

```
>table trkgrp
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos GANSIE1STEP1
GANSIE1STEP1 AXXESS 0 NPDGP NCIT 2W ODP1 MIDL 16 7 16 16 4 5 4
ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N 1 0 0 0 N N NIL NIL ISUP (NETINFO) $ 0 STD N Y NIL 0 N


>pos GANSIE1STEP2
GANSIE1STEP2 AXXESS 0 NPDGP NCIT 2W ODP2 MIDL 16 7 16 16 4 5 4
ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N 1 0 0 0 N N NIL NIL ISUP (NETINFO) $ 0 STD N Y NIL 0 Y
```

In the above example, the last field in table TRKGRP illustrated as bold is the CGSCCDEA field datafilled per trunk. It is a boolean value and it can be datafilled as Y or N.

Table 4 Table TRKGRP

GRPKEY	GRPTYP	TRAFSNO	.....	CGSCCDEA
GANSIE1STEP1	AXXESS	0		N
GANSIE1STEP2	AXXESS	0		Y

45.5.2.1.6 Table release history update

N/A.

45.5.2.1.7 Supplementary information

N/A.

45.5.2.2 Table Control Messages

As for datafill changes there are some restrictions and limitations:

45.5.2.2.1 When attempting to change the value of CGSCCDEA field in table TRKGRP:

a. For trunks ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP:

For these supported protocols, CGSCCDEA field can be changed as illustrated in the below figure.

Figure 1 Changing CGSCCDEA for supported protocols

```
>table trkgrp
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos GITU2IE1N01D
GITU2IE1N01D AXXESS 0 NPDGP NCIT 2W GPX MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 101 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N N 0 0 0 N N NIL NIL ISUP (NETINFO) $ 105 STD N Y NIL 0 N
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYP: AXXESS
>
TRAFSNO: 0
>
.....
CGSCCDEA: N
>y
TUPLE TO BE CHANGED:
GITU2IE1N01D AXXESS 0 NPDGP NCIT 2W GPX MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 101 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y ALL
N N 0 0 0 N N NIL NIL ISUP (NETINFO) $ 105 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

b. For trunks other than ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP CGCCDEA field CAN NOT be changed to ’Y’. If the field is attempted to be changed from ’N’ to ’Y’ for any AXXESS trunk type, following error/warning messages are displayed and modification can not be realized:

1. For trunks other than ISUP/TUP:

“CGSCCDEA can be set to Y for ISUP and TUP protocols.”

Figure 2 Changing CGSCCDEA for trunks other than ISUP/TUP

```
>table trkgrp
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos CR11MANIC1
CR11MANIC1 AXXESS 0 NPDGP NCIT IC MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 N N NODEF NO_OVERRIDE
VOICE_DATA Y
NOPROP N 1 0 0 0 N N NIL NIL CAS 3 STD N Y NIL 0 N
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYP: AXXESS
>
TRAFSNO: 0
>
.....
CGSCCDEA: N
>y
CGSCCDEA can be set to Y for ISUP and TUP protocols.
TUPLE TO BE CHANGED:
CR11MANIC1 AXXESS 0 NPDGP NCIT IC MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 N N NODEF NO_OVERRIDE
VOICE_DATA Y
NOPROP N 1 0 0 0 N N NIL NIL CAS 3 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
CGSCCDEA can be set to Y for ISUP and TUP protocols.
DATA CONSISTENCY ERROR
UNEXPECTED ERROR CONDITION
```

2. For ISUP trunks other than ETSI ISUP V1, V2 and ANSI ISUP:

“CGSCCDEA can be set to Y for ISUP trunks datafilled in Table ISUPATTR as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.”

Figure 3 Changing for ISUP trunks other than E ISUP V1, V2 and ANSI ISUP

```
>table trkgrp
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos GCOLOIE1A01A
GCOLOIE1A01A AXXESS 0 NPDGP NCIT 2W GPX MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 101 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 30 121 0 N N NIL NIL ISUP $ 104 STD N Y NIL 0 N
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYP: AXXESS
>
TRAFSNO: 0
>.....
CGSCCDEA: N
>y
CGSCCDEA can be set to Y for ISUP trunks datafilled in Table ISUPATTRas ETSI ISUP
V1,ETSI ISUP V2 and ANSI ISUP.
TUPLE TO BE CHANGED:
GCOLOIE1A01A AXXESS 0 NPDGP NCIT 2W GPX MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 101 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 30 121 0 N N NIL NIL ISUP $ 104 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>n
DMO REJECTED
>
```

3. For TUP trunks other than RBTUP/BBTUP:

"CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP /BBTUP."

Figure 4 Changing for TUP trunks other than RBTUP/BBTUP

```
>table trkgrp
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>pos GBTUPSTEP1
GBTUPSTEP1 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 N N NODEF NO_OVERRIDE
VOICE_DATA Y
PROT1 N 1 0 0 0 N N NIL NIL TUP 0 STD N Y NIL 0 N
>table tupattr
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TUPATTR
>pos 0
   0                    BTUP N N N   N       N       N  BTUP2W
   CIC          NIL
>quit
TABLE: TRKGRP
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYP: AXXESS
>
TRAFSNO: 0
>.......
CGSCCDEA: N
>y
CGSCCDEA can be set to Y for TUP trunks datafilled
in Table TUPATTR as RBTUP/BBTUP.
TUPLE TO BE CHANGED:
GBTUPSTEP1 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 N N NODEF NO_OVERRIDE
VOICE_DATA Y
PROT1 N 1 0 0 0 N N NIL NIL TUP 0 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

45.5.2.2.2 While adding a new AXXESS trunk in Table TRKGRP:

Following error messages are displayed if the new trunk has the CGSCCDEA field as 'Y' and the trunk is not a ETSI ISUP V1, ETSI ISUPV2, ANSI, RBTUP and BBTUP TRUNK.

CGSCCDEA can be set to Y for ISUP and TUP protocols.

CGSCCDEA can be set to Y for ISUP trunks datafilled in Table ISUPATTR as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.

CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP /BBTUP.

45.5.2.2.3 When CGSCCDEA field is set to 'Y' :

For any of the trunks ETSI ISUP V1, ETSI ISUP V2 ,ANSI, RBTUP, BBTUP; an error message is displayed under the name of the trunk which has the CGSCCDEA field set to 'Y' if there is an attempt to change the protocol in ISUPATTR/TUPATTR tables to a value other than ETSI V1, ETSI V2 , ANSI and RBTUP (protocols that do not support CGPN SCC deactivation) and it is prevented to change the protocol variant in ISUPATTR/TUPATTR tables unless the CGSCCDEA field is changed to 'N'.

"CGSCCDEA field is set to Y in Table TRKGRP"

Figure 5 Changing variant field in Table TUPATTR

```
>table tupattr
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TUPATTR
>pos 101
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUITy
>
VARIANT: RBTUP
>FTUP
ADJNODE:
>nil
OVLPOUTP: N
>
OVERLAP: N
>
.....
CGSCCDEA field is set to Y in Table TRKGRP
TUPLE TO BE CHANGED:
  101  FTUP      THRH  0   NONE  N      NIL      N      N    NIL
    CIC           NIL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>
INVALID REPLY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

When the CGSCCDEA field is set to ‘Y’ in Table TRKGRP, there are some restrictions for changing the ‘Protocol’ and ‘Protidx’ fields of TRKGRP table as follows:

For axxess trunks if the CGCCDEA field is ’Y’, the ‘Protocol’ field in Table Trkgrp can not be changed to any protocol other than ISUP and TUP.

If the Protocol field is attempted to be changed from ISUP or TUP to any other protocol, an error message is displayed and modification can not be realized.

- For an Axxess trunk with the CGSCCDEA field ‘Y’ and protocol field ISUP or TUP in table TRKGRP:

“CGSCCDEA can be set to Y for ISUP and TUP protocols.“

Figure 6 Changing Protocol field in TRKGRP if CGSCCDEA is 'Y'

```
2004/01/09 16:29 SANITY HAS FINISHED HANDAN 2011
TABLE: TRKGRP

>>pos GITU1E1STEP2
GITU1E1STEP2 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 0 0 0 N N NIL NIL ISUP $ 1 STD N Y NIL 0 Y
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUITy
>
GRPTYP: AXXESS
>
TRAFSNO: 0
>
PADGRP: NPDGP
>
                .....
                .....
PROTOCOL: ISUP
>CAS
PROTIDX: 1
>
FWDXMT: STD
>
INTLNTWK: N
>
LOOPBACK: Y
>
POECNAME: NIL   0
>
CGSCCDEA: Y
>
CGSCCDEA can be set to Y for ISUP and TUP protocols.
TUPLE TO BE CHANGED:
GITU1E1STEP2 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 0 0 0 N N NIL NIL CAS 1 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>N
DMO REJECTED
>
```

For axxess trunks if the CGCCDEA field is ’Y’, the ‘Protidx’ field in Table Trkgrp cannot be changed to any index other than the indexes representing the supported variants.

If the Protidx field is attempted to be changed from an index representing a supported variant to any other index of an unsupported variant, an error message is displayed and modification can not be realized.

- For an Axxess trunk with the CGSCCDEA field ‘Y’ and protidx field in table TRKGRP representing a supported variant of ISUP:

“CGSCCDEA can be set to Y for ISUP trunks datafilled

in Table ISUPATTR as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.”

- For an Axxess trunk with the CGSCCDEA field ‘Y’ and protidx field in table TRKGRP representing a supported variant of TUP:

“CGSCCDEA can be set to Y for TUP trunks datafilled in Table TUPATTR as RBTUP/BBTUP.”

Figure 7 Changing Protidx field in TRKGRP if CGSCCDEA is 'Y'

```
2004/01/09 16:29 SANITY HAS FINISHED HANDAN 2011
TABLE: TRKGRP

>>pos GITU1E1STEP2
GITU1E1STEP2 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 0 0 0 N N NIL NIL ISUP $ 1 STD N Y NIL 0 Y
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUITy
>
GRPTYP: AXXESS
>
TRAFSNO: 0

>PADGRP: NPDGP
>
              .....
CCNTLIDX: NIL
>
PROTOCOL: ISUP
>
OPTIONS:
>$
PROTIDX: 1
>215
FWDXMT: STD
>
INTLNTWK: N
>
LOOPBACK: Y
>
POECNAME: NIL   0
>
CGSCCDEA: Y
>
CGSCCDEA can be set to Y for ISUP trunks datafilled
in Table ISUPATTR as ETSI ISUP V1,ETSI ISUP V2 and ANSI ISUP.
TUPLE TO BE CHANGED:
GITU1E1STEP2 AXXESS 0 NPDGP NCIT 2W MAN MIDL 16 7 16 16 4 5 4 ALERTING
NIL_COSGRP 0 901 NONE 0 0 NIL_CUST 1 Y Y NODEF NO_OVERRIDE
VOICE_DATA Y Q764
N 1 0 0 0 N N NIL NIL ISUP $ 215 STD N Y NIL 0 Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>N
```

45.6 Service Orders (SO) (CM & SESM)

N/A.

45.7 Software optionality control (SOC)

N/A.

45.8 Element Management

N/A.

45.9 Command interface changes

N/A.

45.10 Security

N/A.

45.11 Configuration Walkthrough

N/A.

46: Configuration (CN): A00004563

46.1 Hardware and Software Requirements

The functionality provided by this activity is available on **SX05** XPM processors **only**.

46.2 Initial Configuration

None

46.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

46.4 Upgrade Impact

46.4.1 Dump and Restore

Not impacted by this activity.

46.4.2 Element Management Upgrade

N/A

46.5 Data schema (DS) (CM, MIBS, RDB)

46.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKSGRP	CHANGED	UNCHANGED

46.5.2 Table/MIB/Remote Database Schema information

46.5.2.1 Table TRKSGRP

Trunk Subgroup Table

46.5.2.1.1 Functional description

Table TRKSGRP is an existing table that holds information related to trunk subgroups on a per trunk subgroup basis. This activity enhances table TRKSGRP such that an ETSI ISUP version 2 trunk of the new Moroccan ISUP variant can be datafilled.

46.5.2.1.2 Usage sequence and implications (CM Only)

Not impacted by this activity.

46.5.2.1.3 Size

Not impacted by this activity.

46.5.2.1.4 Fields/OIDs

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SGRPVAR	CHANGED	VARIANT	{BASE, GERMANY, ... HONDURAS, **MOROCCO}**	New variant provided by this activity

46.5.2.1.5 Datafill example

Figure 1 Sample TRKSGRP datafill for Moroccan ISUP v2 trunks

```
TABLE: TRKSGRP
SGRPKEY CARDCODE SGRPVAR SGRPVAR
--------------------------------
OGMRISUPV2 0 DS1SIG C7UP OG N N UNEQ NONE Q767 THRH 0 DMS N N
MOROCCO 100_WHITE $ OGN7

ICMRISUPV2 0 DS1SIG C7UP IC N N UNEQ NONE Q767 THRH DMS
MOROCCO 100_WHITE $ ICN7

2WMRISUPV2 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMS N N
MOROCCO 100_WHITE $ 2WN7 CIC
```

Table C7UPTMR is used to datafill the signaling timers applying to a specific trunk subgroup in table TRKSGRP. Table C7UPTMR is not modified by this activity but an example is presented here for completeness.

Figure 2 Sample C7UPTMR datafill for Moroccan ISUP v2 timers

```
TABLE: C7UPTMR

TMRKEY C7UPDIR TMRS OPTIONS
---------------------------
OGN7 OG Q767 15 180 326 60 90 20 180 10 60 10 60 1000 10 120 240 10 $

ICN7 IC Q767 15 180 326 60 90 15 5 15 10 60 10 60 10 60 10 60 10 60
10 60 10 120 240 10 20 4 $

2WN7 2W Q767 15 180 326 60 90 20 15 180 5 15 10 60 10 60 10 60 10 60
10 60 10 60 1000 10 120 240 10 15 20 4 10 $
```

46.5.2.1.6 Table release history update
None

46.5.2.1.7 Supplementary information
None

46.5.2.1.8 Translation verification other tools
Not impacted by this activity

46.6 Service Orders (SO) (CM & SESM)
N/A

46.7 Software optionality control (SOC)
N/A

46.8 Element Management
N/A

46.9 Command interface changes
N/A

46.10 Security
N/A

46.11 Configuration Walkthrough
Not impacted by this activity.

47: Configuration (CN): A00004565

47.1 Hardware and Software Requirements

This activities are supported

- only for SX05 PDTC loads
- only for SX05 GPP with QPO load
- MX77 (development will be done) PLGC and OLG load
- SX05 (only for basic sanity tests will be done) PLGC, QGI loads.

47.2 Initial Configuration

None

47.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

47.4 Upgrade Impact

47.4.1 Dump and Restore

None

47.4.2 Element Management Upgrade

N/A

47.5 Data schema (DS) (CM, MIBS, RDB)

47.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
C7UPTMR	CHANGED	UNCHANGED
ISUPSVC	UNCHANGED	UNCHANGED
xxHEAD (PXHEAD, OFCHEAD, CTHEAD, ACHEAD, FAHEAD, AMHEAD, FTHEAD)	CHANGED	UNCHANGED

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
xxCODE (PXCODE, OFCCODE, CTCODE, ACCODE, FACODE, FTCODE, AMCODE)	CHANGED	UNCHANGED

47.5.2 Table/MIB/Remote Database Schema information

47.5.2.1 Table C7UPTMR

Common Channel Signalling No.7 ISUP Timers

47.5.2.1.1 Functional description

Table C7UPTMR contains call processing and maintenance timers. The timers are datafilled according to trunk subgroup. A new ISUP timer "CRG" is datafilled in table C7UPTMR. CRG timer is started to wait CRG messages after ANM/CON messages in backward metered ISUP calls. This timer is provisioned only for OG and 2W trunks.

47.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

47.5.2.1.3 Size

The minimum and maximum number of tuples allowed in the table C7UPTMR is not changed by this activity.

47.5.2.1.4 Fields/OIDs

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CRG	new	no	{5 TO 2400}	Charge timer in 100 miliseconds.

47.5.2.1.5 Datafill example

The following example shows sample datafill for table C7UPTMR.

Figure 1 Sample C7UPTMR datafill

```
TABLE: C7UPTMR

TMRKEY C7UPDIR TMRS OPTIONS
-------------------------
OGN7 OG Q767 15 180 326 60 90 20 180 10 60 10 60 1000 10 120
40 10 (CRG 400) $
ICN7 IC Q767 15 180 326 60 90 15 5 15 10 60 10 60 10 60 10 60
60 10 60 10120 240 10 20 4 $
```

In this datafill example CRG timer is datafilled as 400 (40 seconds) in C7UPTMR for the tuple OGN7. That "OGN7" is datafilled in TMRNAME field of TRKSGRP table. So the trunk subgroups whose tmrname is OGN7 has a charge timer with the value 40 seconds.

47.5.2.1.6 Table release history update
None

47.5.2.1.7 Supplementary information
None

47.5.2.1.8 Translation verification other tools
None

47.5.2.2 Table ISUPSVC
ISUP Services

47.5.2.2.1 Functional description
This table holds entries for every service that is intended to be switched on or off by datafill. At present it allows entries for INR/INF and IDR/IRS applications.

47.5.2.2.2 Usage sequence and implications (CM Only)
Current datafill order unchanged.

47.5.2.2.3 Size
The minimum and maximum number of tuples allowed in the table C7UPTMR is not changed by this activity.

47.5.2.2.4 Fields/OIDs
Current fields are not changed.

47.5.2.2.5 Datafill example
The following datafill shows default datafill for Moroccan ISUP V2 in table ISUPSVC.

Figure 2 Default Tuple in table ISUPSVC

```
>table isupsvc
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: ISUPSVC
>lis all
TOP
             KEY                                                    SERVICE
-------------------------------------------------------------------------
 MOROCCAN_EIV2   (INR_INF GENERATION_AND_RECEPTION (CGN_REQUESTED)
                   (CPC_REQUESTED) $)$
BOTTOM
>
```

47.5.2.2.6 Table release history update
None

47.5.2.2.7 Supplementary information
None

47.5.2.2.8 Translation verification other tools
None

47.5.2.3 xxHEAD Tables

- PXHEAD - Prefix Digits
- OFCHEAD - Office Code Digits
- CTHEAD - Country Code Digits
- ACHEAD - Access Code Digits
- FAHEAD - Foreign Area Digits
- AMHEAD - Ambiguous Codes
- FTHEAD - Feature

47.5.2.3.1 Functional description
The function of head tables are unchanged.

47.5.2.3.2 Usage sequence and implications (CM Only)
Current datafill order unchanged.

47.5.2.3.3 Size

Table 3 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
xxHEAD (PXHEAD, OFCHEAD, CTHEAD, ACHEAD, FAHEAD, AMHEAD, FTHEAD)	Same	Same	Current limits are unchanged.

47.5.2.3.4 Fields/OIDs

The following table lists fields for HEAD tables.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DFOP	changed	OSEL	RTE (BCKWMTR) CONT (BCKWMTR)	BCKWMTR option is added to the OSEL(option selector) field of HEAD translation tables.

47.5.2.3.5 Datafill example

The following example shows sample datafill for table PXHEAD (Usage in other head tables is the same).

Figure 3 Sample Datafill in Table PXHEAD

```
TABLE: PXHEAD
>
XLANAME
                                                                DFLT
                                                                DFOP
  CON  MAXIDX
-----------------------------------------------------------------
  NETXLA
                                                              SDFLT
DFOP (BCKWMTR) $
NOCON       F
```

47.5.2.3.6 Table release history update

A new translation option, BCKWMTR, is added to be datafilled in OSEL field of head tables.

47.5.2.3.7 Supplementary information

NONE.

47.5.2.3.8 Translation verification other tools

The following example shows the output from traver when it is used to verify BCKWMTR option in table PXHEAD.

Figure 4 Traver Example

```
>traver 1 7835479 7835489 b
TABLE IBNLINES
HOST 02 0 00 09 0 DT STN IBN 7835479 CUST783A 0 0 102 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP REALKC
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 0 0 0 $ ( CBQ 0 0 Y 1) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME NETXLA1
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA1
   (NET N Y 0 N NDGT N Y GEN (LATTR 1 102_NPRT_1 NLCA_NILLA_1)
$ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA SDFLT DFOP BCKWMTR $ NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
7835489
```

Figure 5 Traver Example (Cont)

```
TABLE PXCODE
NETXLA 783 783 CONT ( PF 3) ( MM 7 7) ( CLASS LCL) ( XLT OFC
OFC783)$
TABLE OFCHEAD
OFC783 DFLT TRMT ( OFC VACT)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
5489
TABLE OFCCODE
OFC783 5 5 RTE ( DEST 1)$
TABLE: OFCRTE
KEY:   OFC783    1
 . T OFRT 783
 .  . TABLE OFRT
 .  .  783 DN 102 783 4
 .  .  . TABLE TOFCNAME
 .  .  . 102 783 $
 .  .  . TABLE DNINV
 .  .  . 102 783 5489 L HOST 02 0 10 09
TABLE DNFEAT
TUPLE NOT FOUND
 .  .  . TABLE DNATTRS
 .  .  . TUPLE NOT FOUND
 .  .  . TABLE DNGRPS
 .  .  . TUPLE NOT FOUND
 .  . EXIT TABLE OFRT
EXIT TABLE OFCRTE
TABLE TRIGGRP
REALKC INFOANAL
 . GENTRIG ( CDPN REALKC)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
INAP Route Select Failure TDP:  no subscribed trigger.
INAP Termination Attempt TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 LINE                  1027835489                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 MESAJ2
2 OFL
3 LKOUT

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

47.5.2.4 xxCODE Tables

- PXCODE - Prefix Digits
- OFCCODE - Office Code Digits
- CTCODE - Country Code Digits
- ACCODE - Access Code Digits

- FACODE - Foreign Area Digits
- AMCODE - Ambiguous Codes
- FTCODE - Feature

47.5.2.4.1 Functional description

The function of code tables are unchanged.

47.5.2.4.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

47.5.2.4.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
xxCODE (PXCODE, OFCCODE, CTCODE, ACCODE, FACODE, AMCODE, FTCODE)	Same	Same	Current limits are unchanged.

47.5.2.4.4 Fields/OIDs

The following table lists fields of HEAD tables.

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XLADATA	changed	OSEL	RTE (BCKWMTR) CONT (BCKWMTR)	BCKWMTR option is added to the OSEL(option selector) field of CODE translation tables.

47.5.2.4.5 Datafill example

The following example shows sample datafill for table PXCODE (Usage in other code tables is the same).

Figure 6 Sample Datafill in Table PXHEAD

```
TABLE: PXCODE
>
>lis
 XLANAME        FROMD           TOD
                                                              XLADATA
------------------------------------------------------------------------
  NETXLA          783           783
CONT (PF 3) (MM 7 7) (CLASS LCL) (XLT OFC OFC783) (BCKWMTR) $
>
```

47.5.2.4.6 Table release history update

A new translation option, BCKWMTR, is added to be datafilled in OSEL field of code tables.

47.5.2.4.7 Supplementary information

NONE.

47.5.2.4.8 Translation verification other tools

The following example shows the output from traver when it is used to verify BCKWMTR option in table PXCODE.

Figure 7 Traver Example

```
>traver l 7835479 7835489 b
TABLE IBNLINES
HOST 02 0 00 09 0 DT STN IBN 7835479 CUST783A 0 0 102 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP REALKC
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 0 0 0 $ ( CBQ 0 0 Y 1) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME NETXLA1
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA1
   (NET N Y 0 N NDGT N Y GEN (LATTR 1 102_NPRT_1 NLCA_NILLA_1)
$ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1
NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
7835489
```

Figure 8 Traver Example (Cont)

```
TABLE PXCODE
NETXLA 783 783 CONT ( PF 3) ( MM 7 7) ( CLASS LCL) ( XLT OFC
OFC783) (BCKWMTR) $
TABLE OFCHEAD
OFC783 DFLT TRMT ( OFC VACT)$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
5489
TABLE OFCCODE
OFC783 5 5 RTE ( DEST 1)$
TABLE: OFCRTE
KEY:   OFC783    1
 . T OFRT 783
 .  . TABLE OFRT
 .  .  783 DN 102 783 4
 .  .  . TABLE TOFCNAME
 .  .  . 102 783 $
 .  .  . TABLE DNINV
 .  .  . 102 783 5489 L HOST 02 0 10 09
TABLE DNFEAT
TUPLE NOT FOUND
 .  .  . TABLE DNATTRS
 .  .  . TUPLE NOT FOUND
 .  .  . TABLE DNGRPS
 .  .  . TUPLE NOT FOUND
 .  . EXIT TABLE OFRT
EXIT TABLE OFCRTE
TABLE TRIGGRP
REALKC INFOANAL
 . GENTRIG ( CDPN REALKC)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP:  trigger criteria not met.
INAP Route Select Failure TDP:  no subscribed trigger.
INAP Termination Attempt TDP:  no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 LINE                  1027835489                    ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 MESAJ2
2 OFL
3 LKOUT

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

47.6 Service Orders (SO) (CM & SESM)

N/A

47.7 Software optionality control (SOC)

N/A

47.8 Element Management

N/A

47.9 Command interface changes

N/A

47.10 Security

N/A

47.11 Configuration Walkthrough

Not impacted by this activity

48: Configuration (CN): A00004743

48.1 Hardware and Software Requirements

N/A

48.2 Initial Configuration

N/A

48.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

48.4 Upgrade Impact

N/A

48.5 Data schema (DS) (CM, MIBS, RDB)

48.5.1 New/modified tables, MIBs, or Database Schema

Table 1 Modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/ UNCHANGED)
Subtable CGPNDATA of table CGPNSCRN	Changed	Unchanged
Subtable CDPNDATA of table CDPNSCRN	Changed	Unchanged

48.5.2 Table/MIB/Remote Database Schema information

48.5.2.1 Name: Subtable CGPNDATA of table CGPNSCRN

48.5.2.1.1 Functional description

Please refer to Functional Description section of this DDOC.

48.5.2.1.2 Usage sequence and implications (CM Only)

Unchanged.

48.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples
Subtable CGPNDATA of table CGPNSCRN	Unchanged	Unchanged

48.5.2.1.4 Fields/OIDs

The following table lists changed fields for table Subtable CGPNDATA of table CGPNSCRN.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CGPNOPT	Changed	Yes	{CONTINUE, **BILLCLI}**	Add option BILLCLI in CGPNOPT list

BILLCLI is type {ORIG, MODIF}.

48.5.2.1.5 Datafill example

TABLE: CGPNSCRN CLISCRN: CGPNDATA

FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

106602 106602 RETURN (DIGMAN CGPN 2) $ (**BILLCLI ORIG**) $

48.5.2.1.6 Table release history update

Entry BILLCLI is added to field CDGPNSCRN_OPTIONS in subtable CGPNDATA of table CGPNSCRN.

48.5.2.1.7 Supplementary information

N/A

48.5.2.1.8 Translation verification other tools

N/A

48.5.2.2 Name: Subtable CDPNDATA of table CDPNSCRN

48.5.2.2.1 Functional description

Please refer to section optfn (Functional Description section) of this DDOC.

48.5.2.2.2 Usage sequence and implications (CM Only)
Unchanged.

48.5.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples
Subtable CDPNDATA of table CDPNSCRN	Unchanged	Unchanged

48.5.2.2.4 Fields/OIDs
The following table lists changed fields for table Subtable CDPNDATA of table CDPNSCRN.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CDPNOPT	Changed	Yes	{CONTINUE, **BILLCLI}**	Add option BILLCLI in CDPNOPT list

BILLCLI is type {ORIG, MODIF}.

48.5.2.2.5 Datafill example

TABLE: CDPNSCRN CLISCRN: CDPNDATA

FROMDIGS TODIGS CDPNINDX CCOPTION CDPNOPT

106602 106602 RETURN (DIGMAN CGPN 2) $ (**BILLCLI ORIG**) $

48.5.2.2.6 Table release history update
Entry BILLCLI is added to field CDGPNSCRN_OPTIONS in subtable CDPNDATA of table CDPNSCRN.

48.5.2.2.7 Supplementary information
N/A

48.5.2.2.8 Translation verification other tools
N/A

48.6 Service Orders (SO) (CM & SESM)
N/A

48.7 Software optionality control (SOC)

N/A

48.8 Element Management

N/A

48.9 Command interface changes

N/A

48.10 Security

N/A

48.11 Configuration Walkthrough

N/A

49: Configuration (CN): A00004750

49.1 Hardware and Software Requirements

DMS office with DTCO2.

49.2 Initial Configuration

49.3 Office/Subnet parameters (OP/SP) (CM & SESM)

49.4 Upgrade Impact

49.5 Data schema (DS) (CM, MIBS, RDB)

49.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	CHANGED	UNCHANGED

49.5.2 Table/MIB/Remote Database Schema information

49.5.2.1 Name: <LTCINV>

<LTC Inventory Table>

49.5.2.1.1 Functional description

49.5.2.1.2 Usage sequence and implications (CM Only)

This new optional attribute can only be added when:

1. TYPE_OF_NETWORK in OFCENG is NORTH_AMERICA
2. PM is CPM based DTCO2

49.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	0	4096	Memory is automatically allocated.

49.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <LTCINV>.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LTCINV	CHANGED	OPT_ATTR	EBI	When added, EBI support feature is downloaded to DTCO2.

49.5.2.1.5 Datafill example

The following example shows sample datafill for table <LTCINV>.

PDTC 0 LTEI 7 9 9 C 4 MX85AA QCI17AY1(ABTRK UKPDTC) (PRAB DTCEX)$ (0 32 18 0) (0 32 18 1) (0 32 18 2) (0 32 18 3) (0 32 18 4) (0 32 18 5)(0 32 18 6) (0 32 18 7) (0 32 18 8) (0 32 18 9) (0 32 18 10) (0 32 18 11)(0 32 18 12) (0 32 18 13) (0 32 18 14) (0 32 18 15) $(UTR6) (MSGMX76 HOST)$TURKR1R2 SX05AA $ SX05AA $0SXFWAJ02(CCS7) (FSTR2) (EBI)$6X40FB N

49.5.2.1.6 Table release history update

Optional Attribute EBI is added to OPT_ATTR field of LTCINV for DTCO2s.

49.5.2.1.7 Supplementary information

None

49.6 Service Orders (SO) (CM & SESM)

49.7 Software optionality control (SOC)

49.8 Element Management

49.9 Command interface changes

49.10 Security

49.11 Configuration Walkthrough

50: Configuration (CN): A00005164

50.1 Hardware and Software Requirements

N/A.

50.2 Initial Configuration

N/A.

50.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

50.4 Upgrade Impact

50.4.1 Dump and Restore

None.

50.4.2 Element Management Upgrade

None.

50.5 Data schema (DS) (CM, MIBS, RDB)

50.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
C7UPTMR	CHANGED	UNCHANGED

50.5.2 Table/MIB/Remote Database Schema information

50.5.2.1 Name: C7UPTMR

CCS7 Signalling ISUP Timers Table

50.5.2.1.1 Functional description

N/A.

50.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

50.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
C7UPTMR	0	31	The maximum number of tuples that can be datafilled is 31 with one tuple assigned the value NIL.

50.5.2.1.4 Fields/OIDs

The ranges of timers T5, T13, T15, T17, T19, T21, and T23 which are datafillable through C7UPTMR table were enlarged to 15 minutes by the activity ACT.A00000937 in MMP19 (ISN06) time frame.

Since enlarged timer ranges were supported only on PDTC's equipped with SX05, the following warning was displayed by ACT.A00000937 while datafilling values greater than 320 for NQ764T5 and NQ764T17 fields within BW, IC and OG refinements in C7UPTMR table.

"T5 and T17 timer values greater than 320 are affective only at PDTC's when both units are equipped with SX05."

This activity enhances GWC implementation to support enlarged CCITT timer ranges, therefore, the warning message is modified as follows:

"T5 and T17 timer values greater than 320 are affective only for the following peripherals:

- PDTC (when both units are equipped with SX05)

- GWC"

50.5.2.1.5 Datafill example

50.5.2.1.6 Table release history update

ACT.A00005164 enhanced GWC implementation to support enlarged CCITT timer ranges. The warning message which is displayed while datafilling NQ764T5 and NQ764T17 timers is modified to indicate that the enlarged timer ranges are supported also on GWC's.

50.5.2.1.7 Supplementary information

None.

50.5.2.1.8 Translation verification other tools

C7UPTMR does not use translation verification tools.

50.6 Service Orders (SO) (CM & SESM)

N/A.

50.7 Software optionality control (SOC)

N/A.

50.8 Element Management

N/A.

50.9 Command interface changes

N/A.

50.10 Security

N/A.

50.11 Configuration Walkthrough

N/A.

51: Configuration (CN): A00005802

51.1 Hardware and Software Requirements

None.

51.2 Initial Configuration

Not Applicable

51.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

51.4 Upgrade Impact

51.4.1 Dump and Restore

The feature introduces two new fields in form of a vector in table MNNODE. During the Restore, the type reformat proc for MNNODE will fill this vector set with **$** to indicate current system behavior on the SPM. The current system behavior is MuLaw for OC3-SPMs and Alaw for STM-SPMs.

For upgrades to later releases, the existing companding law and bit inversion option if datafilled in table MNNODE will be retained.

51.4.2 Element Management Upgrade

None

51.5 Data schema (DS) (CM, MIBS, RDB)

51.5.1 Modified tables

table MNNODE.

table MNCKTPAK

table OFCENG

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	CHANGED. Two new fields **complaw** and **bitinv** are added for DMSCP class SPM	UNCHANGED

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNCKTPAK	UNCHANGED	UNCHANGED, Supplementary information added
OFCENG	UNCHANGED	UNCHANGED, Supplementary information added.

51.5.2 Table Schema information

51.5.2.1 Name:

51.5.2.1.1 Managed Network Node table**Functional description**

Table MNNODE stores SPM node specific information. This information includes:

- Class/Variant of SPM.
- Clock reference details of the SPM.
- Resource information that a particular SPM can provide.
- Alarm information for different failures for the SPM.
- EXEC information for CallP.
- Capacity index for the DMSCP SPM

This feature adds two new fields **complaw** and **bitinv** of enum type to DMCSP class of SPM as a vector **compopt**. The craft shall be able to change the p-side companding law and bit inversion option for a OC3-SPM of DMSCP class.

51.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

51.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNNODE	0	86	The memory is allocated dynamically upon the addition of the tuple from the OAMDB pool.

Fields

Table 3 Table field descriptions for MNNODE

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	NODETYPE NODEID	ENUM {0 to 256} BYTE {0 to 85}	This represents the Node type (e.g. SPM). This represents a unique SPM number.
ALIAS	Unchanged		Alphanumeric 1 to 12 characters	This field represents a unique Alias name for the SPM.
NODEINFO	Unchanged	CLASS T_SPMNDV_DMSCP_DATA	{0 to 10}	Represents class of SPM (like SMG4, DMSCP etc.) (refinement for DMSCP with fields as below in Subfield)
	Unchanged	FLOOR	{0 to 99}	This field gives the floor position details.
	Unchanged	CLKMODE	{SYNC}	This represents CLOCK synchronization mode for the MG4K.
	Unchanged	CLKREF	{0 to 5} {*Internal*, *External*, *Line*, *Loop*}	This represents the source and reference for the clock sync. A newly added SPM should be datafilled as LINE. *Internal*:SYNC to MS *External*:SYNC to SRM *Line*:SYNC to OC3 RM. *Loop*:SYNC to active OC3 RM.

Table 3 Table field descriptions for MNNODE

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	Unchanged	LEDTIMER	{0 to 1440}	This type designates time in minutes. If no critical fault has been detected on an SPM for the specified length of time, then LEDs on the SPM will be turned off to extend their life. Value of 0 means that the LEDs will never be turned off.
	Unchanged	RSRUTLIM	1. (table {0 to 27} of *{0 to 27}, {10 to 100}})* 2. 0 to 6	This field represents the resources that shall be provided by the SPM. This also gives the threshold limit for each of the resources.
	Unchanged	ALRMCTRL	1. (table {0 to 21} of *{o to 20}, {{0 to 4}, 0 to 1}))* *2. (0 to 21)*	This field represents the Alarm that should be triggered when the SPM goes to a particular state or any failure occurs. This also gives the severity of the failure and the information about reporting on to the MAP.
	Unchanged	EXECTAB	1. (table {7} of *{o to 63}, {0 to 119})* *2. (0 to 8)*	This field represents the EXEC lineup information which is useful for call processing.
	Unchanged	CAPINDX	{STANDARD,ENHANCED,PREMIUM}	This field represents the SPM Call Processing Capacity type

Table 3 Table field descriptions for MNNODE

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
COMPOPT	**New**		see subfields	COMPANDING OPTION. This field consists of a vector of up to 1 entry in subfields complaw and bitinv. Enter **$** to select current system behavior (MuLaw for OC3-SPMs and ALaw for STM-SPMs). This vector is supported only for OC3-SPM.
	New	**complaw**	ALaw, MuLaw	COMPANDING LAW. This contains the p-side companding law for SPM.
	New	**bitinv**	NBI, OBI, EBI, ABI	BIT INVERSION OPTION. This field contains the bit inversion option for the SPM. Currently only EBI and ABI are supported.

51.5.2.1.4 Datafill example

Figure 1, "Datafill example" shows sample datafill for table MNNODE.

Figure 1 Datafill example

```
Datafill with compopt datafilled -

  NODEKEYALIASNODEINFO
  ----------------------
  SPM 1 SPM_1 DMSCP 1 SYNC LOOP 45 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMREXBYP MN RPT) $ (ABTRK SPMEX)
(AB250 SPM250) (PRAB SPMEX) (PRAB500 SPM250) $ STANDARD (ALAW EBI) $




Datafill where compopt is not required -

  NODEKEYALIASNODEINFO
  ----------------------
  SPM 1 SPM_1 DMSCP 1 SYNC LOOP 45 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMREXBYP MN RPT) $ (ABTRK SPMEX)
(AB250 SPM250) (PRAB SPMEX) (PRAB500 SPM250) $ STANDARD $
```

51.5.2.1.5 Table release history update

SN07:

New vector **compopt** is added to table MNNODE for DMSCP variant of the SPM. This vector consists of two fields - **complaw,** which contains the p-side companding information of that SPM whose values are {Alaw, MuLaw}, and **bitinv,** which contains the bit inversion option of the SPM whose values are {NBI, OBI, EBI, ABI}. The default value of the vector is **$** which indicates that SPM confirms to current system behavior of OC3-SPM having MuLaw and STM-SPM having ALaw.

51.5.2.1.6 Supplementary information

The value for **compopt** can be changed only when the SPM node is in either MANB or OFFL state. Otherwise the following error condition will occur -

ERROR: Both CEMs must be in MANB or OFFL state with no maintenance for COMPOPT change.

By default compopt field will take $ as value over upgrade. If craft datafills value other than $ then following warning will be displayed -

Warning: Datafilling companding law and bit inversion is recommended for non-standard configurations. Use of incorrect values will severely affect voice quality of the SPM.

A warning message will be displayed when **compopt** fields are changed -

Warning: Changing companding law or bit inversion option may severely affect voice quality of the SPM and must be done with care. Perform the following steps to activate the changes in SPM X:

1. BSY the CEMs if not in MANB state.

2. Issue RESETMOD command on both the CEMs.

3. RTS the CEMs.

While changing companding law to MULAW from either $ or ALAW, check is done for STM RM datafill. If STM datafill is found then COMPOPT change will not be allowed. Following error message is displayed.

ERROR: STM RM is datafilled in table MNCKTPAK. MULAW is not appropriate law for the STM-SPM.

51.5.2.1.7 Translation verification other tools

None.

51.5.3 Table Schema information

51.5.3.1 Name:

Managed Network Circuit Pack

51.5.3.2 Supplementary information

Table MNCKTPAK is not changed and no new fields are added to this table by this feature. Only new warning messages are introduced as follows -

While adding an OC3-SPM in table MNCKTPAK, if the p-side companding law in table MNNODE is A-law the following message is displayed -

WARNING: This OC3-SPM has a non-standard companding law datafilled in MNNODE. If this is not desired, please change companding law in MNNODE to the appropriate value before proceeding. If this is desired, please continue.

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT

Actions: If ‘Y’ is entered, tuple addition of OC3 in table MNCKTPAK will be allowed assuming that OC3-SPM with A-Law is the desired configuration.

If ‘N’ is entered, tuple addition will be aborted, the craftsperson has to manually change companding law for that SPM in table MNNODE before proceeding.

While adding a STM-SPM in table MNCKTPAK, if the p-side companding law in table MNNODE is MuLaw, the following error message is displayed -

ERROR: STM-SPM with MuLaw companding is not a supported configuration. Please change companding law in MNNODE before proceeding.

Actions: Tuple addition of STM in table MNCKTPAK is aborted. The craftsperson had to manually change companding law of that SPM in table MNNODE before proceeding.

51.5.4 Table Schema information

51.5.4.1 Name:

OFCENG - Office Engineering Parameter table

51.5.4.2 Supplementary information

Table OFCENG is not changed and no new fields are added to this table by this feature. This section mentions the limitation while changing TYPE_OF_NETWORK parameter.

If TYPE_OF_NETWORK field is changed, all DMSCP SPM tuples in table MNNODE must be verified that the **compopt** field is in the desired configuration for the new TYPE_OF_NETWORK. If they are found otherwise, the craftsperson must manually change **compopt** field for those SPMs to the desired configuration.

51.6 Service Orders (SO) (CM & SESM)

Not Applicable

51.7 Software optionality control (SOC)

Not Applicable

51.8 Element Management

Not Applicable

51.9 Command interface changes

Not Applicable

51.10 Security

Not Applicable

51.11 Configuration Walkthrough

Not Applicable

Performance Management (PF)

Introduction

This chapter describes impacts to performance management, such as operational measurements and performance measurements, for the features planned for this release. Only those features with performance-management impacts are listed.

Featid	Title
A00001914.AA11	CEPT International Line Restriction Enhancements
A00001930.AA14	Last and Total Call Meter Inquiry Services
A00002904.AA12	CTI Toggle

1: Performance (PF): A00001914

1.1 Performance management strategy

N/A

1.2 Performance management tools and utilities

1.3 Performance Measurements (PM), Operational Measurements (OM), and stats

The ILR OM are adopted to support the flexible definition of the barring programs in table ILRCLASS. The ILR OM provides per OM group the number of activations, deactivations, usages and unsuccessful deactivations:

Figure 1 Flexible ILR OM group

```
TACLASS:   ACTIVE
START:2003/05/10 18: 30:00 SAT; STOP: 2003/05/10 18:47:12 SAT;
SLOWSAMPLES:      11 ; FASTSAMPLES:       103 ;
    KEY (RCODE)
     INFO (OMILRINFO)
       ACT              DACT    USGE    UDACT

  02 DIDD
                       10 1 25 5
```

The ILR1 OM group is deleted, because all information is stored in the flexible ILR OM group.

The example above shows an OMSHOW output for the new ILR OM group. It shows for the OM group with R-Code 2 called DIDD 10 activations, 1 deactivation, 25 times a call was barred due to this program and 5 times the deactivation failed. These are stored under ILRCLASS OM group.

Two new OM registers are defined for successful deactivation and unsuccessful temporary deactivation under ILR OM group which includes ILRCERR, ILRUINT, ILRINTG OM registers. These are:

- TEMPDAC
- TEMPUDAC

Figure 2 OMSHOW output for ILR OM group

```
>omshow ilr active
ILR
CLASS:   ACTIVE
START:2003/09/09 16:30:00 TUE; STOP: 2003/09/09 16:40:37 TUE;
SLOWSAMPLES:       7 ; FASTSAMPLES:       64 ;
          ILRCERR   ILRUINT   ILRINTG   TEMPDAC
       TEMPUDAC

        0          0          0          0          0
                   0
```

Figure 3 OMSHOW output for ILRCLASS OM group

```
>omshow ilrclass active
ILRCLASS
CLASS:   ACTIVE
START:2003/09/09 16:30:00 TUE; STOP: 2003/09/09 16:59:53 TUE;
SLOWSAMPLES:       18 ; FASTSAMPLES:       179 ;
     KEY (ILR_CLASS)
          ACT     DEACT     USAGE     UNDACT

   0 NIL
          0         0         0         0

   1 DABE
          0         0         0         0

   2 DNI
          0         0         0         0

   3 DAI
          0         0         0         0

   4 DIDD
          0         0         0         0

   5 DNID
          0         0         0         0

   6 DSSV
          0         0         0         0

   7 DABLE
          0         0         0         0

   8 DANID
          0         0         0         0

   9 DNIC
          0         0         0         0

  10 DAIC
          0         0         0         0
```

1.3.1 PM, OM, and stats format

1.3.2 OM Group template (applies only to DMS)

1.3.2.1 OM description

OM group ILRCLASS provides information about the usage and performance of the International Line Restriction feature (ILR). This OM group stores the counts of usage, activation, successful and unsuccessful attempts of deactivation of ILR feature for related restriction classes.

OM group ILR provides information about successful and unsuccessful temporary deactivation, interrogation of ILR feature and also customer error.

1.3.2.2 Release history update

OM group ILRCLASS has a flexible body and includes registers according to the ILRCLASSes datafilled in table ILRCLASS.

OM group ILR includes registers of the successful and unsuccessful temporary deactivation, interrogation of ILR feature and also customer error.

TEMPDAC: Number of successful attempts fo temporary deactivations of ILR feature.

TEMPUDAC: Number of unsuccessful attempts for temporary deactivations of ILR feature.

1.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 4 OM Group ILR Display

```
>omformat ilr
ILR
        ILRCERR    ILRUINT    ILRINTG    TEMPDAC
      TEMPUDAC
```

Figure 5 OM Group ILRCLASS Display

```
>omformat ilrclass
ILRCLASS
    KEY (ILR_CLASS)
              ACT        DEACT      USAGE          UNDACT
```

1.3.2.4 Group structure

OM groups ILR and ILRCLASS provide ONE tuple per office.

Key field: None

Info field: None

1.3.2.5 Associated OM groups

None

1.3.2.6 Associated functional groups

None

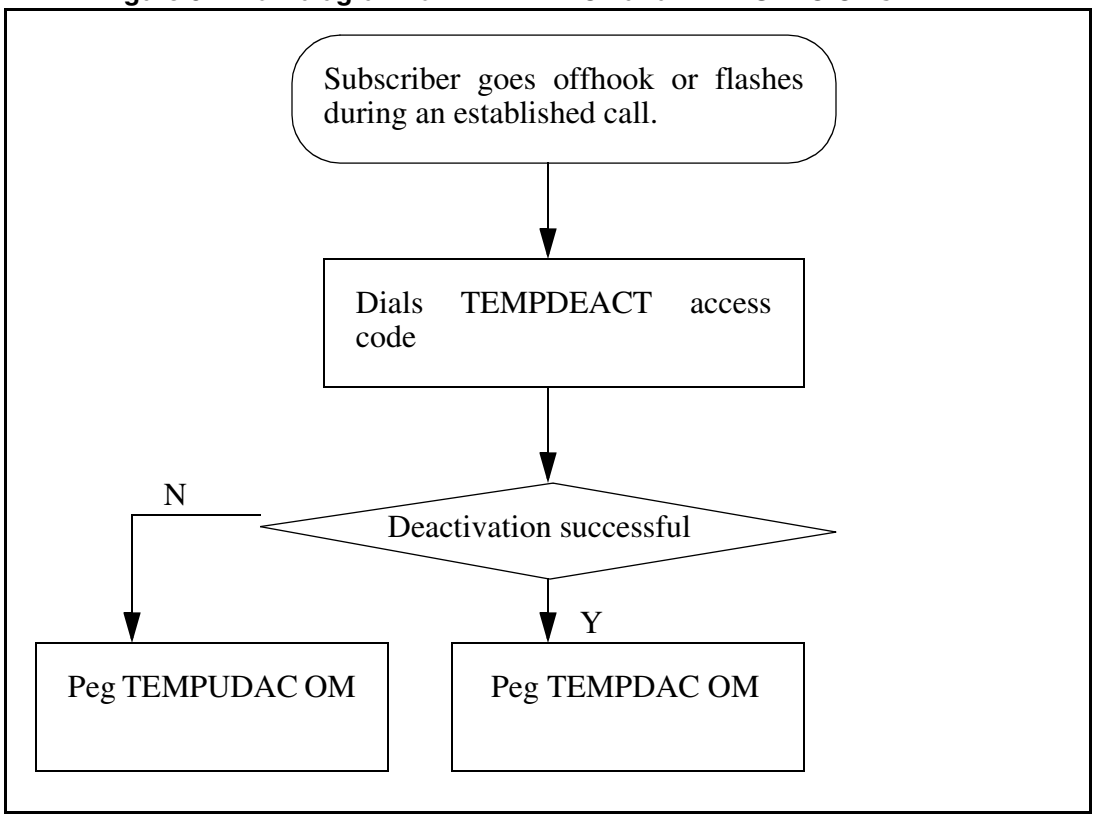
1.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code
International Line Restriction	ISRV0008

1.3.2.8 OM group registers logic flow chart

Figure 6 Flow diagram for TEMPDEACT and TEMPUDAC Oms



1.3.3 Register (applies only to DMS)

1.3.3.1 Register description

Register **TEMPDAC**

Temporary Deactivation of ILR feature.

TEMPDAC is a peg register. It counts the number of Temporary deactivations of ILR feature.

Register **TEMPUDAC**

Unsuccessful Attempts for Temporary Deactivation of ILR feature

TEMPUDAC is a peg register. It counts the number of unsuccessful attempts for temporary deactivations of ILR feature.

1.3.3.2 Register release history update

1.3.3.3 Associated Registers

Existing ILR OMs became more flexible in this activity.

ILR and ILRCLASS OM groups are defined. For detailed information, please refer to the above sections.

1.3.3.4 Associated registers

None

1.3.3.5 Associated logs

None

2: Performance (PF): A00001930

2.1 Performance management strategy

2.2 Performance management tools and utilities

2.3 Performance Measurements (PM), Operational Measurements (OM), and stats

2.3.1 PM, OM, and stats format

2.3.2 CMI OM GROUP

2.3.2.1 CMI OM description

CMI OM Group provides information about the successful and unsuccessful usage and performance of CMI features (SVBI0033 SOC must be ON). CMI OM group has four registers with names CMIATT, CMIUSG, CMIOVFL, and CMICERR. These OM registers are pegged by LCMI and TCMI features. CMI OM group is multi-tuple, which includes LCMI and TCMI tuples.

2.3.2.2 Release history update

The CMI OM group is being introduced by this feature, and implemented in ISN07.

2.3.2.3 Registers

OM group registers display on the MAP terminal as follows:

```
>omformat CMI
CMI
KEY (CMI_OPTION)

          CMIATT  CMIUSG  CMIOVFL CMICERR
```

2.3.2.4 Group structure

OM group provides one tuple for each CMI functionality.

Key field: CMI_OPTION {TCMI, LCMI}

Info field: None

```
>omshow CMI active
CMI

CLASS:   ACTIVE
START:2003/05/25 12:00:00 SUN; STOP: 2003/05/25 12:01:47 SUN;
SLOWSAMPLES:          2 ; FASTSAMPLES:          11 ;
         KEY (CMI_OPTION)

                 CMIATT CMIUSG   CMIOVFL          CMICERR
         TCMI    4       2       1                1
         LCMI    10      9       1                0
```

2.3.2.5 Associated OM groups

None

2.3.2.6 Associated functional groups

None

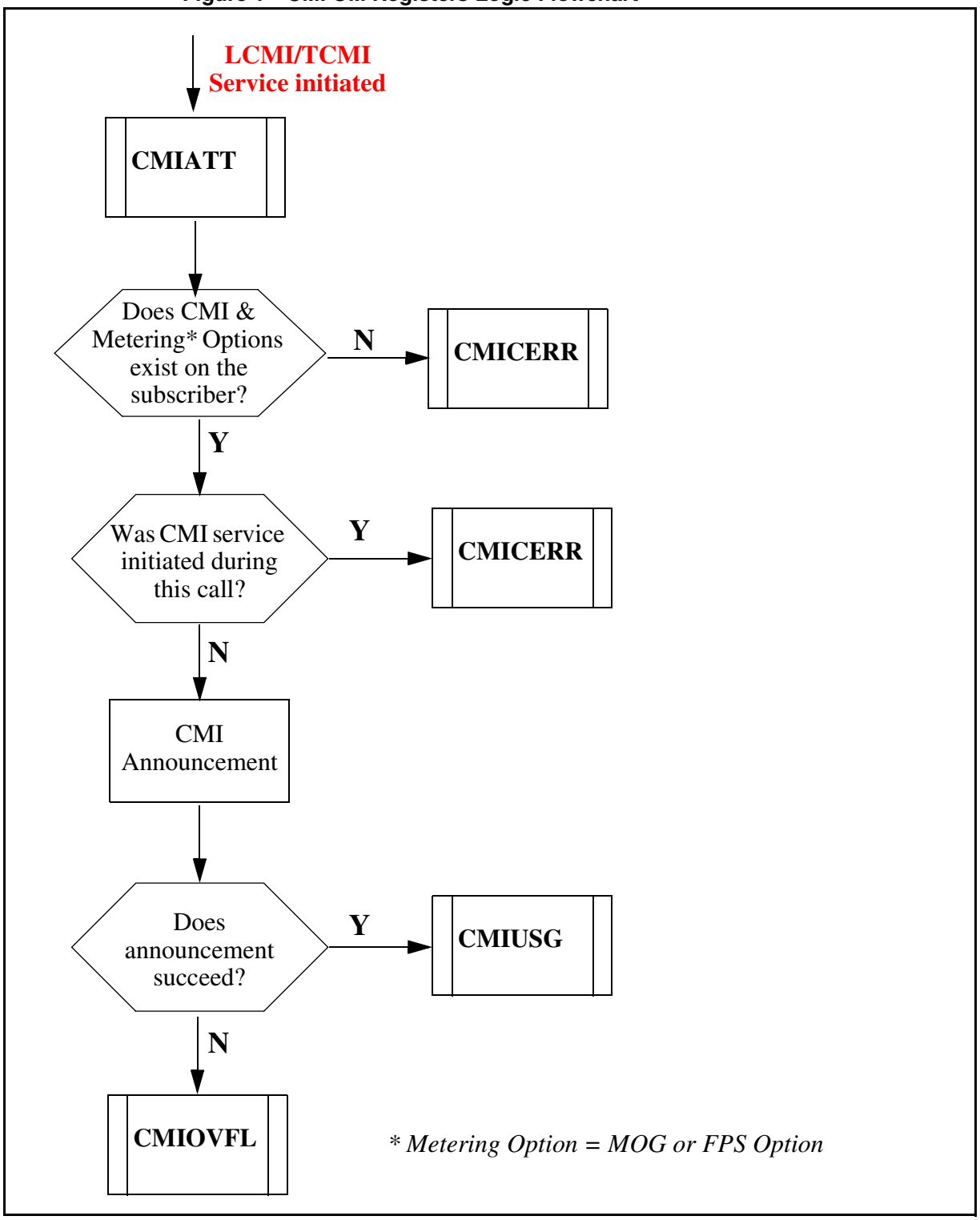
2.3.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code
Total Call Meter Inquiry	
Last Call Meter Inquiry	

2.3.2.8 OM group registers logic flow chart

Figure 1 CMI OM Registers Logic Flowchart



2.3.3 Register CMIATT

2.3.3.1 Register description

This register counts the number of attempts for TCMI/LCMI service to be invoked. Generally this register is incremented each time LCMI or TCMI service is initiated. This means, LCMI/TCMI service is successfully translated through translation table IBNXLA and successfully activated.

2.3.3.2 Register release history update

None

2.3.3.3 Associated registers

None

2.3.3.4 Associated logs

None

2.3.4 Register CMIUSG

2.3.4.1 Register description

This register counts the number of times LCMI/TCMI service is successfully completed. This register is incremented just after the announcement is successfully played

2.3.4.2 .Register release history update

None

2.3.4.3 Associated registers

None

2.3.4.4 Associated logs

None

2.3.5 Register CMIOVFL

2.3.5.1 Register description

This register counts the number of times LCMI/TCMI service can not be successfully completed due to insufficient system resources. It is incremented when the announcement can not be provided to the subscriber.

2.3.5.2 Register release history update

None

2.3.5.3 Associated registers

None

2.3.5.4 Associated logs

None

2.3.6 Register CMICERR

2.3.6.1 Register description

his register counts the number of times CMI service is not provided to the subscriber, due to illegal initiation of the service (i.e. initiation of the CMI service during active call) or subscriber is not allowed to use the service.

2.3.6.2 Register release history update

None

2.3.6.3 Associated registers

None

2.3.6.4 Associated logs

None

3: Performance (PF): A00002904

3.1 Performance management strategy

N/A

3.2 Performance management tools and utilities

N/A

3.3 Performance Measurements (PM), Operational Measurements (OM), and stats

This development is limited to CM. Therefore, only the OM is described here.

3.3.1 PM, OM, and stats format

Standard OM format is used

3.3.2 OM Group template (applies only to DMS)

3.3.2.1 OM description

SCAISRV4

Switch Computer Application Interface service 4

3.3.3 Release history update

OM group SCAISRV4 is being modified in CCM20. Two new registers namely TOGCLLRR and TOGCLLRE are being added to this OM group.

3.3.4 Registers

OM group SCAISRV4 registers display on the MAP terminal as follows:

Figure 1 OM Group SCAISRV4 Display

```
SCAISRV4

CLASS:   ACTIVE
START:1998/11/30 14:00:00 MON; STOP: 1998/11/30 15:45:48 MON;
SLOWSAMPLES:        6 ; FASTSAMPLES:        54 ;

     KEY (SCAI_GROUP)
       CHWRAPRR   CHWRAPRE   CHFRCERR   CHFRCERE
       REAGNPRR   REAGNPRE   CNTRLREL  NCTRLREL
     HELDU TOGCLLRR TOGCLLRE


          0   SCAI_GRP1
                1            3            0            2
                0            0            1            1
                2            1            2
```

3.3.5 Group structure

OM group SCAISRV4 provides tuples for each SCAIGRP

Key field: SCAI_GROUP

Info field: None

Number of tuples: One per SCAI group

The key field identifies the SCAI group name which is a unique character string with a maximum length of 16 characters. The SCAI group is defined in table SCAIGRP.

3.3.6 Associated OM groups

SCAISERV, SCAISRV2, SCAISRV3 are related.All these groups provide OM data on SCAI service usage.

3.3.7 Associated functional groups

None

3.3.8 Associated functionality codes

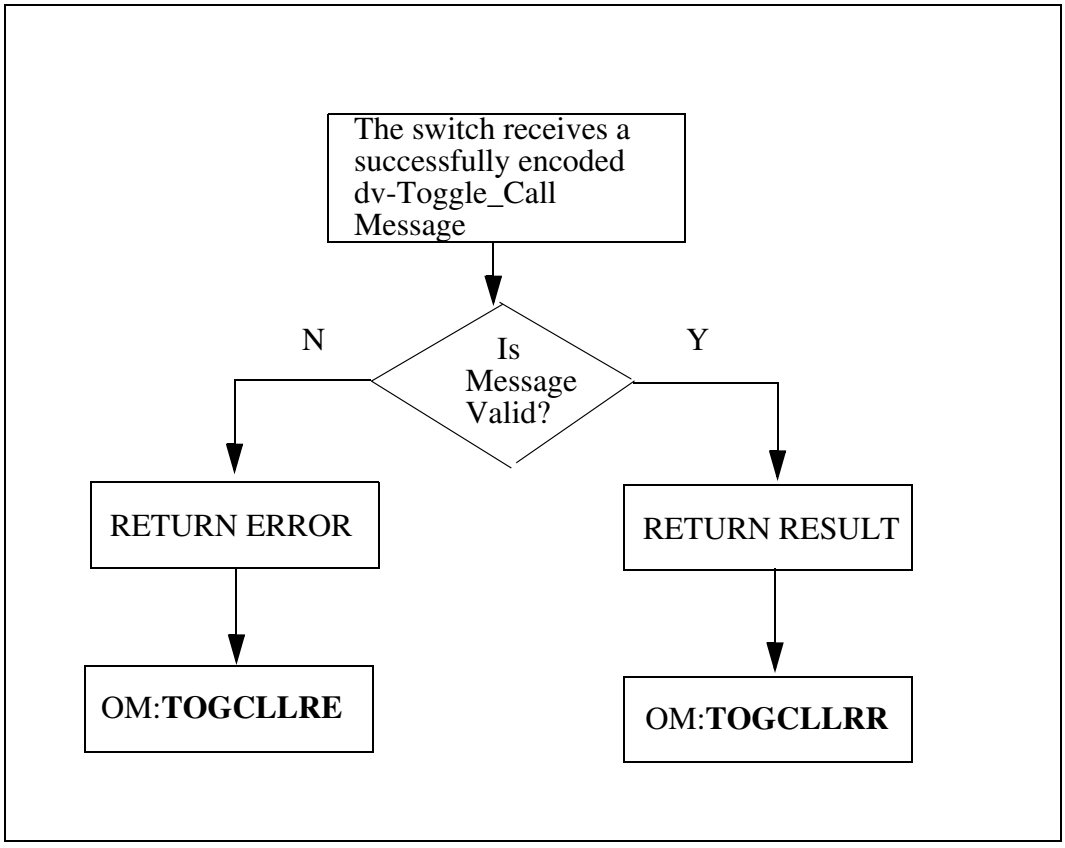
Table 1 Functionality codes associated with OM group <shortGRPNAME>

Functionality	Code

3.3.9 OM logic flow

Flow chart: OM group SCAISRV4 registers

Figure 2 Figure 2:OM group SCAISRV4 register TOGCLLRR, TOGGCLLRE



3.3.10 Register TOGCLLRR

3.3.10.1 Register description

Register: TOGCLLRR

Message: Toggle Call

Pegged when the switch returns a RETURN-RESULT to the host computer in response to a dv_Toggle_Call message.

3.3.10.2 Associated registers

None

3.3.10.3 Associated logs

None

3.3.11 Register TOGCLLRE

3.3.11.1 Register description

Register: TOGCLLRE

Message: Toggle Call

Pegged when the switch returns a RETURN-ERROR to the host computer in response to a dv_Toggle_Call message.

3.3.11.2 Associated registers

None

3.3.11.3 Associated logs

None

Accounting (ACC)

Introduction

This chapter describes new and changed features that are planned for this release.

Featid	Title
A00002053.AA14	AMA Records for Metered Features
A00002364.AA08	CLI/RDN/OCN capture in Billing Record (CDR) for ANSI ISUP and HK ISUP on DRU GSP20

1: Accounting (ACC): A00002053

1.1 Accounting strategy

This feature uses the existing AMA/Billing framework based on the Bellcore AMA Format. The existing structure code SCI_00514 (with call code CCI_006) and the existing module code MCI_612 (with context_id 80040) are used to generate the new AMA record FTR.

The FTR record is generated when a feature metering is done successfully due to usage of the feature actions such as assign, usage, deassign, activation, deactivation or interrogation etc...This record is generated for IBN lines if the SOC option RBIL0014 is ON and the all required datafills are done as given in the Section 2.2.4 of the FN document. The FTR record contains the following information:

- Record Code
- Calling number
- Date
- Time
- Feature code
- Action type
- Feature Metering Count

Additional to this record an AMA log is generated with the name AMAB156 which has the same information as FTR record. If the parameter LOGAMA is ON in table AMAOPTS, the AMAB156 log is printed whenever the FTR record is generated.

The generation of the FTR record for the metered actions of ICR feature option depends on the new office parameter FTR_RECORD_FOR_ICR_OPT in table OFCVAR.

1.2 CM billing changes

1.2.1 Structure codes

No new structure code is created by this feature.

1.2.2 Structure code nnn

Table 1 Structure code

Information	Field number
Structure code	nn
	nn

1.2.3 Module code

No new module code or context identifier is created by this feature.

1.2.4 Module code nnn

Table 2 Module code

Information	Field number	Number of characters
Module code	nn	nn
	nn	nn

1.2.5 Fields

In this feature, some fields of the existing structure code SCI_00514 and the existing module code MCI_612 (context_id 80040) are used for the new FTR AMA Record when the SOC option RBIL0014 is ON.

Calling number, Date and Time information for metered feature action are put in the SCI_00514 fields Originating Open Digits 1, Date and Connect Time respectively, as shown in below:

Calling Number -> ORIGINATING OPEN DIGITS 1

Date -> DATE

Time -> CONNECT TIME

ORIGINATING OPEN DIGITS 1 field in SCI_00514 contains 11 digits. But the Calling Number data of the IBN agent metered for feature actions has 10 digits. So, this data is put in this field as right-justified and the first digit filled by 0.

DATE field of SCI_00514 is filled by the Date data of the metered feature action as in the Table 3.

Table 3 Date field explanation in SCI_00514

BCD Char	Meaning
1	Last Digit of Year
2-3	Month
4-5	Day
8	Sign (hex C)

CONNECT TIME field of SCI_00514 is used to place the Time at which the feature action is metered, as in Table 4.

Table 4 Connect Time field explanation in SCI_00514

BCD Char	Meaning
1-2	Hours
3-4	Minutes
5-6	Seconds
7	Tenths of Seconds
8	Sign (hex C)

Note: Date and Time information are also displayed in the Generic Digits String 2 fields of the appended module code MCI_612 (80040). Please refer to Table 6.

In this feature, EXT TERM OPEN DIGITS 1 field of the SCI_00514 is filled by zeros for the Called DN.

Then the remaining information which are Record Code, Feature Code, Action Code and Feature Meter Count, are put in the Generic Digits String 1 fields of the MCI_612 (80040) as in the following Table 5. In this table, the usage changes are given in the bold format.

Table 5 Generic Digits String 1 usage for new FTR record

BCD Char	Content
1-2	Record Code **is filled as 03 for the new FTR record**.
3-4	Call Class **is not used and filled as 00 in the new FTR record.**
5-6	Call Info **is not used and filled as 00 in the new FTR record.**
7	Unused field (0).

BCD Char	Content
8-15	Pulse Count **is used to hold the following information:** **8-9 Feature Code** **10-11 Action Code** **12-13 Unused (00)** **14-15 Meter Count**
16	Sign (hex C)

The Record Code field contains 2 digits Record Code data which uniquely identifies the type of the record to distinguish it from the other record types generated when SOC option RBIL0014 is ON. It is set to '03' for the new FTR record since the existing record codes are '00' for Turkish CAMA, '01' for IAA and '02' for ICR.

The Call Class (2 digits, from 3 to 4) and Call Info (2 digits, from 5 to 6) fields are not used in the new FTR record. So, these are filled by zero. Also the seventh digit is already unused and 0.

The Pulse Count field has 8 digits from 8 to 15, and for FTR record it is filled by the Feature Code, Action Code and Feature Meter Count information in the following order:

Feature Code (2 digits) -> Pulse Count (the first 2 digits)

Action Code (2 digits) -> Pulse Count (3 and 4th digits)

Space, 00 -> Pulse Count (5 and 6th digits)

Feature Meter Count (2 digits) -> Pulse Count (7 and 8th digits)

In the fields of the Generic Digits String 2 of 80040, the Date and Time values have already existed and they are continued to display in this FTR record with the same format as before (additional to Date and Time information put in the SCI_00514 fields DATE and CONNECT TIME). The explanations for the existing fields of the Generic Digits String 2 are given in Table 6.

Table 6 Existing Generic Digits String 2 fields

BCD Char	Meaning
1-6	Date
7-13	Time
14-15	Unused
16	Sign (hex C)

The example views of this record can be given as in Figure 1 for ‘calldump’ command and Figure 2 for ‘calldump full’ command.

Figure 1 The example view of the FTR Record.

```
> calldump

*HEX ID:AA  STRUCTURE CODE:40514C  CALL CODE:006C  SENSOR TYPE:036C
 SENSOR ID:0000000C  REC OFFICE TYPE:036C  REC OFFICE ID:0000000C
 DATE:30326C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:0C
 SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C
 SIG DIGITS NEXT FIELD:010C  ORIG OPEN DIGITS 1: 01027835406C
 ORIG OPEN DIGITS 2:FFFFFFFFFF  ORIGINATING CHARGE INFO:FFFF
 DOMESTIC/INTL INDICATOR:9C  SIG DIGITS NEXT FIELD:000C
 EXT TERM OPEN DIGITS 1:000000000000000C
 EXT TERM OPEN DIGITS 2:FFFFFFFFFFFFFFFF  CONNECT TIME:0923355C
ELAPSED TIME:000000000C COMPLETION INDICATOR:001C MODULE CODE:612C
 GENERIC CONTEXT ID:8004000C  GENERIC DIGIT STRING ONE:030000021450002C
 GENERIC DIGIT STRING TWO: : 030326092335500C MODULE CODE:000C
```

Figure 2 The example view of the FTR Record.

```
> calldump full
*
HEX ID:                    AA
STRUCTURE CODE:                40514C
CALL CODE:                   006C      STATION PAID
SENSOR TYPE:                 036C      DMS 100F
SENSOR ID:                  0000000C
REC OFFICE TYPE:               036C      DMS 100F
REC OFFICE ID:               0000000C
DATE:                      30326C    MARCH 26, 2003
TIMING IND:
   TIMING GUARD FLAG             0        UNUSED
   SHORT CLD PARTY OFF-HOOK IND  0        UNUSED
   LONG DUR/SERV PTY CAPABILITY IND 0       UNUSED
   UNUSED                    0
   UNUSED                    0C
STUDY IND:
   STUDY TYPE A              0        UNUSED
   STUDY TYPE B              2        NETWORK COMPLETION
   STUDY TYPE C              0        UNUSED
   TEST CALL IND             0        UNUSED
   UNUSED                    0
   ORIG/TERM NANP NUM IND        0        UNUSED
   OPERATOR SERV IND           0C       UNUSED
CLD PTY OFF-HK:              0C       CLD OFF-HOOK DETECTED
SERVICE OBSERVED:              0C       NONE
OPER ACTION:                 0C       ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:             000C      OTHER
SIG DIGITS NEXT FIELD:         010C
ORIG OPEN DIGITS 1:          01027835406C
ORIG OPEN DIGITS 2:          FFFFFFFFFF
ORIGINATING CHARGE INFO:       FFFF
DOMESTIC/INTL INDICATOR:       9C       UNKNOWN
SIG DIGITS NEXT FIELD:         000C
EXT TERM OPEN DIGITS 1:        000000000000000C
EXT TERM OPEN DIGITS 2:        FFFFFFFFFFFFFFFF
CONNECT TIME:                0923355C   09:23:35.5
ELAPSED TIME:               000000000C 000000:00.0
COMPLETION INDICATOR:          001C      COMPLETED: ANSWERED
MODULE CODE:                 612C      GENERIC MOD: TWO DGT STR FMT
GENERIC CONTEXT ID:
   PARSE RULES               80040     ICAMA FIELDS
   SIGNIFICANT DIGITS          00C       NIL
GENERIC DIGIT STRING ONE:
   ICAMA-IAA DATA                  030000021450002C
GENERIC DIGIT STRING TWO:      030326092335500C
MODULE CODE:                 000C      FINAL MODULE
```

In these Figures, Generic Digits String 1 fields are interpreted as in below:

0300000**21**4500**02**C

03: Record Code is FTR (first 2 digits)

00000: Unused space (5 digits after record code)

21: Feature Code (2 digits as 8th and 9th)

45: Action Code (2 digits as 10th and 11th)

00: Two space between Action Code and Meter Count (12th and 13th digits)

02: Meter Count (last 2 digits)

Feature Meter Count information is displayed by 2 digits in the FTR record and AMAB156 log. The data shown in this field reflects the value datafilled in the CHARGE field of table MTRFEAT and the range for the charge value has been defined as 0 to 255 in this table. Although 3 digits data is datafilled in the charge field of MTRFEAT table, the last 2 digits will be displayed in the FTR record and AMAB156 log, as in MTR156 log.

AMAB156 log contains FTR record data (i.e, old MTR 156 data) and it is optionally generated depending on the existing AMA option LOGAMA in table AMAOPTS. If the LOGAMA option is ON , then the AMAB156 log is printed whenever the FTR record is generated. If the LOGAMA option is OFF, then the AMAB156 log is not printed although the FTR record is generated.

Record Code is ‘BE’ in AMAB156 in spite of ‘03’ in FTR Record. Because the Record Code values BB, B8, BD are currently used in the AMA logs of the ICR, ICAMA, IAA records.

Please refer to Figure 3 for the example view of AMAB156 log.

Figure 3 AMAB156 LOG Format Example

```
RSNW4E06BK     AMAB156 MAR26 09:23:36 7216 INFO AMA RECORD DATA
           RECORD CODE = BE
           CALLING NUMBER = 1027835406   FEATURE CODE = 21
           ACTION = 45                   COUNT = 02
           TIME = 0923355                DATE = 030326
```

1.3 Other changes

None.

2: Accounting (ACC): A00002364

2.1 Accounting strategy

None.

2.2 Accounting tools and utilities

None.

2.3 Accounting task flows

None.

2.4 CM billing changes

2.4.1 Structure codes

None.

2.4.2 Structure code nnn

None.

2.4.3 Module code

None.

2.4.4 Module code nnn

None.

2.4.5 Tables (fields)

None.

2.4.6 Field nnn

None.

2.5 Other changes

The feature will expand the billing record CDR to contain an indicator of the CLG_NUM.

The following table shows the DMS-GSP CDR without the expansion:

Table 1 DMS - GSP CDR Format without the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
00	EXP	VPN	INAP		Type of Call				Reccd (F0)							
01	1	1	0	0	OrigDate 2				OrigDate 1				OrigDate 0			
02	OrigTime 3				OrigTime 2				OrigTime 1				OrigTime 0			
03	DiscDate 0				DiscDate 0				1	1	0	0	OrigTime 4			
04	DiscTime 1				DiscTime 0				1	1	0	0	DiscDate 3			
05	1	1	0	0	DiscTime 4				DiscTime 3				DiscTime 2			
06	CallDuration LSW															LSB
07	MSB	CallDuration MSW														
08	MSB	OrigClli														LSB
09	MSB	OrigMem														LSB
10	MSB	TermClli														LSB
11	MSB	TermMem														LSB
12	ClgNum 3				ClgNum 2				ClgNum 1				ClgNum 0			
13	ClgNum 7				ClgNum 6				ClgNum 5				ClgNum 4			
14	ClgNum 11				ClgNum 10				ClgNum 9				ClgNum 8			
15	ClgNum 15				ClgNum 14				ClgNum 13				ClgNum 12			
16	ClgNum 19				ClgNum 18				ClgNum 17				ClgNum 16			

Table 1 DMS - GSP CDR Format without the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
17	ClgNum 23				ClgNum 22				ClgNum 21				ClgNum 20			
18	TNS Value 3				TNS Value 2				TNS Value 1				TNS Value 0			
19	CustCost 1				CustCost 0				TNS Value 5				TNS Value 4			
20	CustCost 5				CustCost 4				CustCost 3				CustCost 2			
21	Billtype								CustCost 7				CustCost 6			
22	DialNum 3				DialNum 2				DialNum 1				DialNum 0			
23	DialNum 7				DialNum 6				DialNum 5				DialNum 4			
24	DialNum 11				DialNum 10				DialNum 9				DialNum 8			
25	DialNum 15				DialNum 14				DialNum 13				DialNum 12			
26	DialNum 19				DialNum 18				DialNum 17				DialNum 16			
27	DialNum 23				DialNum 22				DialNum 21				DialNum 20			
28	0	0	0	0	0	0	0	Answer	TNS Sent	Service Code						
29	Treatment Code								0	0	0	0	0	0	0	0
30	1	1	0	0	CompCd 2				CompCd 1				CompCd 0			
31	Partition Number									Data	Class of Service					
32	CLI Index								Disposition Qualifier							Sat.
33	SeqNum LSW															LSB
34	MSB SeqNum MSW															

Table 1 DMS - GSP CDR Format without the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
35	1	1	0	0	NodeID 2				NodeID 1				NodeID 0			
36	DestNum 3				DestNum 2				DestNum 1				DestNum 0			
37	DestNum 7				DestNum 6				DestNum 5				DestNum 4			
38	DestNum 11				DestNum 10				DestNum 9				DestNum 8			
39	DestNum 15				DestNum 14				DestNum 13				DestNum 12			
40	DestNum 19				DestNum 18				DestNum 17				DestNum 16			
41	DestNum 23				DestNum 22				DestNum 21				DestNum 20			
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	BillNum 1				BillNum 0				0	0	0	0	0	0	0	0
44	BillNum 5				BillNum 4				BillNum 3				BillNum 2			
45	BillNum 9				BillNum 8				BillNum 7				BillNum 6			
46	BillNum 13				BillNum 12				BillNum 11				BillNum 10			
47	BillNum 17				BillNum 16				BillNum 15				BillNum 14			
48	BillNum 21				BillNum 20				BillNum 19				BillNum 18			
49	BillNum 25				BillNum 24				BillNum 23				BillNum 22			
50	BillNum 29				BillNum 28				BillNum 27				BillNum 26			
51	CCD								T_FCI_NUM							
52	CCT								1	1	0	0	CCD			

Table 1 DMS - GSP CDR Format without the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
53	1	1	0	0	CCT											
54	TTON				CustID											
55	Acct_Ext 3				Acct_Ext 2				Acct_Ext 1				Acct_Ext 0			
56	Acct_Ext 7				Acct_Ext 6				Acct_Ext 5				Acct_Ext 4			
57	CPC								Acct_Ext 9				Acct_Ext 8			
58	OutpNum 3				OutpNum 2				OutpNum 1				OutpNum 0			
59	OutpNum 7				OutpNum 6				OutpNum 5				OutpNum 4			
60	OutpNum 11				OutpNum 10				OutpNum 9				OutpNum 8			
61	OutpNum 15				OutpNum 14				OutpNum 13				OutpNum 12			
62	OutpNum 19				OutpNum 18				OutpNum 17				OutpNum 16			
63	OutpNum 23				OutpNum 22				OutpNum 21				OutpNum 20			

The following table shows the DMS-GSP CDR format with the CDR expansion:

Table 2 DMS - GSP CDR Format with the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
00	EXP	VPN	INAP		Type of Call				Reccd (F0)							
01	1	1	0	0	OrigDate 2				OrigDate 1				OrigDate 0			
02	OrigTime 3				OrigTime 2				OrigTime 1				OrigTime 0			

Table 2 DMS - GSP CDR Format with the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
03	DiscDate 0				DiscDate 0				1	1	0	0	OrigTime 4			
04	DiscTime 1				DiscTime 0				1	1	0	0	DiscDate 3			
05	1	1	0	0	DiscTime 4				DiscTime 3				DiscTime 2			
06	CallDuration LSW															LSB
07	MSB	CallDuration MSW														
08	MSB	OrigClli														LSB
09	MSB	OrigMem														LSB
10	MSB	TermClli														LSB
11	MSB	TermMem														LSB
12	ClgNum 3				ClgNum 2				ClgNum 1				ClgNum 0			
13	ClgNum 7				ClgNum 6				ClgNum 5				ClgNum 4			
14	ClgNum 11				ClgNum 10				ClgNum 9				ClgNum 8			
15	ClgNum 15				ClgNum 14				ClgNum 13				ClgNum 12			
16	ClgNum 19				ClgNum 18				ClgNum 17				ClgNum 16			
17	ClgNum 23				ClgNum 22				ClgNum 21				ClgNum 20			
18	TNS Value 3				TNS Value 2				TNS Value 1				TNS Value 0			
19	CustCost 1				CustCost 0				TNS Value 5				TNS Value 4			
20	CustCost 5				CustCost 4				CustCost 3				CustCost 2			

Table 2 DMS - GSP CDR Format with the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
21	Billtype								CustCost 7				CustCost 6			
22	DialNum 3				DialNum 2				DialNum 1				DialNum 0			
23	DialNum 7				DialNum 6				DialNum 5				DialNum 4			
24	DialNum 11				DialNum 10				DialNum 9				DialNum 8			
25	DialNum 15				DialNum 14				DialNum 13				DialNum 12			
26	DialNum 19				DialNum 18				DialNum 17				DialNum 16			
27	DialNum 23				DialNum 22				DialNum 21				DialNum 20			
28	0	0	0	0	0	CLGNUM_IND		Answer	TNS Sent	Service Code						
29	Treatment Code								0	0	0	0	0	0	0	0
30	1	1	0	0	CompCd 2				CompCd 1				CompCd 0			
31	Partition Number									Data	Class of Service					
32	CLI Index								Disposition Qualifier							Sat.
33	SeqNum LSW															LSB
34	MSB SeqNum MSW															
35	1	1	0	0	NodeID 2				NodeID 1				NodeID 0			
36	DestNum 3				DestNum 2				DestNum 1				DestNum 0			
37	DestNum 7				DestNum 6				DestNum 5				DestNum 4			
38	DestNum 11				DestNum 10				DestNum 9				DestNum 8			

Table 2 DMS - GSP CDR Format with the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
39	DestNum 15				DestNum 14				DestNum 13				DestNum 12			
40	DestNum 19				DestNum 18				DestNum 17				DestNum 16			
41	DestNum 23				DestNum 22				DestNum 21				DestNum 20			
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	BillNum 1				BillNum 0				0	0	0	0	0	0	0	0
44	BillNum 5				BillNum 4				BillNum 3				BillNum 2			
45	BillNum 9				BillNum 8				BillNum 7				BillNum 6			
46	BillNum 13				BillNum 12				BillNum 11				BillNum 10			
47	BillNum 17				BillNum 16				BillNum 15				BillNum 14			
48	BillNum 21				BillNum 20				BillNum 19				BillNum 18			
49	BillNum 25				BillNum 24				BillNum 23				BillNum 22			
50	BillNum 29				BillNum 28				BillNum 27				BillNum 26			
51	CCD								T_FCI_NUM							
52	CCT								1	1	0	0	CCD			
53	1	1	0	0	CCT											
54	TTON				CustID											
55	Acct_Ext 3				Acct_Ext 2				Acct_Ext 1				Acct_Ext 0			
56	Acct_Ext 7				Acct_Ext 6				Acct_Ext 5				Acct_Ext 4			

Table 2 DMS - GSP CDR Format with the CDR expansion

Word	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
57	CPC								Acct_Ext 9				Acct_Ext 8			
58	OutpNum 3				OutpNum 2				OutpNum 1				OutpNum 0			
59	OutpNum 7				OutpNum 6				OutpNum 5				OutpNum 4			
60	OutpNum 11				OutpNum 10				OutpNum 9				OutpNum 8			
61	OutpNum 15				OutpNum 14				OutpNum 13				OutpNum 12			
62	OutpNum 19				OutpNum 18				OutpNum 17				OutpNum 16			
63	OutpNum 23				OutpNum 22				OutpNum 21				OutpNum 20			

Succession

SN07 Release Change Reference Manual

DMS on Succession

Copyright © 2004 Nortel Networks
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Information is subject to change without notice. Northern Telecom reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

DMS, MAP, NORTEL, NORTEL NETWORKS, NORTHERN TELECOM, NT, and SUPERNODE are trademarks of Northern Telecom.

Publication number: PLN-SN07-004
Product release: SN06
Document release: Standard 01.02
Date: April 2003
Printed in the United States of America.

NORTEL NETWORKS™

How the world shares ideas.